HAL
open science

Multi-operator greedy routing based on open routers

Daniel Philip Venmani

To cite this version:

Daniel Philip Venmani. Multi-operator greedy routing based on open routers. Other [cs.OH]. Institut National des Télécommunications, 2014. English. NNT : 2014TELE0003 . tel-00997721

HAL Id: tel-00997721

https://theses.hal.science/tel-00997721v1

Submitted on 28 May 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Multi-Operator Greedy Routing Based on Open Routers

Thèse

présentée pour l'obtention du grade de

DOCTEUR EN INFORMATIQUE ET RESEAUX

de

L'Université Pierre et Marie Curie

par

VENMANI Daniel Philip

acceptée sur proposition du jury:

Prof. Dias De Amorim Marcelo, Président, Université Pierre et Marie Curie, France
Prof. Kaldoun Al Agha, Rapporteur, Université Paris-Sud, France
Prof. Raouf Boutaba, Rapporteur, Université de Waterloo, Canada
Prof. Philippe Godlewski, Examinateur, Telecom ParisTech, France
Dr. Laurent Ciavaglia, Examinateur, Alcatel-Lucent Bell Labs, France
Dr. Olivier Festor, Examinateur, INRIA Nancy—Grand Est, France
Dr. Yvon Gourhant, Encadrant, Orange Labs, France
Prof. Djamal Zeghlache, Directeur de thèse, Telecom SudParis, Institut Mines-télécom, France

Ecole Doctorale d'Informatique, Télécommunications
et Electronique de Paris (EDITE de Paris)

Soutenue en Février 2014

Thèse n° 2014 TELE0003

Multi-Operator Greedy Routing Based on Open Routers

Dissertation

submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

of

Pierre and Marie CURIE University

Carried out by

VENMANI Daniel Philip

accepted by the jury committee composed of:

Prof. Dias De Amorim Marcelo, President, Université Pierre et Marie Curie, France
Prof. Kaldoun Al Agha, Rapporteur, Université Paris-Sud, France
Prof. Raouf Boutaba, Rapporteur, Université de Waterloo, Canada
Prof. Philippe Godlewski, Examiner, Telecom ParisTech, France
Dr. Laurent Ciavaglia, External Examiner, Alcatel-Lucent Bell Labs, France
Dr. Olivier Festor, External Examiner, INRIA Nancy—Grand Est, France
Dr. Yvon Gourhant, Advisor, Orange Labs, France
Prof. Djamal Zeghlache, Thesis Director, Telecom SudParis, Institut Mines-télécom, France

Ecole Doctorale d'Informatique, Télécommunications
et Electronique de Paris (EDITE de Paris)

Defended on February 2014

Thesis n° 2014 TELE0003

To my Mother

(1950-1994)

To my Brother

(1974-2013)

...now at peace, greatly missed; who didn't live to see me finish.

Epigraph

நாளை என்றும் நம் கையில் இல்லை
நாம் யாரும் தேவன் கை பொம்மைகளே!
என்றால் கூட போராடு நண்பா
என்றைக்கும் தோற்காது உண்மைகளே !

Special Mention

Ibrahim Houmed, *R&D Program Manager, Orange Labs*

Yvon Gourhant, *R&D Program Manager, Orange Labs*

Marion Duprez, *R&D Program Manager, Orange Labs*

...for trusting me; for giving me the opportunity to do what I like the most to do; for giving me a career break-through.

To **You**, I owe all the success of my career!

Acknowledgements

Life is too short to acknowledge all those creative, beautiful and unpretentious minds, who make our journey worthwhile. Here, I get an opportunity to offer my gratitude to all those personalities, who really made a personal difference to me with their presence. Just saying 'thank-you' is far too little; I can't imagine my accomplishments without their support.

To begin with, foremost, the first person to be acknowledged naturally is my advisor, Dr. Yvon Gourhant, who always maintained a rather pleasant ambiance with me and greatly inspired me to produce excellent research results by getting the best out of me. I will never forget my first interaction with him in the fall of 2010 when as an aspiring young doctoral candidate who had just arrived at Orange Labs, Lannion, I walked into his office and solicited him to describe to me some of the research he was involved with. I had never heard much of the technical details of "mobile backhaul" until that moment of my life and, truth be told, I did not understand much of what he explained that evening of what seemed to me – at that time – a very obscure field of telecommunications. There were memorable moments like this one that made the everyday life of a student pursuing Doctor of Philosophy, a rather amazing experience. To him, I owe all the knowledge that I have gained during the course of this research.

Walking on my way back home after this meeting, the words of the great artist Pablo Picasso kept ringing in my head: "*I am always doing that I cannot do, in order that I may learn how to do it*". I decided to embrace this philosophy and began my research hoping that this was the best way for me to gain the most knowledge; that turned out to be – in retrospect –a very wise choice. After three exciting years, having analyzed millions of experimental data points, having run thousands of simulations, having derived countless equations, and having learned much more than that I could have ever hoped for (all of these happened between 10pm and 4 am every night), I ultimately experienced a personal adventure of the greatest magnitude. During this unique process, my understanding on the mobile backhaul and for the field of telecommunications in general has grown exponentially, the collaboration with other researchers allowed me to produce some very interesting scientific results (15 international publications), and Yvon turned out to be a great advisor and one of the few people on the planet that no person could ever possibly dislike. He has been very pleasant to work with, in experiment upon experiment, always having time to listen and investigate any research issue I might have been struggling with. In short- **I wrote, he improved**! So, thank you Yvon, thank you for believing all the way and for carrying me to every hill and every valley. You lifted me up the whole way and I will always be grateful for everything you have done and for the all the credible works that have been done.

While Yvon monitored my progress at close proximity, I must not forget to thank my professor, Prof. Djamal Zeghlache, who served as a distant supervisor. I would like to first thank him for accepting to be my academic supervisor despite his busy schedules. I would also like to thank him for supporting me at all the technical obstacles during my research and thank him the most for placing his un-ending support and confidence in me and for his views and appreciations for my research ideas. His support by providing valuable advice and start up ideas from his vast experience was an aiding factor in advancing this thesis with a much faster pace.

Sincere thanks to Prof. Kaldoun Al Agha, Rapporteur, Université Paris-Sud, France, Prof. Raouf Boutaba, Rapporteur, University of Waterloo, Canada, for having to spend one of the most invaluable resources, 'Time', for reviewing this dissertation thesis and offering valuable comments. I also wish to thank the professors and the members of my qualifying oral exam and defense committees, Prof. Dias De Amorim Marcelo, Président, Université Pierre et Marie Curie, France, Prof. Philippe Godlewski, Telecom ParisTech, France, Dr. Laurent Ciavaglia, Examinateur, Alcatel-Lucent Bell Labs, France, Dr. Olivier Festor, Examinateur, INRIA Nancy—Grand Est, France and all the anonymous reviewers of the international conferences I submitted and published my articles. They all transferred some part of their wisdom to me one way or another through suggestions, questions that intrigued as well as through constructive criticism.

Aside from those people who were directly related to my research, a number of other people influenced my life directly, leading to obtain my Ph.D. Sometimes I'm lost at what my purpose is and am left wondering, why any of this matters. It is on those occasions, family comes - those who loved and cared for me the most, *unconditionally*. It's the starting boom of a chain reaction. My father, a retired mathematics professor today, who had spent several hours every evening with me personally, during the early years of my life, to teach me Probability, Statistics, Algebra. My brothers - the reason why I am doing this, those who kept insisting me that when I put work in and get things done, it doesn't go unnoticed; it could contribute to my best ever success and that I keep believing in all these years of sacrifices; not to forget to mention my last brother who passed away during the course of my doctoral research, who bought me my first laptop computer with his very own yearly savings. My two most lovely sister-in-laws, my niece- the little princess of our family, my nephews and last but not the least, my dearest friends from India, who replaced my physical presence in my home, for all their affection and constant support, and most of all, patience and understanding towards me, for tolerating my impossibilities.

Orange Labs, my employer, for sponsoring all my professional trips, thus gave me the opportunity to attend some of the best conferences in the world. I would like to thank Mme.Sylvie Gillot, for her continuous support in the administrative tasks at Orange Labs, Lannion, from the beginning until the end of this dissertation thesis.

Abstract

New Approaches for Network-wide Redundancy Elimination for Improving Effective Network Capacity

Revolutionary mobile technologies, such as high-speed packet access 3G (HSPA+) and LTE, have significantly increased mobile data rate over the radio link. While most of the world looks at this revolution as a blessing to their day-to-day life, a little-known fact is that these improvements over the radio access link results in demanding tremendous improvements in bandwidth on the backhaul network. Having said this, today's Internet Service Providers (ISPs) and Mobile Network Operators (MNOs) are intemperately impacted as a result of this excessive smartphone usage. The operational costs (OPEX) associated with traditional backhaul methods are rising faster than the revenue generated by the new data services. Building a mobile backhaul network is very different from building a commercial data network. A mobile backhaul network requires (i) QoS-based traffic with strict requirements on delay and jitter (ii) high availability/reliability. While most ISPs and MNOs have promised advantages of redundancy and resilience to guarantee high availability, there is still the specter of failure in today's networks. The problems of network failures in today's networks can be quickly but clearly ascertained. The underlying observation is that ISPs and MNOs are still exposed to rapid fluctuations and/or unpredicted breakdowns in traffic; it goes without saying that even the largest operators can be affected. But what if, these operators could now put in place designs and mechanisms to improve network survivability to avoid such occurrences? What if mobile network operators can come up with low-cost backhaul solutions together with ensuring the required availability and reliability in the networks?

With this problem statement in-hand, the overarching theme of this dissertation is within the following scopes: (i) to provide low-cost backhaul solutions; the motivation here being able to build networks without over-provisioning and then to bring-in new resources (link capacity/bandwidth) on occasions of unexpected traffic surges as well as on network failure conditions for particularly ensuring premium services (ii) to provide uninterrupted communications even at times of network failure conditions, but without redundancy. Here a slightly greater emphasis is laid on tackling the 'last-mile' link failures. The scope of this dissertation is therefore to propose, design and model novel network architectures for improving effective network survivability and network capacity, at the same time by eliminating network-wide redundancy, adopted within the context of mobile backhaul networks.

Motivated by this, we study the problem of how to share the available resources of a backhaul network among its competitors, with whom a Service Level Agreement (SLA) has been concluded. Thus, we present a systematic study of our proposed solutions focusing on a variety of empirical resource sharing heuristics and optimization frameworks. With this background, our work extends towards a novel fault restoration framework which can cost-effectively provide protection and restoration for the operators, enabling them with a parameterized objective function to choose desired paths based on traffic patterns of their end-customers. We then illustrate the survivability of backhaul networks with reduced amount of physical redundancy, by effectively managing geographically distributed backhaul network equipments which belong to different MNOs using 'logically-centralized' physically-distributed controllers, while meeting strict constraints on network availability and reliability.

Keywords: *Network architecture, Network design, Network resilience, Network algorithms & operations, Software Defined Networking (SDN)/OpenFlow.*

Résumé

De nouvelles approches efficaces pour améliorer la capacité du réseau sans liens de redondance

Les évolutions technologies mobiles majeures, tels que les réseaux mobiles 3G, HSPA+ et LTE, ont augmenté de façon significative la capacité des données véhiculées sur liaison radio. Alors que les avantages de ces évolutions sont évidents à l'usage, un fait moins connu est que ces améliorations portant principalement sur l'accès radio nécessitent aussi des avancées technologiques dans le réseau de collecte (backhaul) pour supporter cette augmentation de bande passante. Les fournisseurs d'accès Internet (FAI) et les opérateurs de réseau mobile doivent relever un réel défi pour accompagner l'usage des smartphones. Les coûts opérationnels associés aux méthodes traditionnelles de backhaul augmentent plus vite que les revenus générés par les nouveaux services de données. Ceci est particulièrement vrai lorsque le réseau backhaul doit lui-même être construit sur des liens radio. Un tel réseau de backhaul mobile nécessite (i) une gestion de qualité de service (QoS) liée au trafic avec des exigences strictes en matière de délai et de gigue, (ii) une haute disponibilité / fiabilité. Alors que la plupart des FAI et des opérateurs de réseau mobile font état des avantages de mécanismes de redondance et de résilience pour garantir une haute disponibilité, force est de constater que les réseaux actuels sont encore exposés à des indisponibilités. Bien que les causes de ces indisponibilités soient claires, les fluctuations rapides et / ou des pannes imprévues du trafic continuent d'affecter les plus grands opérateurs. Mais ces opérateurs ne pourraient-ils pas mettre en place des modèles et des mécanismes pour améliorer la survie des réseaux pour éviter de telles situations ? Les opérateurs de réseaux mobiles peuvent-ils mettre en place ensemble des solutions à faible coût qui assureraient la disponibilité et la fiabilité des réseaux ?

Compte tenu de ce constat, cette thèse vise à : (i) fournir des solutions de backhaul à faible coût ; l'objectif est de construire des réseaux sans fil en ajoutant de nouvelles ressources à la demande plutôt que par sur-dimensionnements, en réponse à un trafic inattendu surgit ou à une défaillance du réseau, afin d'assurer une qualité supérieure à certains services (ii) fournir des communications sans interruption, y compris en cas de défaillance du réseau, mais sans redondance. Un léger focus porte sur l'occurrence de ce problème sur le lien appelé «dernier kilomètre» (last mile). Cette thèse conçoit une nouvelle architecture de réseaux backhaul mobiles et propose une modélisation pour améliorer la survie et la capacité de ces réseaux de manière efficace, sans reposer sur des mécanismes coûteux de redondance passive.

Avec ces motivations, nous étudions le problème de partage de ressources d'un réseau de backhaul entre opérateurs concurrents, pour lesquelles un accord de niveau de service (SLA) a été conclu. Ainsi, nous présentons une étude systématique de solutions proposées portant sur une variété d'heuristiques de partage empiriques et d'optimisation des ressources. Dans ce contexte, nous poursuivons par une étude sur un mécanisme de recouvrement après panne qui assure efficacement et à faible coût la protection et la restauration de ressources, permettant aux opérateurs via une fonction basée sur la programmation par contraintes de choisir et établir de nouveaux chemins en fonction des modèles de trafic des clients finaux. Nous illustrons la capacité de survie des réseaux backhaul disposant d'un faible degré de redondance matérielle, par la gestion efficace d'équipements de réseau de backhaul répartis géographiquement et appartenant à différents opérateurs, en s'appuyant sur des contrôleurs logiquement centralisés mais physiquement distribués, en respectant des contraintes strictes sur la disponibilité et la fiabilité du réseau.

Mots-clés: *Architecture de réseaux backhaul mobiles, Partage de ressources d'un réseau de backhaul, Mécanisme de recouvrement après panne, Optimisation des ressources, Software Defined Networking (SDN)/OpenFlow.*

TABLE OF CONTENTS

Epigraph i

Special Mention ii

Acknowledgements iii

Abstract iv

Résumé v

TABLE OF CONTENTS vi

LIST OF FIGURES vii

Chapter 1 1

Prologue 1

1.1. Opening Comments 2

1.2. Thesis Layout 3

1.3. Research Contributions 5

1.3.1. Part II: Theory and Modeling 5

1.3.1.1. Chapter 3 5

1.3.1.2. Chapter 4 7

1.3.2. Part III: Optimization Techniques for Network Survivability 8

1.3.2.1. Chapter 5 9

1.3.2.2. Chapter 6 10

1.3.2.3. Chapter 7 11

1.3.2.4. Chapter 8 12

1.3.3. Part IV: Proof-of-Concept Experiments for Validation and Verification of OpenFlow Deployment in Mobile Backhaul Networks 13

1.3.3.1. Chapter 9 14

1.3.4. Part V: Substitution Networks based on Software Defined Networking 15

1.3.4.1. Chapter 10 15

1.3.5. Part V: Chapter 11: Research and Deployment challenges and Concluding Discussions of the Dissertation 16

1.4. Pilot: Can I Share my Unused Resources with my Competitors? 17

1.4.1. History of the Future: The Internet and the Mobile Internet 17

1.4.2. Problems of the Present: Apples and Oranges 17

1.4.3. The Challenge to Re-design: Quick Glimpse on Fundamentals 18

1.5. Scope of this Dissertation: Problem Definitions 19

1.5.1. Can I Share my Unused Resources with my Competitors? 19

1.5.2. Service Differentiation among Multiple Operators 20

1.5.3. Network Management as a tool for Service Differentiation between Operators 21

1.6. Bringing-in Software Defined Networking (SDN) as a means for Service Differentiation between Multiple Operators 22

1.6.1. SDN/OpenFlow & MPLS, Better Together or Mutually Exclusive? 23

1.7. Overall Final Remarks 25

Chapter 2 27

State of the Art Techniques for Mobile Network Sharing 27

2.1. Introduction to Network Sharing: When Technology and Business must go Hand-in-Hand. 28

2.1.1. The Context and the Problem 28

2.2. Resource Sharing in Mobile Networks 30

2.2.1. Scoping the Network-Sharing Solution 30

2.3. Network Sharing - Within the Context of Emerging Countries 32

2.3.1. Compensating the Network Quality 32

2.3.2. What can Africa learn from Developed Economies of Network Sharing Experience? ... 34

2.4. Fundamental Limits and Regulatory Framework 35

2.4.1. Regulatory Interests in Infrastructure Sharing 35

2.4.2. Impact on Competition 37

2.4.3. Existing Standardizations on Network Sharing 40

2.5. Risks Involved in Resource Sharing 40

2.6. Wireless Network Virtualization 42

2.7. Concluding Remarks and Discussions on State of the Art Techniques in Mobile Network Sharing 43

2.8. Summary of our Findings 45

Chapter 3 49

Reliability and Availability Analysis of a Novel Shared Backhaul Architecture 49

3.1. Motivation towards this Shared Design 50

3.1.1. Organization of Part I 51

3.2. 3RIS for 4G: A Novel Design and its Reliability Analysis: Part I 51

3.3. System Modeling 52

3.3.1. Formal Definitions 52

3.3.2. Statistical Analysis based on Real Measurement Model 54

3.3.3. State Space Analytical Model for Infrastructure Sharing 57

3.4. Proposed Architectural Design 61

3.5. Give and Take: Characterization of Availability of Multi-State Wireless Backhaul Networks: Part II 64

3.5.1. Organization of Part II 65

3.5.2. Evaluating Approach 65

3.6. Multi-State System Availability Analysis 66

3.6.1.1. Formal Definitions 66

3.6.2. Multi-State Wireless Backhaul Networks Availability Analysis with Sharing between Different MNOs 68

3.7. Illustrative Numerical Evaluation 72

3.7.1. Estimation of State Probabilities from the Markov Model 72

3.7.2. MSS Average Availability of the Wireless Backhaul when Shared 73
3.8. Concluding Discussions 73

Chapter 4 75
Analytical Modeling for Recovery and Re-routing within the Shared Backhaul Architecture 75
4.1. Introductory Statements 76
4.1.1. Concept Visualization 76
4.1.2. Organization of the Chapter 76
4.2. Current Objectives and Contributions 77
4.2.1. Significance of our Results 77
4.3. Analytical Modeling 78
4.3.1. Formal Definition 78
4.3.2. Analytical Model for 1:1 Path Protected Connection 78
4.4. Analytical Model for Link-Bandwidth Sharing 79
4.5. Towards A Probabilistic Model for Fault Restoration through Link-Bandwidth Sharing 81
4.5.1. General Problem Statement 81
4.5.2. Assumptions and Conditions 83
4.5.3. Network Model 84
4.5.4. Probabilistic Modeling for Fault Restoration 84
4.6. Illustrative Numerical Evaluation 87
4.7. Concluding Discussions 89

Chapter 5 93
OpenRoutes: Multi-operator Cooperative Routing for the Survivability of Backhaul Networks 93
5.1. Introductory Statements 94
5.1.1. Concept Visualization 94
5.1.2. Current Objectives and Contributions and Organization of the Chapter 96
5.2. Modeling OpenRoutes Restoration Scheme 98
5.2.1. Overall System Model 98
5.2.2. On Path Computation Model 98
5.2.3. On Bandwidth Computation Model 100
5.2.4. Relaxing Reachability and Restricting Shareability 101
5.3. ILP Formulation based Optimization for $\mathcal{K}$ Alternative Disjoint Paths with Optimal Capacity 103
5.4. Heuristics Algorithms for the best Alternative Backup Path with Optimal Capacity 105
5.4.1. Least Length Shortest Paths (LLSP) 107
5.4.2. Least Delay Shortest Path (LDSP) 107
5.4.3. Ant Colony Optimization (ACO) for Optimal Capacity Path Computation 108

5.5. OpenRoutes Restoration Scheme 112
5.6. Performance Evaluation and Discussions 114
5.6.1. Experimental Set-up and Computational Considerations 114
5.6.1.1. Efficiency of the Three Heuristics Individually on Different Traffic Conditions- With and Without Operator Sharing 115
5.6.2. Efficiency of the Algorithms with Operator Sharing Only - on Different Topologies 120
5.6.3. Influence of Topologies 120
5.6.4. Influence of Sharing 122
5.7. Concluding Discussions 124

Chapter 6 125
Divide and Share: Multi-operator Greedy Routing Based on Sharing with Constraints 125
6.1. Introductory Statements 126
6.1.1. Problem Formulation 126
6.1.2. Motivation and Concept Visualization 126
6.1.3. Current Contributions and Significance of our Results 128
6.2. Issues Affecting Availability in Shared Backup Bandwidth Allocation 129
6.3. Divide and Share Optimization 130
6.3.1. General Problem Statement 130
6.3.2. ILP based Optimization for Link Bandwidth Allocation through Sharing 133
6.3.3. Heuristics based Approach for Link Bandwidth Allocation through Sharing 135
6.3.3.1. Algorithm for Link Bandwidth Allocation through Sharing 135
6.3.3.2. Description of the Algorithm 137
6.3.3.3. Competitive Differentiation 139
6.4. Illustrative Numerical Evaluation 139
6.4.1. Experimental Set-up and Computational Considerations 139
6.4.2. Performance Comparison between ILP and Heuristics. 141
6.5. Concluding Discussions 143

Chapter 7 145
X-Control: A Quasi-Distributed Fault Restoration Mechanism Using Logically Centralized Controllers 145
7.1. Introductory Statements 146
7.1.1. Concept Visualization 146
7.1.2. Motivation 146
7.2. Towards A Quasi-Distributed Fault Restoration 147
7.2.1. Cross-Controller Network Design: When Controllers Talk! 148
7.3. On Characterizing Topology Changes 150
7.3.1. On Modeling Network Convergence 151
7.4. On Optimizing Quasi-Distributed Fault Restoration Using ILP Based Formulations 152

7.5. On Greedy Heuristics Based On Convex Combination 154
7.6. Illustrative Numerical Evaluations 155
7.6.1. Optimal Locations for Logically-centralized Physically-distributed Controllers 155
7.7. Concluding Discussions 158

Chapter 8 161
Stitch-n-Sync: Discreetly Disclosing Topology Information Using Logically Centralized Controllers 161
8.1. Introductory Statements 162
8.1.1. Current contributions and Organization of the Chapter 162
8.2. Towards A Multi-Topology Shared Architecture 163
8.2.1. Discreetly Disclosing Topology Information: Stitch n Sync! 163
8.2.2. Challenges Posed by Sharing between Multiple Operators/ Domains 164
8.3. On Maximizing Network Survivability 165
8.3.1. On Modeling Inter-Domain Synchronization (IDS) 166
8.4. On Optimizing Quasi-Distributed Topology Sharing Using ILP Based Formulations 167
8.5. Illustrative Numerical Evaluations 169
8.5.1. Efficiency of Logically-centralized Physically-Distributed Approach - With and without controller Collaboration 170
8.6. Related Works 174
8.7. Concluding Discussions 175

Chapter 9 179
Can SDN/OpenFlow be Adapted for Mobile Backhaul Networks? 179
9.1. Introductory Statements 180
9.2. Background and Concept Visualization 181
9.2.1. OpenFlow Architecture in brief 182
9.3. Resource Sharing Strategies: Illustrative Examples 191
9.4. Performance Evaluation 194
9.4.1. Quantitative analysis on Virtualization Capabilities 194
9.4.2. Quantitative analysis on Network Management Capabilities 195
9.4.2.1. Experimental Setup 196
9.4.3. Performance Metrics and Analysis 196
9.4.3.1. Throughput Analysis 196
9.4.3.2. Delay Analysis 197
9.4.3.3. Network Utilization Efficiency 198
9.4.3.4. Normalized Received Traffic 199
9.5. Concluding Discussions 199

Chapter 10 203
Substitution Networks Based on SDN- A Radical View 203

10.1. Introductory Statements 204
10.2. Problem Characterization: Background and Existing Solutions 205
10.3. Approaching the Problem through Substitution Networks (SNs) 207
10.3.1. Inspirations for Substitution Networks (SNs) 207
10.3.2. Substitution Networks (SNs) in Wireless Backhaul Networks 208
10.3.3. Shortcomings of Substitution Networks (SNs) that Hinder a Wide Adoption into Wireless Backhaul Networks 209
10.3.4. Towards a Centralized Approach for Substitution Networks (SNs) 210
10.4. Concept Visualization 211
10.4.1. The Application of the Approach to the Problem: OpenFlow 211
10.4.2. Substitution Networks (SNs) based on Software Defined Networking (SDN) 213
10.5. Experimental Evaluations 215
10.5.1. Design and Implementation 215
10.5.2. Evaluation and Results 219
10.6. Discussions and Conclusions 221

Chapter 11 223
Concluding Discussions - Recovery without Redundancy is possible! 223

Bibliography 233

LIST OF FIGURES

Figure 1: An illustration of mobile backhaul network topology. 19
Figure 2: Infrastructure sharing scoping model and dimensions..... 31
Figure 3: Number of mobile operators present by country, Africa [Source: Analysis Mason, 2013], Countries colored red, orange and yellow all face intense competition. 33
Figure 4: Unavailability results of the MW scenarios as a function of the number of hop 54
Figure 5: Cost Enhancement Coefficient as a function of unavailability results of the MW scenarios 55
Figure 6: Percentage increment in cost as a function of unavailability results of the MW scenarios 56
Figure 7: State diagram for availability analysis of a parallel redundant system 59
Figure 8: State diagram for reliability analysis of a parallel redundant system 59
Figure 9: Last mile chain topology with redundant links 63
Figure 10: Resiliency design flow using infrastructure sharing 64
Figure 11: An illustrative example network topology portraying resiliency design flow using infrastructure sharing within the country Kenya. 64
Figure 12: Multi-state system reliability analysis diagram for wireless backhaul network with infrastructure sharing..... 69
Figure 13: Multi-state system availability analysis diagram for wireless backhaul network with infrastructure sharing..... 69
Figure 14: Estimation of state probabilities of wireless backhaul network with infrastructure sharing 72
Figure 15: Estimation of Instantaneous availability for wireless backhaul network with infrastructure sharing..... 73
Figure 16: An illustrative example network topology portraying resiliency design flow using infrastructure sharing within the country Kenya. 82
Figure 17: Recovery from link congestion through backhaul sharing. 82
Figure 18: Traffic flow design with infrastructure sharing under faulty conditions with arrow on the bottom indicating traffic from the recipient and arrows on the top indicates the traffic of the donor. 83
Figure 19: Backhaul link-bandwidth allocation through sharing. 83
Figure 20: # of connections provisioned using both schemes. 88
Figure 21: Blocking Probability values for both schemes. 88
Figure 22: End-to-end delay measurement for both schemes. 89
Figure 23: An illustrative figure describing reachability and shareability when the host node of one MNO tries to reach another MNO node when a failure occurs. Here, A indicates the host node, trying to re-route disrupted traffic. 103
Figure 24: Illustration of Maximum satisfaction Ratio (MSR) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology). 116
Figure 25: Illustration of Network Resource Utilization (NRU) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology). 118
Figure 26: Illustration of End-to-end Throughput (EET) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology). 119
Figure 27: Illustration of blocking probability for various topologies when all the three heuristics (LLSP+LDSP+ACO) are combined for (a) $\theta ij = 0$ (no resource sharing) (b)$\theta ij = 0.5$ (50% resource sharing). 121
Figure 28: Illustration of blocking probability (a) for $\theta ij = 0$ (no resource sharing) (b) for $\theta ij = 0.5$ (50% resource sharing) on a Full-mesh topology. 123
Figure 29: Traffic flow design with infrastructure sharing under faulty conditions with arrow on the bottom indicating traffic from the recipient and arrows on the top indicates the traffic of the donor. 132

Figure 30: Backhaul link bandwidth allocation through sharing. 132
Figure 31: Illustration of 14-Node NSFNET topology. 141
Figure 32: Illustration of Resource Overhead versus Number of Nodes. 141
Figure 33: Illustration of Blocking probablility versus Number of Nodes. 142
Figure 34: Illustration of Cost versus Number of Nodes. 143
Figure 35: An illustrative example outlining Quasi-Distributed Fault Restoration Mechanism for the U.S. Two MNOs share their resource (links/bandwidth capacity) by discreetly sharing their topology information using cross-controllers, making a 'resilient' topology, thus avoiding the need for redundancy in the already existing topology. Multiple stand-by controllers can takeover in case of failure of the controller itself. 149
Figure 36: An illustration of convex combination technique for controller placement. Given three faulty locations a, b, c in a plane as shown, the point P is a convex combination of the three faulty locations, while Q is not. 155
Figure 37: Topology (A) and topology (B) used in the simulations. 156
Figure 38: An illustration of restoration latency due to optimal controller placements for A and B for various disconnected node-pairs. 157
Figure 39: An illustration of multiple controller placements for A and B. 158
Figure 40: An illustrative example outlining Quasi-Distributed Topology Information Sharing framework for the U.S. Two MNOs share their resource (links/bandwidth capacity) by discreetly sharing their topology information using cross-controllers, making a 'resilient' topology, thus avoiding the need for redundancy in the already existing topology. Multiple stand-by controllers can takeover in case of failure of the controller itself. Best viewed in Color. 164
Figure 41: An illustration of merging or 'stitching' two different MNO topologies (a) and (b) into one single topology (c), in which controllers were placed in order to reduce the cost of over-provisioning in already existing networks with special mention on overlapping links and nodes at five different locations (d). 169
Figure 42: An illustration of Blocking Probability. 172
Figure 43: An illustration of Average Link utilization. 173
Figure 44: An illustration of Overall Network Throughput. 174
Figure 45: Illustration of architectural Flow diagram of Software Defined Networking (SDN). . 181
Figure 46: Access Network sharing between operators using Virtualization (Thanks to OpenFlow FlowVisor) 185
Figure 47: Illustration of recovery from link congestion through backhaul sharing. 191
Figure 48: Backhaul Network sharing strategies between operators using Virtualization based on traffic needs. 193
Figure 49: Performance comparison for Throughput. 197
Figure 50: Performance comparison for Delay. 198
Figure 51: Performance comparison for Network Utilization. 198
Figure 52: Performance comparison for Received Throughput. 199
Figure 53: Figure illustrating backup path protection in wireless microwave backhaul in 3G/4G. 206
Figure 54: Architectural design illustrating the elimination of back-up path. 208
Figure 55: Architectural design illustrating the integration of Substitution Node. 209
Figure 56: Figure illustrating OpenFlow Fields that are used to match against flow table entries to match different actions to be performed by the switch upon receiving a packet. This header represents OpenFlow version 1.0.0. 212
Figure 57: Flow diagram of Open Flow packets. 213
Figure 58: Architectural design illustrating Substitution Networks based on SDN. 215
Figure 59: Average latency to install flows on an OpenFlow switch. 220
Figure 60: Packet Loss Rate on a link before and after introducing SN. 221
Figure 61: An illustrative example network topology portraying resilience design flow using infrastructure sharing within the country France. Two MNOs: one at the top (north), another in south (with circles) are joined by just another additional link (green colour thick link), making a 'resilient' ring topology. 226
Figure 62: Traffic re-route resulting from backhaul network sharing due to a link/node failure in the backhaul between several mobile network operators. 227

Résumé Etendu

Dans les réseaux de communication sans fil d'aujourd'hui, les faisceaux hertziens sont fréquemment considérés pour construire des réseaux de collecte de réseaux mobiles cellulaires, offrant plus de flexibilité que des lignes louées et des fibres optiques, notamment en Europe et en Afrique. Mais, leur inconvénient réside généralement sur la probabilité de défaillance ou de congestion. Diverses techniques ont été proposées afin de les protéger contre les défaillances potentielles (pannes de liens et défaillances matériels). Du point de vue de l'utilisateur final, il existe plusieurs scénarios:

- Dans le meilleur cas, le trafic réseau des utilisateurs finaux est parfaitement réacheminé à travers d'autres liens, avec un minimum de perturbations ou pas en service.

- Dans d'autres cas, en particulier lorsque plusieurs pannes se produisent simultanément, les utilisateurs finaux peuvent rencontrer des problèmes. Ils peuvent être incapables d'accéder au réseau, ils peuvent rencontrer des problèmes de qualité comme des communications voix de mauvaise qualité ou des débits Internet réduits, les appels peuvent être interrompus ou pas établis. Il est important de noter que ces problèmes peuvent aussi affecter les utilisateurs finaux sur les localités voisines en raison de la surcharge de trafic lié au réacheminement.

Dans un univers de plus en plus dépendant des communications mobiles, toute interruption de service est préjudiciable aux utilisateurs finaux. De plus, il faut considérer la conséquence de défaillances du réseau de collecte pour les fournisseurs de services et opérateurs réseaux. C'est un problème difficile à résoudre dans un réseau dynamique, avec des flux «élastiques», et la mobilité.

Ainsi, lorsqu'une faute intervient sur le réseau de collecte, qu'il s'agisse d'une simple faute sur un seul lien ou d'une défaillance dans un équipement, ou bien de plusieurs fautes/défaillances simultanées, les exploitants du réseau travaillent sans relâche pour rétablir rapidement le service de façon à minimiser l'impact sur les utilisateurs finaux. Bien que la redondance peut prémunir les clients contre les effets de pannes, c'est une solution coûteuse car elle nécessite d'allouer en permanence des ressources supplémentaires (cartes, liens, équipements, et capacité des liens), qui double quasiment le coût, pour pouvoir établir un chemin de secours à tout moment. Même si les chemins de secours peuvent être aussi utilisés durant le fonctionnement en l'absence de panne, cela peut ne pas être la solution la plus optimale car les liens de secours ne peuvent être chargés complètement.

Dans ce contexte, en se limitant aux réseaux de collecte des opérateurs de réseaux mobiles, nous résumons les problèmes suivants :

Problème 1: Comment assurer la disponibilité sur le «dernier mile» d'un réseau de collecte qui n'est généralement pas redondé pour des raisons d'économie (impact limité aux clients derrière ce lien) ?

Problème 2: Comment améliorer la disponibilité de l'architecture de collecte des opérateurs de réseaux mobiles à moindre coût (sans redondance) ?

Problème 3: Comment éviter la congestion dans le réseau de collecte en cas de panne/défaillance ?

L'objetif de cette thèse est de répondre à ces questions relatives à la lutte contre les défaillances du réseau de collecte, sans sur-provisionnement. Ainsi, dans cette thèse, nous décrivons les architectures et des algorithmes qui permettent de réaliser cet objectif. Comme pour tout travail scientifique, cette thèse a soulevé plus de questions qu'elle n'en a résolus, dont certaines sont illustrées dans la dernière partie de ce chapitre. Ce chapitre donne un aperçu en français des différentes contributions de cette thèse.

Tout d'abord, nous étudions le problème de partage de ressources d'un réseau de collecte entre opérateurs concurrents, pour lequel un accord de niveau de service (SLA – Service Level Agreement-) a été conclu. Ainsi, nous présentons de manière empirique les solutions proposées portant sur une variété d'heuristiques de partage et d'optimisation des ressources. Dans ce contexte, nous poursuivons par une étude d'un mécanisme de recouvrement après panne qui assure efficacement et à faible coût la protection de ressources, permettant aux opérateurs via une fonction basée sur la programmation par contraintes de choisir et d'établir de nouveaux chemins en fonction des modèles de trafic des clients finaux. Nous illustrons la capacité de résilience des réseaux de collecte disposant d'un faible degré de redondance matérielle, par la gestion efficace d'équipements répartis géographiquement et appartenant à différents opérateurs, en s'appuyant sur des contrôleurs logiquement centralisés mais physiquement distribués, en respectant des contraintes strictes sur la disponibilité et la fiabilité du réseau. Ceci est représenté dans les figures A, B et C.

Sur la figure A, deux opérateurs se partagent les liens de raccordement. La topologie de l'opérateur A est représentée en haut de la figure. Celle avec des cercles est la topologie d'un autre opérateur B qui accepte de partager les liens de son réseau. Lorsque les liens situés aux 'derniers miles' sont reliés par un simple lien supplémentaire, nous observons que la topologie en anneau

résultante offre plus de protection que la topologie initiale, y compris sur le « dernier mile ». Il est donc évident que notre système de protection permet d'améliorer la disponibilité puisque le trafic sur le chemin principal défaillant basculera rapidement sur le chemin de sauvegarde utilisant les ressources de l'autre opérateur. Notre travail s'applique aux opérateurs Tier I, Tier II, les FAI et les grands opérateurs de réseaux de collecte répartis géographiquement, où le contrôle permanent et évolutif de l'ensemble du réseau composé d'un grand nombre d'équipements hétérogènes devient inévitable.

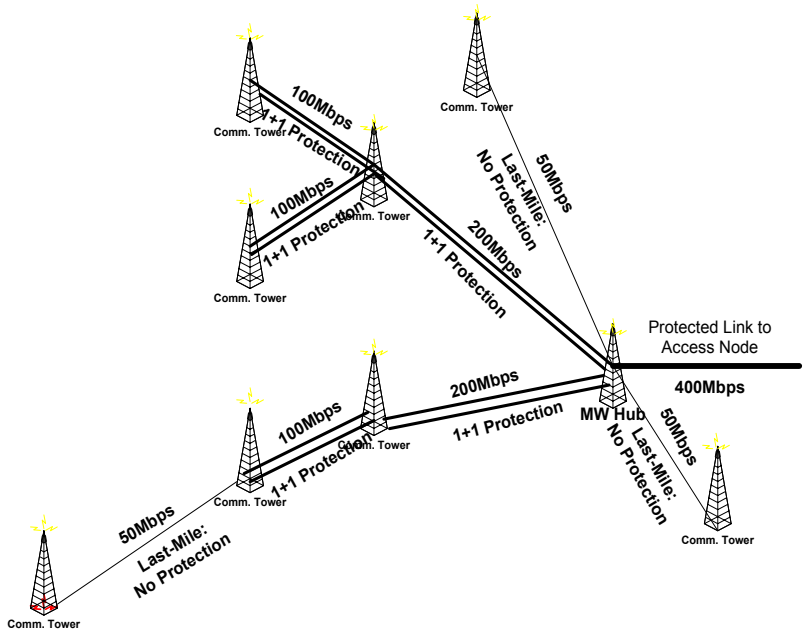


Figure A. Dernier mile d'une topologie en chaîne avec des liens redondants.

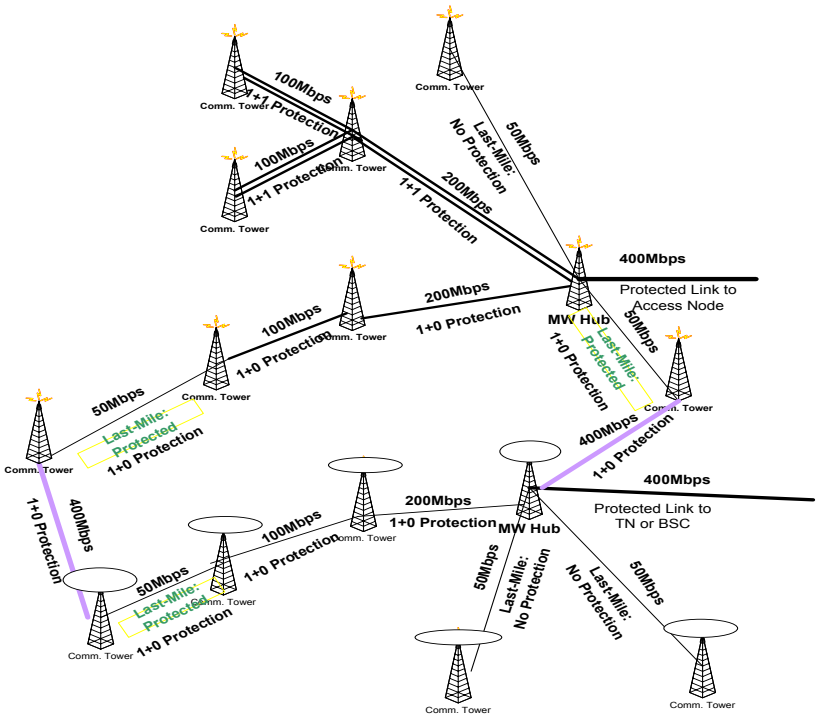


Figure B. Schéma illustrant la résilience basée sur le partage d'infrastructure.

Figure C. Une topologie indicative par exemple décrivant le schéma de résilience basé sur le partage d'infrastructure dans le pays France. Deux opérateurs de téléphonie mobile: un en haut (nord), l'autre dans le sud (avec des cercles) sont interconnectés par des liens supplémentaires (couleur verte de lien d'épaisseur), représentant un "élastique" et formant une topologie en anneau.

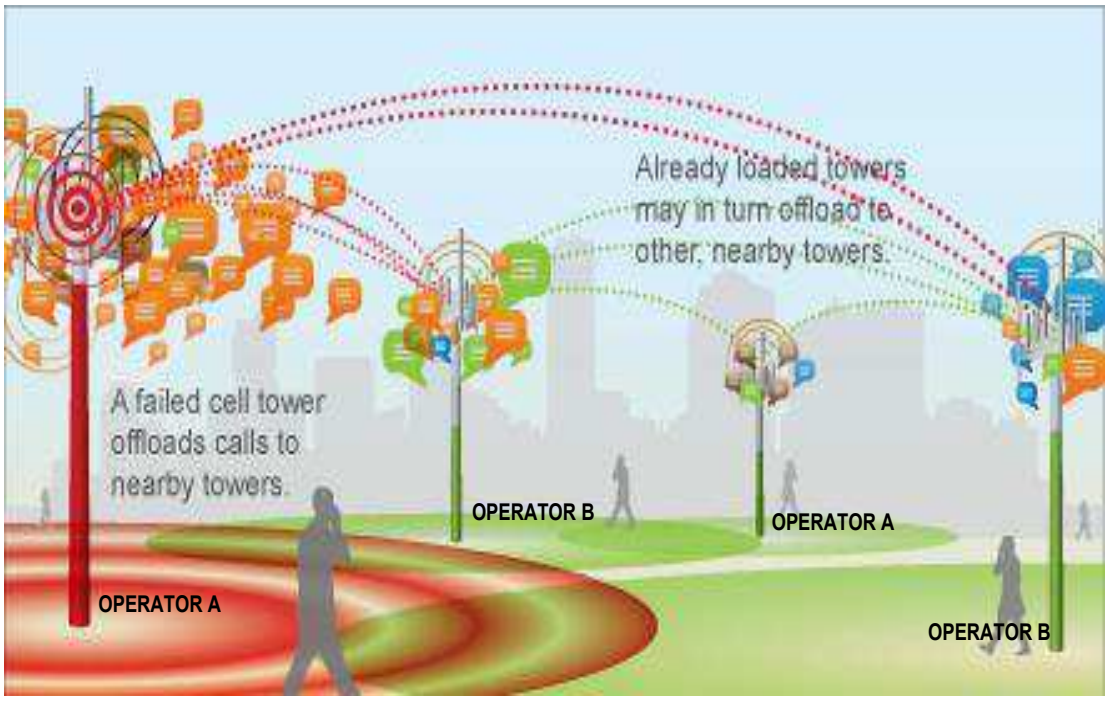


Figure D. nouvel itinéraire de trafic résultant du partage de réseau d'accès en raison d'une défaillance lien / nœud dans le backhaul entre plusieurs opérateurs de réseaux mobiles.

Avec cette première contribution, la thèse adresse les points suivants :

- **Définir l'objectif du partage d'infrastructure** adapté au contexte des réseaux mobiles et surtout des réseaux de collecte mobile via une approche de réseaux ouverts ; **élaborer un protocole de routage efficace** ('greedy') multi chemins qui alloue des ressources appartenant à différents opérateurs.

- **Optimiser et évaluer la performance des nouvelles architectures** pour la résilience («survivability») des réseaux de collecte mobile, les approches axées sur mesure pour assurer un fonctionnement robuste des systèmes en réseau dans des conditions exceptionnelles, telles que les catastrophes naturelles / artificielles.

- **Modéliser et développer des algorithmes de routage** à la demande via les nouvelles approches (e.g., **Software Defined Networking –SDN-**) pour réduire la complexité de la gestion du réseau, et rendre les réseaux plus robustes, plus flexibles, et moins complexes.

- **Faire la preuve de concept** des algorithmes pour démontrer la faisabilité pratique entre modélisation et implémentation.

Dans ce contexte, cette thèse a abordé les points suivants :

Partie II: Théorie et Modélisation

• Proposition d'une nouvelle architecture pour augmenter la fiabilité et réduire les coûts de construction de réseaux de collecte terrestres. Ce nouveau concept que nous avons appelé 3RIS (Résilience, Reliability –fiabilité-, redondance par Infrastructure Sharing –partage d'infrastructure-) fournit une solution pour améliorer la fiabilité sans investissements supplémentaires, basé sur la partage du réseau de collecte avec un autre opérateur. Nous avons évalué nos résultats par un système parallèle 2 - chemin simple en utilisant le modèle de chaînes de Markov.

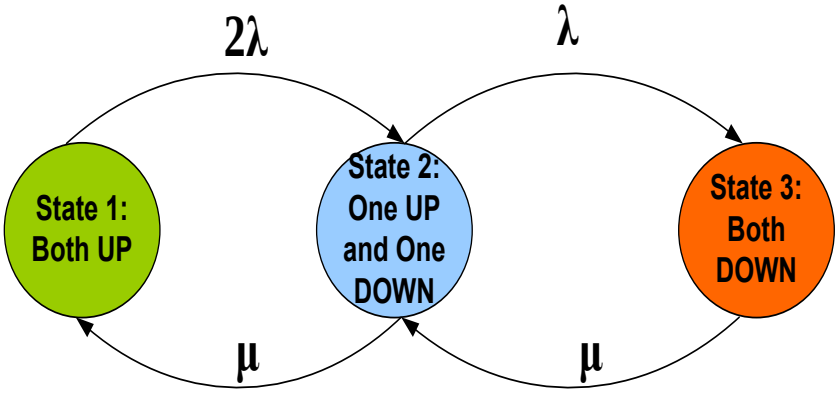


Figure E. 'State diagram' pour l'analyse de la disponibilité d'un système parallèle redondant.

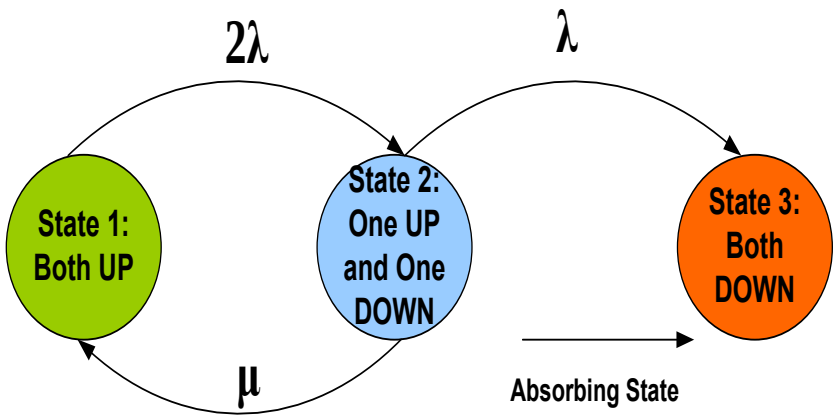


Figure F. 'State diagram' pour l'analyse de la fiabilité d'un système parallèle redondant.

Ces propositions ont été publiées dans les conférences suivantes:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Preliminary analysis of 4G-LTE mobile network sharing for improving resiliency and operator differentiation", in Proc. of 1st International Conference on e-Technologies and Networks for Development (ICeND'11) 2011; also published in Communications in Computer and Information Science (CCIS) Series of Springer-Verlag LNCS 2011, Volume 171, Part 5, pp: 73-93.

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "3RIS for 4G: A new approach for increasing availability and reducing costs for LTE networks", in Proc. of 14th IEEE International Conference on Advanced Communication Technology (ICACT'12), Phoenix Park, PyeongChang, South Korea, February 2012.

• Proposition d'une approche taillée sur mesure, qui adopte le concept Système Multi-State (MSS), basé sur le modèle de chaînes de Markov, pour assurer un fonctionnement robuste des systèmes en réseau dans des conditions inattendues telles que les catastrophes naturelles / artificielles. Les valeurs utilisées pour le calcul sont basées sur des valeurs réelles de coupure du réseau à partir d'un type Tier-I MNO (qui doit rester anonyme pour des raisons de confidentialité).

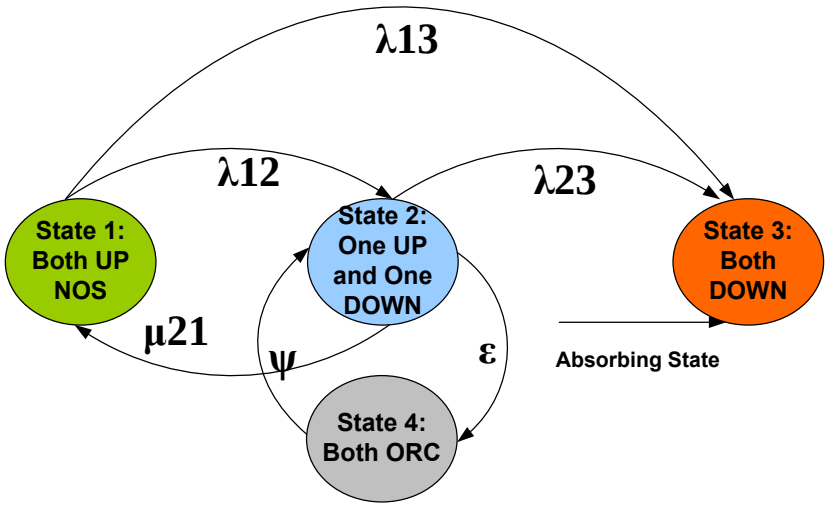


Figure G. 'Multi-state system reliability analysis diagram' pour le réseau de liens sans fil avec partage d'infrastructure.

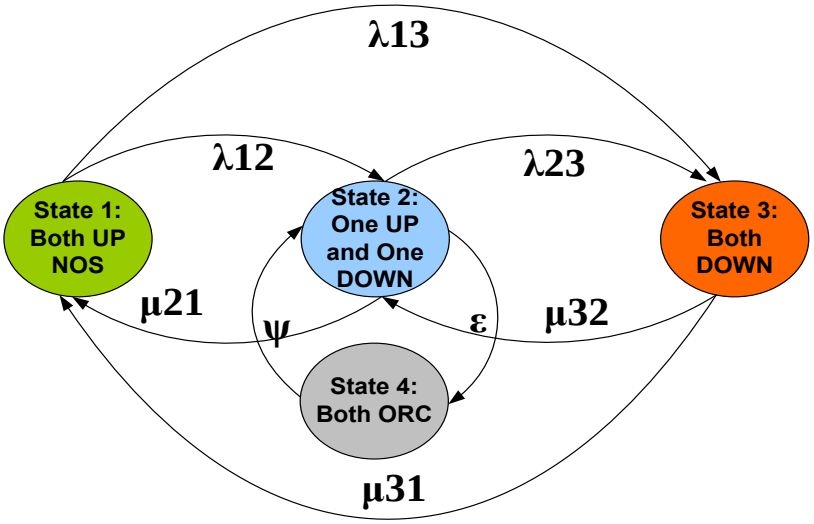


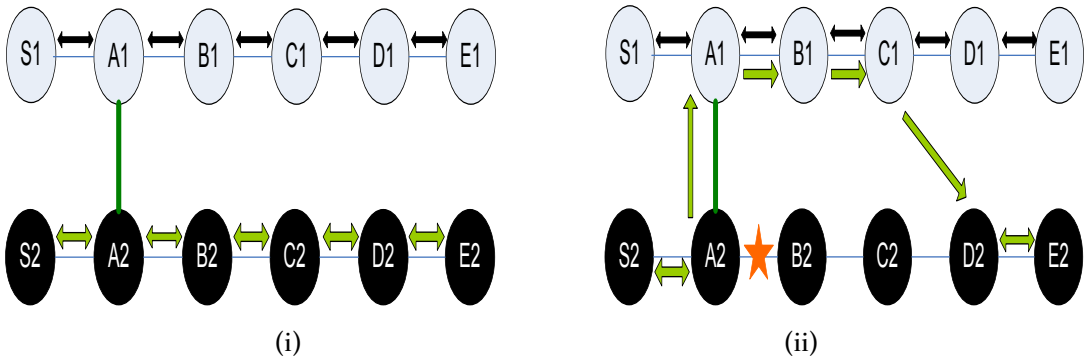
Figure H. 'Multi-state system availability analysis diagram' for pour le réseau de liens sans fil avec partage d'infrastructures.

Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Give and Take: Characterization of availability of multi-state wireless backhaul Networks", in Proc. of 76th IEEE International Conference on Vehicular Technology Conference (VTC- Fall'12), Quebec, Canada, September 2012.

• Illustre un mécanisme flexible de re-routage pour cette architecture, où les chemins de secours peuvent utiliser des liens disjoints physiquement de l'autre operateur. Grâce à ce travail, nous

avons pu affirmer que le problème d'interrompre simultanément le chemin principal et le chemin de secours des différents opérateurs de réseaux mobiles n'est donc pas du tout probable. Suite à cela, nous avons développé un modèle analytique sur les chemins de secours et le re-routage basé sur la théorie des probabilités qui permet de comprendre comment le trafic utilisateur est re-routé vers un composant de réseau, lorsque les opérateurs partagent la bande passante de leurs liens respectifs. Nous l'appelons ROFL.



i) flux de trafic avec le partage d'infrastructure dans des conditions normales.

ii) Une situation où il y a une panne et / ou une congestion du réseau entre le dernier-mile et moyen-mille au sein du réseau de transmission.

Figure K. Evitement de la congestion de lien à travers le partage de réseau de collecte.

Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "ROFL: Restoration of failures through link-bandwidth sharing," In Proc. of 2nd International Workshop on Rural Communications (RuralComm'12) co-located with 54th IEEE International Conference on Global Communications (GLOBECOM'12), Anaheim, U.S.A, December 2012.

Partie III : Techniques d'optimisation

• Ensuite, nous avons développé » OpenRoutes ', une illustration simple et systématique d'un modèle qui illustre une approche totalement différente pour calculer les chemins disjoints alternatifs avec une capacité optimale, dans un réseau de liaisons sans fil, basé sur le partage entre opérateurs de téléphonie mobile, sans affecter les flux de trafic existants. L'objectif de notre approche a été formulé en utilisant ILP (Integer Linear Programming), sur la base de nos définitions du modèle. Étant donné que ces formulations ILP sont très complexes à résoudre pour de grands réseaux, nous en avons tiré trois algorithmes basés sur des heuristiques simples mais efficaces. Ces propositions ont été publiées dans les conférences suivantes:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenRoutes: Multi-operator cooperative routing over maximally disjoint paths for the survivability of wireless backhaul," In Proc. of 9th IEEE/IFIP International Workshop on Design of Reliable Communication Networks (DRCN'13), Budapest, Hungary, February 2013.

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenRoutes: Augmenting Survivability with Reduced Redundancy- A Topology based Analysis," In Proc. of 19th ACM Annual International Symposium on Mobile Computing and Networking 2013 (MobiCom'13), Miami, Florida (Poster) (In Press), October 2013.

• La suite des travaux consistent à optimiser les ressources quand un MNO décide de partager ses principales ressources avec un autre opérateur mobile pour servir de ressources de secours, sans mettre en péril sa propre qualité de service (QoS). Nous avons développé une méthodologie systématique pour définir efficacement de manière optimale les limites de capacité à offrir pour offrir une expérience de haute qualité (QoE), c'est à dire définir le seuil supérieur et la limite inférieure d'utilisation des ressources par un autre réseau de collecte ORM pour chaque connexion passant par un lien défaillant.

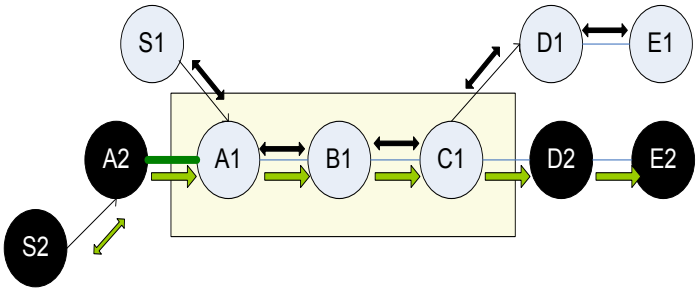


Figure L. flux de trafic avec le partage d'infrastructure dans des conditions défectueuses, matérialisées par la flèche en dessous des liens indiquant le sens vers le destinataire et les flèches sur le dessus indiquant le sens vers la source.

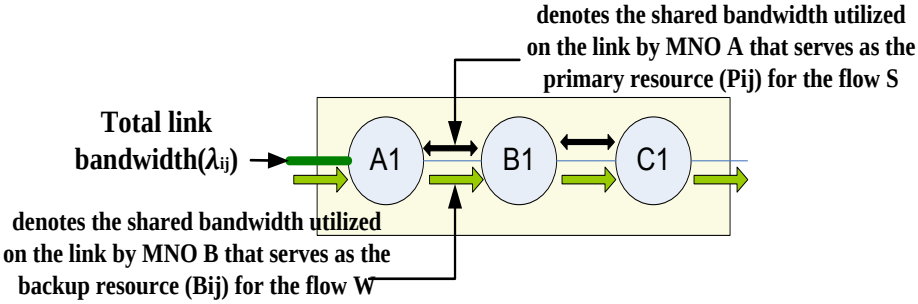


Figure M. Allocation de bande passante à travers le partage.

Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Divide and Share: A New approach for optimizing backup resource allocation in LTE mobile networks backhaul," in Proc. of 8th IEEE/IFIP International Conference on Network and Service Management (CNSM'12), in cooperation with ACM SIGCOMM, Las Vegas, U.S.A, (Short Paper), October 2012.

• La prochaine étape fut d'adapter nos solutions à une architecture SDN (Software Defined Networking). Suite à cela, nous avons défini un paradigme architectural «multi-topologie-partagée» pour la conception d'un réseau de communication en adaptant l'approche logique centralisée et très précisément vers une approche quasi-distribuée. Plus encore, notre approche exploite l'approche émergente SDN / OpenFlow [1] sur la maximisation de la capacité de survie du réseau grâce à la coopération bilatérale entre plusieurs opérateurs de réseaux mobiles, décrite par un scénario portant sur une étude de cas réaliste.

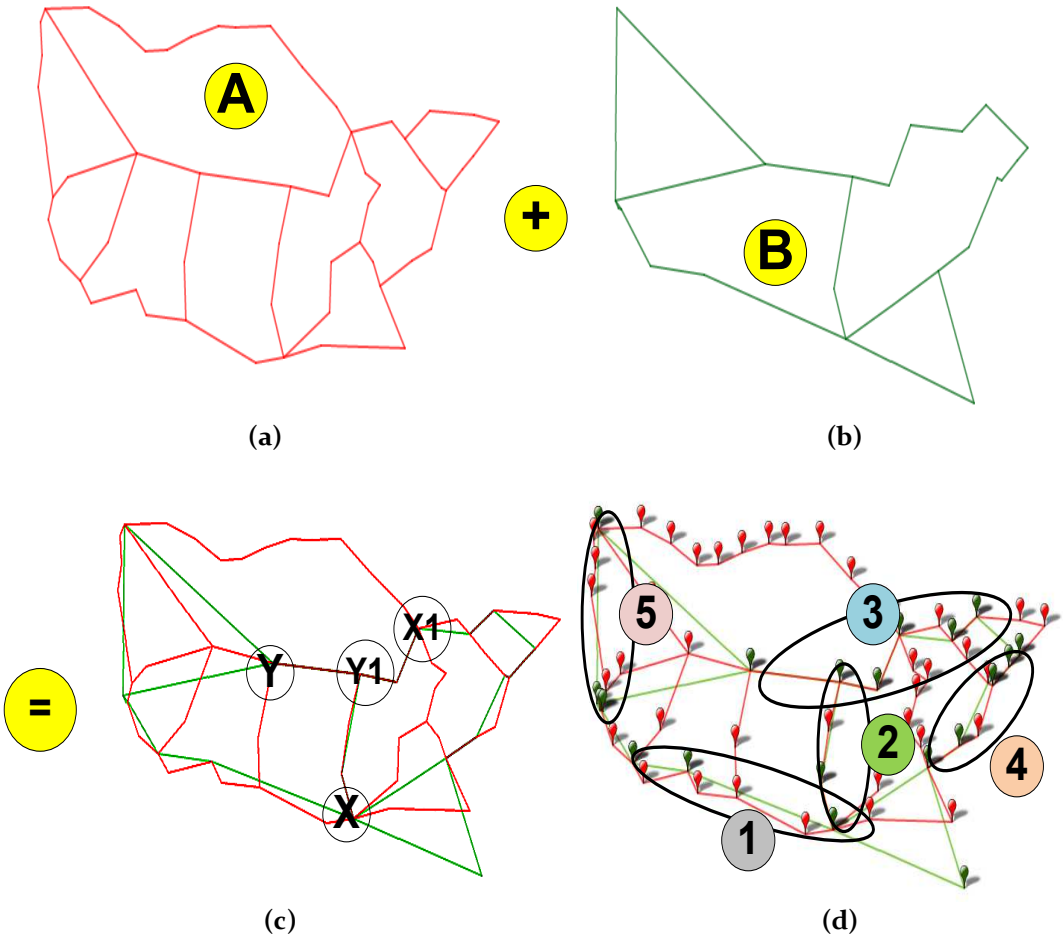


Figure N. Illustration de la fusion ou «couture » entre deux topologies différentes MNO (a) et (b) en une seule topologie (c), où les contrôleurs ont été placés afin de réduire le coût de sur-dimensionnement des réseaux existants avec des liens et des nœuds de chevauchement à cinq endroits différents (d).

Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Stitch-n-Sync: Discreetly Disclosing Topology Information Using Logically Centralized Controllers", in Proc. of 3rd International Workshop on Capacity Sharing (CSWS'13) co-located with the 21st IEEE International Conference on Network Protocols (ICNP'13), Gottingen, Germany, (In Press), October 2013.

• Dans ce cadre, nous avons défini un nouveau paradigme architectural en adaptant l'approche logique centralisée et plus particulièrement vers une approche quasi-distribuée. Pour des raisons

qui apparaitront plus clairement plus tard, nous appelons le régime résultant X -Control. Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "X-Control: A Quasi-Distributed Fault Restoration Mechanism Using Logically Centralized Controllers," in Proc. of 38th Annual IEEE Conference on Local Computer Networks (LCN'13), Sydney, Australia, (Short Paper) (In Press), October 2013.

Partie IV: Evaluation de la performance de SDN / OpenFlow

• Cette partie de la thèse traite de la faisabilité du partage de réseau de collecte mobile via une approche de réseau ouvert, basé sur OpenFlow. Nous évaluons la faisabilité pratique de nos concepts architecturaux proposés et adaptées dans le cadre de Software Defined Networking (SDN) / OpenFlow. En démontrant la possibilité d'adapter le mécanisme OpenFlow existant à l'architecture de réseau de collecte mobile, nous cherchons à définir l'impact du degré de partage dans différents scénarios, où le verrou principal réside dans la définition des politiques flexibles et extensibles qui peuvent être modifiés dynamiquement. Ces propositions ont été publiées dans les conférences suivantes:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenFlow as an architecture for e-Node B virtualization," in Proc. of 3rd ICST International Conference on e-Infrastructure and e-Services for Developing Countries (AFRICOMM'11); also published in Springer-Verlag LNICST, 2011, pp: 49-63.

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, " Demystifying Link Congestion in 4G-LTE Backhaul using OpenFlow," in Proc. of 5th IEEE/ IFIP International Conference on New Technologies, Mobility and Security (NTMS'12) 2012.

Partie V: Réseaux de Substitution

• Dans le même contexte, nous avons proposé une solution tenant compte des réseaux de substitution (SN) comme un moyen pour l'établissement de chemin de secours pour surmonter la surcharge du réseau temporaire. Notre approche considère la technologie Software Defined Networking (SDN) en raison de sa flexibilité pour intégrer diverses générations futures d'équipements ainsi que de son approche centralisée reposant sur la séparation entre le plan de contrôle et de plan de transfert. Nous avons démontré la possibilité d'ajuster la bande passante sur un ensemble de liens et équipements de manière dynamique en fonction des besoins de trafic des différents utilisateurs finaux, ce qui garantit la qualité de service (QoS) requise.

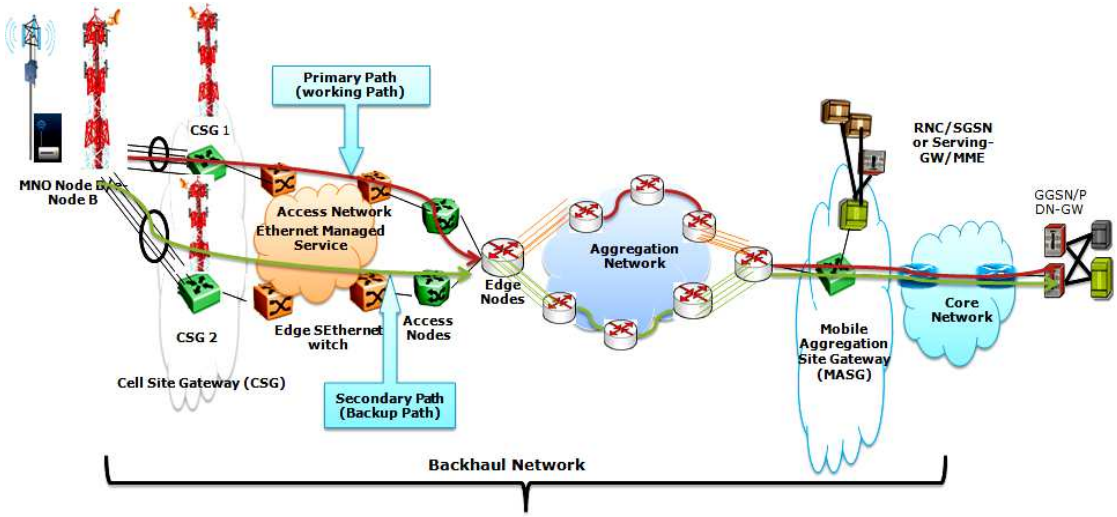


Figure O. illustrant la protection de chemin de sauvegarde en backhaul micro-ondes sans fil en 3G/4G.

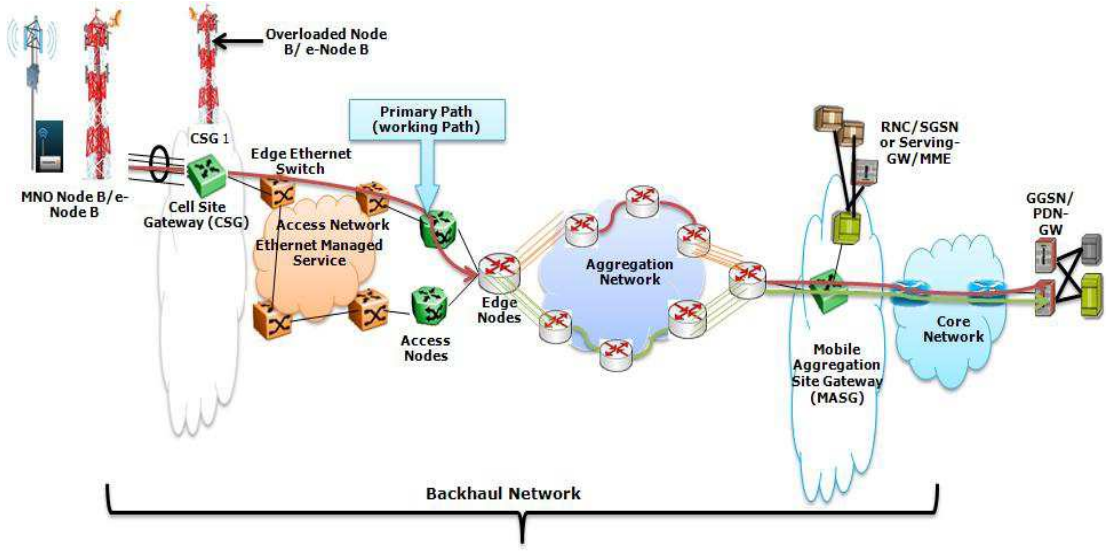


Figure P. conception architecturale illustrant l'élimination de chemin de back-up.

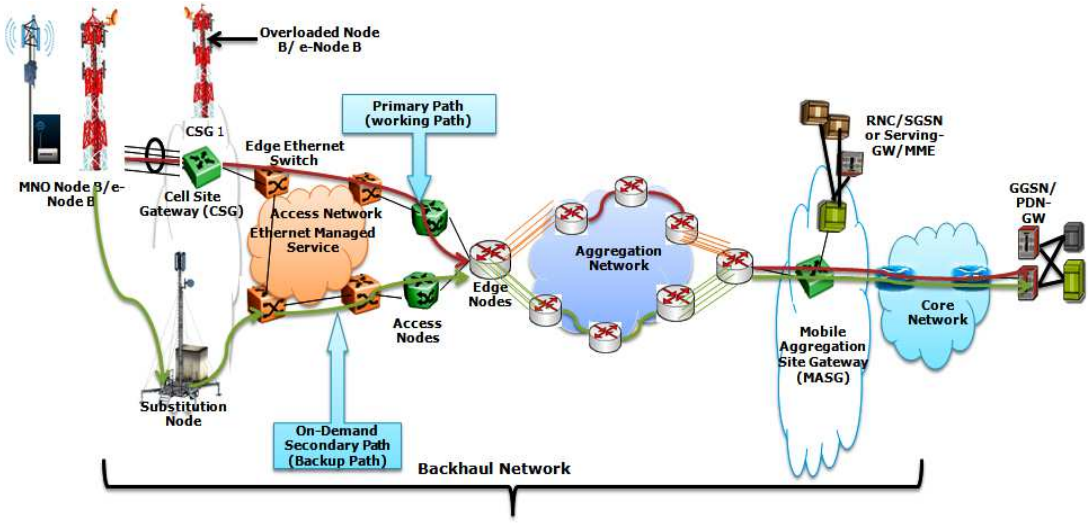


Figure Q. Architecture illustrant l'intégration de nœuds de substitution.

Ces propositions ont été publiées dans la conférence suivante:

- Venmani Daniel Philip, Yvon Gourhant, Laurent Reynard, Prosper Chemouil and Djamal Zeghlache,, "Substitution Networks based on Software Defined Networking," In Proc. of 4th ICST International Conference on Ad Hoc Networks (AdhocNets'12), Paris, France, September 2012.

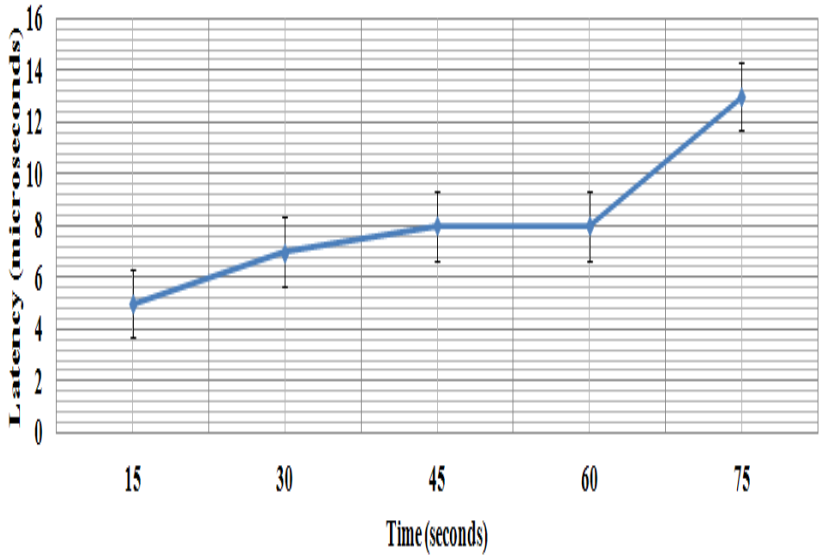


Figure R. Temps de latence moyen pour installer les flux sur un switch OpenFlow.

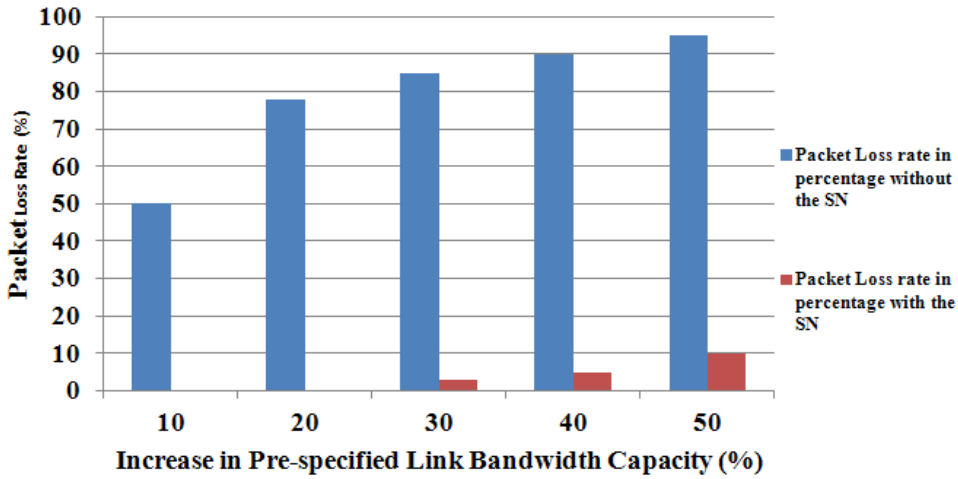


Figure S. Packet Loss Rate sur un lien avant et après l'introduction de nœud de substitution.

Le défi du déploiement de nouvelles architectures

Comme indiqué dans cette thèse, le déploiement de stratégies de collecte à faible coût, notamment celles fondées sur les technologies émergentes telles que Software Defined Networking (SDN)/OpenFlow, peut à première vue ne pas correspondre aux exigences qui seront

difficiles à traiter avec une approche commune pour réacheminer les transports, en particulier compte tenu de l'environnement de multi-opérateur.

D'une part, les exigences de collecte ont été constantes entre les deux stratégies (MPLS-TP et IP/MPLS) décrites dans les premiers chapitres (Chapitre 1). Cette convergence des exigences est dûe au fait que quel que soit le point de départ, tous les opérateurs ont le même objectif final qui est un réseau LTE basé pour le haut débit mobile.

D'autre part, SDN, basé sur une gestion séparant le plan de contrôle du plan de transfert, et d'autre part la virtualisation présente une nouvelle dimension pour l'amélioration et le développement. Le transfert des résultats et des concepts de recherche de topologies réelles impose des contraintes et des exigences supplémentaires indéniablement. Dans ce contexte, dans cette section, nous présentons un aperçu des défis de recherche et les difficultés que les opérateurs pourraient rencontrer en intégrant la technologie SDN dans les réseaux de collecte mobile.

D'un point de vue général, l'approche basée sur SDN/OpenFlow lève certainement des défis, notamment la stabilité et des problèmes d'évolutivité, compte tenu de l'approche centralisée. Le passage à l'échelle du contrôleur centralisé a été le sujet de récentes propositions [26] - [28] . Dans un environnement de communication mobile, nous constatons que les éléments de réseau tels que le Node B ou e-Node B eux-mêmes peuvent être un point de panne unique ainsi qu'un goulot d'étranglement plus que le contrôleur lui-même. L'utilisation de OpenFlow, où les flux peuvent être identifiés par une correspondance avec une chaîne de caractère et que le routage est basé sur une fonction de hachage (comme ECMP), réduit la charge du plan de contrôle (détaillées au chapitre 10), mais permet au contrôleur de gérer efficacement le trafic. En outre, nous considérons que SDN présente un contrôle central et une visibilité de la topologie complète. Lorsque l'on considère les réseaux mobiles, la divulgation de la topologie du réseau n'est pas souhaitée par les opérateurs, afin de préserver la confidentialité. Cependant, l'une de nos contributions, au chapitre 8, ouvre la première étape vers la visibilité de la topologie d'un point de vue théorique.

Bien que fondé sur la destination, le plus court chemin peut être calculé de manière distribuée (chapitre 7), SDN est basé sur la meilleure façon de répondre à acheminer les données. Cela signifie qu'il y a beaucoup plus d'informations dans le chemin de données OpenFlow au-delà de celles utilisées pour le transfert standard (filtres, marquage, politique de routage, QoS politique, etc.). Et il y a beaucoup d'utilisations plus souhaitables pour les réseaux que le simple transfert basé sur la destination. Nous voyons cela comme une solution minimaliste, renforcer le potentiel des services Internet, ainsi que les réseaux mobiles qui restent résolument situés au bord.

L'intention est également de rendre le réseau plus rentable en permettant un contrôle plus étroit du dimensionnement et de la planification des capacités de manière plus précise. Nous espérons que cette thèse va stimuler la recherche. Notre travail s'oriente actuellement dans plusieurs directions. Nous poursuivons l'évaluation de performance dans [29] accordant une attention particulière à l'étalonnage de la mesure fondée sur le contrôle d'admission. Nous cherchons également des algorithmes plus efficaces pour réaliser le contrôle d'admission tel que Packet Fair Queuing (PFQ) et des mécanismes pour faciliter la mise en œuvre. De plus, il est nécessaire d'ajouter un moyen de fusionner OpenFlow avec le réseau IP traditionnel dans le réseau de collecte, lorsqu'un un grand nombre d'utilisateurs dépasse les capacités maximales. Il existe déjà des propositions pour interfonctionner OpenFlow et MPLS (Ericsson) générant un nouveau type de réseau IP qui offre une combinaison de connectivité ouverte et des politiques de gestion.

Et c'est là que la technologie n'est pas compatible avec les réseaux réels. Bien sûr, il semble possible qu'il y a au moins un déploiement de réseau WAN largement médiatisé (sur le campus de Stanford) où le réseau des équipements reçoivent leur état de FIB à partir d'une application centralisée SDN utilisant OpenFlow. Mais il faut savoir que pour remplacer pleinement toutes les fonctionnalités de MPLS nécessaires, OpenFlow et SDN devront évoluer pour offrir les mêmes caractéristiques et fonctions. L'ajout de ces caractéristiques et de ces fonctions rendront–ils OpenFlow et SDN aussi complexes à l'avenir que MPLS l'est aujourd'hui? Si c'est le cas, ce sera l'industrie qui a gagné. Alors, s'agit-il simplement de déplacer le problème de la complexité ailleurs? D'autre part, en essayant de déployer une solution utilisant OpenFlow classique ne fonctionnera certainement pas. Pour commencer, l'utilisation de n-tuplets (par flux, ou même par paire source / destination) entraînera très probablement dans le tableau la saturation de l'espace mémoire. Même avec de très grandes tables (des centaines de milliers), la solution est peu susceptible d'être adaptée.

De plus, pour utiliser efficacement le matériel, il est nécessaire d'utiliser des techniques de 'multi-pathing'. Il est très peu probable (selon mon expérience) que le contrôleur ayant participé à l'établissement du flux aura les caractéristiques de performance et d'échelle souhaitées. Par conséquent, le multi-pathing doit être réalisé au niveau matériel (ce qui est possible dans une version ultérieure d'OpenFlow comme 1.1 et 1.2). Compte tenu de ces contraintes, une approche SDN aurait probablement beaucoup ressemblée à un protocole de routage traditionnel. Autrement dit, le résultat serait probablement basé sur le préfixe IP de destination (afin que nous puissions profiter de l'agrégation et de réduire les contraintes de table par un facteur de N sur les paires source-destination). En outre, la détection de défaillance multi-pathing, et le lien devrait être fait sur le switch.

SDN a jusqu'ici été utilisé principalement pour optimiser les ressources des centres de données

dans le Cloud. Mais il a aussi été beaucoup discuté dans le domaine des télécoms et les opérateurs ont testé des applications SDN pour les éléments de réseau opérationnels. L'application de SDN pour le transport et l'optimisation de backhaul est si récente qu'il reste du travail pour faire adopter SDN par les fournisseurs de services. Cependant, la recherche suggère que le RPS peut presque réduire de moitié le surcoût du backhaul, ce qui représente pour les opérateurs un peu moins de 5 milliards de dollars en dépenses en capital en 2017. Un rapport de Strategy Analytics publié l'an dernier a révélé un écart $9,2 milliards entre la bande passante utilisée et la capacité de backhaul. Le trafic de données mobiles augmente, l'investissement nécessaire pour répondre aux attentes de l'expérience client des utilisateurs s'accroît. Un manque de capacité dans les réseaux de collecte apparait déjà à et l'écart de capacité dans le backhaul peut atteindre 16Pb (mégaoctets) à l'échelle mondiale d'ici 2017, selon Strategy Analytics. Dans un rapport de suivi publié par Tellabs aujourd'hui, Strategy Analytics prévoit que le RPS peut apporter une économie aux opérateurs mobiles de plus de 4 milliards de dollars en dépenses en capital en 2017. Ces économies proviennent de cinq applications SDN clés pour les réseaux de liaison mobiles et peuvent aider à combler près de la moitié de l'écart identifié dans la Stratégie Analytics du rapport précédent en offrant le partage de la charge du réseau et l'allocation des ressources dynamiques. En outre la nouvelle gestion de commande et des ressources SDN sera considérablement plus faible vis-à-vis des dépenses sur les opérations réseau backhaul (OPEX).

En conclusion générale, les étapes de l'évolution du réseau connexes envisagent que SDN / OpenFlow seront communs et la différence se situera si tous les opérateurs connaîtront toutes les étapes de transformation ou si certains peuvent accélérer ou sauter une ou deux étapes. Les opérateurs historiques avec une infrastructure existante ont la tâche la plus complexe devant eux. Le défi réside dans la complexité de la gestion de la transition vers le transport par paquets tout en maintenant en vigueur la qualité des services existants. Pendant de nombreuses années à venir le backhaul devra accueillir non seulement HSPA+ et LTE, mais aussi fournir simultanément une solution de transport pour une gamme complète de transport de technologies RAN. Le transport par faisceaux hertziens en mode hybride aujourd'hui et le mode paquets pur remplacent l'encapsulation dans un transport TDM qui jusqu'à présent prédominait. Et finalement, les réseaux 2G seront désactivés permettant le réseau de transport de paquets pur pour le haut débit mobile.

Part I

Introduction and State of the Art

"I'm quite hard on myself but the pressure comes from me. Being a Scientist, it's all in some way very neurotically linked to your self-esteem and I think you've got to understand where your anxiety comes from." – ***Stephen Hawking, Theoretical Physicist, Cosmologist.***

Chapter 1

Prologue

In this dissertation, we address the problems of (i) tackling rapidly fluctuating network data traffic during network failure conditions as well as during network traffic surge (ii) improving network survivability and therefore increasing the reliability and availability – of mobile backhaul networks. Among others, one naive solution to tackle these two problems together is to increase the link capacity, otherwise termed as over-provisioning. However, in the light of the various challenges for the Mobile Network Operators (MNOs), increasing the capacity ultimately would have an enormous impact on the cost investments. Having said this, through this dissertation, we argue over the necessity for every independent MNO within a geography to build permanent backup paths (redundant paths) – because the capacity which is allocated for the backup path is not 'always' actively filled-in as much as the capacity allocated for the primary path. Our arguments lead to a novel design in which two or more MNOs share each other's unused network resources mutually (links/bandwidth capacities), up to a certain extent without exceeding their limits on resource sharing, thereby saving on over-provisioning costs. Motivated by this, we study the problem of how to share the available resources of a backhaul network among its competitors, with whom a Service Level Agreement (SLA) has been concluded. We present a systematic study of our proposed solution focusing on a variety of empirical resource sharing heuristics and optimization frameworks.

1.1. Opening Comments

"We believe that Telecom network mobile data traffic in the South Island and Lower North Island is now flowing again after our engineers rebooted the system. However, it's possible that there may be further disruptions to services due to intermittent problems as the system catches-up with data traffic demand."- XT Mobile Network, Aug 23, 2013.

"France Telecom to compensate its customers following nine hours of network failure (France) - July 9, 2012".

"Network failure at T-Mobile Netherlands affecting 2 million customers solved after 24 hours (Netherlands) - March 29, 2011."

"Gaz gives Zain 48 hours to resolve network failure (Zambia) - July 6, 2009."

The above statements are not merely an exaggeration of the headlines cited from popular news channels, but true depictions on the reality of today's mobile communications networks, be it in a developed country or in an emerging economy and the list can go on! These evidences are intended to be a brief, necessarily cursory and an incomplete history about network failures. Having said this, while most Internet Service Providers (ISPs) and Mobile Network Operators (MNOs) have promised advantages of redundancy and resilience from the start, there is still the specter of failure. With this figure of speech, the problems of network failures in today's networks can be quickly but clearly ascertained. The underlying observation is that MNOs and ISPs are still exposed to unpredicted breakdowns and/or rapid fluctuations in traffic; it goes without saying that even the largest operators can be affected. But what if, these operators could now put in place designs and mechanisms to improve network survivability to avoid such occurrences? What if mobile network operators can come up with low-cost backhaul solutions together with ensuring the required availability and reliability in the networks?

In the late 2010, my scientific supervisors and I, were able to formalize the research subject of this dissertation, pondering over the above noted problem statements, briefly falling under the following context, i.e., (i) how to tackle rapid fluctuations in network data traffic resulting due to network failure conditions as well as unexpected traffic surges, (ii) consequently how to improve network survivability - within the context of backhaul networks of cellular networks, while focusing particularly towards the emerging markets such as the BRICS (Brazil, Russia, India, China, South Africa) economies and the Sub-Saharan African countries (Nigeria, Uganda, Tanzania, Kenya etc.) Eventually through our subsequent discussions, we agreed-upon that there is one naive solution to tackle these two problems together, i.e., to increase the link capacity,

otherwise called as over-provisioning the network. However, in the light of the various challenges today faced by the ISPs/MNOs, increasing the capacity ultimately leads to increasing the cost. This might result in staggering CapEx (Capital Expenditure) and OpEx (Operational Expenditure) for them, especially in those emerging economies; thus this solution is not cost-efficient at all.

With this problem statement in-hand, the overarching theme of this dissertation is within the following scopes: (i) to provide low-cost backhaul solutions; the motivation here being able to build networks without over-provisioning and then to add new resources (link capacity/bandwidth) in case of failure for particularly ensuring premium services (ii) to provide uninterrupted communications even at times of network failure conditions, but without redundancy. Here a slightly greater emphasis is laid on tackling the 'last-mile' link failures. With this being the keen focus, this dissertation aims to develop efficient approaches to improve the reliability and availability of networks integrated with link failures, node hardware failures. The scope of this dissertation is therefore to propose, design and model novel network architectures for improving effective network survivability and network capacity, at the same time by eliminating network-wide redundancy, adopted within the context of mobile backhaul networks. Ultimately, the topics addressed in this dissertation span over a range of subjects such as Fault Management, Network Optimization, Inter-Domain Policy Routing, Greedy Routing, Cooperative Routing and the emerging Software Defined Networking technology. The research methodologies and results are performed at the system level and the network level. The proposed solutions target these problems to help operators improve their network availability and reliability. It is of the author's great pleasure that this research has added some valuable contributions that ultimately brings-in some technological betterment to improve the network survivability of future mobile networks.

1.2. Thesis Layout

The research results of this dissertation can be scrutinized and boiled-down into five separate but conjoint parts that address the problem in a systematic fashion targeting on two specific proposed solutions – (i) sharing the already existing backhaul architecture between two (or more) MNOs (Infrastructure Sharing) and (ii) adaptation of a new architecture based on Substitution Networks, wherein a temporary wireless network that has rapid deployment capability to back-up a base network is brought-in; in particular focusing on designing and evaluating 'shared' architectural solutions followed by developing routing and forwarding solutions for these specific architectures. Each part of this dissertation begins with a short introduction to the problem that is being addressed, and its context. This is followed by the respective models to be used therein. Any new notation that is particular to the part of

dissertation is also introduced here. The dissertation itself is based on several mathematical formula and equations. The continuity of the equations is restricted to individual chapters to avoid ambiguity, i.e., the equation numbers start and end within each chapter and therefore the next chapter begins with a new set of equation numbers. Wherever appropriate, each chapter ends with numerical examples or simulations. The document is structured in the way such that to avoid forward references for exclusive details; nevertheless references there-in are aptly acknowledged.

With this start, a brief outline of each of the chapters in the dissertation is as follows: the dissertation begins by exploring the existing state of the art techniques in network sharing and gives an in-depth insight on the pros and cons of network sharing. This is elaborated in Chapter 2. This is accompanied briefly by network virtualization in the same chapter. As network virtualization can be a form of network sharing technique, it becomes inevitable to get into the details of the current state of the art in network virtualization techniques. This includes specific details about the emerging Software Defined Networking (SDN)/OpenFlow technology. This concludes Part I of the dissertation. On a general note, it is worth remarking that Part I is introductory in nature and furnishes the background material for the rest of the dissertation. It is through this extensive research, the dissertation finds its main ideas for combining the key attributes of SDN and network sharing in the context of backhaul network sharing.

Following this are Chapter 3 and Chapter 4. In the process we propose and evaluate the analytical results targeting on reliability and availability analysis of our novel architectures using Markov chains, Probability and Statistics and present in these chapters, marking the beginning of our novel solutions, providing solid foundations to the rest of the dissertation. With this, Part II is brought to an end.

On continuation of this are Chapters 5, 6, 7 and 8. These chapters exclusively focus on network optimization techniques that include design, modeling and optimization of backhaul network resources that can cost-effectively provide protection and restoration to improve network survivability. Specific 'greedy' and 'cooperative' routing and forwarding algorithms, particular to our problem statement have been proposed and implemented. Following this, we then investigate optimization techniques for incorporating SDN within the backhaul of MNOs, which is one key contribution of this dissertation. This brings an end to Part III of the dissertation.

With a solid theoretical foundation of our proposed solutions from our previous chapters, the curiosity to explore the possibility of our proposed solutions in 'real' world grew-up and hence the necessity to perform simulations 'close to the real world scenario' to bring-in proof-of-concept arouse. Following this, is Chapter 9, covered as part of Part IV of the dissertation, where

several proof-of-concept experiments were carried out to demonstrate the practical feasibility of our proposed architectures, comparing our solutions to the existing state of the art solutions.

The fifth and final part of the dissertation moves further down presenting a primitive emulated prototype illustrating substitution networks. Within this scope, the dissertation explores the possibilities of adapting the SDN architecture to substitution network design and our results confirm that, this emerging SDN technology has more to offer while adapted for the backhaul networks. To start with, a bandwidth management algorithm has been implemented for re-routing network traffic onto a substitution node, under network failure conditions, using NOX (OpenFlow) controller. While we do not yet have a concrete proof that supports both infrastructure sharing and substitution networks side by side, we believe that the bandwidth management algorithm we present in this chapter constitutes sufficient conditions for the existence of both the solutions in real world.

1.3. Research Contributions

We summarize here the original contributions of this thesis. All of the ideas presented in this thesis have been submitted and duly published, either in a peer-reviewed international conference or a workshop or as a poster, those that are closely related to (but not limited to) the areas of Networks and Networking, Network Optimization, and Network Management.

1.3.1. Part II: Theory and Modeling

This part of the thesis is completely devoted to designing analytical models to support our proposed solutions mathematically.

1.3.1.1. Chapter 3

<u>Novel Backhaul Architectural Design: Concept Evaluation and Analytical Modeling:</u> This chapter takes a more accurate look into the existing mechanisms to bring down the impact of failures in backhaul networks. Classical protection mechanisms such as the 1+N, 1:N, M:N have been accounted so far by MNOs to recover the traffic after a failure occurs by re-routing it through another backup path before the failure is physically repaired, to guarantee continuous availability. These approaches, however, incur additional investments that do not result in resource and cost-efficient networks. Furthermore, we were able to conclude that despite the existing resilience mechanisms, there are occasions when the network resources are not available for the end users, all of the time. Besides, to reduce CapEx (Capital Expenditure), on most occasions, MNOs do not consider the choice of

provisioning an additional backup link as backup path to protect the last-hop of the "last-mile" link that connects rural and/or remote areas. Therefore, it goes without saying that current resilience mechanisms are based on over-dimensioning and re-routing mechanisms are mainly deployed on core networks but they cost too much for being largely deployed till the last-mile backhaul network compared to the probability of outage. Having said this, the first part of this chapter calls-for novel re-designing backhaul solutions that can cost-effectively decrease the overall unavailability time. Taking this premise as our starting point, the latter part of this chapter unfolds an analytical model for the proposed architectural design based on Markov Chain model that has been developed to show the advantages of infrastructure sharing. The mathematical equations for the reliability model were derived on the basis of Continuous-Time Markov Chains. To summarize, the research contributions of this chapter are:

- Thorough analysis of existing backhaul network topology designs, majorly focusing on microwave backhaul design to 'backup' last-mile link failures without over-provisioning.

- Proposed a novel solution for increasing reliability and reducing network costs of building mobile backhaul networks. This new concept that we have termed as Resiliency, Reliability, Redundancy by Infrastructure Sharing (3RIS) provides a solution to improve reliability without additional cost investments, by sharing another operator's microwave backhaul.

- We evaluated our results by a simple 2-path parallel system using State Space Markov Chain model.

- The advantage of the model is that it can be applied to any system with high complexities. The technique is effective for small and large-scale systems. As long as the system's reliability equation can be derived analytically, the model can be used to solve the reliability allocation problem.

These proposals were published in the following papers:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Preliminary analysis of 4G-LTE mobile network sharing for improving resiliency and operator differentiation", in Proc. of 1st International Conference on e-Technologies and Networks for Development (ICeND'11) 2011; also published in Communications in Computer and Information Science (CCIS) Series of Springer-Verlag LNCS 2011, Volume 171, Part 5, pp: 73-93.

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "3RIS for 4G: A new

approach for increasing availability and reducing costs for LTE networks", in Proc. of 14th IEEE International Conference on Advanced Communication Technology (ICACT'12), Phoenix Park, PyeongChang, South Korea, February 2012.

Multi-State System (MSS) Approach using Discrete-state Continuous-time Markov Chain Model: Convinced with the preliminary findings on the research subject, we go further down to a deeper space and provide a very different view on the availability analysis of the newly proposed architectural design based on the Multi-State System (MSS) approach using Discrete-state Continuous-time Markov chain model. We begin by demonstrating the availability of wireless communication networks supported by microwave backhaul links while two different MNOs share their working paths as an alternative for backup paths. Our results show that such a jointly- constructed network was available to meet the required demand of the total system more than 99.8 % of the time. The original contributions in this chapter are:

- To the best of our knowledge, this is the first work so far[1] that adopts the concept Multi-State System (MSS) approach using Discrete-state Continuous-time Markov chain model.

- A measurement-driven approach to ensure robust operation of networked systems under unexpected conditions such as natural/unnatural disasters has been analytically developed. Measurement in the sense that the values used for the calculation were based on real-world network failure values from a typical Tier-I MNO (who shall remain anonymous for the sake of confidentiality).

- Typical numerical values supporting our theory have been presented.

The contribution has been duly acknowledged in the following proceedings:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Give and Take: Characterization of availability of multi-state wireless backhaul Networks", in Proc. of 76th IEEE International Conference on Vehicular Technology Conference (VTC- Fall'12), Quebec, Canada, September 2012.

1.3.1.2. Chapter 4

Analytical Modeling for Recovery and Re-routing: While the reliability of shared backhaul networks has been successfully demonstrated analytically earlier, we go forward to model fault recovery and re-routing for such a 'shared' architecture. Therefore, in this chapter, we

1 Statement is based on an IEEE VTC-Fall 2012 Anonymous Reviewer's comments.

introduce a novel fault recovery scheme through link-bandwidth sharing among different MNOs. Our model for recovery and re-routing strongly rely on the availability of the architecture. Therefore, we begin by demonstrating the availability of wireless communication networks supported by microwave backhaul links while two different MNOs share their working paths as an alternative for backup paths. This will help in tackling the high bandwidth requirements apart from serving as a backup under link failure situations without any additional cost investments. We proceed further towards a probabilistic model for fault restoration to reroute traffic flows in the event of link failures while two different MNOs share their backhaul link-bandwidth. The original contributions in this chapter are:

- Illustrated a flexible re-routing scheme, where backup capacity can traverse via physically separate routes of another MNOs backhaul and therefore we were able to affirm that the problem to interrupt both the primary path and the backup path of different MNOs simultaneously, is therefore not likely at all.

- Provided a systematic optimistic illustration that exemplifies a completely new availability analysis to evaluate the availability gained within MNOs' backhaul when they share their backhaul link-bandwidth together.

- Developed a path-based proactive analytical model for recovery and re-routing based on probability theory that enables to understand how the user traffic is re-routed around a failing network component, when MNOs share their backhaul link-bandwidth together. We call this as ROFL (Restoration of Failures through Link-Bandwidth Sharing).

The associated publication for the original work is:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "ROFL: Restoration of failures through link-bandwidth sharing," In Proc. of 2nd International Workshop on Rural Communications (RuralComm'12) co-located with 54th IEEE International Conference on Global Communications (GLOBECOM'12), Anaheim, U.S.A, December 2012.

1.3.2. Part III: Optimization Techniques for Network Survivability

This part of the thesis focuses on network optimization techniques to improve network survivability by evaluating metrics such as network throughput, resource utilization efficiency, blocking probability etc.

1.3.2.1. Chapter 5

Multi-operator Cooperative Routing for Network Survivability: With analytical evaluations in-hand, the next part of the dissertation deals with optimization frameworks. Here we identify the complexities in routing and dynamically rebalancing traffic across diverse end-to-end available paths in response to individual failure events along a backhaul network which is built out of sharing between different MNOs. The optimization objective that we have set is straight-forward here. There are different MNOs within a country who has built the nation's backhaul network topology together. Now, when one of them encounters a link/node failure at a specific geographic location, the disrupted connections must be re-routed appropriately, across the most optimal path of the topology, according to their traffic class. For instance, if a disrupted connection belongs to real time (conversational/streaming class), then it can not tolerate a new alternative path with high delay. Alternatively, a traffic class belonging to the best effort type (interactive/ background class) may tolerate medium to large delay values, but may require alternative paths with high bandwidth. With this being the focus, this chapter centers on three routing heuristics for the survivability of backhaul networks. Specifically, we provide a methodology for selecting the most optimal candidate alternative path according to the QoS requirements of the disrupted traffic, from a set of multiple paths computed. For reasons which are made clear, we call the resulting scheme as 'OpenRoutes'. In association with this, we therefore claim the following contributions:

- A simple and systematic model illustration that exemplifies an entirely different approach to compute alternative disjoint paths with optimal capacity, in a wireless backhaul network that has emerged out of sharing between different MNOs, without affecting any of the other MNOs' existing traffic flows.

- Consequently, the objective of our approach has been formulated using ILP, based on our model definitions. The proposed ILP formulations use the dual-simplex method linear programming, which essentially captures all the restraining conditions for computing multiple alternative paths, on every edge between any pair of vertices of our network topology.

- Since such ILP formulations are very complex to solve for medium/large networks, in what follows then, we appeal for three simple yet efficient heuristic algorithms. While there are several approaches to solve this kind of problem formulations, the first two of our heuristics extensively relies on the properties of the classical Dijkstra's algorithm, while the third one relies on the Ant Colony Optimization (ACO) algorithm.

- We demonstrated that our approach attempts to minimize network disruption cost-effectively, by maximizing the unused network resources, by appropriately selecting paths even when the network links are under a high congestion level. This renders MNOs with a parameterized objective function to choose the desired paths based on traffic patterns of their end-customers.

Focalizing towards this, the results were published in the following conferences:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenRoutes: Multi-operator cooperative routing over maximally disjoint paths for the survivability of wireless backhaul," In Proc. of 9th IEEE/IFIP International Workshop on Design of Reliable Communication Networks (DRCN'13), Budapest, Hungary, February 2013.

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenRoutes: Augmenting Survivability with Reduced Redundancy- A Topology based Analysis," In Proc. of 19th ACM Annual International Symposium on Mobile Computing and Networking 2013 (MobiCom'13), Miami, Florida (Poster), October 2013.

1.3.2.2. Chapter 6

<u>Multi-operator Greedy Routing Based on Sharing with Constraints:</u> While 'OpenRoutes' specifically targeted on routing disrupted connections across multiple MNO backhaul networks based on their respective traffic class, in this chapter we analyze the link capacity requirements when two different Mobile Network Operators (MNOs) decide to "divide and share" their primary resource (working path) as an alternative for investing in a backup path. That is, increasing the amount of sharing will naturally increase the risk that might create an inter-relatedness of one or more MNOs. High inter-relatedness could lead to under-utilization or over-utilization of the network resources by their partner. If one partner over-utilizes the sharing commitments, then the position of the other partner would be weakened. Another barrier for the MNOs is the fact that sharing can lead to loss of non-optimal long term capacity provisioning decisions. Therefore, we center our focus towards the "optimum configuration choice" for backhaul resource provisioning between the MNOs agreeing to share their primary resource (working path), so that the overall bandwidth reservation for the backup path would be minimal, thus minimizing the total cost for additional backup resource. Within this context, we tackle the problem of dealing with a complex decision for setting the maximum and minimum bounds in link capacity that can be shared and utilized between the MNOs' who agree to share. This decision consists in determining the optimal configuration of total link bandwidth capacity to handle the additional traffic demand due to a new connection request which arrives from the sharing MNO. To examine and to develop practicable performance bounds on resource

sharing, we make an estimation of the resource utilization and derive integer linear programming (ILP) counterparts. Given the complexities of solving ILP, we also propose heuristic-based resource provisioning algorithm which allows MNOs to share their primary resource with (an)other MNO(s), without having to sacrifice their own traffic demand requirements. Because our model uses preference orderings of outcomes to establish equilibria for computing both primary link capacity and backup link capacity, it allows for a quick exploration of the limits regarding resource sharing. This can help both the MNOs and the regulators to evaluate the strategic decision regarding (backhaul) resource sharing in a typical oligopoly telecom market. Original contributions can be summarized as below:

- Optimization of resources when one MNO decides to share their primary resource with another MNO which would serve as backup resource, without jeopardizing their own quality-of-service (QoS) requirements.

- A systematic optimistic methodology to efficiently define the capacity bounds in its ability to offer a high quality of experience (QoE) for subscribers, i.e. to define the upper and the lower bounds of the traffic through another MNOs' backhaul network for each connection going through a failed link.

The associated conference publication is:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Divide and Share: A New approach for optimizing backup resource allocation in LTE mobile networks backhaul," in Proc. of 8th IEEE/IFIP International Conference on Network and Service Management (CNSM'12), in cooperation with ACM SIGCOMM, Las Vegas, U.S.A, (Short Paper), October 2012.

1.3.2.3. Chapter 7

<u>Adapting Software Defined Networking for Mobile Backhaul Networks:</u> Thus far, we have discussed on how backhaul network resources could be shared among multiple MNOs. To tackle the management complexity of a backhaul network that comprises of several MNOs/ISPs 'heterogeneous' network equipments, an alternative approach involves centralized management and network-wide control using logically centralized controllers - accountable for collecting, computing, and maintaining the state required by the individual network equipments, to operate coherently. While such physical centralization is good as a first order evaluation example, practical deployment of such architectural design to various application scenarios, such as ours, may be restricted by questions about the overall scalability, restoration latency, convergence delay of the physically centralized controller.

With this background, here we illustrate the survivability of backhaul networks with reduced amount of physical redundancy, by effectively managing geographically distributed backhaul network equipments which belong to different MNOs using 'logically-centralized' physically-distributed controllers, while meeting strict constraints on network availability and reliability. Our contributions in this work exclusively focus on:

- Illustrating a restoration architectural design paradigm of a communication network by adapting the logically centralized approach and more specifically towards a Quasi-Distributed approach. For reasons which are made clear later, we call the resulting scheme as Cross-Control (X-Control).

- Consequently, our scheme has been developed and evaluated with proof of correctness specifically including (i) an extensive stochastic model which characterizes our problem as a multi-constrained optimization problem (ii) completely new Integer Linear Programming (ILP) formulations based on the model definitions (iii) an efficient greedy heuristics based on convex combination technique [12] to solve the formulated ILP model (iv) performance evaluation on real network topologies.

Novelty of our contributions was recognized as a publication in:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "X-Control: A Quasi-Distributed Fault Restoration Mechanism Using Logically Centralized Controllers," in Proc. of IEEE 15th International Conference on High Performance Switching and Routing (HPSR'14), Vancouver, Canada (In Press), July 2014.

1.3.2.4. Chapter 8

<u>How Multiple Operators can share their Topologies - Topology-Sharing:</u> From the above discussions, one recurring question is on the complexity to decide what MNOs should reveal and what not to reveal, i.e. competitive MNOs are typically long-known for their shrewdness to conceal their underlying network topology information. Having said this, we propose a quasi-distributed topology information sharing framework for network operators based on logically centralized controllers. Through our approach, we present a topology information sharing scheme in which two or more MNOs can cooperatively and more importantly-discreetly, reveal their topology information for the sake of utilizing the unused available resources of each other, at times of network failure situations. Our approach has been formulated and developed based on a novel key metric to 'tune' the amount of information sharing. Based on extensive simulations, we then investigate the impacts of network topology information sharing on the network capacity. The overall

feasibility is illustrated through significant numerical results. Summary of the contributions are thus the following:

- Illustrating a novel 'multi-topology shared' architectural design paradigm of a communication network by adapting the logically centralized approach and very specifically towards a Quasi-Distributed approach. More significantly, our approach exploits the recently emerging SDN/OpenFlow approach [1] on maximizing the network survivability through bilateral cooperation between several MNOs, elaborately described by a real world use case scenario.

- Subsequently, we formulated and developed a key metric that is based on mathematical modeling to characterize our problem as an optimization problem.

- Based on the model definitions, we proceed forward to define and elaborate on our Integer Linear Programming (ILP) formulations.

- Performance evaluation on real network topologies illustrates the numerical results showing its support to the theory and proof of correctness.

Very interesting results paving the way towards a different direction in resource sharing were part of the publication proceedings of:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "Stitch-n-Sync: Discreetly Disclosing Topology Information Using Logically Centralized Controllers", in Proc. of 3rd International Workshop on Capacity Sharing (CSWS'13) co-located with the 21st IEEE International Conference on Network Protocols (ICNP'13), Gottingen, Germany, October 2013.

1.3.3. Part IV: Proof-of-Concept Experiments for Validation and Verification of OpenFlow Deployment in Mobile Backhaul Networks

This part of the thesis focuses on evaluating the practical feasibility of our proposed solutions. We propose a solution based on Software Defined Networking (SDN) that enables OpenFlow based switches and controllers. By demonstrating the feasibility of adapting the existing OpenFlow mechanism to mobile backhaul network architecture, we illustrate the evolution of network sharing via an open network approach, based on OpenFlow. With OpenFlow, we seek to define how far it can be gone within the sharing scenarios based on the architecture of LTE/EPC defined in 3GPP, where the key lock is to open facilities to define flexible and extensible policies.

1.3.3.1. Chapter 9

Experimental Results on OpenFlow Protocol's Performance on Virtualization Property for Mobile Networks: Because a part of our argument is that network sharing by means of virtualization based-on SDN, could open new doors not only towards cost reduction but also gives the operators the flexibility they want in terms of traffic prioritization, we carried out simulations to prove that the OpenFlow protocol can be better-off compared to layer 2 switching based on standard VLAN virtualization. Based on our results, we could conclude that SDN allows virtualization of an existing network infrastructure, to start at least between two operators in parallel thus enabling dynamic modification of the properties of one network operator without disruption of service in the other operator. The research contributions can be summarized as:

- A novel solution has been proposed based on exploring OpenFlow as an architecture for e-Node B virtualization where resource sharing takes place from the access network part of the mobile network extending to the backhaul until the core network.

- Demonstrated the feasibility of adapting the existing OpenFlow protocol to mobile network architecture that illustrates the evolution of network sharing where two or more different MNOs can share their existing infrastructure based on the traffic patterns of their end-users. This proposal has been theoretically validated in Chapter 6 and this chapter serves as the proof-of-concept for the same.

Experimental results were published in the following conference publication:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, "OpenFlow as an architecture for e-Node B virtualization," in Proc. of 3rd ICST International Conference on e-Infrastructure and e-Services for Developing Countries (AFRICOMM'11); also published in Springer-Verlag LNICST, 2011, pp: 49-63.

Experimental Results Comparing OpenFlow vs IP vs MPLS Performance: Moving forward, the curiosity to discover the performance of SDN's network management capabilities with the classical mechanisms drew the attention. It therefore became necessary to compare OpenFlow with the existing network management protocols such as MPLS, which has consistently performed satisfactorily in MNOs backhaul networks. Therefore, we carried out experiments and discuss our experimental results to visualize the effect of performance by considering IP, MPLS and OpenFlow based backbone networks to evaluate their effect on the network performance.

These experimental results were invited to be published in:

- Venmani Daniel Philip, Yvon Gourhant and Djamal Zeghlache, " Demystifying Link Congestion in 4G-LTE Backhaul using OpenFlow," in Proc. of 5th IEEE/ IFIP International Conference on New Technologies, Mobility and Security (NTMS'12) 2012.

1.3.4. Part V: Substitution Networks based on Software Defined Networking

This last part of the thesis attempts a small but significant step towards the evaluation of a prototype that focuses on network optimization techniques to improve network survivability by jointly considering factors such as resource utilization efficiency, blocking probability etc.

1.3.4.1. Chapter 10

Implementation of a Novel Bandwidth Management Algorithm: As a first step, we have evaluated our approach based on OpenFlow by a novel algorithm that guarantees the required performance in terms of bandwidth management to satisfy QoS to every user within a network, irrespective of the "chaotic" situation, typically an overloaded network situation. Our method outlines a bandwidth management framework based on OpenFlow. Briefly, when the centralized controller detects the OpenFlow enabled SN, it creates a new path via the SN and re-routes the traffic, thus guaranteeing the QoS to end-users. The key contributions in this chapter can be summarized as below:

- A novel network design proposal demonstrating the adaptability of SDN for substitution network. The attempt is different and completely novel.

- We incorporate SDN to tackle the problem of a centralized control of multiple diverse vendor equipments and thus we adopt OpenFlow to demonstrate the feasibility of our proposed network design.

- Moreover, through this solution, we demonstrate the possibility to adjust the bandwidth on a set of links and switches dynamically according to the traffic needs of individual end-users, which guarantees the required QoS.

The results of this contribution were invited to be published in:

- Venmani Daniel Philip, Yvon Gourhant, Laurent Reynard, Prosper Chemouil and Djamal Zeghlache,, "Substitution Networks based on Software Defined Networking," In Proc. of 4th ICST International Conference on Ad Hoc Networks (AdhocNets'12), Paris, France, September 2012.

1.3.5. Part V: Chapter 11: Research and Deployment challenges and Concluding Discussions of the Dissertation

Here we detail our motivation and objective to carry out this dissertation thesis to answer these questions relating to tackling network traffic surge and backhaul network failures, without over-provisioning. As a conclusion, in this chapter, we briefly summarize the architectures and algorithms that accomplish these goals. As with any scientific work, it has brought up more questions than it has solved, some of which are illustrated in the latter part of this chapter. Before that, in this chapter, however, the contributions of the thesis are glued together to give a better picture of the choice of research conducted.

1.4. Pilot: Can I Share my Unused Resources with my Competitors?

1.4.1. History of the Future: The Internet and the Mobile Internet

"**We will have more Internet, larger number of users, more mobile access, more speed, more things online and more appliances we can control over the Internet**". This is how the celebrated Computer Scientist and Chief Internet Evangelist at Google, Vinton G. Cerf, described the evolution of Internet from his very own vision.

Indeed, the Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is after all, a world-wide broadcasting instrument, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers, without regard for geographic locations. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying this exciting new technology.

With the Internet revolution witnessing its maximum impact into the common man's day-to-day life, it eventually led to a new paradigm of nomadic computing and communications, which enabled users to 'move' from one place to another and stay connected to the Internet- the era of Mobile Communications technology, which subsequently but rapidly led to the era of the Mobile Internet. The mass hysteria that came to be known as 'the mobile phones', and today subtly evolving to be called as 'the Smartphones' in the modern world, has become such an indispensable part of our lives that it has been started to be perceived that life without a smartphone would certainly lead to 'atleast' some sort of disorderliness in our every day lives. Today, terms like "E-mail ID", "Download", "Chatting", etc. even trip lightly off the random person on the street. Having to witness this change, it becomes more than just a business requirement for Mobile Network Operators (MNOs) to provide seamless connectivity together with allowing for fairness for data and broadband services in today's communication world.

1.4.2. Problems of the Present: Apples and Oranges

That being said, advanced mobile broadband networks design require a certain level of sophistication together with a perfect melange of management simplicity for two reasons: (i) to

support the ever increasing network traffic load [2], (ii) as well as to guarantee continuous availability [3]. This is still missing in mobile networks today. Designed to carry voice and 'some' data, legacy mobile networks were designed for predictability and 'one-size-fits-all' services and are not yet exclusively equipped to handle dynamic traffic flows and highly customized quality of service (QoS) requirements of the future. And today it is evolving to permit more sophisticated forms of pricing and cost recovery, sometimes perceived as a painful requirement in this commercial world and without any surprise, in future it will not be cost-efficient anymore to extend the network resources in the same ratio than the traffic demand. The most pressing question for the future of the mobile networks is not how the technology will change, but how the process of change and evolution itself will be managed. Thus, due to the continuous network and service evolution in wireless communications, future wireless ecosystem necessitates for designing cost-efficient network architectures to provide efficient, ubiquitous and always available broadband wireless access to current and future Internet-based applications and to evolve seamlessly into the future "pure" packet network architecture.

1.4.3. The Challenge to Re-design: Quick Glimpse on Fundamentals

The first priority in capturing the broadband opportunity is to provide more capacity and coverage in the access network. Current industry consensus points towards HSPA+ and LTE as the two coexisting radio access technologies to deliver capacities needed to fulfill user expectations. WiMAX will also have its place in the market, as DSL substitution in emerging markets or as niche application in public infrastructure elsewhere. Within this context, today overwhelming majority of traffic generated on mobile broadband is data. This data traffic from the access side is gradually causing congestion at the backhaul side. This gradual transition is the driving force behind key trends in 'Mobile Backhaul transport' evolution. To understand these trends, we provide a very brief technical definition of Mobile Backhaul network itself.

Mobile Backhaul is the transport network that provides connectivity from Radio Access base stations (i.e. cell sites) to their corresponding control and switching elements located deeper in the core of the network. Backhaul network spans from the Cell Site Transport Gateways, 'Last Mile' Domain, Aggregation Domain, through to the Metro Network Domain and ending with the Core Network Transport Gateways. Transport Nodes reside at the border of each of the domains and they provide traffic management capabilities such as switching and performance

2 Here colloquially termed as 'Apples' - a problem caused by the emergence of smartphone devices such as the Apple manufactured iPhone etc.

3 Here colloquially termed as 'Oranges' – an always unresolved problem faced by MNOs such as Orange etc. until today to provide high availability for the customer against transport network failures (e.g. link failure or node failure) by adding redundancy.

monitoring. Backhaul network can use a variety of physical transmission technologies including optical fibre, microwave radio, copper DSL and occasionally satellite. There is more variety of physical transmission in the Last Mile and Aggregation domains with microwave radio having a majority share, whilst the Metro and Core networks predominantly employ high capacity WDM optical transmission.

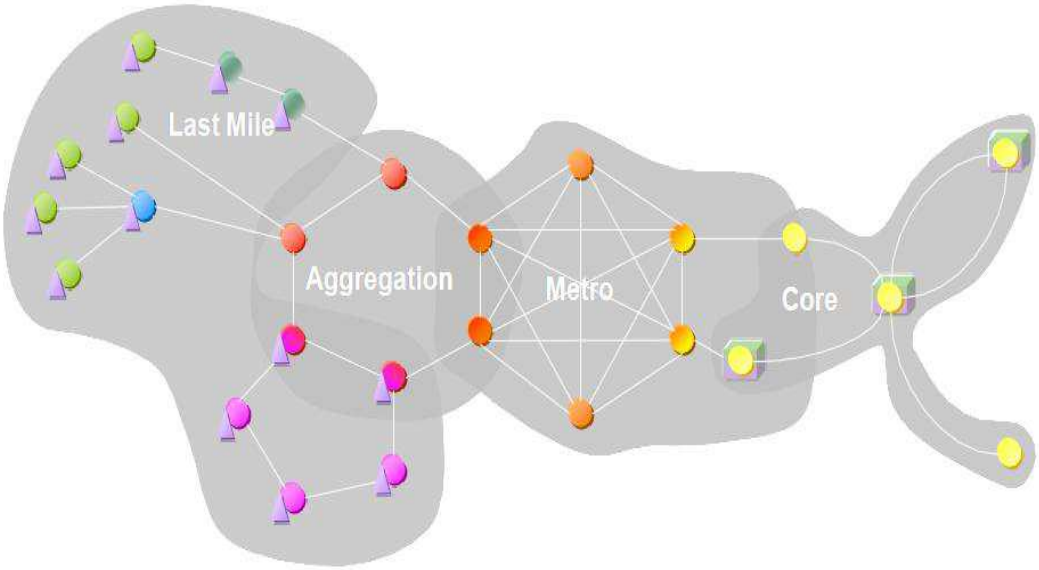


Figure 1: An illustration of mobile backhaul network topology.

Taking this definition of the Mobile Backhaul as the starting point, we define the scope of this dissertation thesis in the following sections.

1.5. Scope of this Dissertation: Problem Definitions

1.5.1. Can I Share my Unused Resources with my Competitors?

Deliberately posing a question 'Can I share my unused resources with my competitors for the sake of protection?' leads to a very different direction. In mobile networks, the role of resilience is increasing, the services, and the capacities that these services use have to be protected to survive failures, e.g., link failures, node failures etc. However, there is always a trade off between the availability to be guaranteed to these services on the one hand and between the costs of guaranteeing this availability on the other hand. This cost consists of two parts. First, the network resources (e.g., link capacities, node capacities) utilized for protection often referred to as CapEx (Capital Expenditure). Second, the complexity of employing these resilience strategies, including steady flooding of routing and state information, their processing, as well as the calculation of optimal working and protection paths. This is often referred to as OpEx

(Operational Expenditure). In practice, Dedicated Protection (1+1 or 1:1) is still the most widespread resilience approach due to its simplicity. However, dedicated protection itself requires always more transmission capacities than the working paths! The reason is, that the working path is always the shortest, while the protection one is the next shortest available, that should typically be disjoint from the working one. When considering the fact, that protection resources are used very rarely and for very short time, using dedicated protection is wasting of resources! Shared protection has the idea that up to one failure at time is assumed, and then working paths, that do not have any common element that can fail can share resources allocated for their protection. This saves a significant amount of transmission capacities. There is only one problem. Namely, before we can take decision on what resources can be shared for protecting a new demand, we have to check for all protection paths, whether their working paths have any common element! If they have, their capacities have to be summed up. This requires not only topology and link state information to be flooded maintained and processed, but also information on all demands, and their working and protection paths has to be maintained. In a single domain operated by a single operator/provider this information can be exchanged, however, in a multi-provider environment there are not yet adequate protocols, neither the scalability allows nor are the operators willing to allow access to their strategic information.

1.5.2. Service Differentiation among Multiple Operators

While considering sharing the existing resources with another MNO, who is in fact a competitor, differentiation is the name of the game. As mobile operators begin to share their existing backhaul resource, the upside of adopting a differentiated mobile broadband strategy is potentially significant. To stand out from the crowd, competing operators will need to offer a widespread, high-quality user experience and a range of differentiated services to attract different subscriber types. This presents competing mobile operators with a challenge and an opportunity, which falls under the following criteria:

- To stand out and attract users with the best possible quality of experience (QoE), delivered from an excellent network with extensive broadband coverage.

- To sell mobile broadband services at price/performance levels that suit all users, devices and services by introducing differentiation.

- To control costs while delivering a QoE that consistently meets or exceeds user expectations.

This means the network operators must be able to deliver the appropriate user Quality of Experience (QoE) with the speed, capacity and constant availability demanded by users, even at

times when they allow another operator to share their unused resources. With properly differentiated mobile broadband services, operators will be able to differentiate themselves with each other in a competing market as well as reach a broader customer base and achieve a more balanced relationship between revenue and resource utilization for individual subscribers. Differentiation can be defined based on a variety of needs, for example, while premium subscribers will want to know that they are getting the best possible data rates at all times, basic subscribers may be happy to accept that they will have limited access to mobile broadband services at certain times of day, at certain locations, or even to specific sites or social communities, or some customers will require high-bandwidth connections with ultra-high reliability, while others will only need best-effort connectivity during the night.

On the other hand, competing operators want to take maximum levels of control over their networks but without jeopardizing the flexibility to dynamically share their resources in order to continue to control network costs. Gaining end-to-end control over the mobile broadband service-delivery pipe will be important in driving the backhaul network sharing strategies. From a technical point of view, the challenge is to gain the required level of intelligence and control over the network resources at every stage – all the way from the servers handling customer care and billing, through the core and radio networks, to end-user devices – to create and deliver differentiated services profitably. Only with such control over the mobile broadband service pipe can operators truly differentiate their service packages and ensure this differentiation is delivered for best use of network resources and best value for users, when considering sharing their resources among themselves.

1.5.3. Network Management as a tool for Service Differentiation between Operators

From our earlier discussions thus far in this dissertation, it becomes inevitable that competing operators should transition their network into a flexible, intelligent resource that can deliver just the right level of differentiation to maintain their competition. These differentiation capabilities strengthen the link between operators' commercial and marketing strategies and objectives and the technical capabilities needed to deliver them. Delivering the required granularity of control over network resources that operators need to create differentiated mobile broadband offerings, demands much more than just excellent devices and network equipments. This involves intelligent, end-to-end traffic management together with the right transport mechanism in avoiding excessive capital expenditure.

While deeply looking into the existing state of the art mechanisms, TDM transport is inherently inefficient in carrying today's data traffic which is overwhelmingly packet data. This is due to

rigid framing structures of E1, ATM and SDH protocols that cannot encapsulate variable data frames without a significant loss of capacity. It is difficult to fit square pegs in round holes and the only long term solution is to employ packet transport based on Ethernet and MPLS.

The migration to packet in the Aggregation and Metro will be different to the one in the Last Mile. Today there are large numbers of ATM and Next-Generation SDH solutions in the Aggregation and Metro networks, originally deployed to support 3G and 2G RAN over the previous decade. By now these networks are beginning to age and are becoming more expensive to run from the perspective of power and footprint efficiency. Also in some cases the capacity is running out and with increasing data traffic on the network incremental upgrades are becoming less and less effective. To reduce the Total Cost of Ownership (TCO) Aggregation and Metro networks need to be gradually refreshed and upgraded to MPLS based transport. There are two technology options available to operators, MPLS-TP and IP/MPLS, and the choice between the two depends on the trade-off between flexibility of IP/MPLS dynamic switching and OAM control and resilience of MPLS-TP. Both technologies bring strong PWE functionality and as such are well suited to support gradual migration from the legacy protocols.

As it provides high level of OAM capability analogous to ATM and SDH, MPLS-TP is the logical choice for the network wide deployment acting as an underlying connectivity protocol. On the other hand IP/MPLS provides more routing intelligence and will be tactically deployed in the selected points in the network to support routing functions of LTE. Another key advantage in the selective use of IP functionality is that it reduces equipment complexity and therefore reduces power and footprint consumption across the network.

1.6. Bringing-in Software Defined Networking (SDN) as a means for Service Differentiation between Multiple Operators

However, both of these technologies (MPLS-TP and IP/MPLS) will need to continue to be proven in the large scale carrier networks before being widely adopted. Nonetheless, the recently emerging Software Defined Networking (SDN) is now beginning to take its peak and in this section, we place our arguments whether OpenFlow will replace MPLS [4]. The key reason towards this comes historically from the fact that ATM replaced Frame Relay (FR), and MPLS then replaced ATM. And although Frame Rely was primarily a WAN technology, ATM and MPLS are also deployable in the LAN. Furthermore, enterprise network design and architectures have remained rigid over the past decade, whereas applications and systems have evolved. Today's

4 A very detailed experimental evaluation has been studied in Part IV of this dissertation.

networks are managed very much on a device-to-device basis, relying on manual intervention. This eventually paves the necessity to adapt to a more flexible network management tool, namely the SDN architecture. With SDN, we can orchestrate network services and automate control of the network according to high-level policies, rather than low-level network device configurations. By eliminating manual device-to-device configuration, network resources can be optimized to lower costs and increase competitiveness. So, the question then becomes: Will SDN replace MPLS at some point in the future?

1.6.1. SDN/OpenFlow & MPLS, Better Together or Mutually Exclusive?

Fundamental to our understanding, today from an operational point of view, MPLS is deemed "too complex", amongst other arguments against MPLS. Becoming "too complex" however, is not the only argument that makes believe OpenFlow will replace MPLS. We briefly present a few more to support our arguments here. At one point in time, ATM solved many problems and had many advanced features. But as the technology matured, was more widely deployed and became more feature rich, it evolved into a very complex technology. About that same timeframe, MPLS was being developed and started to find its pace. It looked simple, it looked "kind of" like ATM in terms of virtual circuits (LSPs in MPLS speak), and it looked like it was starting to gain industry support. Fast forward a decade or so and MPLS is now very widely deployed but as it has matured in terms of features and functionality, it has become more complex. And, ATM is dead. And, hence the necessity to invent something that has similar features like MPLS, but less complex, grew. SDN solutions using OpenFlow, from a high level, can provide some of the basic machinery in terms of forwarding packets as MPLS does (or IP, for that matter). Distributed network routing and signaling protocols ultimately create state to populate the forwarding information base (FIB) of a router or switch, and a centralized SDN application using OpenFlow could also populate the FIB of a router or switch. And for the start, this is our first argument to believe SDN with OpenFlow could indeed replace MPLS. However, we believe the industry is beginning to re-appreciate all that MPLS provides and is re-realizing how widely deployed it is. In other words, today the possibility to integrate the technologies instead of having them compete against each other is strongly considered. Perhaps leveraging the OpenFlow classification abilities at the edge of a network using a centralized application, while maintaining the MPLS-based distributed signaling and forwarding state in the core of the network; or adding an SDN & OpenFlow logical network "overlay" or "slice" to an existing production network for research purposes; or perhaps even to opportunistically override the normal forwarding decisions for specific packet flows in the network in order to "steer" those flows to some sort of analytics device or value-add services appliance. Those are a few examples, but there are many.

The last but not the least, one of the fundamental differences between legacy and SDN is in the move from fixed to non-deterministic bandwidth planning and management. This flexibility of SDN transport allows for a much finer and more flexible differentiation in the Quality of Service (QoS) provisioning on different traffic flows. Therefore there is a requirement for a powerful set of policy-based QoS capabilities to release and monetize the value of differentiated bandwidth services. In a typical scenario, high availability bandwidth will be allocated to voice and signaling traffic, followed by real time services, with other data traffic taking the lowest priority. Adding to this, another key solution that SDN can offer is the capability to deliver network virtualization, which can relieve the demands of virtualization and workload mobility that many networks can not accommodate. As virtual machines are provisioned and migrated, the administrator in a traditional network would have to log into each router or switch and issue a series of commands via command line interface, which is very poor prone and time consuming and this can eliminated by the use of SDN. The table below summarizes the existing network management tools giving a brief comparison over each of them.

Thus, OpenFlow and SDN can clearly add value and additional services into existing networks and therefore, we believe that SDN/OpenFlow and MPLS are "better together" and are not mutually exclusive. In other words, a hybrid network approach seems to be the most feasible and promising option. With this as a very strong base, all of our architectural designs and algorithms in this dissertation have been implemented. That is, no particular algorithm necessitates the need for any of these specific network management tools (MPLS or SDN), instead our architectures and algorithms portrays the feasibility to adopt any of the existing ones.

TABLE I. MPLS-TP, IP/MPLS AND SDN/OPENFLOW COMPARISON

	MPLS-TP	**IP/MPLS**	**SDN/ OpenFlow**
Service Model	P2P, L2VPN (VPLS)	L3VPN (most common), L2VPN	L3VPN, L2VPN
Transport Oriented	Yes	No	Yes
Transport Mechanism	Pseudo-wire (PW) over LSP	IP over MPLS/PW/LSP	OpenFlow Protocol
Data Plane	MPLS	MPLS	Variety of protocols together.
Control Plane	Static (NMS), GMPLS (under proposal).	BGP, RSVP-TE, LDPOSPF-TE.	OpenFlow Protocol
QoS Support	E-LSP/L-LSP	E-LSP/L-LSP	Fine-grained
OAM & NMS	MPLS-TE	MPLS	SNMP
Multicast	H-VPLS, IGMP Proxy/Snooping	IP Multicast	IP Multicast (under proposal).
Synchronization	TDM/SDH, Sync, Ethernet, 1588v2	Application Specific	Application Specific
Security	MPLS-based	MPLS-based	OpenFlow-based

1.7. Overall Final Remarks

Today's traffic data explosion for mobile backhaul presents the view of dramatic changes in transport network architecture over the next decade. These changes are driven by the new ways in which businesses and consumers will use mobile telecommunication networks in the future. The explosion in demand for mobile broadband services represents a major growth opportunity for network operators who will increasingly look for new mobile backhaul solutions to deliver differentiated high quality services at optimal cost. Backhaul is thus, not just a cost problem; it is an integral part of a sophisticated engine delivering new business models and profitability.

Coming back to the question posed in the title of this Chapter: "Can I share my unused resources with my competitors?", the answer is positive and that is all about it in this dissertation. Although the competitors will never want to share their strategic and confidential information needed for sharing their available unused resources with their competitors, based only on aggregated views of the topology and on the advertised free capacities of this aggregated topology we can still perform sharing of resources.

*"We can't solve problems by using the same kind of thinking we used when we created them." – **Albert Einstein, Theoretical Physicist.***

Chapter 2

State of the Art Techniques for Mobile Network Sharing

Sharing an existing network infrastructure has been keenly considered as a potential alternative to reduce Capital Expenditure (CapEx) by Mobile Network Operators (MNOs). From a high level point-of-view, operators offer a variety of reasons for not engaging in sharing deals, often fearing the operational complexity they may bring, the up-front transformation costs, and the potential loss of control over their own destinies. None of these reasons really hold-up under analysis, however, especially given the potential for substantial savings in the cost of operating shared networks and the range of potential governance models that sharing parties can choose from. With this being the focus, we exclusively dedicate this chapter to discuss the pros and cons on the existing network sharing techniques and strategies that would permit two or more mobile network operators to share their infrastructure. With the foremost objective of this dissertation being centered on 'sharing', it makes it thus inevitable to dive into the thorough details of the existing network sharing techniques, thus gradually and subtly laying our foundation towards backhaul networks sharing. The result of the research work here consequently eased our understanding on the opportunities, challenges, and risks that network sharing throw upon operators and subsequently endowed us to reinforce our research objective.

2.1. Introduction to Network Sharing: When Technology and Business must go Hand-in-Hand.

The year 2007 marked the beginning of a new era in the history of mobile communications, when the very first iPhone 2G model was released and went on sale in the United States on June 29 at 6:00 pm local time. Over the subsequent years, this changed everything - the craze and the enthusiasm for a common man [5] to intend to buy his very own smartphone rapidly rose to the top; the way the common man perceived his outlook towards smartphone usage drastically transformed; the intense spark that drove other smartphone manufacturers to vigorously come-up with their own products with much reduced price, sky-rocketed. While the iPhone 2G was a blessing towards the beginning of an unprecedented smartphone usage, the downside of how Mobile Network Operators (MNOs) [6] were impacted as a result of excessive smartphone usage, follows in the preceding sections.

2.1.1. The Context and the Problem

Ever since then, the evolution in access network technologies such as from the second generation mobile communication (2G) to the third generation mobile communication (3G), from the third generation mobile communication (3G) to the fourth generation mobile communication (4G), and today even from the fourth generation mobile communication (4G) to the fifth generation mobile communication (5G), as well as the revolution and rivalry between smartphone devices manufacturers- have been going hand-in-hand. Consequently, mobile data traffic has been increasing at an unprecedented rate well beyond the capacity of today's[7] most prevalent 3G network. This, nevertheless to say, is not a surprise for operators, for they have been cautiously monitoring the disconnection between the average revenue per user (ARPU) and the associated cash costs per user (CCPU). Despite the remarkable volume increase of broadband data over mobile networks, mobile data revenue is falling fast. Researchers from the mobile networking community and the financial sectors forecast that by 2014, an average mobile user will consume 7GB of traffic per month which is 5.4 times more than today's average user consumes per month, and the total mobile data traffic throughout the world will reach about 3.6 Exabyte per month, 39 times increase from 2009 at a compound annual rate of 108% [1]. It is also predicted that about 66% of this traffic is mobile video data [2]. As stated before, the main drive behind this

5 Perhaps, this is an exaggeration while we consider 'common man' considering the entire globe, seven continents; nevertheless the focus here is to insist how iPhone usage altered mobile network traffic atleast within its market scope in industrialized countries.

6 From now onwards, throughput this dissertation, the terms Mobile Network Operators (MNOs) and Operators are used interchangeably.

7 At the time of writing this dissertation, 3G was the most prevalent access network technology based on the lead author's residence in Lannion, France.

explosive growth is the increase in smart mobile devices that offer ubiquitous Internet access and diverse multimedia authoring and playback capabilities.

Adding to this, the 'flat-rate' mobile data tariffs are another typical example where most users are offered the same price points regardless of the value that data access has to them. For more than a decade, MNOs have devised complicated pricing schemes, designed to decrease price transparency and to lure customers on to more profitable plans. The challenge is that these pricing schemes are seldom rooted in increasing value for the customer, and are inflexible by design to avoid exploitation of core Telco services. That again limits the opportunity to grow with the customer as their value of using the services increases. With flat-rates, mobile subscribers are taking full advantage of their smartphones and tablets. The amount of data-traffic transported by 2G and 3G cellular infrastructures is surpassing all expectations and several indicators are showing an extremely strong growth for mobile data-traffic over the coming years (Reference). For the operators, this growth is proving cumbersome to manage. Not to forget to mention that in particular, in urban areas, cellular access networks are showing increasing signs of congestion- at the access network part as well as at the backhaul network part, especially at peak hours.

There are several solutions to this explosive traffic growth problem. The first is to scale the network capacity by building out more cell towers and base stations or upgrading the network to the next generation networks such as LTE (Long Term Evolution) and WiMax (Worldwide Interoperability for Microwave Access), as well as providing low cost solutions such as pico-cell, femto-cell deployments. While the ongoing deployment of LTE and/or WiMax, with a higher radio access capacity, is expected to help avoid congestion at the access network side, this is not a winning strategy, especially under a flat price structure where revenue is independent of data usage. The second is to adopt a usage based price plan which limits heavy data usages. While price restructuring is rather inevitable, pure usage based plans are likely to backfire by singling out a particular sector of user groups, e.g., smartphone user groups, which have the highest potential for future revenue growth.

Starting from the above considerations, in this chapter, we focus on commercial considerations as well as regulatory mandates which appear to be driving the increasing trend for MNOs to adopt a 'new' strategy to tackle the increasing network traffic, here onwards called as 'Network sharing', with 3G providing an added impetus to assess the commercial and regulatory viability. We assessed the following areas that we think as the fundamental questions to be answered while dealing with network sharing:

- Is network sharing increasingly being considered by operators?
- If yes, why network sharing is being considered by operators?

- How network sharing arrangements can be scoped?
- What is the scope of network sharing in emerging countries?
- What are the challenges and risks are in realizing network sharing arrangements?

2.2. Resource Sharing in Mobile Networks

The classical approach adopted by operators to have an exclusive control of their network resources such as spectrum, sites, transmission lines, backhaul infrastructure, core networks, etc. does no longer remain as an option for operators, if they are keen to find solutions to reduce their CapEx and OpEx, as network costs make up a significant part of an operator's cost position—typically accounting for 60% to 80% of CapEx and about 20% of OpEx [3]. That is to say, the traditional model of single ownership of all network layers and elements is beginning to be challenged. With growing competitive intensity among operators and rapid price declines, over the past few years MNOs are facing increased margin pressure and the need to systematically improve their cost position. To address this reality, operators are adopting multiple strategies, with network sharing emerging as a relatively 'new' and more radical mechanism to substantially and sustainably improve network costs.

2.2.1. Scoping the Network-Sharing Solution

The strategic rationale for engaging in infrastructure sharing differs between new entrant and incumbent operators, 2G and 3G networks and mature and developing markets. We typically pursue the following key scoping dimensions to define network sharing:

- **Depth of sharing**. One key issue is how fully infrastructure and equipment will be shared between operators. At the most common and basic level, site co-location is the most limited form of network sharing. As a next step, the sharing of passive infrastructure elements, such as construction works, power generators, or antennas, has been considered as heavy site sharing. The more radical network sharing discussions now include sharing active Telco infrastructure such as cabinets and TRX pooling. Nokia Siemens Networks (NSN), Ericsson, and other equipment vendors are increasingly moving to support such solutions. Network sharing for joint 3G RAN build-out is today more common place and technologically better supported. Early deals such as Telia and Tele 2, Telenor and Three in Sweden, and Vodafone and Optus in Australia are evidence of this trend. Vendors such as NSN and Huawei offer solutions allowing for two-way (and in the future, more than two-way) sharing of RAN equipment, thereby enabling a

single site to be linked to multiple operator core networks.

- **Extent of sharing**. The first network-sharing deals, such as those in Sweden or Australia, focused on sharing the 3G RAN build-out between operators. However, as operators are looking to raise additional cost effects, the newest discussions (in the United Kingdom, for example) go beyond joint 3G build-out and actually consolidate existing 2G RAN legacy networks into one joint network. Nevertheless, operators are now becoming more ambitious and are looking to extend sharing benefits from 3G to legacy 2G RAN networks. This implies consolidating the existing 2G RAN networks of multiple operators into one joint network. Technologically, such solutions are more difficult.

- **Reach of sharing**. As noted earlier, network sharing is often considered first for rural coverage, particularly if coverage requirements demand an economically challenging build-out. Nevertheless, full country-wide sharing is increasingly considered as operators seek more comprehensive sharing models and attempt to avoid the operational complexities of splitting a nationwide RAN network into shared and non-shared parts.

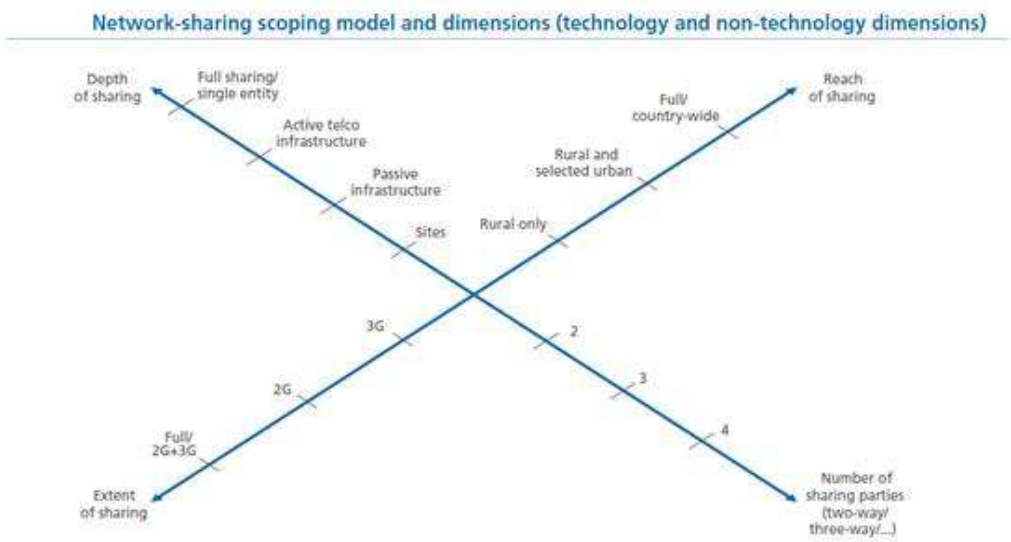


Figure 2: Infrastructure sharing scoping model and dimensions

- **Number of sharing parties**. Currently, two-way sharing between two operators is the standard. Nevertheless, and particularly for 3G build-out, more ambitious models are being considered in some countries. This would potentially bring together all operators in a given country to create a single RAN national network, provided that the technology solution supports such an undertaking.

2.3. Network Sharing - Within the Context of Emerging Countries

While the founding basics and the scope of network sharing have been discussed earlier, we direct our attention towards the scope of network sharing in emerging markets. The key motivation here is that the exhilaration of the smartphone growth, today, is starting to pave way to the biggest opportunity for MNOs - to connect the next five billion smartphone users to the Internet. The rapid growth of smartphones around the globe which took the wireless market by storm, exceeding the 'one billion mark' back in October 2012, lead to the saturation of the US and western European markets. As markets become more saturated, competition between operators expands from winning user share to winning revenue share. Therefore, Internet Service Providers (ISPs) and MNOs from the developed economies are looking for growth outside their native markets and are targeting emerging markets where the remaining five billion users are still to connect to the Internet. Having said this, we discuss the most important challenges in connecting the next five billion smartphone users to the Internet, which are primarily the business models and the regulatory frameworks that are in dire need of innovation.

2.3.1. Compensating the Network Quality

The mobile telecoms industry in Africa has burgeoned in recent years, but slowing revenue growth, increasing costs and shareholders demanding returns are forcing operators to consider the next wave of investment. In this section, we examine the idiosyncrasies of emerging markets and the business model innovations that are needed to close the smartphone gap. With this defining the scope, focusing towards emerging countries where rapid deployment of new generation mobile communications systems is currently beginning to take its peak, enhancing reach through the creation of low cost infrastructure is the need of the hour. To maintain competition and stay unbeaten in the global market, operators need to push out to rural and remote areas. Africa as a whole is characterized by a very low penetration rate of fixed networks (e.g. only 0.7% in Senegal, 3% in Cameroon). By contrast, a significant and rising part of the population owns a mobile phone and mobile penetration has grown dramatically in Africa during the past 5 years, from 29% to 69%. [4]. The rurality of the population as well as its insolvency acts as a brake upon prospective deployment of fixed infrastructures, taking into account the huge investments necessary to install wired solutions.

While satellite-based access solutions (VSAT) are too expensive to be deployed widely, a growing set of alternative technologies have emerged that raise hope for ambitious broadband access roll-outs through contained CapEx. In particular, in emerging countries such as the sub-Saharan

African countries like Kenya, Uganda, Nigeria as well as the Eastern European countries, it is undesirable for each operator, to replicate expensive telecom infrastructure to reach the subscribers in remote rural areas, even if they were able to afford it. According to GSMA Intelligence, 358 million people on the continent are now connected. This growth has been driven by the issue of new licenses: the average number of GSM licenses in African countries is currently 3.8, and at least 13 countries have four or more GSM operators (Figure 3).

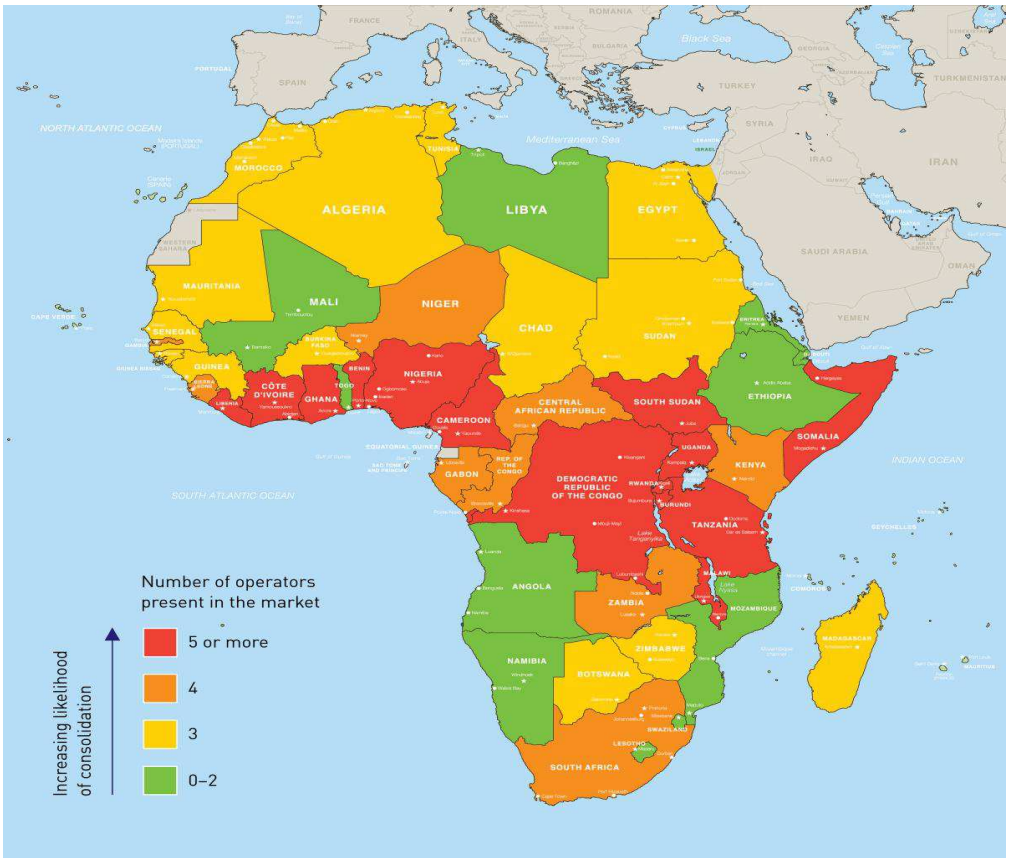


Figure 3: Number of mobile operators present by country, Africa [Source: Analysis Mason, 2013], Countries colored red, orange and yellow all face intense competition.

Another dimension to take into account while considering network sharing solutions for emerging countries is, the often poor network quality. This is a consequence of the need to build low-cost networks that must remain profitable with the bottom-of-the-pyramid segments. In addition, there are other infrastructure challenges, like power outages, inefficient frequency and spectrum allocations. This network quality challenge is fundamental, and does not magically go away by adding 3G or 4G. As network capacity increases and usage grows, the gap between peak hour and off peak traffic increases. As such, the cost structure of running a mobile network is very much related to peak capacity, implying that there is a lot of capital that is not working outside of peak. This calls for operators to start thinking better in terms of optimization as well as yield management. Combined with need to use discounts smarter, growing ARPU and developing customer profitability, more dynamic pricing and capacity utilization strategies are needed.

Nonetheless, just like in the industrialized economies, the CapEx for this is beyond imagination and are simply not addressable through the revenues currently generated. Adding to this, the population distribution patterns in emerging countries complicate the situation since access to telecom services varies significantly between urban and rural areas leaving operators in these countries to balance the cost of operations in congested and saturated urban setups with the costs of new network rollouts in other areas. This results in declining ARPU and leaves operators with lesser amount of re-investible funds for expansion of service, which otherwise could have been far more widespread by now.

2.3.2. What can Africa learn from Developed Economies of Network Sharing Experience?

- **Sharing deals can be struck and successfully executed, so executives do not need to be afraid of them.** Large groups, such as Vodafone and Orange, have been involved both in active sharing and in Africa, so these companies will lead the way in understanding the benefits and the processes.

- **The most proactive operator often gets the best deal.** When a network sharing deal between two operators has been struck, then the remaining operators in that country are obliged to respond. An operator that actively engages with its best partner and is first in securing a deal, develops a real competitive advantage.

- **Regulators and competition authorities need to be cognizant of the value of active network sharing.** Mergers and acquisitions can deliver greater benefits to the operators, but the competitive impact on the market should not be ignored. Regulators should be aware of the different network sharing models, the impact on spectrum and how a transaction can best be used to improve the overall market – a particularly relevant point, given that the current regulatory model of issuing new licenses to increase competition will not work in maturing markets.

Consolidation in Africa will happen – it is just a matter of timing. Proactive operators can drive that consolidation through mergers and acquisitions and network sharing, and by matching strategies with market position and regulatory approval. Sitting back and waiting for the returns to roll in is no longer an option. Only proactive business leaders will be winners in the now inevitable network consolidation across Africa. Having said this, it is thus worth noting that commercial considerations rather than regulatory mandates, appear to be driving the increasing trend for MNOs to adopt a variety of infrastructure models.

2.4. Fundamental Limits and Regulatory Framework

Promoting network sharing has been gaining attention among the telecom regulators and policy makers to encourage mobile network deployment and coverage improvement in the un-served less populated areas, be it in developed countries or emerging economies. A fundamental objective of resource sharing is to find a stable operating point based on certain fairness and efficiency criteria [5]. Many well-known concepts, like proportional fairness [6] and bargaining theory [7], were derived in a context other than wireless communication. The used utility models do not typically explicitly model resource or infrastructure sharing [8]. The concept of collaborative networks is gaining momentum and it is also closely related to the idea of infrastructure sharing [9]. From the past researches, infrastructure sharing solutions have proven to be a critical lever contributing to the growth of the telecommunication sector and are very promising in emerging countries where the market is growing fast. In this context, there are a wide variety of technological approaches that appear from today's perspective, considering current technologies have already reached its maturity state and there have been a number of best practices that have been identified in order to promote passive and active mobile infrastructure sharing [10].

2.4.1. Regulatory Interests in Infrastructure Sharing

Regulatory interest in infrastructure sharing is three-fold; it has efficiency, competition and environmental aspects. Before granting approval to infrastructure sharing, national regulatory authorities (NRAs) typically weigh up the positive efficiency and consumer gains against the possible competitive harm and assess whether the gains have been incurred in the lowest cost manner. The following are the positive outcomes which include:

- Optimization of scarce resources and positive environmental impacts;
- Decrease in duplication of investment, thereby reducing CapEx and OpEx;
- Positive incentives to roll out into underserved areas;
- Improved quality of service, particularly in congested areas;
- Product and technological innovation as operators compete on service differentiation;
- Increased consumer choice as entry and expansion become easier; and
- Reductions in wholesale and retail prices for mobile services.

These positive outcomes are weighed against any competition concerns arising from a decrease in network competition or refusal to provide access. Thus regulators must distinguish cases where dominant operators act to hinder competition from situations where they act so as to meet

competition, recognizing that the latter is necessary for the existence of a healthy competitive market. Regulatory measures aiming to foster competition in the short term may harm it in the longer term. For example, imposing shared access mandates on an incumbent's facilities will tend to increase competition in the short term but decrease long-term incentives for network rollout and the likelihood of two or more viable competing networks in the long term. We summarize on the following initial analysis into regulatory approaches:

• Infrastructure sharing is usually commercially driven rather than mandated by regulators;

• Regulatory approval is almost always given for passive infrastructure sharing and in many cases regulators encourage MNOs to enter into commercial agreements. Acknowledgement is given to the environmental and efficiency benefits of sharing and the generally limited competition impact. In some cases, it has been noted that site sharing could increase competition by allowing operators access to key sites necessary to compete on quality of service and coverage;

• In most cases regulatory approval is also given to RAN sharing as MNOs maintain separate logical networks so the impact on network competition is assessed to be neutral;

• Proposals for active network sharing such as core network sharing or national roaming may require more market specific, competition analysis than passive sharing and RAN sharing;

• Competition rules apply to national roaming agreements. Regulators tend to permit national roaming where networks are either in their early stages of roll-out or in rural or peripheral geographic areas. Increasingly regulatory authorities, including the EU Commission, are stating that the competitive harm initially associated with national roaming may be lower than first envisaged and therefore a greater number of national roaming agreements are being permitted; and our analysis suggests that there has been an increase in the number of commercially driven infrastructure sharing agreements between operators.

This can be attributed to a number of drivers, although we narrow-down to the following three key factors are:

(i) 3G/4G licensing, and the associated need to new entrants to quickly establish national coverage and for new site acquisition by all operators;
(ii) Downward pressure on ARPU leading operators to seek cost savings; and
(iii) Congestion in urban areas alongside a lack of new sites.

Regulators usually take a competition-based approach to assessing requests for sharing approval, based upon an analysis of efficiencies versus competitive harm and considering national market

conditions. For the most part, this has led to passive infrastructure sharing and RAN sharing being approved and often actively encouraged and, increasingly, for more active forms of sharing to be allowed, subject to roll-out obligations.

2.4.2. Impact on Competition

Regulators face the challenging task of correctly distinguishing cases where dominant operators act to harm competition from situations where non-dominant operators act so as to meet competition. Whereas the former may provide grounds for intervention, the latter is necessary for the existence of a healthy competitive market. These competitive assessments are usually undertaken on the basis of national competition laws and typically assess whether: (i) the efficiency gains outweigh any competitive harm; and (ii) whether the same level of efficiency can be achieved in a less harmful manner. This task is complicated by the consideration of the relevant time horizon. In the short term, regulatory measures aiming to foster competition may harm competition in the longer term. For example, imposing regulatory mandates for shared access to an incumbent's assets and facilities will tend to increase competition in the short term. However, it will reduce competition in the long term as it decreases incentives for network roll-out hence decreasing the likelihood of two or more competing networks viable in the long term and this is particularly true when operators have to upgrade their network (e.g. 3G to 4G). When considering this issue, it is important that regulators consider both retail and wholesale mobile markets since where there is effective end-to-end competition in retail markets it is usually not necessary to regulate wholesale markets.

Infrastructure sharing can be a business strategy allowing firms to lower costs and prices to consumers, and to increase competition by facilitating speedy network roll-out for new entrants [10]. Refusal to share infrastructure or excessive charging for infrastructure facilities may, if pursued by a dominant provider, affect competition adversely. From a regulatory point of view it is relevant to distinguish between the following forms of sharing. They are (i) Site and mast sharing (passive sharing), (ii) RAN sharing, (iii) Core network sharing, (iv) National roaming.

In the following, the potential competitive impact of each of these is considered separately.

- **Site and mast sharing.** Site sharing (co-location) and mast sharing is normally considered not to materially affect competition since operators retain control over their own networks. In the context of the European Framework for Communications Services, site sharing has always been encouraged (never mandated), although not as a means to increase competition but for efficiency and environmental reasons, as outlined above. Where cost savings are achieved then these may be passed on to consumers in the form

of lower prices. In many situations operators may be expected to draw up agreements for site sharing on a commercial and voluntary basis. However, there may be reasons why operators may not wish to share infrastructure. Incumbents with a large, costly network may not want to share their assets thereby creating a temporary barrier to entry. Whilst this needs to be traded-off against incentives to build a viable second or third network in the long-term, where such sharing is refused in particular in rural or peripheral areas the effect may be to reduce competition. However, this is more relevant to national roaming and is therefore discussed further below. Cyprus is the only example where it has been suggested that the lack of availability of passive infrastructure, and in particular sites and masts has held up or slowed entry and progress of the second mobile competitor. This has been exacerbated by the fact that the legal framework for the erection of masts and sites was unclear, planning permission hard to obtain, and the fact that both entrant and the incumbent faced a situation where many masts and sites were built illegally due to the slow planning process. Regulators could conclude, in such situations, that mandating access to sites and masts may ease network roll-out and increase the degree of competition between entrant and incumbent. However mandating passive infrastructure sharing may not necessarily be the most effective remedy for nurturing competition.

Furthermore, it may be less costly in terms of investment incentives to streamline planning laws rather than imposing onerous conditions on existing operators which may be difficult and costly to implement. Implementation of site and mast sharing appears to be a challenging task where property rights of existing masts and sites are unresolved. This may in some countries be exacerbated where the legal framework is not sufficiently robust to allow firms to have confidence in the enforceability of contracts and agreements signed between them and where there is a general lack of confidence in the court system more generally.

The regulator may be able to provide encouragement and incentives for commercial sharing agreements to occur absent of regulatory mandate. This could include simplified planning processes for shared sites or potential tax breaks. A market-based solution to infrastructure sharing may better reflect changing market conditions and lead to greater flexibility for both the party requesting and the party providing access.

- **RAN sharing:** RAN sharing has generally been considered as competitively neutral in Europe and in the US so far with regulators. Agreements have, for example been put in place in Spain, and are also considered in the UK between T-Mobile and Hutchison and in Italy between Wind and Hutchison.

- **Core network sharing:** Core network sharing is in its infancy and although commercial proposals have been discussed, there are limited examples of this occurring in practice. Whilst such agreements may lead to greater efficiency, principally through economies of scale effects, regulators may be concerned about the impact of decreasing wholesale competition. However, provided that the retail mobile market remains competitive then there may be limited opportunities for vertically integrated MNOs to leverage any increase in wholesale market power into the retail market. Therefore the competitive harm to consumers may be minimal compared to the efficiency gains. However, any robust conclusion could only be drawn following a review of the proposed sharing deal and with reference to the particular market conditions.

- **National roaming:** National roaming has in the past been more controversial than the other forms of sharing considered above, although there is an established regulatory view today that is also widely accepted amongst operators. Generally, national roaming is accepted and sometimes encouraged, where (i) A new entrant needs to build out his network quickly, (ii) Demand and ARPU are estimated to remain too low to justify the roll-out of a second or third network, such as in rural or peripheral areas.

In Europe, two competition cases during the early phases of network roll-out helped establish the principles that underpin the current regulatory views on the potential impact of roaming on competition. In 2006 in O2, Commission the Commission argued that national roaming, by definition, restricts mobile network-based competition with respect to the scope and speed of coverage, retail prices, network quality and transmission rates. The European Commission agreed to exempt national roaming from competition law temporarily in urban areas for a short start-up period until O2 had set up its own network. However it envisaged that this exemption would be phased out across specific cities and regions covering about 50% of the population by the end of 2008. The European Commission also intended that roaming in rural areas should have been phased out by the end of 2008. The European Court of First Instance (CFI) annulled the European Commission's decision holding that the Commission had not presented sufficient evidence regarding the effect of the national roaming agreement on competition, and the Commission decision's claim that national roaming per se qualifies as an agreement between competitors restricting competition (Article 81(1)). The CFI also noted that roaming may benefit competition in that it may allow the smallest competitors to compete on a more equal basis with major players.

However, generally it is agreed that there is a trade-off between national roaming and long-term competition between networks, in particular where roaming occurs in urban areas or more generally regions where the market can take more than one or two players each with their own

networks. As noted above, roaming differs from RAN sharing in that one operator actually uses another operator's network, implying that the two are not competing in the operation and build of network infrastructure.

2.4.3. Existing Standardizations on Network Sharing

As per [11], there are two architectures for network sharing that have been standardized. Hence, according to it, a network sharing architecture shall allow different core network operators to connect to a shared radio access network. The operators do not only share the radio network elements, but may also share the radio resources themselves. As a result of this, the Multi-Operator Core Network (MOCN) configuration, in which multiple Core Networks (CN) nodes, operated by different operators, is connected to the RAN is only shared, in other words the e-Node B is only shared by the operators. Another sharing configuration called the Gateway Core Network (GWCN) in which Mobility Management Entity (MME) is shared in addition to the RAN. Less equipments (e-Node B and MME) are shared in LTE when compared to the former 3G-UMTS (Node B, Radio Network Controller (RNC), Mobile Switching Centre (MSC), Serving GPRS Support Node (SGSN)) in this case. In addition to the above two described network sharing scenarios of [11], there are also few other scenarios that are proposed in the [12]. They are Multiple Core Networks Sharing common radio access network as per the 3GPP Release 99 architectural standards, Geographically Split Networks Sharing, Common Network Sharing, Common Spectrum Network sharing, Multiple Radio Access Networks sharing common core network. Again in [11], exclusive details of Network sharing for UMTS Terrestrial Radio Access Network (UMTS) and E-UTRAN are covered. According to [13], E-UTRAN shall support for multi relationship E-UTRAN nodes and Evolved Packet Core (EPC) nodes by the establishment of S1-flex. However, the above mentioned network sharing standardizations deal only with RAN sharing, gives a very little insight on core network sharing but does not give any specification for backhaul infrastructure sharing while in addition to the RAN sharing, operators may also decide to share the backhaul in some models (e.g. Geographical Split model) with and without access network sharing.

2.5. Risks Involved in Resource Sharing

Recalling from the introduction on network sharing, i.e. the ability to share portions and/or components of mobile networks with competitors allows sharing operators to reduce their CapEx spending, as active and passive infrastructure elements are jointly utilized, and it enables them to cut OpEx as the underlying operations are performed together. Given the specific depth and reach of the sharing solution, about one-third of all 3G network costs and one-fourth of all 2G network costs can be reduced (Figure 2). However, with a high degree of shared resources

using today's technologies, the stimulation for competition is gradually reducing and nevertheless to say, network sharing also carries key risks and issues that must be anticipated:

- **Deal closure.** Ultimately, every network sharing deal requires significant alignment and commitment between operators that typically compete. The clearer each negotiating operator is about the desired network sharing arrangement, the more likely the negotiations will be successful. Network sharing discussions often fail, even at advanced stages, because the operators have not sufficiently thought through their own positions.

- **Alignment on network quality and service levels**. Sharing a network significantly reduces the opportunity to compete on the basis of network quality or coverage.

- **Speed to market with new services**. Innovative new services (e.g., requiring new RAN software releases and features) will usually require joint agreement on network configurations between the sharing operators.

- **Ability to "market" network capacity**. Network sharing is based on the more efficient utilization of network infrastructure and capacity. Consequently, it does reduce the ability to independently fill capacity through abundance pricing (large bundles, flat-rates) or wholesale (MVNO, reseller) arrangements.

- **Alignment on technology evolution and priorities**. Network sharing will largely force operators to agree to a common network evolution strategy and migration plan, and it could limit the ability to sustain legacy services. In addition, it reinforces the dependency to network vendors; operators do not like that.

- **Alignment on operational priorities and targets**. Sharing network operations and maintenance staff does require alignment on operational priorities like network simplification strategy and operational targets (e.g., mean time to repair).

- **Threat of being left behind**. Network sharing can create a sort of *prisoner's dilemma* [8] in the marketplace. When it becomes apparent that multiple operators are seriously considering entering into network-sharing arrangements, this places significant pressure on the remaining operators to push into such discussions as well. Otherwise, they risk being isolated in the marketplace while being hampered by a disadvantageous cost position.

8 The prisoner's dilemma is a canonical example of a game analyzed in game theory that shows why two individuals might not cooperate, even if it appears that it is in their best interests to do so.

2.6. Wireless Network Virtualization

The ability to enable the existence of multiple virtual networks on a common infrastructure even with different network architectures has been gaining critical importance in recent years. An aim of our ongoing research is to take pragmatic approach towards applying operator differentiation and provide a solution to improve traffic prioritization primarily for 4G-LTE mobile networks among operators by setting up a network composed of individual virtualized network components such as nodes, routers. Hence, in this section, we explore the various virtualization opportunities currently existing in today's networks.

Virtualization of any infrastructure, be it a simple computer or a router in the internet, gives the ability to operators for managing their virtual networks, independent of other coexisting virtual networks. Within the context of network virtualization, the cellular architecture can be seen as a huge physical infrastructure hosting multiple virtual networks owned by different mobile network operators, thus enabling each operator to dynamically adjust in switching resources and set to a geographic location. It has already a published result that different operators might manage different virtual networks, all hosted on the Internet, but sharing the same physical infrastructure [14]. Besides imparting savings in equipment costs by not having the need to invest, deploy and by splitting the network into isolated virtual networks introduces flexibility in hosting easily configurable virtual networks on a common infrastructure that can be optimized independently by operators to maximize network utility. From another perspective, the brighter side for the users is that they have the liberty to connect to one or more virtual networks depending on which utility they would like to maximize. Besides, being able to offer various services to the customers, by such techniques, the network itself would become a service. Resources needed by such a virtual network can be allocated in an always-available manner or dynamically, as and when/where needed. Network virtualization will allow operators to share the same physical infrastructure and have networks coexisting in a flexible, dynamic manner utilizing the available resources more efficiently. This implies that the physical infrastructure needs to be virtualized into a number of virtual resources being offered to the different virtual networks. While virtualization for servers, routers and wire line links in the internet architecture has already been extensively studied in the literature [15-19], the wireless part has not yet received major consideration within today's research. This involves applying the current operating system virtualization experience for network components, leading to virtual network resources like virtual routers, virtual links, and virtual base stations. Two forms of virtualized networks are widely used today: Virtual Local Area Networks (VLANs) and Virtual Private Networks (VPNs). In enterprise and data center networks, virtual local area network (VLAN) technology is commonplace and continues to evolve. VLANs like IEEE 802.1Q [vla03] operate mainly on the link layer, subdividing a switched Local Area Network (LAN) into several distinct

groups either by assigning the different ports of a switch to different VLANs or by tagging link layer frames with VLAN identifiers and then routing accordingly. VPNs like IPSec, on the other hand, establish a network layer tunnel to either connect two networks (site-to-site), one network and a host (site-to-end) or two hosts (end-to-end) with an encrypted and/or authenticated channel over the Internet. Such virtualization approaches are focusing on the virtualization of links whereas the approach described in this paper deals with the virtualization of a whole network infrastructure. In backbone networks, virtualization in the form of different protocol families utilizing a single multiprotocol label switching (MPLS) core network, virtual private networks (both layer-2 and layer-3) and tunneling technologies (e.g., IPSec) are widely used and allow some degree of sharing of common physical infrastructures. A number of research initiatives and projects all over the globe have started focusing on Network Virtualization, e.g. GENI [20] [21], PLANETLAB [22], VINI [23], CABO [24], Cabernet [25] in the United States; 4WARD [26] [27] in Europe, AKARI [28], AsiaFI [29] in Asia and many others. This shows that the current direction in designing the Future Internet is going in favor of having multiple coexisting architectures, instead of only one, where each architecture is designed and customized to fit and satisfy a specific type of network requirements rather than trying to come up with one global architecture that fits all. That is why Network Virtualization will play a vital role as it helps diversifying the Future Internet into separate Virtual Networks (VNets) that are isolated and can run different architectures within.

2.7. Concluding Remarks and Discussions on State of the Art Techniques in Mobile Network Sharing

As the mobile communications sector continues its relentless expansion with more subscribers and more advanced services generating ever-greater volumes of traffic, it turn-out to be invariably appearing for operators to invest more in their infrastructure to meet the end-user demand. Network congestion or mobbing and traffic overloading is resource-sharing problem, which will upswing whenever resources are not enough to meet users demands. From our analysis, it goes without saying that infrastructure sharing provides the alternative solution for network operators to radically and substantially improve their competitive cost position. Network sharing that comes in several flavors reduces the investment requirements of operators and in many cases the speed with which they can deploy new technologies, while forcing them to rethink and adjust the basis on which they try to achieve and sustain competitive advantage. Certain mobile industry leaders even believe that network sharing will become indispensable for future competitiveness. Though up-front infrastructure transformation costs can be high, they can be paid for by future savings or mitigated through emerging alternative financing arrangements. The more recent trend to active network sharing provides growing opportunities to vendors to secure network management outsourcing contracts as well as to develop

equipment designed for sharing deployments. Most important, operators should act quickly to make network sharing arrangements. The early movers will be in a position to shape deals with partners of their choice, giving them a distinct cost advantage in their markets. And operators that have plans to implement long-term evolution (LTE) networks soon will find that these deployments can benefit significantly from well-planned network-sharing deals. At the same time on the regulatory side network sharing raises concerns that larger operators may form sharing arrangements that exclude their smaller brethren, and are therefore being used arguably as a form of anti-competitive discrimination.

Focalization on emerging markets, ISPs and MNOs are both important pieces in connecting the next 5 billion smartphone customers. The key takeaway here is that the business model innovation for devices, networks and services, is still is in its early infancy. There is a huge need to remove friction, increase flexibility, and become more analytics-driven in pricing and distribution. Pricing of not just mobile tariffs, but also retailing of network connectivity will be a key element in this development going forward. Operators who understand the barriers to use of mobile services in emerging countries are not only well positioned for future growth, but more importantly positioned to shape user behavior for the future. At the same time, they have still not found a lean way of co-producing the right customer experience for these users.

In western markets, the global, scale-centric Internet model and the legacy local Telco model exist side by side. The business model of almost unlimited data subscriptions avoids the friction between service providers and Telcos. Emerging market characteristics challenge this model, increasing the friction, and force the Internet service companies into more integrated business models with Telco's. The theory goes that a future investor would be wise to set up network sharing agreements – indeed if such an investor came from Europe or the Indian sub-continent, it could point to a number of successful arrangements. However, something that any investor would need to remember is that whilst network sharing would help an operator bring down costs, in Africa, structural costs would still remain high, due to power shortage and poor infrastructure. Furthermore, would existing operators really want to share their infrastructure with a new competitor?

Questions about loss of network competitiveness, ownership of assets, and regulatory directives all need to be addressed if the potential benefits of network sharing are to be realized while its potential pitfalls are sidestepped or their consequences mitigated. It would be ironic if in a "back to the future scenario" it turned out in the long run (although such a conclusion is premature today) that RANs were a natural monopoly that should be regulated like an old-fashioned utility. This scenario could be implemented with a neutral host or exchange operation positioned to unite, consolidate, and manage the networks of all operators. Of course this scenario would also

not lack its own problems or reasons for criticism. They are the same ones that stimulated the widespread liberalization of telecommunications markets in the 1980s and 1990s and the rejection of utility-like regulation, namely concerns about impediments to innovation and sluggishness in deploying new and improved transport technologies.

And finally, one important open question: How big of an impact will the smartphone growth in BRIC countries and emerging countries like the Sub-Saharan African countries – and the resulting behavioral changes in consumers – have on global innovation. The lack of market understanding and unwillingness of certain operators to give away any competitive advantage, might question about how willing are operators to embrace the future opportunities rather than trying to preserve their legacy business models. Either way, given the promise of cost savings, network sharing is sure to be seriously considered and implemented by more and more operators around the world. Nevertheless, given the significant risk and sheer complexity of network sharing, operators should not embark on this journey lightly. Operators should understand the full impact network sharing has on their figures, operations, and organization. Anticipating these unique challenges will be central to ensuring deal closure and realizing the significant bottom-line benefits network sharing can provide.

2.8. Summary of our Findings

Whilst technically it could be possible for operators to share any amount of equipment, implementation can be complex for some forms of sharing. This is particularly true where existing networks are being joined together as opposed to the rolling out of a new, single network. Considerations that must be addressed include the load-bearing capacity of towers, space within sites, tilt and height of the antenna and adverse effects on quality of service (QoS) when antennas are combined and differing standards employed by the equipment vendor. Therefore, infrastructure sharing takes different forms due to their relative technical and commercial diversity among different players.

- **MNOs in mature markets**. Infrastructure sharing may reduce operating costs and provide additional capacity in congested areas where space for sites and towers is limited. It may also provide an additional source of revenue but may be limited by differing strategic objectives.

- **MNOs in developing markets**. Infrastructure sharing may expand coverage into previously un-served geographic areas. This is facilitated via national roaming or by reducing subscriber acquisition costs (SACs) by sharing sites and masts or the radio access network (RAN).

- **Congested urban centers**. Infrastructure sharing is also increasingly being used in congested urban centers where new site acquisition is difficult. However, it may be less likely to occur in markets where coverage is used as a service differentiator and, if mandated, could potentially reduce investment incentives for continued network roll-out.

- **3G/4G network operators**. Operators are taking the opportunity to reduce CapEx and OpEx by sharing infrastructure from the start of the build-out. This is technically more attractive than joining existing 2G networks since operators, in many markets, are seeking to use 3G to differentiate their products and services, rather than networks. Sharing a new network removes the complexity and cost associated with re-planning existing networks but requires commercial agreement on operations and upgrade costs.

- **New entrants**. National roaming can be used for a limited fixed period, usually the first few years of network deployment, to quickly expand coverage and in instances where initial cash flows are limited.

- **Third party infrastructure providers**. Infrastructure funds are showing more interest in acquiring or establishing third party mast or radio network businesses.

- **Network equipment manufacturers**. Infrastructure sharing may reduce revenues as less equipment is required by operators. However by assisting in the network planning process and offering managed network services, equipment manufacturers may be able to differentiate their offerings.

Part II

Theory and Modeling

*"As far as the laws of mathematics refer to reality, they are not certain, and as far as they are certain, they do not refer to reality." – **Albert Einstein, Theoretical Physicist.***

Chapter 3

Reliability and Availability Analysis of a Novel Shared Backhaul Architecture

Reliability and Availability are two most commonly used terms to evaluate the lifetime of a system. In simple words, reliability is a measure of how long the item performs its intended function while availability is a measure of the percentage of time the equipment is in an operable state. Reliability is a measure of the probability that a system or a unit will perform its intended function for a specified interval under stated conditions while Availability could be defined as the probability that a system or a unit will be in an operable state at a random time. Analyses based on reliability and availability predictions will help assess design options and can lead to definition of maintenance support concepts that will increase future system performance, anticipate logistics and maintenance resource needs, and provide long term savings in operations and maintenance costs based on optimization of logistics support. With this motivation, the first part of this chapter unfolds a simple 2-path parallel system analytical reliability function to demonstrate the reliability for our proposed architectural design based on Markov Chain model. With the reliability analysis in-hand, we go further and provide a very different analysis to illustrate the availability gain of the newly proposed architectural design based on the Multi-State System (MSS) approach using Discrete-state Continuous-time Markov chain model. This is covered in the latter part of this chapter. Our results show that such a jointly- constructed network was available to meet the required demand of the total system more than 99.8 % of the time.

3.1. Motivation towards this Shared Design

One of the most important requirements of a carrier-class transport service is its high availability for the customer. Since networks are repairable systems from the view-point of reliability, the measure "unavailability" has been used in resilience design. Any failure that occurs in a transport network (e.g. link failure or node failure) decreases the total availability of that network. Therefore it is crucial to integrate redundancy and resilience in the network design in order to provide the network with an ability to recover itself from potential failures. A considerable proportion of substantial investments towards this provisioning resilience are dedicated to the backhaul segment alone. Converging towards this concept of resilience, our focus centered on modeling and analysing the reliability and availability of the backhaul infrastructure of the mobile network architecture, in this chapter. Therefore within this context, focusing towards the wireless backhaul of MNOs, we summarize the following problems:

Problem 1: How to avoid link failures that are inevitable at the “last-mile” of the backhaul since there is no enough redundancy?

Problem 2: How to improve the availability of backhaul architecture of MNOs without redundancy?

Problem 3: How to avoid the backhaul bottlenecks that are due to the high bandwidth demands and/or link failures?

In recent years, considerable attention has been given by research community to the design of resilient networks and technologies [30]-[32]. A variety of measures for network reliability and availability has been proposed [33], [34]. These may be classified broadly into three categories: network survivability, network vulnerability, and network availability. The former two measures are limited to the concept of graph theory, but have penetrated into telecommunication systems. The third one not only concerns the various failure modes of network elements, but also the degraded performance of a network due to faults in network elements. Taking this premise as our starting point, in this chapter we model our novel concept of infrastructure sharing considering sharing the backhaul networks with another operator under link failure conditions. Here we deal with a network design in which resource sharing is extended to the next level where multiple network operators share their own backhaul resources for increasing their network reliability as well as reducing their network unavailability time. This new concept that we have termed as Resiliency, Reliability, Redundancy by Infrastructure Sharing (3RIS) investigates the effects of high-reliability link sharing among primary and backup paths of different MNOs. Our work applies 1+N (N≥2) protection scheme to satisfy ultra-high availability requirements.

3.1.1. Organization of Part I

This chapter is divided into two parts. The first part of this chapter deals with Reliability analysis and is structured as follows. Section 3.2 elaborates our motivation to carry out research within this area with a very brief state of the art in existing resilience mechanisms. We proceed further to demonstrate how the existing fault tolerant solutions in real networks based on over-provisioning are not very cost-effective and are still prone to failures, with solid numerical values. With the results of the cost–based evaluation in section 3.3, we evaluate our proposed solution by an analytical model where we have demonstrated with an architectural model for infrastructure sharing which concludes the first part of this chapter.

3.2. 3RIS for 4G: A Novel Design and its Reliability Analysis: Part I

Approaches to evaluate a system's reliability (and therefore the availability) can be broadly categorised as measurement-based and model-based approach. Our results in this chapter are evaluated based on both of them. In the first part of the chapter, statistical analysis (measurement-based) of the costs that are associated with the microwave backhaul solution for real Orange 3G networks, especially for the last mile and middle mile, are evaluated and presented. Through these results, we illustrate the impact of enormous CapEx and OpEx that MNOs invest for improving the availability on their backhaul networks. Following the measurement-based results, we proceed further with the model-based approach to evaluate our proposal of infrastructure sharing. The proposed solution has been evaluated by analytical model that has been developed to show the advantages of backhaul sharing that helps MNOs to reduce their over-provisioning costs. Our justification to adopt an analytical model is that, they are more of an abstraction of the real system than a discrete-event simulation model that require tight confidence bounds in the solutions obtained. The mathematical equations for the reliability model were derived on the basis of Continuous-Time Markov Chains developed by [35], [36]. Furthermore, Fault Tree (FT) [37] or Reliability Block Diagram (RBD) [37], [38] cannot used to model our case, since it is not possible to model reliability-with-repair using such models and these models cannot represent the system dependency occurring in real systems. Instead, we need to resort to Markov chains. Through our analytical model approach, we conclude that when backhaul networks are shared between multiple different operators, every operator involved in sharing could be able to gain an increase in the mean life of each intermediate link by a factor $\mu/3\lambda$where μ represents single repair rate and λ is the failure rate of an intermediate link, instead of investing for an additional back up path independently.

3.3. System Modeling

3.3.1. Formal Definitions

- Resilience is defined as the ability of a system to withstand a number of sub-system and components failures while continuing to operate normally [39].

- Reliability is defined as the ability of an item to perform a required function under given conditions for a given time interval [39]. It is the conditional probability at a given confidence level that a system will perform its intended function properly without failure and satisfy specified performance requirements during a given time interval $[0, t]$ when used in the manner and for the purpose intended while operating under the specified application and operation environment stress levels. Let the random variable X be the time to failure of the system. Then , reliability $R(t)$ is given by,

$$R(t) = P\ (X > t) = 1 - F(t) \tag{1}$$

where X is time to failure, $F(t)$ is the distribution function of the item's lifetime, and $P\ (X > t)$ is the probability that the time to failure is greater then time "t". In practice, Mean Time Between Failure (MTBF) is used as a measure of reliability [39]. It is the expected value of the time between two consecutive failures. The MTBF and reliability are related mathematically as follows:

$$MTBF = \int_0^\infty R(t)dt \tag{2}$$

- Availability is defined as the ability of a component to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided [11]. Considering microwave backhaul links, availability depends on the nodes and links reliability, maintenance logistic. The maintenance logistic is characterized by the parameter Mean Time to Repair (MTTR), which represents the average time needed to repair/restore a failure and bring it back into operation. The availability at any point "t" in time, denoted by A(t), is called point-wise availability, instantaneous availability, or transient availability. However, in practice, the steady state availability denoted by " A " is often used and is given by,

$$A = \frac{MTBF}{MTTR + MTBF} \tag{3}$$

An important difference between reliability and availability is that reliability refers to failure-free operation during an interval, while availability refers to failure-free operation at a given instant of time, and usually, at the time when a device or system is first accessed to provide a required function or service. MTBF gives a measure of reliability, while MTBF and MTTR together provide a measure of availability.

- A discrete-state continuous-time stochastic process $\{X(t)|t \geq 0\}$ is called a Markov chain if, for $t_0 < t_1 < .... < t_n < t$, the Conditional Probability Mass Function satisfies the following Markov property [35]:

$$P\ (X(t) = x|X(t_n) = x_n, X(t_{n-1}) = x_{n-1}, \dots, X(t_0) = x_0)$$
$$P\ (X(t) = x|X(t_n) = x_n) \tag{4}$$

- A Continuous Time Markov Chain is characterized by state changes that can occur at any arbitrary time [35]. A Continuous Time Markov Chain can be completely described by:

  -Initial state probability vector for $X(t_0)$:

$$P\ (X(t_0) = k), \quad where, \qquad k = 0,1,2, \dots \tag{5}$$

  -Transition probability functions (over an interval)

$$p_{ij}\ (v,t) = P|X(t) = j|X(v) = i), for\ 0 \leq v \leq t, and\ i,j = 0,1,2, \dots$$

$$p_{ij}\ (v,t) = \begin{cases} 1, & if\ i = j \\ 0, & Otherwise \end{cases} \qquad and \tag{6}$$

$$\sum_{j\ \varepsilon I} p_{ij}\ (v,t) = 1, \forall\ i;, 0 \leq v \leq t \tag{7}$$

Now, the probability mass function of $X(t)$,

$$\pi_j(t) = P(X(t) = j) \tag{8}$$

Using the theorem of total probability,

$$\pi_j(t) = \sum_{i\ \varepsilon I} P\ (X(t) = j|X(v) = i)\ P(X(v) = i) \tag{9}$$

If v = 0 in the above equation, we get,

$$\pi_j(t) = \sum_{i \, \varepsilon I} p_{ij}(0,t)\pi_i(0) \tag{10}$$

3.3.2. Statistical Analysis based on Real Measurement Model

Developing the "cost of availability" relationship will give the engineer an understanding of how to best concentrate the effort and allocate resources. The first step is to determine the relationship between the cost of improvement and availability. The preferred approach would be to formulate the cost function from actual cost data by estimating the different costs associated with different vendors or different component models a function of availability. The costs associated with each stage of improvement could be quantified if a reliability growth program is in place. We adopted the same approach in quantifying our results. Therefore, here, a cost-based evaluation associated with the microwave backhaul solution for Orange 3G networks, especially for the last mile and middle mile were evaluated. Even if we are conscious that the figures here refers to a given system with specific reliability figures and politics of maintenance, the evaluations that were made for the results of this chapter are concrete examples of the availability results that could be transposable for any network design.

Considering the evaluated results concluded by evidence from the real network, the results below show that in a microwave backhaul, there are always downtimes by default system configurations, be it chain or ring topologies, without any already existing redundant links. Although the values vary widely between chain and ring topologies, there is atleast a minimum downtime of 56 min/year for both of them. Unavailability results as a function of number of hops from 1 to 6 hops and E1 interfaces are reported for all the microwave scenarios in figure 4.

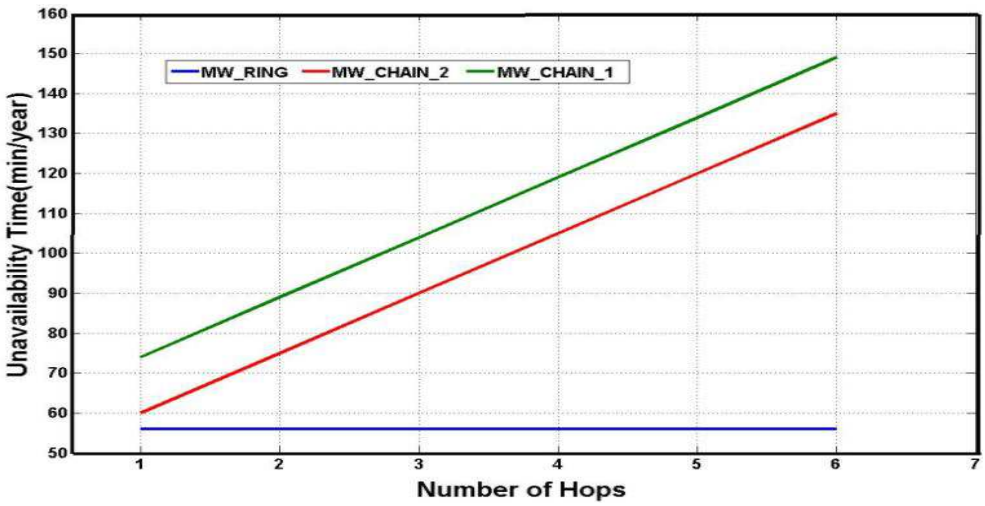


Figure 4: Unavailability results of the MW scenarios as a function of the number of hop.

In figure 4, MW_CHAIN_1 is chain topology with low protection, i.e. N+1 protection and similarly MW_CHAIN_2 is chain topology with high protection, i.e. N+2 protection. Addition of hop leads to an additional increase of 16 min/year downtime in case of the microwave chain topology scenarios. The ring topology is hop number independent with a constant downtime value around 56 min/year. Thus evident of having respective downtimes for any kind of topological configuration, it therefore necessitates the need to add more redundant links. Hence, the next step led to the evaluation of the cost that each operator invested for the sake of adding redundancy to improve the reliability of their microwave backhaul.

Figure 5 shows the analysed results incurred out of the cost evaluation. For the sake of company confidentially and business reasons, we have not represented the actual figures of costs. Instead, we defined a new term called Cost Enhancement Co-efficient (CEC). This term is defined as follows:

$$CEC = \frac{C_{max} - C_{min}}{C_{min}} \tag{11}$$

where,

- CEC stands for Cost Enhancement Co-efficient.
- C_{max} is the maximum cost invested to bring down the unavailability time (in minutes per year) to a minimum value by adding the highest possible redundancy.
- C_{min} is the minimum cost invested to bring down the unavailability time (in minutes per year) to a minimum value by adding the least possible redundancy.

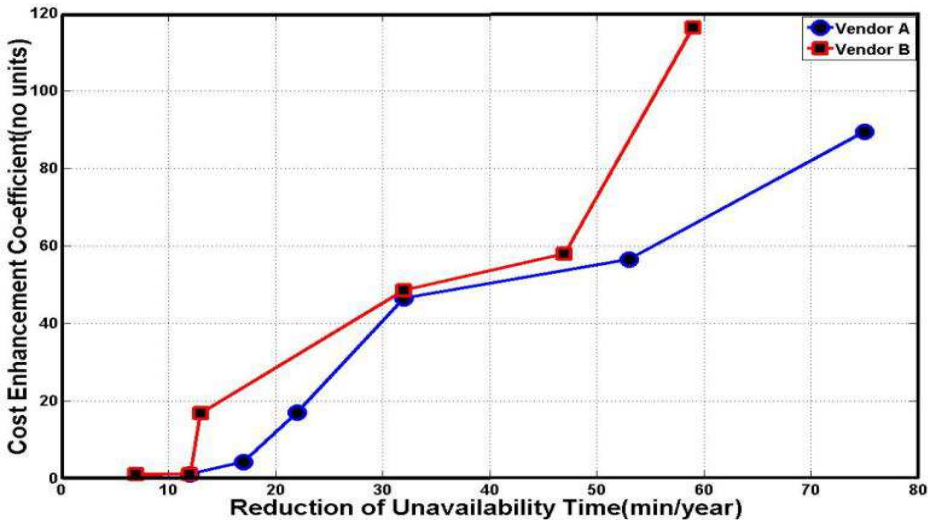


Figure 5: Cost Enhancement Coefficient as a function of unavailability results of the MW scenarios.

We evaluated the results for two different network equipment vendors who play a major role in the telecommunication world in Europe and Asia. From the curves, it is observable that in order

to bring down the unavailability time from 20 min/year to 10 min/year, the operator has to invest atleast 10 times higher cost than the initial cost. To be more decipherable, let us consider the performance of the equipment of the vendor A in figure 5. By default, the equipment is expected to have downtime value of 117 min/year without any redundant links. In order to bring the downtime to (117-75) min/year, (the last point in the curve), i.e. 42 min/year, the minimum achievable value for downtime, the cost that would incur for the operator is 88 times higher than the initial cost that the operator would have invested to bring down the unavailability time reduced to (117-10) min/year, i.e. 107 min/year. This amount that the operator had to invest to bring down their downtimes is enormously high. If this is the case for improving reliability at only a particular destination in the backhaul network, then the cost investment for the complete backhaul network is a night-mare.

Proceeding further, to emphasize furthermore on the cost investments that incur for the network operators, we continued to analyse the cost increments as a function of percentage. This is depicted in figure 6. We infer that just to reduce the unavailability value by a small fraction, the percentage increase in cost is extraordinarily tremendous. For example, looking at performance of vendor A, there is an increment of almost 100% in cost to bring down the network unavailability time to a minimum of 56 min/year from the original unavailable time value of 117 min/year. To elaborate it on a more perceivable way, let us say that an operator uses equipments supplied by vendor A that has a default downtime of 117 min/year without adding any redundant links. In order to improve the availability of the network, the operator must add redundancy. For this, in order to bring the downtime from 117 min/year to 107 min/year, i.e. to achieve a reduction of downtime of 10 min/year, the operator has to invest atleast 20% more than the initial cost that he would invest. Eventually, to obtain satisfactory results in reducing downtimes, the operator is forced to invest almost 100% more than the cost of the initial investments.

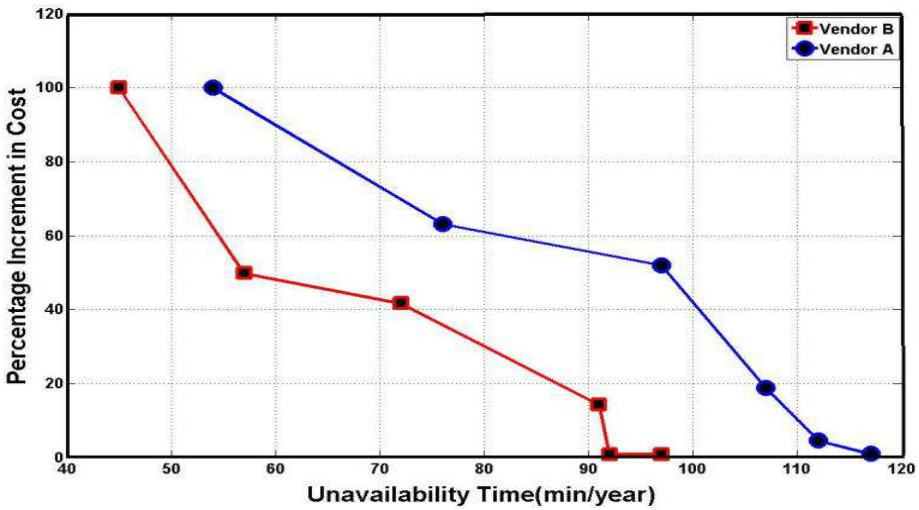


Figure 6: Percentage increment in cost as a function of unavailability results of the MW scenarios.

The above analyses fundamentally paved the way to come up with a solution that can cost effectively offer the same availability. In order to realise this, we opted for backhaul infrastructure sharing, where two operators share their backhaul networks for the purpose of increased availability without investing additional costs for backhaul.

3.3.3. State Space Analytical Model for Infrastructure Sharing

Here, we describe our mathematical equations to illustrate the reliability of our proposed architecture that were derived on the basis of Continuous-Time Markov Chains developed by [7]. In general, the cost as a function of the redundancy for each intermediate link attempting to improve the reliability of the overall system is quantified to prove that the design changes resulting in a system is needlessly expensive when redesigned. Consider an operator backhaul network consisting of n intermediate links connecting till the last mile from the core network. Firstly, the network operators' objective is to make all of the intermediate links of that backbone network reliable by adding redundancy. This is usually achieved by setting up a primary path and backup path. Secondly, the network operator makes an effort to accomplish that goal with a minimum cost. The above stated problem is formulated as a nonlinear programming problem as follows [9]:

$$Problem: min\ C = \sum_{i=1}^{n} C_P C_B \tag{1}$$

where,

n - number of intermediate links

c_P - cost of setting up a primary path

c_B- cost of setting up a backup path (redundant path)

C – the cumulative cost of the total backhaul network

This formulation is designed to achieve a minimum total system cost. For the same, the first step will be to obtain the system's analytical reliability function in terms of the reliability of intermediate links. The next step is to obtain a relationship for the cost of each component as a function of its reliability. An empirical relationship is derived based on past experiences and data for similar components. The basic formula to calculate the probability of a system failure is given as below. Any system can be ascertained to be cumulative of many duplicate elements for the sake of redundancy. As a result, each duplicate component added to the system decreases the probability of system failure according to the formula:

9 We do not get into the details of solving this non linear programming at this point in this dissertation. The idea is only to define the problem.

$$P = \sum_{i=1}^{n} P_P P_B \tag{2}$$

where,

n - number of components

p_P- probability of primary path failing

p_B- probability of backup failing (double failures)

P - the probability of the whole network outage (system failure)

However, as a corollary to the above, as stated before in the problem statement, each duplicate component added to the system also increases the cost of setting up the system. This is given by the formula:

$$C_i = \sum_{i=1}^{n} C_P C_B \tag{3}$$

The above equation to calculate the probability of a system failure assumes independence of failure events. That means that the probability of a backup path failing given that a primary path has already failed is the same as that of backup path failing when primary path has not failed. Under such situations, the cost that is invested for redundancy becomes ineffective. There are situations where this is reasonably justifiable, such as using both the primary path and the secondary path connected to the same aggregation node, whereby if one link is failed, the other would too. Therefore, it is evident that there is always a cost associated with changing the backhaul design of a mobile network that may be due to the additional links for redundancy for the sake of avoiding link failures.

With this motivation, we begin our model assuming each of the two operators provisions their own network with only one path and shares the back-up path with another operator. One path serves working path (primary path) and the other path serves as the protection light path (backup path) and vice versa for each of the two operators who decide to share their backhaul. Fundamentally, each of the two operators provisions their own network with only one path and shares the back-up the path with another operator. One path serves as working path (primary path) and the other path serves as the protection light path (backup path) and vice versa for each of the two operators who decide to share their backhaul. For our model, we assumed that these two paths exist in parallel for the sake of redundancy and this is true for the most of the cases in backhaul topologies connecting till the last mile. This is illustrated below in figure 7. Each path has a failure rate of λ. The repair rate is μ. For the availability analysis, the state space is shown as follows:

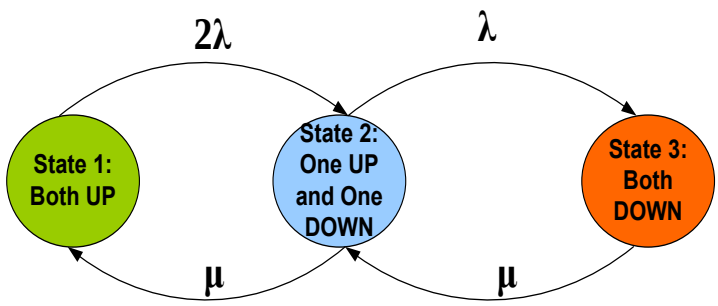


Figure 7: State diagram for availability analysis of a parallel redundant system.

For reliability analysis, since we do not consider the repair once the system is in down state, all the down states will be considered as "absorbing" states, in a reliability model. Hence in our model we get,

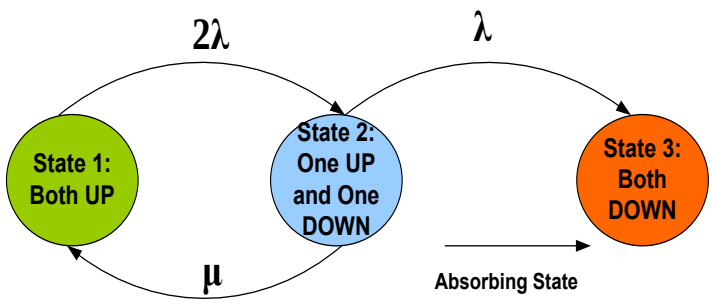


Figure 8: State diagram for reliability analysis of a parallel redundant system.

Note that the above Markov chain is a reliability model with repair since component repair is allowed if the system has not failed. It is also possible to construct a reliability model without repair. When both paths, i.e. primary path and the backup paths, have failed the system is considered to have failed and no recovery is possible. Let the number of properly functioning components be the state of the system. The state space is {0, 1, 2}, where 0 is the absorbing state. The state diagram is given in figure 8. Assume that the initial state of the Markov chain is 2; that is,

$$C\pi_2(0) = 1, \pi_k(0) = 0, for\ k = 0,1, \text{ then} \tag{12}$$

$$\pi_j(t) = p_{2j}(t), \tag{13}$$

And the system of differential equations is written based on the rule:

Rate of build-up = Rate of flow IN - Rate of flow OUT

Thus the system of differential equations are given by,

$$\frac{d\pi_2(t)}{dt} = -2\lambda\pi_2(t) + \mu\pi_1(t),$$

$$\frac{d\pi_1(t)}{dt} = 2\lambda\pi_2(t) - (\lambda + \mu)\pi_1(t),$$

$$\frac{d\pi_0(t)}{dt} = \lambda\pi_1(t). \tag{14}$$

Applying Laplace transform to the above set of equations, we can reduce this system to:

$$s\overline{\pi_2}(s) - 1 = -2\lambda\overline{\pi_2}(s) + \mu\overline{\pi_1}(s),$$

$$s\overline{\pi_1}(s) = 2\lambda\overline{\pi_2}(s) - (\lambda + \mu)\overline{\pi_1}(s),$$

$$s\overline{\pi_0}(s) = \lambda\overline{\pi_1}(s). \tag{15}$$

Solving the above equation for $\overline{\pi_0}(s)$, we get,

$$\overline{\pi_0}(s) = \frac{2\lambda^2}{s[s^2 + (3\lambda + \mu)s + 2\lambda^2]} \tag{16}$$

After an inversion, we can obtain $\pi_0(t)$, the probability that no components are operating at time t ≤o. Let Y be the time to failure of the system; then $\pi_0(t)$ is the probability that the system has failed at or before time t. Thus the reliability of the system is,

$$R(t) = 1 - \pi_0(t) \tag{17}$$

The Laplace transform of the failure density function can be thus written as,

$$f_Y(t) = -\frac{dR}{dt} = \frac{d\pi_0(t)}{dt}, \qquad \text{given by}$$

$$L_Y(s) = \overline{f_Y}(s) = s\overline{\pi_0}(s) - \pi_2(0)\,, \tag{18}$$

$$L_Y(s) = \frac{2\lambda^2}{[s^2 + (3\lambda + \mu)s + 2\lambda^2]} \tag{19}$$

The denominator can be factored so that,

$$s^2 + (3\lambda + \mu)s + 2\lambda^2 = (s + \alpha_1)(s + \alpha_2) \tag{20}$$

and the preceding expression can be rearranged so that

$$L_Y(s) = \frac{2\lambda^2}{\alpha_1 - \alpha_2}\left(\frac{1}{s + \alpha_2} - \frac{1}{s + \alpha_1}\right), where \tag{21}$$

$$\alpha_1, \alpha_2 = \frac{(3\lambda + \mu) \pm \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}}{2} \tag{22}$$

Inverting the transform in $L_Y(s)$, we get,

$$f_Y(t) = \frac{2\lambda^2}{\alpha_1 - \alpha_2}(e^{-\alpha_2 t} - e^{-\alpha_1 t}) \tag{23}$$

and hence the reliability becomes,

$$R(t) = \int_t^\infty f_Y(x)dx = \frac{2\lambda^2}{\alpha_1 - \alpha_2}\left(\frac{e^{-\alpha_2 t}}{\alpha_2} - \frac{e^{-\alpha_1 t}}{\alpha_1}\right) \tag{24}$$

As per eq. (2), the MTBF of the system is given by,

$$E|Y| = \int_0^\infty R(t)dt = \frac{2\lambda^2}{\alpha_1 - \alpha_2}\left(\frac{1}{\alpha_2^2} - \frac{1}{\alpha_1^2}\right) = \frac{2\lambda^2(\alpha_1 + \alpha_2)}{{\alpha_1}^2.{\alpha_2}^2} \tag{25}$$

$$E|Y| == \frac{2\lambda^2(3\lambda + \mu)}{(2\lambda^2)^2} = \frac{3}{2\lambda} + \frac{\mu}{2\lambda^2} \tag{26}$$

From the above equation, it is evident that the MTBF of an intermediate microwave link that comprises of an additional backup path in parallel shared with another operator, for the sake of redundancy, increases by a mean life of $\mu/2\lambda^2$, or by a factor:

$$1 + \frac{\mu/2\lambda^2}{3/2\lambda} = \frac{\mu}{3\lambda} + 1$$

The same equation, while in the absence of an additional backup path, (i.e.,$\mu = 0$), would be equal to the first term, $3/2\lambda$ in expression (25). Therefore, from the above analytical evaluation, it is evident that sharing an additional link with another operator instead of having to invest one by themselves, will increase of reliability of each intermediate link, for every operator who agree to share the links.

3.4. Proposed Architectural Design

Therefore based on our analytical modeling, we contemplated the appropriateness of allocating another secondary backup paths permanently, considering the awful cost investments associated with it for the MNOs, especially in the developing economies. We argued that permanently provisioning a secondary backup path (i) incurs an additional cost investment which is as similar in magnitude as the initial "huge" cost investments that is incurred for setting up the primary path, (ii) even though backup paths may serve as an additional carrier to carry the extra traffic

load of the primary working path under link/node failure conditions and/or network overloaded situations, this may not be the most optimal solution, because, in typical real world conditions, the capacity which is allocated for the secondary path is not always actively filled-in as much as the capacity allocated for the primary path. Emphasizing on these pitfalls, we call-for the idea of "re-designing" backup path provisioning scheme, which not only should result in investing less for redundancy but also should satisfy the mere availability requirements for the MNOs. Our arguments lead to a design consideration in which the primary resource (working path) of one MNO could be re-provisioned as the backup resource (backup path) for another MNO - exclusively at times when a link fails, when resource utilization exceeds a threshold and/or when the network state changes to achieve better resource utilization, for any one of the MNOs, by connecting both of the MNOs last mile links.

With this in mind, as a next step, we propose our solution on the architectural design of backhaul networks by infrastructure sharing. Before to proceed, the question that very often engineers have to answer is related to the selection of the best and most reliable network topology. It has been proved from the prospective of the individual microwave path availability analysis of [4] for a linear topology of the five cell-site network, the average unavailability per BTS is 0.003% (availability = 99.997%); for the star/hub topology, the average unavailability per BTS is 0.0018% (availability = 99.9982 %), and for the ring topology, 0.00000007% (availability = 99.99999993%). Therefore, the resulting topology arising out of microwave backhaul network infrastructure sharing between two operators has to result in a ring topology that will result in minimum CAPEX, thus providing superior availability and resiliency. For this, we choose a real topology of Orange networks. Again, for confidentiality reasons, the geographical location of this topology is un-revealed. The topology below represents a chain topology till the last mile. Since, this is a chain topology every intermediate link has a double protection, i.e. a primary path and backup path. However, the last hop of the last mile link is never protected and the failures accounting in the last mile are not avoided at all. Further, any link failure in the backhaul architecture of mobile networks will not only reduce the service availability but also alter the network's topology.

Figure 9 shows the topological evolution of a chain topology into a ring topology, which results in the protection of a last mile link as well as cost reduction due to elimination of an extra backup link for both the operators. Since the evolved architecture is a ring topology, MNOs who agreed to share and build the backhaul topology together, need not invest for another additional secondary link to include redundancy across their own chain topology. According to our architecture, each network operator shares another operator's working path as their backup path. As it can be seen in figure 9, there are two different operators who share the microwave backhaul links. The one at the top of the figure (in the north of the country) is the topology of

operator A. The one below with circles (in the south of the country) is the topology of another operator who agrees to share the backhaul links. When the last miles of both the operators are connected by another additional link (green colour thick link), we observe that the ring topology network that has evolved, provides more protection including the last miles compared to a microwave chain topology. In addition to offering more protection, the other advantage is that the sharing operators need not invest for another additional link to include redundancy across their entire chain topology. This provides a solution for network operators to reduce the total cost of building a backhaul network since they obviate the need for an additional backup path. Besides, our solution (i) benefits the MNOs to reduce the total cost of building a backhaul network since they obviate the need for additional backup resource; (ii) it is a problem solver for disaster recovery situations, like the tsunami and earthquake affected Japan, where MNOs are willing to share and invest to bring back the technology as soon as possible and (iii) enable quick roll-out of new technologies like the 4G-LTE without having to invest more for backhaul in emerging economies.

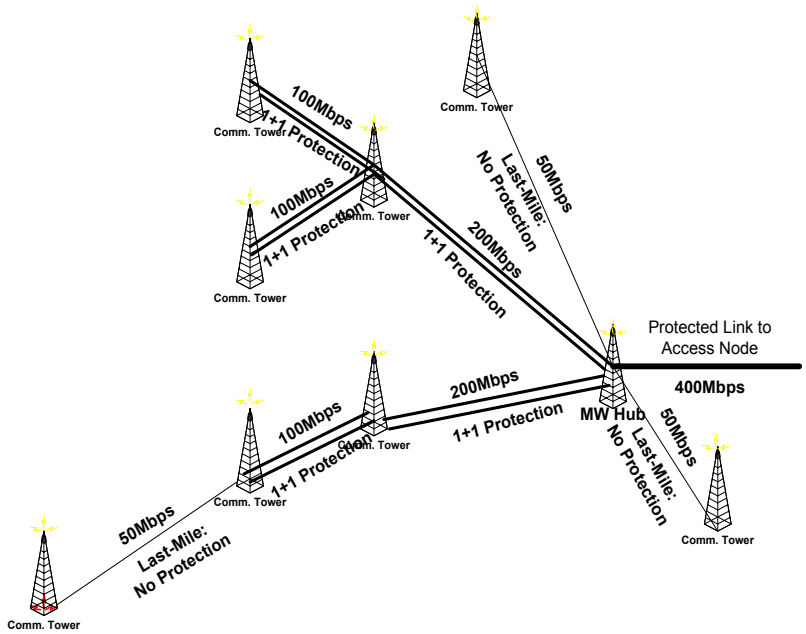


Figure 9: Last mile chain topology with redundant links.

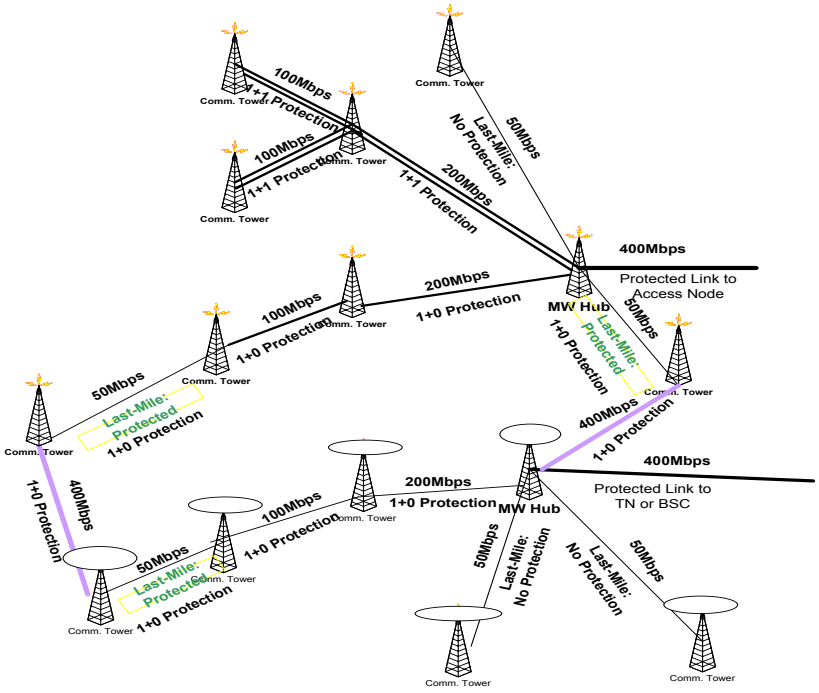


Figure 10: Resiliency design flow using infrastructure sharing.

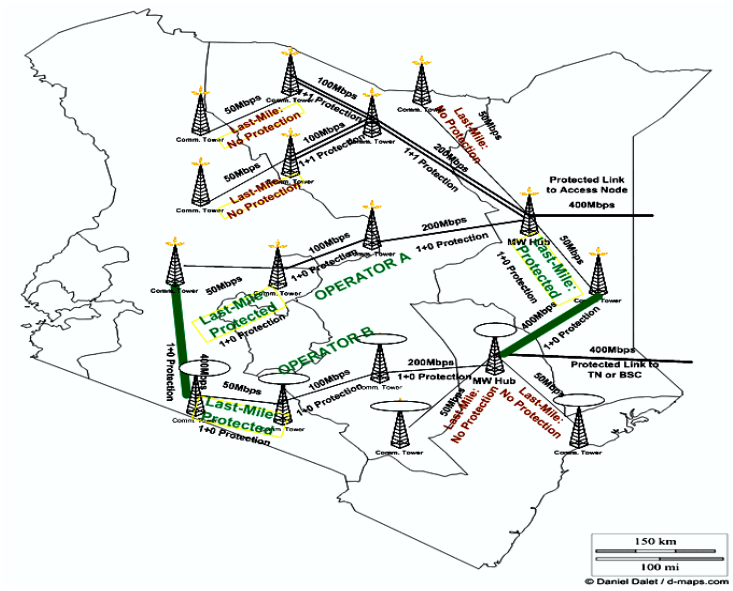


Figure 11: An illustrative example network topology portraying resiliency design flow using infrastructure sharing within the country Kenya.

3.5. Give and Take: Characterization of Availability of Multi-State Wireless Backhaul Networks: Part II

Now, in this part, we provide an availability analysis to illustrate the availability within network operators' backhaul at times when a path is blocked due to link/node failure and/or when

resource utilization exceeds a threshold and/or when the network state changes to achieve better resource utilization. We call it "Give and Take" here, because network operators "give" a part of their working path bandwidth to another network operator with whom the Service Level Agreement (SLA) is concluded, without jeopardizing their own availability requirements. This working path is used by another operator as their backup path. At the same time, operators also "take" bandwidth from the sharing operators if there is a surge for more bandwidth within their own backhaul. We consider measures of availability analysis within the context of Multi-State Systems (MSS) theory [40] where each of the MNOs' backhaul can have different performance levels ranging from perfect functioning to complete failure. Our approach presents a model representing demand as a continuous-time Markov chain [41], [42] with four different logical state spaces. We propose a general approach to describe, model and evaluate the availability characteristics of the microwave backhaul systems with various types of failures and repair scenarios. Such failures may change the state of the backhaul system and the quality of its operation, but do not necessarily lead to complete system failure.

3.5.1. Organization of Part II

From here begins the second part of this chapter. The rest of the part is organized in the following order and we thus enunciate this here to give the reader a quick overview of our work in this part. In what follows next is the Section 3.6 that describes our adapted approach of MSS theory with a very brief description. For readers who might require an initial clear understanding on MSS theory, reading [40] is strongly encouraged. Section 3.7 gets deeper into the subject with a formal introduction to the preliminaries and then directly into the analysis. Here, we have supported our approach based on MSS theory analytically. A general model for describing availability process in backhaul systems while being shared among MNOs with gradual failures is proposed. Section 3.8 illustrates the numerical results showing its support to the theory. Finally, Section 3.9 gives the concluding remarks for the chapter with our claim to support backhaul link sharing under link failure situations.

3.5.2. Evaluating Approach

Approaches to evaluate a system's availability studies are common by two main characteristics: the life-time of the system and its steady state characteristics under some assumptions about repair process. The ways to evaluate these characteristics depend on the approach to the following two aspects: probabilistic and structural. Probabilistic aspect deals with calculation of the system states probabilities, and uses them in availability calculations. The structural aspect considers kind of direct evaluation of reliability characteristics for any given structure of a particular system. Here we deal with probabilistic aspect of modeling system availability and

focus on both of its common characteristics. While the probabilistic aspect of modeling system availability is being considered, it can be further categorized as the binary state and multi-state models. Traditional binary-state availability models allow only two possible states for a system and its components: perfect functioning (up or 1) and complete failure (down or 0). However, many real-world complex systems have different levels of performances for which one cannot formulate an "all or nothing" type of availability criterion, especially when the performance of one component is affected by the performance of another component. Such systems are defined as the Multi-State Systems (MSS). Estimation of the availability and optimizing the design of the MSS is gaining popularity and has been widely studied in literature [43], [44]. MSS availability and reliability evaluation can be carried out based on three different approaches [45], namely the stochastic process that mainly deals with the Markov Model (MM) approach; the structure function approach, where Boolean models are extended for the multi-valued case; and Monte Carlo simulation. Our proposed solution has been evaluated by the stochastic model approach for the MSS. The proposed model has been developed to show the advantages of sharing backhaul links between two or more different network operators to enable quick roll-out of new technologies and to improve the overall network resource utilization capacity. Our present work here elicits the architectural design of our previous part but provides a completely new availability analysis to illustrate our architectural design. Furthermore, to the best of our knowledge, no previous work analyzes resource sharing in wireless backhaul architecture between different MNOs within the context of the MSS theory.

Our proposed solution has been evaluated by the stochastic model approach that has been developed to show the advantages of backhaul link sharing between two different MNOs to improve the overall capacity. We adapted to stochastic models as they are more of an abstraction of the real system than a discrete-event simulation model that require tight confidence bounds in the solutions obtained. Furthermore, our results here are evaluated based on the Markov chain method, also for the following reasons: it is appropriate for quantitative analysis of availability and reliability of systems; it can be used with large, complex systems; it is not only useful, but often irreplaceable, for assessing repairable systems. Therefore, here we adopt Markov Model approach that considers of multi- state model to analyze the availability of microwave links when shared.

3.6. Multi-State System Availability Analysis

3.6.1.1. Formal Definitions

To define systems with degrading components in the MSS availability analysis model, we assume that the system under consideration has the reliability state set denoted as s can have

$\{0,1,,2,\dots z\}$ different states, where the state o is the worst state and the state z is the best state, for any system element j, where $j = \{1,2,\dots n\}$. The system reliability states degrade with time t without repair. The above assumptions mean that the system states degrade in time only from better to worse, corresponding to the performance rates, represented by the set $g_j = \{g_{j1}, g_{j2}, \dots g_{js}\}$ where g_{js} is the performance rate of element j in the state s.The performance rate $G_j(t)$ of element j at any instant t ≥ 0 is a discrete-state continuous-time stochastic process that takes its values from g_j: $G_j(t) \varepsilon\, g_j$. The system structure function $G(t) = \Phi\big(G_1(t), \dots . G_n(t)\big)$ produces the stochastic process corresponding to the output performance of the entire MSS. In practice, a desired level of system performance (demand $W(t)$) also can be represented by a discrete-state continuous-time stochastic process. For reliability assessment, MSS output performance and the desired performance level ($W(t)$) are often assumed to be independent stochastic processes. The desired relation between the system performance and the demand at any time instant t can be expressed by the acceptability function $\Phi\big(G(t), W(t)\big)$. In many practical cases, the MSS performance should be equal to or exceed the demand. So, in such cases, the acceptability function takes the following form:

$$\Phi\big(G(t), W(t)\big) = G(t) - W(t) \tag{27}$$

and the criterion of state acceptability can be expressed as,

$$\Phi\big(G(t), W(t)\big) \geq 0 \tag{28}$$

A general expression defining MSS reliability measures can be written in the following form:

$$R = E\left\{\mathcal{F}[\Phi\big(G(t), W(t)\big)]\right\} \tag{29}$$

where E denotes the expectation symbol, $\mathcal{F}$ is the function that determines corresponding type of reliability measure, and Φ, the acceptability function. Many important MSS reliability measures can be derived from the expression (29) depending on the functional $\mathcal{F}$ that may be determined in different ways. For example, it may be a probability $Pr\{\Phi\big(G(t), W(t)\big)\} \geq 0$ throughout a specified time interval $[0, t]$ and the acceptability function (27) will be non negative. In this case, this probability characterizes MSS availability. It may be also an expectation of an appropriate function up to the time of the MSS, s initial entrance into the set of unacceptable states, where $\Phi\big(G(t), W(t)\big) < 0$ is the number of such entrances within time interval $[0, t]$ and so on. For a wireless backhaul system where the available capacity at time instant t is $G(t)$ and the corresponding load demand is $W(t)$, if the acceptability function is defined as:

$$\Phi\big(G(t), W(t)\big) = \begin{cases} W(t) - G(t), & if\ W(t) > G(t) \\ 0, & if\ W(t) \leq G(t) \end{cases} \tag{30}$$

3.6.2. Multi-State Wireless Backhaul Networks Availability Analysis with Sharing between Different MNOs

The following assumptions and conditions are adapted for our model, thus making it as a MSS with four different logical state spaces:

A. Assumptions and Conditions

Assumption 1: Our model assumes that there are only two operators (MNO A and MNO B) who agree to share their backhaul. However, our solution can be practically possible allowing any number of MNOs to share, provided they are all within the same geographical zone, i.e. within one country.

Assumption 2: For obtaining system performance values $\Phi\big(G_1(t), G_2(t)\big)$, we set each MNO's backhaul bandwidth to 200Mbps link. Taking advantage of the now available granularity features, e.g. MPLS-TE, OpenFlow [46], MNOs "split" capacity according to the sharing MNO's requirements. For our simplification, we assume that each MNO allows the sharing MNO to "give and take" up to a maximum of 75Mbps of their link bandwidth for the sake of resiliency and redundancy and also for over-provisioning.

B. Four States (Multi-State) while MNOs Share

State 1- Both UP (Normal Operating State (NOS)): The working paths (primary path) of both the MNOs utilize their bandwidth capacity fully, i.e. no failure encountered by any of the MNOs and hence sharing backhaul link bandwidth becomes unnecessary. We call this as NOS.

State 2- One UP and One DOWN: One operator (MNO A) is faced with a link failure in its own backhaul and thus down, whereas the sharing operator (MNO B) functions under normal operating conditions, i.e. no failures.

State 3- Both DOWN: Both of the MNOs have encountered network outage due to failures at the same time and hence they are down at the same time. This is defined as the Absorbing State where resource sharing between MNOs becomes void and necessitates manual intervention.

State 4- Both ORC (Operating at Reduced Capacity): This is a special case, which categorizes our model as a multi-state system, since there is no absolute "UP or DOWN" state. As per our assumption, when there is a link failure in MNO A backhaul, the MNO B shares the reserved bandwidth with MNO A. The state of MNO A changes from state "DOWN" to "UP". However,

both the MNOs can not utilize their fullest bandwidth capacity now, since they are allowing the other MNO to take a part of their bandwidth. It is an intermediate state that is not categorized into a complete failure or a perfect functioning. This state is the state that we define as the Operating at Reduced Capacity state. At this state, MNOs decide which kind of their traffic (high revenue generating premium customers' traffic and/or delay sensitive voice call customers' traffic) must be given more priority than the rest due to the limited available shared bandwidth.

C. State Space Diagram and State Probabilities

Our model encompasses all the transitions caused by the each element's failures and repairs that correspond to the transition intensities which are expressed by the element's failure and repair rates. Each path that encounters a failure has a failure rate of λ. The repair rate is μ. Also, the transition to the intermediate ORC state is represented as ε and the transition from the intermediate ORC state is ψ. Failure and repairs cause element transition from one state to another state.

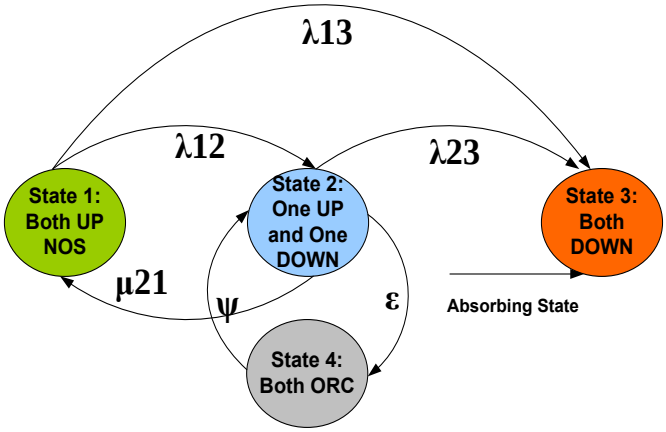


Figure 12: Multi-state system reliability analysis diagram for wireless backhaul network with infrastructure sharing.

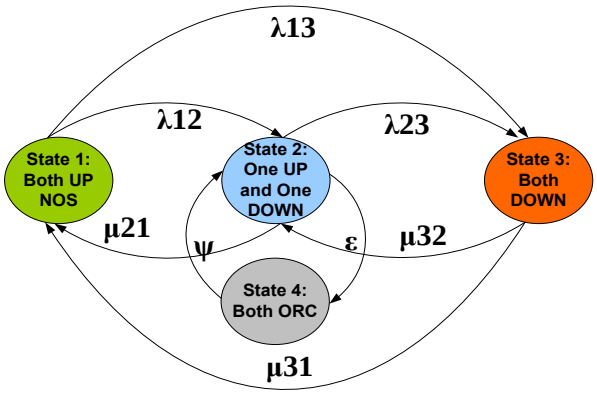


Figure 13: Multi-state system availability analysis diagram for wireless backhaul network with infrastructure sharing.

From the state space diagrams seen in figure 12 and figure 13, with assumption that the state 1 is the best state of our system under analysis, there is a transition from the state 1 to the state 2 if failure (λ_{12}) occurs in the state 1; then if the repair (μ_{21}) will be completed, the system will be back to the previous highest state 1. Similarly, there is a transition from the state 2 to the state 3 if failure (λ_{23}) occurs in the state 2; however, the state does not return back to the previous highest state since there is no repair under reliability analysis, as in figure 13. In addition, there is a transition to the state 4 with transition intensity rate ε and back to the state 2 with transition intensity rate ψ when there is a failure or demand variation when the system is in the state 2. The corresponding performance g_s is associated with each state transition. Table II indicates the system states and the corresponding performances calculated based on our assumed values from Section IV (B).

TABLE II. SYSTEM STATE AND PERFORMANCE

System States	State of the elements	System Performance $\Phi(G_1(t), G_2(t)) = G_1(t) + G_2(t)$
1	$\{g_{11}, g_{22}\} = \{200, 200\}$	$g_1 = 400$ Mbps
2	$\{g_{12}, g_{22}\} = \{0, 200\}$	$g_2 = 200$ Mbps
3	$\{g_{13}, g_{23}\} = \{0, 0\}$	$g_3 = 0$ Mbps
4	$\{g_{14}, g_{24}\} = \{75,125\}$	$g_4 = 200$Mbps

From the table, it can be observed that the performance of the system in the state 1 achieves the best performance with $g_1 = 400$ Mbps, where both of the MNOs demands could be met satisfactorily. Without doubt, the performance of the system in the state 3 is the worst, where both of the MNOs demands could not be satisfied at all due to link failure situation. Now, observing the state 2 and the state 4, they both show the same system performance with $g_2 = 200$ Mbps and $g_4 = 200$Mbps respectively. Nevertheless, what is interesting is that with the state 2 system performance, only MNO B demands are satisfied while MNO A demands are not. With our solution through sharing the backhaul links, analyzing the state 4 system performance, what could be deduced is that both MNO A as well as MNO Bs demands (if not completely) could be satisfied, since they both have atleast limited shared-bandwidth available.

The next step is to determine the state probabilities $P_s(t)$ of the element's performance process $G_j(t)$ at time. Formally,

$$P_s(t) = Pr\{G_j(t)\varepsilon\, g_{js}\}\, where\ s = \{0,1,,2,\dots z\}: t \geq 0 \tag{31}$$

Accordingly, the Kolgomorov's system of differential equations for finding the state probabilities $P_s(t)$ for the homogeneous Markov process is:

$$\frac{dP_s(t)}{dt} = P_s(t)\, V(t) \tag{32}$$

where, $P_s(t)$ indicates the system-state probability vector at time t, whose entries are the system state probabilities at t and $V(t)$ denotes the transition-rate matrix, whose entries are the component failure, repair and intensity rate. Based on the developed multi-state system space diagram, the mathematical equations using Markov chain were developed and therefore, the corresponding system of differential equations is written as:

$$\frac{dP_s(t)}{dt} = P_s(t)\begin{bmatrix} -(\lambda_{12}+\lambda_{13}) & \mu_{21} & \mu_{31} & 0 \\ \lambda_{12} & -(\lambda_{23}+\mu_{21}+\varepsilon) & \mu_{32} & \psi \\ \lambda_{13} & \lambda_{23} & -(\mu_{32}+\mu_{31}) & 0 \\ 0 & \varepsilon & 0 & -\psi \end{bmatrix} \tag{33}$$

D. Estimation of Transition Probabilities

Failure and repairs cause element transition from one state to another state. The estimation of transition probabilities are calculated on assumptions based on the real-world performance data. Table III shows the values that were used for the numerical illustrations. To know how the values were obtained, please refer [7]. Transition values λ and μ considered here represents the failure and repair rate for a microwave chain topology.

TABLE III. TRANSITION RATES OF ALL STATES

	System States			
System States	**1**	**2**	**3**	**4**
1	0.0	0.017241	0.034482	0.0
2	0.022777	0.0	0.017241	0.00002
3	0.001388	0.022777	0.0	0.0
4	0.0	0.00002	0.0	0.0

As we know that the initial state of the Markov chain, i.e. state 1 gives the best performance, $P_1(0) = 1$, and for the rest $s = 2,3,4$, $P_s(0) = 0$. Therefore, solving (7) using Laplace transformation under the initial conditions, we determine the state probabilities $P_s(t)$. Figure 14 illustrates this graphically.

E. Multi-State System Availability and its Demand

Based on the state probabilities which are determined from the Markov model for all the system elements, we define the availability of the entire shared backhaul architecture, as a measure

which indicates the probability of the network to work normally under determinate time t and demand $W(t)$, where $W(t)$ is a random process that can take discrete values from the set $W = \{W_1, \dots, W_M\}$. Therefore, the MSS availability $A\left(t, W(t)\right)$ at instant $t > 0$ for random constant demand W(t)for the wireless backhaul when shared is written as:

$$A\left(t, W(t)\right) = \sum_{i=1}^{k} \left[\!\left[\mathrm{P_s(t)}.\left(\mathrm{g_{js}} - \mathrm{W(t)}\right) \right]\!\right] \ \forall\, k \leq n \tag{34}$$

3.7. Illustrative Numerical Evaluation

3.7.1. Estimation of State Probabilities from the Markov Model

As a first step, we determine the probability of each system state defined earlier, with the corresponding system performance. This enables us to evaluate the availability of the entire backhaul architecture evolved out of sharing between MNOs. Figure 11 shows the evaluated system state probabilities as function of time obtained by solving (33). The probability that each element provides a performance rate is based on each value of system performance and the values of failure and repair rates. It can be observed that the state 1, which is the best state of the system with no failures at all has the highest probability to satisfy the demand W(t)during the operation days. On the other hand, the state having the next highest probability to meet the demand is the state 4. This is due to the very low transition rate from the state 2 to the state 4. This implies that when MNOs share their link bandwidth, the overall performance is nearly as good as they operate without any failures at all.

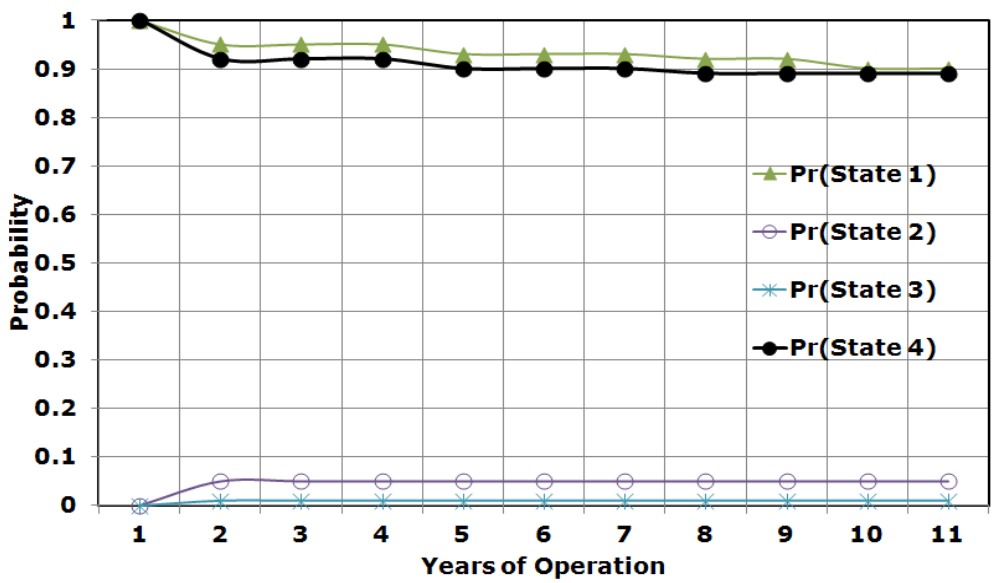


Figure 14: Estimation of state probabilities of wireless backhaul network with infrastructure sharing

3.7.2. MSS Average Availability of the Wireless Backhaul when Shared

Based on the state probabilities, we now measure the availability. From the state diagrams, each state represents the set of acceptable states based on the required demand W(t). We use (8) to calculate the average availability. This is obtained by the summation of the calculated state probability values of only the acceptable states, i.e. states 1, 2 and 4.

Figure 15: Estimation of Instantaneous availability for wireless backhaul network with infrastructure sharing

The availability of entire backhaul architecture evolved out of sharing between MNOs is shown in figure 15. We observe that total system availability is greater than 99. 8%. If the required demand is within the limits of the allocated bandwidth capacity, then we observe that all the states satisfied the required availability requirement except state 3, which is the absorbing state. In this case, the state 3 would be an unacceptable state which is not considered for the calculation of the system availability. We also notice that the availability decreases through time anyway. This is only due to the performance degradation that arises due to wear and tear effects.

3.8. Concluding Discussions

Wireless standards such as the 4G-LTE keep on evolving but the backhaul architecture remain the same. A first thought and a simple solution to enable quick roll-out of new technologies like the 4G-LTE without having to invest more for backhaul is presented in this chapter. As discussed in the chapter, we have presented a novel resource sharing framework which can cost-effectively provide protection services without jeopardizing guaranteed availability requirements for the

MNOs. We evaluated our results, first by a simple 2-path parallel system and then using Multi-state system (MSS) using State Space Markov Chain model. The advantage of the models is that it can be applied to any system with high complexities. The technique is effective for small and large-scale systems. As long as the system's reliability equation can be derived analytically, the model can be used to solve the reliability allocation problem.

Our approach here is to define which type of traffic needs to be protected all the time, and which can have a lower level of protection. True, the above scenario does not offer a 100% protection scheme like in the SDH world. It does however offer 100% protection level for the premium (i.e. revenue generating) traffic during partial network downtime, while leaving some headroom for low priority service so as to avoid starvation. From a first glance it may seem like we have reduced availability, but in truth, the system ensures that premium types of service never fail and have a guaranteed channel regardless of any other traffic. Thus, MNOs improve the availability of their revenue generating services to ensure high-quality, uninterrupted user experience, and increase link capacity to offer more data services. By adopting the proposed solution to achieve backhaul infrastructure sharing, networks operators could decrease their unavailability time without having to invest more for adding redundancy. Henceforth, the cost reductions will lead to a reduction of business risk for the involved operators. The cost and energy reduction in this scenario is of a similar magnitude, since more traffic can be served with the same links before additional sites are needed. With all these in mind, backhaul infrastructure sharing could be one of the problem solvers to tackle the issue of restoring network failures or undermining peak traffic problems.

*"Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true." – **Bertrand Russell, British philosopher, Logician, Mathematician.***

Chapter 4

Analytical Modeling for Recovery and Re-routing within the Shared Backhaul Architecture

Little attention has been given to understanding the fault recovery characteristics and performance tuning of backhaul networks. This chapter focuses on the modeling aspects of the fault recovery and re-routing in backhaul networks, to understand, as well as to improve their behavior in network failure and recovery scenarios. Here, we consider our shared architecture based on our earlier proposal from previous chapter, to model our system. Our model is designed irrespective of the underlying routing protocol, i.e. any existing routing protocol such as the Internet Group Management Protocol (IGMP) and the Open Shortest Path First (OSPF) protocol can be idealized for the proposed modeling. The analytical model presented here, enable us to describe the interplay of the recovery and re-routing procedures in such a shared architecture design, which is completely novel, considering the existing analytical models developed so far towards fault recovery. In general, the failure recovery of our modeling is found to be affected in terms the availability of the shared resources among the MNOs.

4.1. Introductory Statements

4.1.1. Concept Visualization

Existing recovery mechanisms make backhaul networks fault-tolerant. Fault tolerance refers to the ability of the network to reconfigure and re-establish communication upon a failure. Usual recovery mechanisms that deal with network failures can be divided into protection and restoration. The protection mechanism activates in advance backup resource that will be used in case of failure, while the restoration mechanism takes over backup resource upon a failure; that is why protection mechanisms can recover quickly but are more demanding in terms of resource. Restoration mechanisms are less demanding when it comes to resource and therefore may be less costly than protection mechanisms in term of initial investments, but they generate longer service disruption. This service disruption can present one of the most important impacts for the network operator in the form of the revenue loss and business disruptions.

Having said this, in this chapter, we introduce a novel fault recovery scheme through link-bandwidth sharing among different MNOs. We first develop an availability-analysis model for connections with different protection schemes (i.e. dedicated protected and shared protected). Through this model, we show how a connection's availability is affected by resource sharing. Based on the analytical model, we then develop our fault recovery model. Our model for recovery and re-routing does not require any additional resources and therefore our restoration scheme is less demanding when it comes to availability of redundant resources and therefore less costly than protection mechanisms in term of initial investments, while at the same time providing faster recovery against failures. To illustrate this, we begin by demonstrating the availability of wireless communication networks supported by microwave backhaul links while two different MNOs share their working paths as an alternative for backup paths. This will help in tackling the high bandwidth requirements apart from serving as a backup under link failure situations without any additional cost investments. With the analytical evaluations of the availability gain in-hand, we proceed further towards a probabilistic model for fault restoration to reroute traffic flows in the event of link failures, which is based on the availability modeling.

4.1.2. Organization of the Chapter

This chapter is divided into two parts. The first part of this chapter deals with an analytical model providing an availability analysis of the shared backhaul architecture. This is completely different from what has been done in the previous chapter. The motivation to carry out another availability analysis is that the results of this model form the basis for a novel fault recovery and re-routing model which is detailed in the latter part of this chapter. With this basis, the rest of

the chapter has been structured as follows. In the first part of this chapter, we analyse the availability gain for wireless backhaul architecture that is evolved out of sharing between two different MNOs. We make a comparative analysis of the availability modeling of our design to the classical 1:1 backup path protection design. We claim that it is feasible to come-up with such a far more efficient network design that can handle link failures at lesser cost investments while still being to able to offer as much availability as offered by the 1:1 backup path protection design. With the availability analysis in hand, in what follows next in the second part of this chapter, we go forward by presenting a probabilistic model for fault restoration that aims at re-routing user traffic between different MNOs' backhaul, thus improving the overall transport network reliability of the wireless backhaul.

4.2. Current Objectives and Contributions

Now, in this work, focusing towards link-bandwidth sharing within the backhaul of different MNOs, we furthermore target the following aspects:

- Provide a systematic optimistic illustration that exemplifies a completely new availability analysis to evaluate the availability gained within MNOs' backhaul when they share their backhaul link-bandwidth together.

- Develop a path-based proactive restoration analytical model based on probability theory that enables to understand how the user traffic is re-routed around a failing network component, when MNOs share their backhaul link-bandwidth together. We call this as ROFL (Restoration of Failures through Link-Bandwidth Sharing).We claim that with a flexible recovery scheme, backup capacity can traverse via physically separate routes of another MNOs backhaul and therefore the problem to interrupt both the primary path and the backup path of different MNOs simultaneously, is therefore not likely at all.

4.2.1. Significance of our Results

Within the context of this chapter, we have kept our model and assumptions relatively modest to explore different options for exhibiting the availability gained because of sharing between different MNOs. Nevertheless, the results presented in this chapter enable to understand that the assumptions are reasonable. Furthermore, the probabilistic model in place for fault restoration provides a solution to tackle the problem of link failures by encompassing a scheme by which restoration techniques can be enhanced to by-pass the failed equipment before routing convergence actually takes place. By employing our model, we demonstrate how a node in a microwave backhaul network shared between different MNOs can apply this to improve resilience, thus improving the packet delivery capability. We have supported our approach

analytically as well as numerically. The approach presented here can serve as a practicable utility to exploratively evaluate sharing strategies. Furthermore the insights obtained here gives input into further R&D, MNO and regulators, especially on addressing technical interdependencies resulting from sharing, providing a better Quality of Experience (QoE) for the end-users.

4.3. Analytical Modeling

As a first step, we analyze the availability gained when MNOs decide to "divide and share" their link-bandwidth and utilize the resources of (an)other MNO(s) as their backup resource. For the discussion that follows, we restricted our model with only two MNOs: MNO A = Donor 'D' and MNO B = Recipient 'R' that agree to share their backhaul link-bandwidth (from now-on this convention is strictly followed). A Donor 'D' is the one (i) who is not stumbled by link/node failures; (ii) who is operating under normal conditions and (iii) who has sufficient bandwidth reserved that can be shared according to Service Level Agreement (SLA). A Recipient 'R' is the one who encounters link/node failure and thus requires the "reserved" bandwidth of the donor. Nevertheless to say, our solution can be practically extended allowing any number of MNOs to divide and share, provided they are all within the same geographical zone, i.e. within one country.

4.3.1. Formal Definition

The end-to-end path availability A_{ij}, for a connection C on a microwave link with end points (i, j) along a set of microwave links denoted by E, can be computed as the product of availabilities a_{ij} of all individual links. Formally,

$$A_{ij} = \prod_{i,j \varepsilon E} a_{ij} \ \forall C \tag{1}$$

4.3.2. Analytical Model for 1:1 Path Protected Connection

In the traditional 1:1 protection, every MNO employs an additional backup path in addition to the primary path. Connections are carried by one primary path, i.e. the working path W and protected by one backup path B which is link disjoint. When working path W fails, traffic will be switched to B as long as W is unavailable for a connection C. Therefore, the total availability of the entire backhaul network is computed as:

$$A_{ij} = A_W + [(1 - A_W) \times A_B] \ \forall C \tag{2}$$

This can be otherwise written as,

$$A_{ij} = [1 - (1 - A_W) \times (1 - A_B)] \, \forall C \tag{3}$$

where, A_W is the availability of the working path and A_B is the availability of the backup path. For our illustration here, we restrict ourselves with this protection scheme, since our aim here is to prove that it is possible for the MNOs to have a protection scheme that provides as much protection as the 1:1 scheme above but with lesser cost investments.

4.4. Analytical Model for Link-Bandwidth Sharing

Now according to our earlier design, we eliminate the need for provisioning the additional backup path B in each of the MNO's backhaul and compensate this by a separate share of "spare" resource S that is always reserved on the working path of each of the MNOs' backhaul for their respective recipient. This spare resource can be used as the backup path by the recipient to carry extra traffic that would be preempted if the normal traffic was disrupted by a failure. We represent the availability of this spare resource as A_S.

To deduce the total availability of the entire backhaul that is evolved out of sharing between two different MNOs, we first need to deduce the individual availability of each MNO separately. First, the availability of the donor is as follows:

$$A_{ij}(donor\ alone) = A_{W1} + [(1 - A_{W1}) \times A_{S2}] \, \forall C \tag{4}$$

where A_{W1} is the availability of the resource (working path only) of the donor. A_{s2} denotes the availability of the "spare" resource which is reserved for the donor on the recipients' working path. This is vice versa in case of the recipient also.

$$A_{ij}(recipient\ alone) = A_{W2} + [(1 - A_{W2}) \times A_{S1}] \, \forall C \tag{5}$$

where A_{W2} is the availability of the resource (working path only) of the recipient. A_{s1} denotes the availability of the "spare" resource which is reserved for the recipient on the donor's path.

If the sharing resources are dedicated to a connection C then, let's say, when the working path W2 of the recipient fails, traffic will be switched to working path W1 of the donor as long as W2 is unavailable. It is now equivalent of having a dedicated working path W and a backup path B, where analogously working path W (that failed) is equivalent to W2 of the recipient and backup path B is equivalent to W1 of the donor. Therefore, the total availability of the entire backhaul network that has evolved out of sharing the backhaul between two different MNOs can be

deduced as follows:

$$A_{ij\ (total)} = \{A_{W1} + [(1 - A_{W1}) \times A_{S2}]\} + \{A_{W2} + [(1 - A_{W2}) \times A_{S1}]\}\ \forall C \qquad (6)$$

Let's assume that both the MNOs have agreed to reserve the same amount of spare resource (link-bandwidth) for each of them in their SLA. Then, A_{S1} becomes equal to A_{S2}.

$$\text{i.e., } A_{S1} = A_{S2} = A_S \qquad (7)$$

Now, (6) becomes,

$$A_{ij\ (total)} = \{A_{W1} + [(1 - A_{W1}) \times A_S]\} + \{A_{W2} + [(1 - A_{W2}) \times A_S]\}\ \forall C \qquad (8)$$

This can be otherwise written as,

$$A_{ij\ (total)} = \{[1 - (1 - A_{W1}) \times (1 - A_S)]\}.\{[1 - (1 - A_{W2}) \times (1 - A_S)]\}\ \forall C \qquad (9)$$

Therefore,

$$A_{ij\ (total)} = A_S \times [1 - (1 - A_{W1}) \times (1 - A_{W2})]\ \forall C \qquad (10)$$

where A_{W1} represents the availability of the working path of the donor which excludes the resource reservation made for the recipient. Similarly A_{W2} represents the availability of the working path of the recipient which excludes the resource reservation made for the donor. In a typical real microwave chain topology, just as in figure 1, there are usually E links, where E denotes the number of hops or the set of all microwave links between source s and destination d. At times MNOs extend the number of hops to extend coverage to rural and/or remote areas. Under such occasions, the total availability becomes,

$$A_{ij} = \prod_{i,j=1}^{E} A_{Sij} \times \left\{ \prod_{i,j=1}^{E+1} \left[1 - (1 - A_{W1ij}) \times \left(1 - A_{W2ij}\right)\right] \right\} \qquad (11)$$

where, A_{Sij} represents the availability of the shared spare resource that is reserved all along E hops and A_{w1ij}, A_{W2ij} represents the availabilities of the working paths of the donor and the recipient that excludes the resource reservation for backup resource for each of them on all E hops respectively. Therefore from (3) and (10) as evident as it is, the additional term A_S provides the availability that is equivalent of an additional backup path as included in the traditional 1:1 provisioning strategy for path protection. Towards a further extended analysis, looking at a country with more than two different MNOs, let's say K different MNOs, where all of them are willing to co-operate and share (e.g. India), there might be situations where more than one MNO

would want to share $\mathcal{N}$ working path link-bandwidth. In this case, all possible K MNOs would have $\mathcal{N}$ link-bandwidth sharing situation. For this case, A_{Sij} is computed by first calculating all $A_{Wxij}(x = 1,2, \dots K$ and $A_{Wyij}(y = x + 1, \dots K)$ individually. Then the total availability A_{ij} is computed. In a simple form, we can state the generalized availability of a connection C with K MNOs sharing $\mathcal{N}$ backup path is as follows:

$$A_{ij} = \prod_{i,j=1}^{E} A_{Sij} \times \left\{ \prod_{i,j=1}^{E+1} \left[1 - \left(\prod_{x=1}^{K} D_{Wxij} \right) \times \left(\prod_{y=x+1}^{K} R_{Wyij} \right) \right] \right\} \quad \forall C \tag{12}$$

where,

$$D_{Wxij} = (1 - A_{Wxij}) \text{ and } R_{Wyij} = \left(1 - A_{Wyij}\right).$$

Thus, the above availability analysis not only convinces us that sharing the backhaul link-bandwidth by excluding the need for an additional backup path results in reduced cost investments but also enables us to understand the additional availability that the MNOs gain when they share their working paths with (an)other MNO(s).

4.5. Towards A Probabilistic Model for Fault Restoration through Link-Bandwidth Sharing

4.5.1. General Problem Statement

With the availability analysis put forward, we proceed further to the next step to illustrate how fault restoration within the MNOs' backhaul is carried out and thus recovery of traffic from the recipient's backhaul to the donor's backhaul takes place. To illustrate this, we narrowed-down the architectural overview in figure 16 to a simple block diagram representation in figure 17 for the ease of understanding. Essentially, our proposal encompasses the 4G-LTE architectural design.

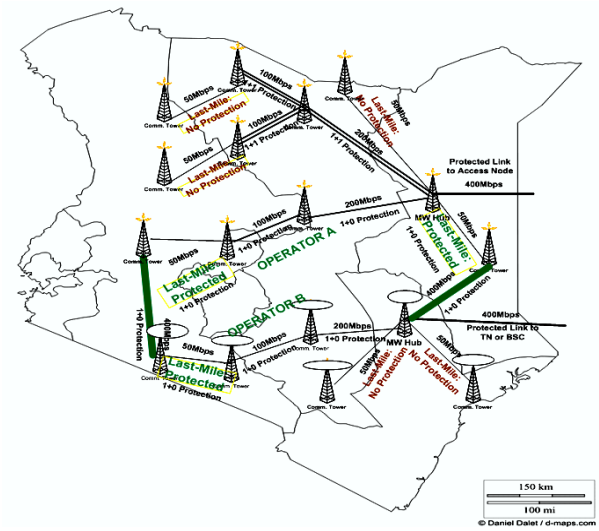
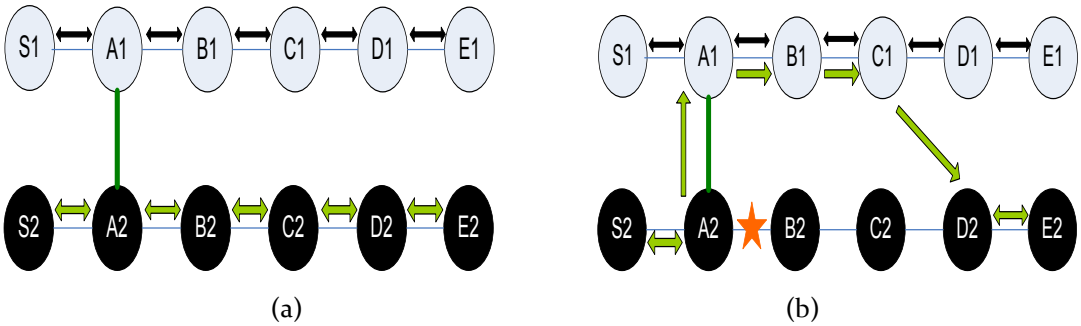


Figure 16: An illustrative example network topology portraying resiliency design flow using infrastructure sharing within the country Kenya.



a) Traffic flow design with infrastructure sharing under normal conditions.

b) A situation where there is a fault and /or network congestion between the last-mile and middle-mile links within the backhaul.

Figure 17: Recovery from link congestion through backhaul sharing.

In figure 17(a), S1, S2 indicate the end consumers for MNO A and MNO B respectively. A1, A2 are the last-mile links of both MNOs that are connected using an additional link. B1, B2 are the access nodes which is a part of middle-mile, C1, C2 represents the aggregation nodes, D1, D2 denotes the core network such as the Service Gateway (S-GW) and Packet Data Network Gateway (PDN-GW) and finally E1, E2 represents the Internet. The initial flow of traffic for MNO A is as follows: : S1↔ A1↔ B1↔ C1↔ D1↔ E1 and similarly for MNO B is S2↔A2↔ B2↔ C2↔ D2↔ E2, each of them carrying their own traffic in their own backhaul respectively. The edge routers maintain tables which record all the information including the traffic type, consumed bandwidth, its path. For any disruption that occurs in the last-mile, the node on either side of the failure reroutes the traffic in the other direction due to the backup ring. For e.g. from figure 17 (b), say for MNO B-the recipient, i.e. when the traffic between A2 and B2 is interrupted, the traffic has to be re-routed and take a different path such as: S2↔ A2↔ A1↔ B1↔ C1↔ D2↔E2,

depicted in figure 17(b). Under such situation, the failure has to be detected and thus the interrupted flow along the failed link is re-routed from source to destination across the donor's backhaul links. The unaffected flows across the routing paths of the donor are not disturbed. At this time, the node S2 will not know the primary path S2↔A2↔ B2↔ C2↔ D2↔ E2 is invalid after all. During the restoration process, each node executes restoration upon a failure without any coordination of other nodes.

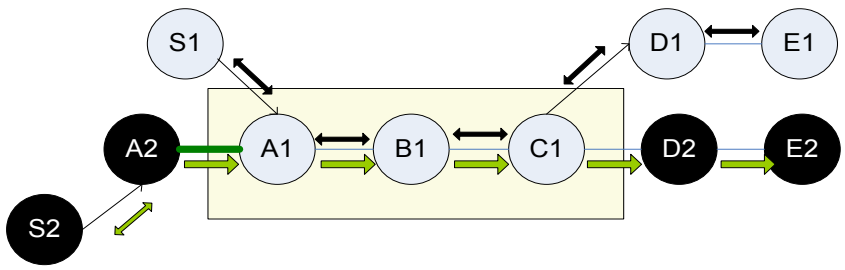


Figure 18: Traffic flow design with infrastructure sharing under faulty conditions with arrow on the bottom indicating traffic from the recipient and arrows on the top indicates the traffic of the donor.

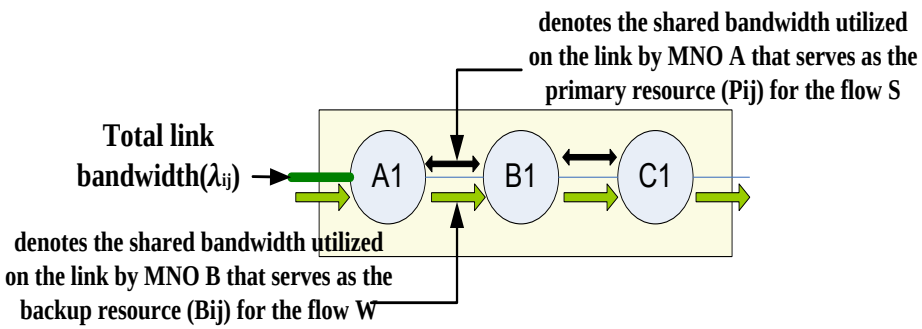


Figure 19: Backhaul link-bandwidth allocation through sharing.

4.5.2. Assumptions and Conditions

The following assumptions and conditions are adopted for modeling our fault restoration scheme:

- This thesis (chapter) exclusively focuses on how fault restoration takes place and the user traffic is re-routed between different MNOs backhaul architecture, with the assumption that there is enough spare capacity on the donor's backhaul.

- It is well-known that single-node failures are different from single-link failures in that the failure of a node disables all the links directly connected to it. However, for the sake of simplicity, based on the results of [47], we narrowed-down the problem of node failures to link failure problems in this chapter.

- We determine the "UP" state of every microwave link between each node independently. Furthermore, when a link failure is encountered, it is the node that is on either direction of the failed link that will immediately switch the traffic around the backup path. We call this as "Host Node". For e.g. from figure 17 (b), the host node is the node A2 of MNO B (the recipient) and source node is the node S2.

- We adapt to a restoration scheme where backup paths are pre-computed. As elaborated earlier, there might be situations where there are K different MNOs willing to divide and share $\mathcal{N}$ working path link-bandwidth. Under such occasions where there are multiple backup paths for a single destination, only one of them will be chosen during failure recovery.

4.5.3. Network Model

Formal Notations: The physical backhaul network topology is represented as a weighted graph G = (V, E) where V is the set of the vertices of the graph containing the nodes (edge routers and switches) of the network. The set E of the edges of the graph contains the links of the network such that any two distinct nodes V_i and V_j forms an edge $ij \in E(G)$ if there is a direct link between them. Therefore, the total number of links that constitutes the backhaul network topology becomes $\sum_{ij\varepsilon E} l_{ij}$, where l_{ij} denotes a link between the microwave edge ij . All links are assumed to be bidirectional. Thus, our wireless microwave backhaul network that has evolved out of sharing between MNOs can be analyzed as a random bi-directional graph.

Objective: Let C be an incoming connection request on the recipient's backhaul between source s and destination d on a microwave link(i, j).The k-th connection request for the recipient is thus represented as $C_{ijk,R}$. Our objective is to model how to successfully restore this connection upon a failure and re-route it across the backhaul of the donor.

4.5.4. Probabilistic Modeling for Fault Restoration

Recovery from a network failure predominantly takes into account two important performance metrics for restoration schemes. They are (i) the end-to-end connection blocking probability and (ii) the average recovery and re-route times. On a general note, the 50ms restoration latency and 50% restoration capacity overhead associated with SONET BLSR rings are benchmark figures for these two metrics. In order to evaluate the above mentioned two metrics, we thus go forward with our proposed model.

Degree of Re-routability (DoR): In order to determine the blocking probability of a

connection, as a first step, we calculate the probability of a failed connection $C_{ijk,R}$ to be re-routed successfully. To do this, we begin with defining the term Degree of Re-routability (DoR). This is defined by the probability of a failed connection $C_{ijk,R}$ within the recipient's backhaul to be re-routed successfully, within $\mathcal{N}$ attempts, with each attempt signifying each available backup path on one of the donor's backhaul. Therefore, DoR for any of the first $\mathcal{X}$ attempts can be formally written as:

$$DoR_{Single_MNO} = \mathcal{P}_{C_{ijk,R}}(\mathcal{X} \leq \mathcal{N}) = 1 - (1 - \mathcal{P}_S)^{\mathcal{N}} \tag{13}$$

The above equation takes into account that there is only one donor for an MNO who is faced with a link failure. As discussed earlier in the availability analysis, if there are K different MNOs, who are willing to share their available link-bandwidth at the same time with one recipient, then the probability of a failed connection $C_{ijk,R}$ to be restored successfully in any of the first $\mathcal{X}$ attempts is given by:

$$DoR_{K_MNO} = \mathcal{P}_{C_{ijk,R}}(\mathcal{X} \leq \mathcal{N}) = \prod_{i=1}^{K}[1 - (1 - \mathcal{P}_S(i))^{\mathcal{N}}] \tag{14}$$

where, $\mathcal{P}_{C_{ijk,R}}$ is the probability of successfully recovery a failed connection $C_{ijk,R}$, across the total available shared bandwidth $A_{ij(total)}$ shared out of K different MNOs as in (12) and $\mathcal{P}_S$ is the probability of successfully recovery a failed connection across the total available shared bandwidth $A_{ij(total)}$ as in (10). In practice, this probability to successfully re-route a failed connection should presumably be higher on the first attempt if the backup path selection algorithm is optimized perfectly. With the probability of successful recovery in hand from (13) and (14), we proceed to determine the probability of unsuccessful attempts before a successful restoration. This is given as,

$$\mathcal{P}_F = (1 - \mathcal{P}_{C_{ijk,R}})^m, 0 < m < \mathcal{X} - 1 \tag{15}$$

where, $\mathcal{P}_F$ is the probability of a connection $C_{ijk,R}$ to be refused by the donor. m denotes the number of failed attempts. This probability of a connection being refused depends upon various factors such as abrupt spike in traffic load, unstable traffic characteristics on the donor's backhaul and/or unacceptable QoS request by the recipient. Therefore the blocking probability of a failed connection $C_{ijk,R}$ on a recipient's backhaul to traverse through the donor's backhaul is given by,

$$BR_{Recipient} = b.\sum_{ij\varepsilon E} C_{ijk,R} \tag{16}$$

where, $BR_{Recipient}$ is the blocking rate of the recipient and b is the blocking probability that is determined from (15).

Recovery and Re-Route Times (RRT): The next performance metric of interest is the Recovery and Re-route Times (RRT). We define RRT as the total mean time ($E(T_{RRT})$) taken for a connection $C_{ijk,R}$ to be re-routed successfully from a recipients' backhaul onto a donor's backhaul. In other words, RRT is the sum of the mean total delay encountered during each unsuccessful attempt $\left(E(T_{failed_attempt})\right)$ and the sum of the mean total delay experienced by a connection traversing Emicrowave hops across a backhaul topology $\left(E(t_P + t_C)\right)$.

Firstly, to determine $E(T_{failed_attempt})$, we rely upon the mean number of attempts $E(m)$. This is clearly based on the above determined probabilistic values of successful and unsuccessful attempts to re-route a failed connection. From (15), the mean number of unsuccessful attempts is given by,

$$E(m) = \frac{\sum_{m=1}^{\mathcal{X}-1} \mathcal{P}_F}{\mathcal{X}} \tag{17}$$

Or, it can be written as,

$$E(m) = \frac{\sum_{m=1}^{\mathcal{X}-1} \left(1 - \mathcal{P}_{C_{ijk,R}}\right)^m}{\mathcal{X}} \tag{18}$$

Now, we denote the total delay involved in the mean number of unsuccessful attempts as $(T_{failed_attempt})$.Thus, the mean total delay for each unsuccessful attempt is therefore:

$$\mathrm{E}(T_{failed_attempt}) = \frac{1}{m}\left\{\sum_{m=1}^{\mathcal{X}-1}(T_{failed_attempt}) \times \frac{\sum_{m=1}^{\mathcal{X}-1} \left(1 - \mathcal{P}_{C_{ijk,R}}\right)^m}{\mathcal{X}}\right\} \tag{19}$$

Secondly, we should determine $E.(t_P + t_C)$. It involves the computation of two separate delays. First, to determine the mean propagation delay $E(t_P)$. In a typical real microwave chain topology, just as in figure 1, when there are usually E hops, if the fault occurs exactly at the last-mile as indicated in the figure 2(b) (which is indeed the major focus of this chapter), the backup route towards the donor's backhaul may be short and restoration may be fast since the last miles are connected. If the fault occurs at the middle-mile, i.e. between B2 and C2 or near the core network, i.e. between C2 and D2, the restoration may take time due to the fact that the connection $C_{ijk,R}$ traverses a much longer path. Thus, the mean propagation delay $E(t_P)$ experienced by a connection $C_{ijk,R}$ is,

$$E(t_P) = \frac{\sum_{h=1}^{E} t_P}{E} \tag{20}$$

The above estimated propagation delay for a connection $C_{ijk,R}$ is assumed to be linearly proportional to the number of microwave hops. In reality this means, a connection traveling E microwave hops will experience mean propagation delay $E(t_P)$ where t_P is a delay constant

depending on the characteristics of each microwave hop. Next to determine the mean computational delay $E(t_C)$. $E(t_C)$for a successful attempt is the sum of store-and-forwarding delays and processing delays at each hop E (queuing delays are assumed to be minimal compared to a fixed time t_C representing packet processing including acceptance/rejection decisions and packet forwarding).

Therefore, the total mean time ($E(T_{RRT})$) taken for a connection $C_{ijk,R}$ to be re-routed successfully from a recipients' backhaul onto a donor's backhaul is given by:

$$E(T_{RRT}) = E(T_{failed_attempt}) + E(t_P + t_C) \tag{21}$$

In reality, any connection due to microwave backhaul sharing between different MNOs will encounter much less downtime in the presence of any number (single link or even double link) of link failures if the contribution of the reconfiguration time from primary path of one MNO to backup path of another MNO is cautiously taken care, just as proposed above in our model. Nevertheless, in practice, it is relatively negligible, usually on the order of a few tens of milliseconds with respect to the manual failure repair times which are on the order of hours and the connection's holding time on the order of weeks or months, especially in emerging economies, due to the lack of sophisticated logistics.

4.6. Illustrative Numerical Evaluation

Number of Connnections Provisioned: Figure 20 demonstrates the number of connections provisioned with the two different approaches by simulating at least 10000 to 20000 connection requests, for different network loads on random network topologies. We observe that there are more connections provisioned with our link sharing approach than the 1:1 sharing approach. This is essentially due to the additional spare resource obtained in Eq.(10) that was available. However, as the network load increases, it is obvious that both the provisioning schemes suffer from slight network congestion.

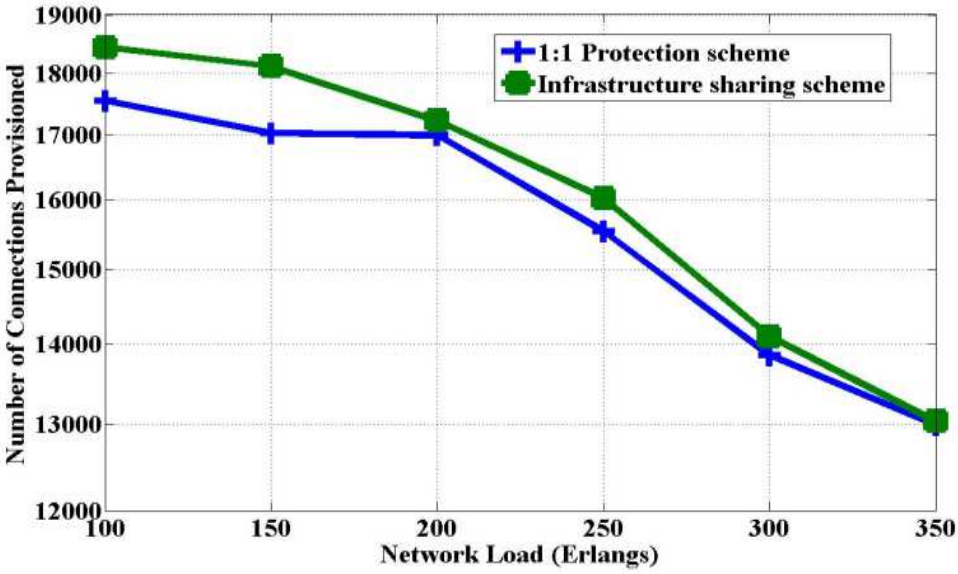


Figure 20: # of connections provisioned using both schemes.

Blocking Probability: The blocking probability is a measure of the number of connection requests rejected against the total number of connection requests. The main measure here is to compare the performance of the 1:1 based approach and our approach. We find that a connection is less likely to be blocked by our approach than the 1:1 approach. Figure 21 compares the blocking probabilities for the 1:1 protection scheme and our approach, obtained by solving Eq. (16). Again, this is also due to the fact that we were able to gain more availability with our provisioning approach.

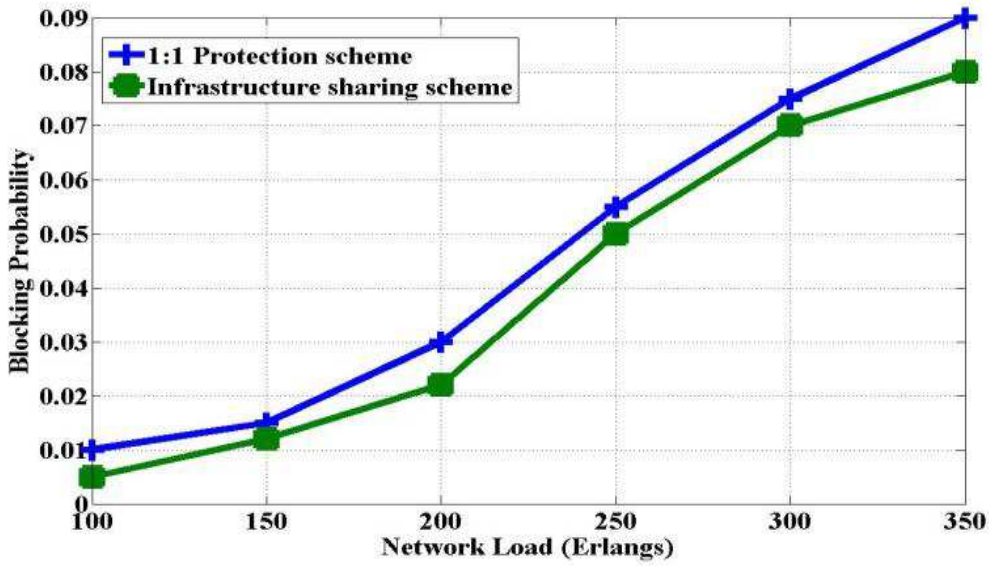


Figure 21: Blocking Probability values for both schemes.

Recovery and Re-route Times (RRT): The third part of evaluation is to illustrate the recovery and re-route time delays on the network as in figure 22. Eq. (21) was essentially used for this evaluation. According to our model, RRT basically depends the blocking probability, which depends on the availability of resources. Just like the previous evaluations, we find that a connection encounters lesser delay by our approach than the 1:1 approach. This is due to the fact that every incoming connection gets sufficiently more resources by our approach than the 1:1 approach and thus less congestion.

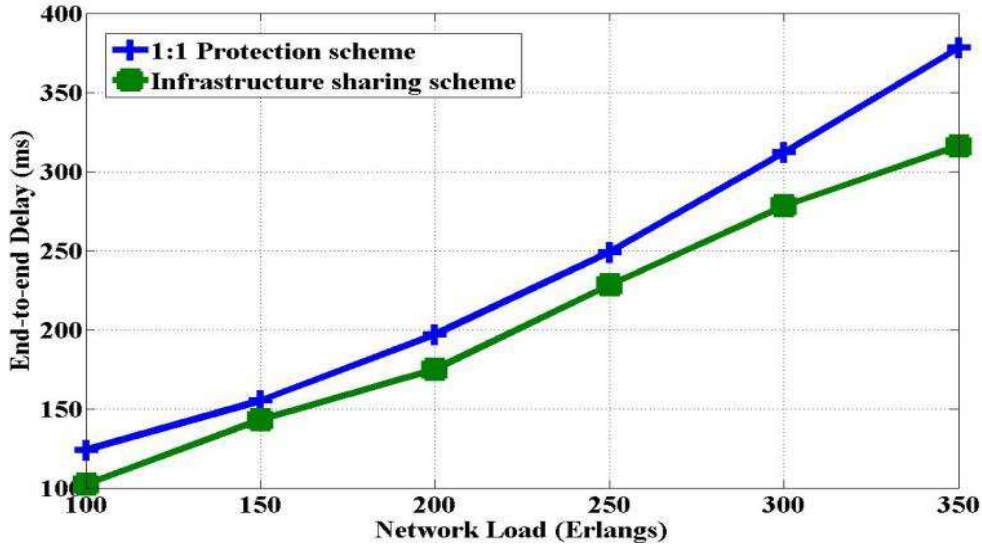


Figure 22: End-to-end delay measurement for both schemes.

4.7. Concluding Discussions

The fault recovery behavior of an end-to-end shared architecture is modeled and presented in this chapter. Analytical models are developed that provide recovery time of the newly proposed shared architecture. Here, the recovery behavior and interactions with the available shared resources are studied. The theoretical investigations through the development of analytical models carried-out here give us a deeper understanding of the potential of our architectural design and our sharing mechanism. We presented the equations that represent the trade-off between the value of the required accuracy of the fault recovery and re-routing, in correspondence with the value of the systems availability. Here, we quantify the restoration behavior of the network architecture in association with the availability of shared resources. We apply a re-dimensioning technique, which is a logical step in effectively re-balancing the network resources and addressing the issue of fairness among MNOs. The tradeoff in utilizing such measures is clearly shown in terms of the typical as well the worst case additional capacity required at each link and node.

The results clearly outline the limitations of going to a best-effort mode for non-critical applications and motivate further study in both traffic engineering techniques as well as measures for systematically over-provisioning the network to allow graceful degradation. Furthermore, our results motivate a more careful study of classification of applications and traffic engineering as well as detailed post-failure management plans to better address the needs of reliable communication within such shared scenario among multiple MNOs. To this end, we go forward to propose as future work that we are currently investigating techniques to maximize post-failure performance given a set of constraints as discussed above, but the discussion is outside the scope of this work.

Part III

Optimization Techniques for Network Survivability

"Programming is one of the most difficult branches of applied mathematics; the poorer mathematicians had better remain pure mathematicians." — ***Edsger Dijkstra, Computer Scientist, Inventor of Shortest Path Algorithm.***

Chapter 5

OpenRoutes: Multi-operator Cooperative Routing for the Survivability of Backhaul Networks

With analytical evaluations in-hand, the next part of the dissertation deals with optimization frameworks. In this chapter, we identify the complexities in routing and dynamically rebalancing traffic across diverse end-to-end available paths in response to individual failure events along a backhaul network which is built out of sharing between different MNOs. The optimization objective that we have set is straight-forward here. There are different MNOs within a country who has built the nation's backhaul network topology together. Now, when one of them encounters a link/node failure at a specific geographic location, the disrupted connections must be re-routed appropriately, across the most optimal path of the topology, according to their traffic class. With this being the focus, this chapter centers on three routing heuristics for the survivability of backhaul networks. Specifically, we provide a methodology for selecting the most optimal candidate alternative path according to the QoS requirements of the disrupted traffic, from a set of multiple paths computed. For reasons which are made clear later, we call the resulting scheme as 'OpenRoutes'. Our system provides the network designer with some trade-offs in the space of redundancy through additional backup links shared with another MNO against the size of a failure domain, so you can—in theory—build larger, less- redundant failure domains.

5.1. Introductory Statements

5.1.1. Concept Visualization

Network survivability is an important consideration in network design and its real-time operation. In order to avoid the data loss that might result due to network failure situations, various protection and restoration mechanisms have been proposed and studied in the literature [48]-[56] to recover traffic after a failure occurs and before the failure is physically repaired. Path protection in communication networks is an end-to-end protection scheme used in connection oriented circuits in different network architectures to protect against inevitable failures on service providers' network that might affect the services offered to end customers. Any failure occurred at any point along the path of a circuit will cause the end nodes to move/pick the traffic to/from a new route. Other techniques to protect telecommunications networks against failures are: Channel Protection, Link Protection, Segment-Protection, and P-cycle Protection.

The current state of the art in protection and restoration techniques [57]-[60] lead to the understanding that fault-tolerant designs comes with a cost and that diversification in multiple forms [61]-[65] could be an enabler to bring down such cost. One such theory-to-practice break-through solution is the shared backup path protection (SBPP). Here MNOs utilize their backup paths when the traffic demands change over time due to failures and/or traffic spikes, in order to reduce the cost invested for redundancy. It allows bandwidth sharing amongst backup paths leading to some bandwidth savings while continuing to guarantee 100% failure recovery. Within the single-failure context, 100% failure recovery condition is expressed with the condition that the working paths of the backup paths that share bandwidth must be disjoint. Routing for shared protection aims to identify the working and backup paths that minimize the total bandwidth consumption. Here we consider the problem for the networks with bandwidth guaranteed connections such as MPLS, ATM or OpenFlow networks. Existing solutions follow two paradigms: static routing (off-line) and dynamic routing (on-line). In static routing, the network traffic, i.e. requests for connections, are assumed to be stable and are given as input to the routing model. The working and backup capacities are then optimized for every network links, see, e.g., in [66]–[69]. Conversely, dynamic routing is proposed for dynamically changed traffic and requests for connections are routed one at a time without taking into account any information on the future requests, see, e.g., [70]–[72]. As the time goes, the total allocated bandwidth will be larger (less optimized) than as if routing policy with a global view on the arriving connections or at least a forecast about them had been applied. It is known and has been already studied in [73], [74] that, if we use dynamic routing but reorganize the existing paths in the network, working bandwidth could be freed and increased bandwidth sharing for the backup bandwidth can be obtained leading to a greater resource saving. The reorganization

includes finding alternate paths for the existing working and backup paths and then rerouting some working and backup paths. Moving the traffic of a connection on a new working path implies service interruption, and therefore a disorder for the user, that is to be avoided as much as possible. However, backup paths are generally inactive until a failure occurs. They can be replaced by new ones without any impact on service availability. Therefore, a reorganization scheme in which only backup paths are rerouted offer a good mean to answer to the drawback of the possible bandwidth waste involved in dynamic routing due to the uncertainty about estimating and anticipating the future connection requests.

There are multitude of literature reviews and research articles that talk about QoS routing using maximally disjoint paths; break-through works that describe how to load-balance through a network topology. All these works focus precisely on one ISP/operator network topology. Our work extends to the next level of routing with constraints on a topology that is evolved out of sharing between two or more different MNOs. That said, there are several constrains that has to be tackled in such a situation. We point out a few of them. End-to-end routing in connection-oriented broadband networks, which satisfies end-user quality of service (QoS) constraints, is an extremely complex problem. While, QoS is measured in many different ways such as signal quality, service availability, service reliability, restoration time, service restorability, etc. our interest is in the availabilities of service paths (i.e., connections) since availability is one of the key concerns of customers. The term re-routing in this dissertation thesis refers to the change of data transmission from primary path (say, from Operator 1) to a backup path (say, to Operator 2) after a failure in the data-plane. The complexity of the problem is compounded in multi-domain, multi-provider networks for a number of reasons. For example, operators of some public networks may not wish to fully disclose their internal network topologies and a highly detailed picture of their quality of service capabilities, as this information is sensitive (e.g. for their competitors). However, they do not wish to turn network traffic away, which would traverse their network regardless of the source, as it represents revenue. These two facets are in contradiction. Another challenge is that individual operators may wish to use their own internal routing algorithms, at least for routing within their own domains. End-to-end routing is typically an all or none proposition, i.e. it needs all the QoS information from all the underlying networks, in order to be able to satisfy (optimally or otherwise) the desired end-to-end QoS constraints of the end user. This is in direct contradiction to the desire of network operators to have their own routing algorithms, since they need and use internal routing algorithms to compete against each other. The efficient solution to this problem will become one of the most important challenges facing competing/cooperating public broadband network operators in the future, as the customer demand for global broadband networks, which span public network operator boundaries, grows. We propose thus solutions for rerouting backup paths with objective to seize the backup capacity, especially considering a scenario when multiple operators (multi-domain)

are involved in sharing their available paths (resources). The solutions differ from the backup path reroute solutions, see, e.g., [75], which aim to improve the service availability at dual failures.

5.1.2. Current Objectives and Contributions and Organization of the Chapter

Within the context of dynamic routing models for shared path protection in multi-operator networks, in this chapter, we identify the complexities in routing and dynamically rebalancing traffic across diverse end-to-end available paths in response to individual failure events along a backhaul network *which is built out of sharing between different MNOs*. Unlike most previous work, we present a framework in this chapter to provide differentiated protection services to meet customers' availability requirements cost effectively. The objective here is straight-forward. There are different MNOs within a country who has built the nation's backhaul network topology together. Now, when one of them encounters a link/node failure at a specific geographic location, the disrupted connections must be re-routed appropriately, across the most optimal path of the topology, according to their traffic class. For instance, if a disrupted connection belongs to real time (conversational/streaming class), then it can not tolerate a new alternative path with high delay. Alternatively, a traffic class belonging to the best effort type (interactive/ background class) may tolerate medium to large delay values, but may require alternative paths with high bandwidth. This complexity in routing is narrowed down while considering a topology with only two diverse paths which are provisioned: a primary/working path for one MNO and a secondary/backup path of another sharing MNO (i.e. two sides of a microwave ring network topology, just as in Chapters 3 and 4). Clearly, this is the simplest configuration, because there is only one alternative path for the disrupted traffic to be re-routed (The question on how to "split and share" the available bandwidth in that alternative path between MNOs has already been tackled by us in Chapter 6). As we move from simple (i.e. ring) to complicated (i.e. mesh/grid) network topologies (which is close to circumstantial realities in practical networks), determining diverse secondary path(s) which is disjoint/maximally disjoint from the failed/overloaded primary path becomes increasingly difficult and poses new uncertainties about path computation, load balancing together with QoS routing.

That being said, the present work centers on a restoration scheme for the survivability of wireless backhaul networks. Specifically, we provide a methodology for selecting the most optimal candidate alternative path according to the QoS requirements of the disrupted traffic, from a set of multiple paths computed. For reasons which are made clear, we call the resulting scheme as *OpenRoutes (MNOs open their routes for each other)*. Our network architecture has three key features:

Path Computation and routing: In our architecture, the routers do not compute (or recompute) paths, reducing router overhead and improving path stability. Instead, the management system computes paths that over sufficient diversity across a range of failure scenarios, including correlated failures of multiple links.

Path-level failure detection: The ingress routers perform failure recovery based only on which paths have failed. A minimalist control plane performs path-level failure detection and notification, in contrast to the link-level probing and network-wide flooding common in today's intra-domain routing protocols. This leads to simpler, cheaper routers.

Local adaptation to path failures: Upon detecting path failures, the ingress router rebalances the traffic on the remaining paths, based only on which path(s) failed not on load information. This avoids having the routers distribute real-time updates about link load and prevents instability. Instead, the management system pre-computes the reactions to path failures and configures the routers accordingly.

Precisely, our contributions sums-up to:

- A simple and systematic model illustration that exemplifies an entirely different approach to compute alternative disjoint paths with optimal capacity, in a wireless backhaul network *that has emerged out of sharing between different MNOs*, without affecting any of the other MNOs' existing traffic flows – detailed in Section IV.

- Consequently, the objective of our approach has been formulated using ILP, based on our model definitions. The proposed ILP formulations use the dual-simplex method linear programming, which essentially captures all the restraining conditions for computing multiple alternative paths, on every edge between any pair of vertices of our network topology - detailed in Section V.

- Since such ILP formulations are very complex to solve for medium/large networks, in what follows then, we appeal for three simple yet efficient heuristic algorithms. While there are several approaches to solve this kind of problem formulations, the first two of our heuristics extensively relies on the properties of the classical Dijkstra's algorithm [76], while the third one relies on the Ant Colony Optimization (ACO) meta-heuristic algorithm [77] - detailed in Section VI, VII.

- Our approach attempts to minimize network disruption cost-effectively, by maximizing the unused network resources, by appropriately selecting paths even

when the network links are under a high congestion level. This renders MNOs with a parameterized objective function to choose the desired paths based on traffic patterns of their end-customers - detailed in Section VIII.

5.2. Modeling OpenRoutes Restoration Scheme

5.2.1. Overall System Model

The physical backhaul network topology is represented as a weighted graph $G = (V, E, \Lambda, D, L)$ where V represents the set of the vertices containing the nodes (microwave towers, edge routers, switches, gateways etc). E represents the edges of the graph containing the links such that any two distinct vertices V_i and V_j form an edge if there is a direct microwave link $e \in E(G)$ between them for all $ij \varepsilon E$ and $(i, j) \varepsilon V$. $\Lambda : E \rightarrow Z+$ specifies link bandwidth on each microwave link. Delay function $D : E \rightarrow R+$ assigns a non-negative weight to each link e, denoted by a weight vector $\overrightarrow{w}(e) = (w_1^e, w_2^e, \dots, w_m^e)$. All links are assumed to be bidirectional. $k_{ij}^{(t)} \in L(G)$ denotes a disrupted connection request which has to be re-routed.

5.2.2. On Path Computation Model

Let V_s represent the source node and V_d represent the destination node. Let $P_{Primary} = \{ (V_s, V_{P1}), (V_{P1}, V_{h1}), (V_{h1}, V_{h2}), \dots, (V_{Pn}, V_d)\}$ denote the primary path which contains the set of edges between each pair of vertices, constructed by the MNO by default. We determine the "UP" state of every microwave link between each pair of vertices independently. Therefore, when a failure occurs in this path $P_{Primary}$, it is one of the nodes which is on either direction of the failed link that will immediately switch the traffic to a new alternative path, denoted by $P_{alt} = \{ (V_{B1}, V_{B2}), (V_{B2}, V_{B3}), \dots, (V_{Bn}, V_d)\}$ and thus the disrupted connection along the failed link is re-routed to the destination node V_d. We denote V_h as the fault-restoration node (adjacent to the failure). We call it as "Host Node". In practice, there are two nodes adjacent to failed link, i.e. $V_h = \{V_{h1}, V_{h2}\}$ and each of them tries to find $\mathcal{K}$ different alternative paths. However, through our approach, we pick the most optimal path according to the QoS requirement of the disrupted traffic, among the pre-determined set. $P(V_h, V_d) = \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}$ denotes the set of newly computed alternative feasible paths between host node and destination node.

A. **Perceptual Dimensions:** In our approach, we use the link quality metric values that correspond to the links of a path to compute the aggregated routing metric value of a path. Among the various link quality metrics proposed in the literature for wireless networks such as delay, bandwidth, distance (hop-count), bit error-rate etc., we choose distance (hop-count) and delay, as our general quality metrics. Thus, the aggregated

routing metric of a path is computed as the sum $\sum_i x_i$ of the link quality metric values x_i. This aggregated routing metric of a path is commonly monotonic, signifying that either $f\ (X, x) \leq X$ or $f\ (X, x) \geq X$ for any aggregated metric value X and any link quality metric value x, where f denotes the aggregation operator (i.e., summation $\sum_i x_i$). Clearly, if the link quality metric values are non-negative, then aggregated routing metric values of a path are monotonically increasing, while if link quality values are non-positive, then aggregated routing metric values of a path are monotonically decreasing.

B. **Shortest Paths based on Distance:** Therefore, as a first step, we proceed computing the shortest paths between V_h and V_d based on the distance. A shortest path is defined as the path with the smallest number of intermediate nodes and if there are no other paths from the vertex V_h to V_d of shorter length. This path is denoted as $P_S(V_h, V_d)$. The distance (length) from a vertex V_h to V_d, denoted as $\delta(V_h, V_d)$ is the length of the shortest path, formally represented as,

$$\delta(V_h, V_d) = |P_S(V_h, V_d)| \tag{1}$$

With this, we now introduce a new binary variable $\propto_{\mathcal{K}}^{k_{ij}^{(t)}}$ to determine if there exists atleast one alternative path for a disrupted connection $k_{ij}^{(t)}$ in the network topology for all $(i, j)\varepsilon V$ and ijε E at time instant t, defined by:

$$\propto_{\mathcal{K}}^{k_{ij}^{(t)}} = \begin{cases} 1, if\ \exists\ \mathcal{K} : \{\{(P_1 \cap P_2) \cap \ldots (P_{\mathcal{K}-1} \cap\ P_{\mathcal{K}})\} \neq \emptyset\ \} \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad Otherwise \end{cases} \tag{2}$$

C. **Shortest Paths based on Delay:** However, it is not straight-forward to ascertain that the path with the least distance $\delta(V_h, V_d)$ will have the minimum delay, because the delay function $D(e)\ \in G$ varies with time according to arbitrary values [30]. Therefore, now we extend further to formulate the shortest path computation based on delay. By adding the individual weights of each link associated with every path, the end-to-end delays of each path can be computed. Formally, this is represented as:

$$\tau_d = \sum_{e \in E} w_i^e\ ,\ \forall\ i\ \in (1, 2, \ldots m); m = \ number\ of\ links \tag{3}$$

Similarly, the delay of every other feasible $\mathcal{K}$ different alternative path is calculated as well. The minimal delay value corresponds to the most optimal shortest path. We call this as *Minimum Achievable Delay (MAD)* denoted by Δ. Thus,

$$\Delta = \{min\ \{\tau_d\} \mid \tau_d \in \{\tau_{d1}, \tau_{d2}, \tau_{d3}, \dots \tau_{d\mathcal{K}-1}, \tau_{d\mathcal{K}}\}\} \quad (4)$$

D. **Degree of Disjointness (DoD):** Following this, the next problem to handle here is to ensure that the $\mathcal{K}$ different alternative paths computed between V_h and V_d are maximally disjoint of exclusive dedication. Consequently, maximally disjoint paths increase dual link failure survivability effectively, i.e., the disrupted traffic can always be restored on all dual link failures between pairs of nodes, no matter if link failures occur sequentially or simultaneously in a specific geographic zone. Furthermore, constructing disjoint topology solutions removes the need to manually manage link costs, while adding only moderate complexity at the protocol level. Therefore, with the aim of constructing maximally disjoint paths efficiently between the primary path $P_{Primary}$(the path which contains the failed link and therefore the host node V_h) and backup path, we impose the *Degree of Disjointness (DoD)*. Degree of Disjointness of the new alternative path with respect to the primary path is defined as:

$$DoD\ (\varphi) = 1 - \frac{|P_{Primary}\ \cap\ P_{alt}|}{|P_{Primary}|} \quad (5)$$

If the value of φ is closer to 1, then the disjointness between the newly computed path and the failed primary path is maximum; 0 value indicates that the paths are maximally overlapping, indicating that the diversity between them is negligibly low. If the diversity is low, it implies that the probability of encountering a failed path once again is more. With these in hand, in what follows next, we define bandwidth parameters such that the pre-computed $\mathcal{K}$ different alternative paths satisfy the optimal capacity requirement[10] as well.

5.2.3. On Bandwidth Computation Model

In parametrizing this model, we converge on the terms *Unconstrained Bandwidth (B-UNCON)* and *Constrained Bandwidth (B-CON)* of a link e denoted by λ_{ij} and U_{ij}, respectively. Unconstrained Bandwidth is defined as the available bandwidth of a link which is not occupied by any of the flows of the network. Thus, a disrupted connection flowing through a B-UNCON link can fully exploit the available capacity. On the other hand, a B-CON link has already been occupied by some or many of the flows of the network and therefore available only for low priority pre-emptible traffic. The present-age edge routers' capability to maintain tables which record all the information including the traffic types, consumed bandwidth, its path etc. could

10 Optimal capacity is the required capacity of a path which MUST be sufficient enough to satisfy a disrupted connection request.

facilitate to identify B-UNCON links and B-CON links. This, in anyway, does not violate operator's privacy policy; because the MNOs reveal only if the link is filled-in or not. As a criterion for choosing the appropriate alternative path with the most optimal capacity according to the disrupted connection's traffic class, our algorithm chooses between B-UNCON and B-CON links of the network topology. This way, we take care of two very important factors: (i) a failed connection does not disturb a link which already has some or many of other MNOs' traffic flowing through it (ii) as well as, a failed connection is not rejected/dropped due to the fact that a link does not contain the optimal capacity.

With these parameters, we now introduce another binary variable $\beta_{\mathcal{K}}^{k_{ij}^{(t)}}$ to determine the availability of an alternative path with optimal capacity for a disrupted connection $k_{ij}^{(t)}$, for all $(i,j)\varepsilon V$ and $ij\varepsilon\ E$ at time instant t, defined by:

$$\beta_{\mathcal{K}}^{k_{ij}^{(t)}} = \begin{cases} 1, if \sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} .\lambda_{ij} \geq 1; \sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} .U_{ij} \geq 1 \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad Otherwise \end{cases} \tag{6}$$

5.2.4. Relaxing Reachability and Restricting Shareability

Through our multi-operator scenario, we want to demonstrate the survivability of backhaul networks with reduced amount of physical redundancy, by sharing the already existing physical nodes/links of the topology, among MNOs. Naturally, we shall assume that every vertex belonging to any MNO in the topology G is reachable from the host node V_h. Accordingly, we define the term *Length of Reachability (LoR)* of a new alternative path. It is defined as the ratio of the path length of P_{alt} to the path length of $P_{Primary}$ .This is done in order to minimize the length of the new alternative path and bring it as close as to the length of the primary path. This is defined as:

$$LoR\ (\partial) = \frac{|\ P_{alt}\ |}{|P_{Primary}|} \tag{7}$$

If the value of ∂ is closer to 1, it indicates that the length of the newly computed path is the same as the failed primary path. Nevertheless, the reachability of any vertex, say V_n from V_h is not enough to imply the existence of an edge-disjoint path from V_h to V_n; there exists more than one edge-disjoint path if and only if there is no edge contained in all paths from V_h to V_n.

Upon relaxing the ability of a node to reach every other node in the network topology, we stringently impose the following two constraints - *Minimum Capacity constraints and Maximum Capacity constraints* - which we categorize as *Shareability Index*. Shareability refers to the extent to which available capacity is shareable. It is a measure that limits the utilization of available

capacity of a link by the disrupted connections. This is imposed in order to restrict a disrupted connection from occupying all of the available capacity of a B-UNCON link (since it is not occupied by any of other flows of the network) such that there is adequate capacity left-out for the MNO that actually owns it - when the MNO needs it.

Consequently, we limit the utilization range for the disrupted connections by setting thresholds on every network link. We call this as *Shareability Index*, denoted by θ_{ij}. This value indicates the maximum acceptable utilization range for a disrupted connection. Utilization range exceeding the shareability indicates congestion and thus the next failed connection automatically looks for another B-UNCON link. By this way, we make sure that the MNO that owns the link is not jeopardized at all. Since the values of these thresholds may be determined according to the network management policies in operator networks, our scheme assumes that these values have been pre-set and remain the same throughout the course of restoration. Henceforth, this concretizes *our restoration scheme as a multi-operator scheme with cooperation*. Figure 23 pictorially illustrates *Reachability and Shareability*.

The point A represents a node of an operator that is trying to reach other nodes in a combined network topology. Here, B, C, D, E, F, G all represents the nodes of other operators who agreed upon sharing. The computation process begins when the node A tries to reach all other neighbouring nodes (here B, C, D). This we call as *Reachability*, the 'liberty' for a node to reach other neighboring nodes and select the nodes those that have sufficient bandwidth to share (representing Shareability here). In a similar way, the path computation process proceeds until a path that satisfies the constraints (detailed later below) is selected.

To determine whether the capacity of any link $(i,j)\varepsilon V$and $ij\varepsilon\, E$ in the network is within the acceptable utilization range (above the set threshold limit) at a time instant t, we introduce another binary variable, defined by:

$$\delta_n = \begin{cases} 1, if \sum_{e\in E}\sum_{\lambda\in\Lambda} \beta_{\mathcal{K}}^{k_{ij}^{(t)}} \geq \theta_{ij}, \forall\, ij \in\ E; n = (1,2 \ldots \mathcal{K}) \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad Otherwise \end{cases} \tag{8}$$

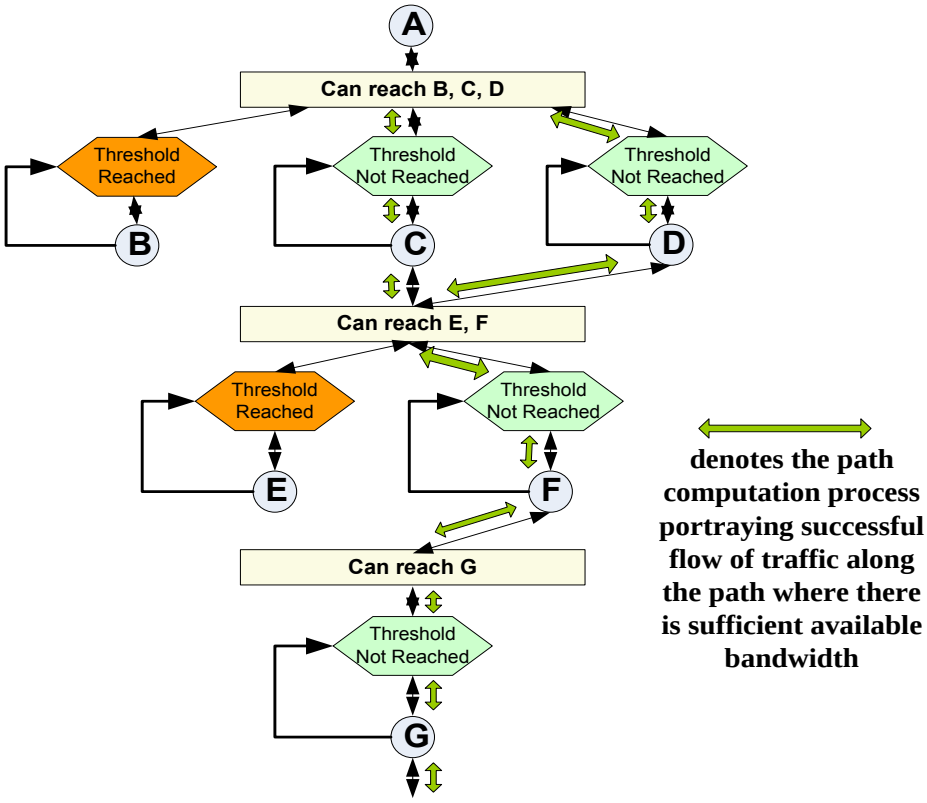


Figure 23: An illustrative figure describing reachability and shareability when the host node of one MNO tries to reach another MNO node when a failure occurs. Here, A indicates the host node, trying to re-route disrupted traffic.

5.3. ILP Formulation based Optimization for $\mathcal{K}$ Alternative Disjoint Paths with Optimal Capacity

Objective: Let $k_{ij}^{(t)}$ be a disrupted connection request on the primary path $P_{Primary}$ at time instant t. Our objective is to find an alternative path from a vertex V_h to the destination vertex V_d with the most optimal capacity. Our ILP formulation outputs a set of $\mathcal{K}$ different alternative paths those which satisfy the constraints and from this set, the most optimal path is chosen according to the traffic type. By this, a connection upon a failure is successfully restored and re-routed across the appropriate alternative back path P_{alt}.

Variables: $\propto_{\mathcal{K}}^{k_{ij}^{(t)}}$ and $\beta_{\mathcal{K}}^{k_{ij}^{(t)}}$ are the variables in this problem. $\propto_{\mathcal{K}}^{k_{ij}^{(t)}}, \beta_{\mathcal{K}}^{k_{ij}^{(t)}} = 1$ if the connection $k_{ij}^{(t)}$ is able to successfully traverse through the new alternative path; else $\propto_{\mathcal{K}}^{k_{ij}^{(t)}}, \beta_{\mathcal{K}}^{k_{ij}^{(t)}} = 0$.

Thus, our ILP model can be formulated as:

$$\textbf{Minimize}\left(\left(\varepsilon\sum_{\mathbf{e}\in E}\sum_{\boldsymbol{\lambda}\in\Lambda}\tau_d\right)+\left((\mathbf{1}-\varepsilon)\sum_{\boldsymbol{n}=\mathbf{1}}^{\mathcal{K}}\delta_n\right)\right) \tag{9}$$

subject to:

- On Path Computation constraints.

$$\sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} > 0, \forall\, ij \in\ E\,, (i,j)\ \in V \tag{10}$$

$$0 <<< \varphi \leq 1, \qquad \forall\, ij \in\ E\,, (i,j)\ \in V, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}\ \in\ G \tag{11}$$

$$\partial \cong 1, \qquad \forall\, ij \in\ E\,, (i,j)\ \in V, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}\ \in\ G \tag{12}$$

$$\left(\sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} \times\ \tau_d\right) \leq \Delta\ , \forall\, ij \in\ E\,, (i,j)\ \in V, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\} \in\ G \tag{13}$$

$$\sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ji}^{(t)}} \leq 1; \sum_{e\in E}\sum_{\lambda\in\Lambda} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} \leq 1, \forall\, ij \in\ E\,, (i,j) \in V, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\} \in G \tag{14}$$

$$\sum_{i:ij\varepsilon E} \propto_{\mathcal{K}}^{k_{ji}^{(t)}} - \sum_{j:ij\varepsilon E} \propto_{\mathcal{K}}^{k_{ij}^{(t)}} = \begin{cases} 1, & i = V_h \\ -1, & i = V_d \\ 0\,, & otherwise \end{cases}, \tag{15}$$
$$\forall\, ij \in\ E\,, (i,j)\ \in V, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\} \in\ G$$

- On Bandwidth Computation Constraints.

$$U_{ij} \leq \sum_{e\in E}\sum_{\lambda\in\Lambda} \beta_{\mathcal{K}}^{k_{ij}^{(t)}} \leq \lambda_{ij}, \forall\, ij \in\ E, (i,j)\ \in V \tag{16}$$

$$\beta_{\mathcal{K}}^{k_{ij}^{(t)}} \geq\ max\ \{\ \lambda_{ij}\ |\ (\lambda_{ij}) \in B - UNCON\}, \forall\, ij \in\ E \tag{17}$$

$$\sum_{e\in E}\sum_{\lambda\in\Lambda} \beta_{\mathcal{K}}^{k_{ij}^{(t)}} = 1, \forall\, ij \in\ E, \forall\, \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}\ \in\ G \tag{18}$$

$$\propto_{\mathcal{K}}^{k_{ij}^{(t)}}, \beta_{\mathcal{K}}^{k_{ij}^{(t)}}\ and\ \delta_n\ \in\ \{0,1\}, such\ that\ ij \in E \tag{19}$$

The objective function illustrated above in (9) aims at finding the shortest alternative path while ensuring that the selected shortest path has the optimal capacity. Here, $\varepsilon \in [0, 1]$ is a small weighting coefficient that we have assigned arbitrarily such that it identifies between choosing a path with the least delay and the most optimal capacity. Assigning the value 1 to ε results in finding the shortest path which has the minimum delay without taking into account if that shortest path has the optimal capacity or not. Assigning 0 to ε results in finding an alternative path which has the optimal capacity but may not be necessarily have the least delay. It is up to

the MNO network manager to decide the priority based on their end customer patterns. For instance, if the majority of the end customers belong to real-time voice call users who can not tolerate delay, then assigning 1 to ε be the best optimal solution. On the other hand, if the majority of the end customers are HTTP based customers, then assigning 0 to ε will do the justification. This makes our objective ILP formulation subjected to two different categories of constraints. First, the alternative shortest path computation constraints are required to ensure that the constructed paths will not contradict the capability of nodes and links. Second, bandwidth parameters must be satisfied to ensure that the constructed shortest paths satisfy the QoS requirements. Constraint (10) ensures that there is atleast one available alternative path existing in the network topology. By constraint (11), we ensure that the constructed alternative/secondary paths have disjointness as close to 1 as possible, thus maximally disjoint. Constraint (12) ensures that the length of the new alternative path is as close as the length of the primary path. By constraint (13), we enforce that the delay of the newly discovered alternative path should be less than or equal to the minimum imposed delay Δ. Constraint (14) ensures for loop-free routing over the newly computed maximally disjoint paths. Constraint (15) gives the flow balance for the new backup path which is established from V_h to V_d. In the rest of chapter, we will refer to (15) as the flow continuity constraint. This constraint ensures that the path established from V_h to V_d is continuous. Next stage, as a criterion for choosing the shortest path - with optimal capacity, we ensure by (16), that there is enough bandwidth resource for the disrupted connection. This constraint also restricts the capacity of a link, which means that the assigned link does not disturb any existing connections. By this, we assume that, in each of the MNOs backhaul, the available capacity of the links for meeting the unexpected increase of disrupted connection requests is considered to derive the maximum number of further requests, which can be successfully served by the links distributed over the network. Constraint (17) ensures that the chosen alternative path has the most optimal capacity. By (18), we ensure that there is atleast a path with optimal capacity for the failed connection $k_{ij}^{(t)}$ to be successfully routed. Equation (19) indicates that $\propto_{\mathcal{K}}^{k_{ij}^{(t)}}$, $\beta_{\mathcal{K}}^{k_{ij}^{(t)}}$ and δ_n are binary variables. Our ILP model essentially captures all the restraining conditions on every edge between any pair of vertices of the network topology, so that a candidate alternative backup path can be chosen according to the respective traffic classes. The effect on the ILP is that the binary variables are basically converted into integer flow variables (calling for more than a simple relaxation of these variables).

5.4. Heuristics Algorithms for the best Alternative Backup Path with Optimal Capacity

The ILP formulations of section V deal with variables which are closely associated to link parameterization. Although this sort of ILP formulation gives an optimal solution, these

formulations are restricted only to small or medium size networks due to the time consumption they take to solve a large number of binary variables. Therefore, we propose three path computation algorithms in a heuristic manner for appropriately solving the optimization problem formulated earlier. As we detailed before, for each disrupted connection $k_{ij}^{(t)}$, we select the best alternative path with the most optimal capacity. By employing a modified version of Yen's algorithm [78] that simultaneously computes the distances from a given host node V_h to destination node V_d in the graph G, we compute the total lengths of the shortest paths from V_h to V_d in the graph, in an amount of time that is proportional to a single instance of Dijkstra's algorithm. Once computed, the choice of a path i for a connection $k_{ij}^{(t)}$ is selected according to the QoS requirement of the given connection request. The pseudo-code of the algorithm is described in Algorithm 1. The algorithm begins by calculating, for the chosen pair of nodes, the shortest path P^* (line 1). The algorithm performs $\mathcal{K}$ iterations. At the ith iteration, the algorithm gets the shortest path stored in the candidates set D. This path is the ith shortest path from V_h to V_d in the graph. Then, it calculates the deviation node V_t of this path from all the $(i-1)$ paths in X. The deviation node ensures that the pre-computed shortest paths do not overlap. To avoid recalculating already computed paths, the algorithm removes nodes and links as explained in lines 9, 10. Now, in the residual graph, the shortest path P' between deviation node and destination is calculated. Then, P' is concatenated with the sub-path of the ith shortest path from $V_h$to V_t.The newly constructed path is saved in the set of candidates D. All deleted nodes and links are restored (line 14), and the algorithm comes to the successor of deviation node in the ith shortest path.

ALGORITHM 1 HEURISTICS FOR FINDING THE $\mathcal{K}$ -SHORTEST PATHS

```
P* ← Dijkstra (s, t)
D ← {P*} //set of candidates
X ← { } //set of K shortest paths
for i = 1 to K
    P ← the shortest path in D
    v ← the deviation node (P, X)
    X ← X + {P}
    while v! = t
        remove all nodes of P from s to v
            remove all output links of V that belong to X
            P' ← Dijkstra (v, t)
            concatenate P' with the sub-path of P from s to v
            D ← D + {P'}
            restore all removed nodes and links
            v ← successor (v, P)
```

5.4.1. Least Length Shortest Paths (LLSP)

Now we present our first heuristics. In this approach, the algorithm selects the shortest path by examining the number of intermediate nodes for each computed paths, those which satisfy all the constraints. To this end, the algorithm re-uses the calculated distances $\delta(V_h, V_d)$ of each path from (1). With the value of distances in hand, the algorithm lists the paths in ascending order. Lines 1 to 7 of Algorithm 2 describe this. The path with the least value of the length is chosen as the most optimal path.

5.4.2. Least Delay Shortest Path (LDSP)

Similar to LLSP, the algorithm here finds the shortest paths considering the delay function, which is calculated from the minimum delay τ_d between all pairs from (3). It then computes the priority of each path based on Algorithm 2. The paths with least delay are listed in increasing order and finally the path with the least value of the delay is the most optimal path.

ALGORITHM 2 HEURISTICS FOR LLSP/LDSP

IN 1: $P^* \leftarrow$ Dijkstra (V_h, V_d)

IN 2: $\xi \leftarrow \{P^*\}$ //set of candidate $\mathcal{K}$ shortest paths

Sort the best value of (ξ), where $\xi = \{\delta(V_h, V_d)\}$ or $\{\tau_d\}$

// ***Objective:*** place the elements of ξ in ascending order

1: n := length[ξ]

2: **for** i := 1 to n

3: // ***Objective:*** place the correct number in $\xi[i]$

4: j := ***FindIndexOfLeast***(ξ, i, n)

5: swap $\xi[i]$ with $\xi[j]$

// L.I. $\xi[1 \ldots i]$ the i least values sorted

6: **end-for**

7: end-procedure

FindIndexOfLeast(ξ, i, n)

// ***Objective:*** return j in the range $[i, n]$: $\xi[j] \leq \xi[k]$ $\forall$ k in range $[i, n]$

1.1: least ξt := i ;

1.2: **for** j := $i + 1$ to n

1.3: **if** ($\xi[j]$ < ξ[least ξt]) least ξt := j

// L.I. ξ [least ξt] least among $\xi[i \ldots j]$

1.4: **end-for**

1.5: **return** least ξt

1.6: end-procedure

The complexity of the above two class of algorithms is *O(KN (M+Nlog(N))*. Both LLSP and LDSP are used primarily for re-routing delay sensitive traffic such as the real-time traffic, primarily due to their modest computational complexity. Although both LLSP and LDSP heuristics are based on resembling computational scheme (Algorithm 2), we will observe from our results (Section VIII) that they produce different results depending upon topologies.

5.4.3. Ant Colony Optimization (ACO) for Optimal Capacity Path Computation

In this third approach, we propose an efficient meta-heuristic based algorithm based on the Ant Colony Optimization (ACO) meta-heuristic algorithm [77]. Since it requires unacceptably long

time to obtain an optimal solution for selecting the best optimal path from a pre-computed set of paths, our approach insists on this meta-heuristic approach as it allows for some space to improve in reserved bandwidth. With the maturity of advanced meta-heuristics, interesting and effective approaches have been proposed increasingly to determine global optima of various complex problems. To name a few, the most commonly used approaches are: Simulated Annealing (SA) [79], Tabu Search (TS) [80], Ant Colony Optimization (ACO) [77], Genetic Algorithm (GA) [81]. All the above mentioned classes of heuristics bring-out almost the same performance, provided they are chosen and manipulated according to the type of the problem statement. The first three approaches, i.e. SA, TS and ACO, are best-fit for problems requiring local search within a pre-selected group, while GA is known to be more efficient and effective considering global search. Consequently, the algorithm to be adopted should be chosen based on two factors: local or global search is the dominant factor and how natural can be the given problem formalized with the given method. We believe that in case of OpenRoutes, the problem is such that good solutions are already narrowed-down in a pre-computed set and they are not too far from each other to be picked-out. Therefore, we concentrated on local search methods. The most important operator of SA and TS is crossover, which cannot be realized in an easy to use way for the given problem. As a consequence, we will propose an ACO based approach in this section to solve the problem of selecting the most optimal alternative path.

Briefly, ACO is a stochastic construction procedure built on probability that iteratively adds solution components to partial solutions based on Heuristics and Trace/Pheromone trail for solving computational problems which can be reduced to selecting best paths in graph networks - inspired by the behavior of ants finding the most optimal path from their nests to the food reservoir. The fundamental principle engages N_{Max} iterations and for every iteration the following steps are executed: (i) Formation of the optimal solutions by each ant among A_{Max} ants and (ii) Updating the Pheromone trail. ACO adapts to an optimization scheme where each ant among A_{Max} ants builds the solution step by step, by adding a new additional component in each step. The component to be added is chosen according to the attractiveness of the new constructed solution (i.e., the current solution augmented by the selected component) which is called the heuristic, and the amount of pheromone deposits, which represents how this component is evaluated during the previous iterations by all ants.

Formation of the Optimal Solution: Built on the same principles, our algorithm computes the best path iteratively from the chosen set of paths. Analogously, A_{Max} represents m disrupted connections and N_{Max} represents $\mathcal{K}$ alternative paths. Once computed, the choice of the next component (i.e., a new path j for a connection l) is selected according to a given probability. Exploitation [25] is one solution which acquires the knowledge and experience of other ants (in our case, disrupted connections) into account to determine the best optimal path and it is used

with a probability q_0. On the other hand, Exploration [77] does not employ any previous statistics and it is adopted with a probability$(1 - q_0)$. In this case, the next component (in our case, a new path for a connection l) is selected according to a probability given by:

$$P_{lj} = \frac{\tau_{lj}^{\propto_{ANT}} \eta_{lj}^{\beta_{ANT}}}{\sum_{k \in N_l} \tau_{lk}^{\propto_{ANT}} \eta_{lk}^{\beta_{ANT}}} \tag{20}$$

where N_l is the set of all possible paths for the solution component l (i.e., $|N_l| = k$). η_{lj} and τ_{lj}denote the heuristic value given in equation (9), and the pheromone trail of the jth path for flow l respectively. $\propto_{ANT}$ and β_{ANT} determine the relative importance of η_{lj} and τ_{lj}, respectively. As mentioned before, in Exploitation, the experience of the other ants is used. Indeed, among the possible components to add, the one with the highest value of $\tau_{lj}^{\propto_{ANT}} \times \eta_{lj}^{\beta_{ANT}}$ is selected. The criterion to choose the best solution is the objective function given in equation (9).

Updating the Pheromone Trails: At the end of each iteration, the pheromones trail values of all possible paths for the solution component l (solution component here refers to the most optimal path) are updated. This is formally given as follows:

$$\tau_{lj}^{\propto_{ANT}} = (1 - \rho)\tau_{lj}^{\propto_{ANT}} + \Delta_{ij}^{Best} \tag{21}$$

where ρ is the decay coefficient of the pheromone indicating how fast the pheromone deposits fade-away. The higher the intensity of the deposits of the pheromone trail deposited on an edge between any two pair of nodes, the larger is the probability that, that particular edge will be chosen. Consequently, every ant deposits more pheromones on all edges it had traversed, after the completion of a journey (iteration), if the journey (the path length of the selected path) is short. At the end of every iteration, trails of pheromones evaporate. Henceforth, we define $\Delta_{ij}^{Best} = \frac{Q}{\eta^{Best}}$ if flow l is routed through the jth path in the best solution of the current iteration, 0 otherwise, and Q is a constant called the pheromone update constant. Here, η^{Best} is computed as [1/Objective function value of the best solution]. In order to determine this value, we refer equation (9).

The key point for the heuristics is that it begins by determining the requested bandwidth for the disrupted connection, which is heavily based on our model definitions from section IV and then ACO meta- heuristic guides the algorithm to explore efficiently the graph of solutions to select an appropriate path. Since our heuristics is based on ACO, it involves iterations to find the best optimal solution. Henceforth, this heuristics primarily addresses traffic flows which can tolerate delay at the expense of finding an optimal path with more capacity, in order to make sure that the chosen path has the required capacity. This capacity must be greater than or equal to the

capacity of a B-UNCON link (λ_{ij}). ACO based heuristics is detailed in Algorithm 3.

The efficacy of the ACO heuristics makes it virtually possible for a single domain to decide on its own on the optimal flow of inter-domain traffic through its nodes (routers/gateways) using only the information about accessibility of given destinations via particular gateways (pheromone trails) having no knowledge of the overall network topology, routing resources, and end-to-end traffic demand.

Remark 1: Even though ACO involves iterations, this heuristics can also be used to re-route delay sensitive traffic flows when the size of the network topology is relatively small. This is because, the number of iterations will not be more than the number of arcs in the graph G, because λ_{ij} is equal to an arc parameter in the graph G. Nonetheless, the specificity of the proposed algorithm is to pick the first feasible path or terminate at a maximal number of calculated paths $\mathcal{K}_max$ given as an input parameter. The computational complexity involved for our algorithm is $O\ (m * \mathcal{K}_max * L * N)$, given that m is the number of connections, $\mathcal{K}_max$ is the total number of pre-computed paths, L is the size of E and N is the size of V.

ALGORITHM 3 HEURISTICS FOR ANT COLONY OPTIMIZATION FOR THE BEST ALTERNATIVE PATH WITH OPTIMAL BACKUP CAPACITY

IN 1: $P^* \leftarrow$ Dijkstra (V_h, V_d)
IN 2: $\xi \leftarrow \{P^*\}$ //set of candidate $\mathcal{K}$ shortest paths
1: Loop
2: Randomly position m disrupted connections on $\mathcal{K}$ alternative paths.
3: **for** path = 1 to $\mathcal{K}$
4: **for** disrupted connection = 1 to m
5: {each connection builds a solution by adding one path after the other}
6: Select probabilistically the next path according to *exploration* and *exploitation* mechanism.
7: Apply the *local trial updating rule*
8: **end-for**
9: **end-for**
10: Apply the *global trial updating rule* using the best path
11: Until end_condition

5.5. OpenRoutes Restoration Scheme

The schema for our methodology for selecting the most optimal candidate alternative path according to the QoS requirements of the disrupted traffic, from a set of multiple paths computed, is given in Schema 1. Our prime focus is on the optimal transmission of a disrupted connection from a source to destination through sets of nodes belonging to different MNOs, which may act as cooperating relays. Fundamental to the understanding of the routing problem was the understanding of the optimal bandwidth resource allocation for a disrupted connection from a set of source nodes to a set of destination nodes, without having to disturb any of the other existing connections. We presented solutions to this problem, and used these as the basis for solving multi-operator cooperative routing. This would be an automatic process running in the control plane of the network continuously solving objective function (9) in real time, and adapting to changing traffic and link availability conditions. The entire procedure would be distributed across a set of MNOs domains those that are collaborating, with each domain being accountable for optimizing its own routing process as well as for computing the inter-domain information it is responsible for, without having to know the other MNOs topological configurations. Thus, MNOs would only have to cooperate sparingly. Furthermore, our framework does not emphasis specifically on any particular ad-hoc routing protocol or shortest path routing protocol. Any existing routing protocol such OSPF, AODV, etc. as well as, say, a traffic engineered MPLS network [82]-[84], or an OpenFlow enabled network [85], [86] could be adopted according to the application and needs.

To implement OpenRoutes scheme for a disrupted connection $k_{ij}^{(t)}$ of requested bandwidth $\mathcal{B}_{k_{ij}^{(t)}}$, we can use any signaling protocol that can reserve the requested bandwidth. This signaling protocol indicates each node along the computed path about the requested backup bandwidth. To avoid the expense of maintaining per-flow state, we can take advantage of the algorithm for the partial information scenario proposed in [70]. However, description of how the signaling protocol works in-detail is beyond the scope of this work.

SCHEMA 1 MULTI-OPERATOR COOPERATIVE ROUTING OVER MAXIMALLY DISJOINT PATHS (OPENROUTES) SCHEME

INPUT: Physical backhaul network topology $G = (V, E, \Lambda, D, L)$ with the set of $\mathcal{K}$ alternative paths $P^* = \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}$ computed based on Distance and/or Delay; Incoming disrupted connection request $k_{ij}^{(t)}$.

OUTPUT: The best alternative path with optimal capacity among $\mathcal{K}$ alternate paths for each disrupted connection is established satisfying the constraints (best case result); or connection $k_{ij}^{(t)}$ is refused if no such path(s) is found (worst case result).

STEP 1) Let V_h contain the set of pre-computed paths $P^* = \{P_1, P_2, \dots P_S, \dots, P_{\mathcal{K}-1}, P_{\mathcal{K}}\}$ obtained for a pre-determined time period, $\mathcal{K}$ being the number of alternative paths computed. Any i^{th} received path P_i contains a path composed of an ordered set of intermediate nodes $N_i = (V_h, V_{i1}, V_{i2}, \dots, V_{i(d-1)}, V_d)$ and an ordered set of intermediate links $L_i = \left(l_h, l_{i1}, l_{i2}, \dots, l_{i(d-1)}, l_d\right)$ with path length $\delta(P_i)$ and delay $\tau_d(P_i)$ where $\delta(P_i) = |L_i|$ and $\tau_d(P_i)$ is directly associated to the weight of the links in the ith path, $\forall i = 1,2,3 \dots, \mathcal{K}$.

STEP 2) Now**,** for every disrupted connection $k_{ij}^{(t)}$, check for the following two constraints:

STEP 2.a) ***Minimum Capacity constraints:*** Compute the minimum capacity required by $k_{ij}^{(t)}$ based on the following condition: $0 < \mathcal{B}_{k_{ij}^{(t)}} \leq U_{ij}$,where $\mathcal{B}_{k_{ij}^{(t)}}$ denotes requested bandwidth of an individual connection $k_{ij}^{(t)}$. If condition true, go to Step 3; or else go to Step 2b.

STEP 2.b) ***Maximum Capacity constraints:*** Compute the maximum capacity required by $k_{ij}^{(t)}$ based on the following condition: $U_{ij} < \mathcal{B}_{k_{ij}^{(t)}} \leq \lambda_{ij}$, where $\mathcal{B}_{k_{ij}^{(t)}}$ denotes requested bandwidth of an individual connection $k_{ij}^{(t)}$. If true, go to Step 4; else (elephant flows) refuse the incoming connection $k_{ij}^{(t)}$.

STEP 3) Find the least value between $\delta(P_i)$ and $\tau_d(P_i)$, from the set $\xi \leftarrow \{P^*\}$ where $i = 1,2,3 \dots, \mathcal{K}$. The path $P_i = (V_h, V_{i1}, V_{i2}, \dots, V_{i(d)-1}, V_d)$ from the set of computed received paths P^* corresponding to this least value is the best alternative path with the most optimal capacity for the respective disrupted connection $k_{ij}^{(t)}$.

STEP 4) Select the first path $P_1 = (V_h, V_{11}, V_{12}, \dots, V_{1(d)-1}, V_d)$ from P^* and check if the available capacity of this alternative path $\mathbb{C}_P \geq \lambda_{ij}$, where $\mathbb{C}_P$ is the capacity of this path P_1. If true, assign P_1 as

the best alternative path with the most optimal capacity for the respective disrupted connection $k_{ij}^{(t)}$; else iterate this $\mathcal{K}_max$ times until the condition is satisfied.

STEP 5) Connection $k_{ij}^{(t)}$ is re-routed successfully according to its QoS traffic class along the best alternative path with the optimal capacity.

STEP 6) Update *Pheromones* for all disrupted connections $k_{ij}^{(t)}$.

5.6. Performance Evaluation and Discussions

5.6.1. Experimental Set-up and Computational Considerations

In this section, we present numerical illustrations towards the realization of our scheme. We compare our results against two reference schemes: Shortest Path routing scheme [76] and Beam Search algorithm [87]. In order to get an overall picture of the attainable performance gain of our framework, we evaluated our results based on the following three criteria: (i) First we evaluate the efficiency of our three heuristics algorithms individually, on different traffic conditions - with and without operator sharing. (ii) Second, we combine all the three heuristics into one. This is basically how our OpenRoutes scheme should be executed, if an MNO experiences traffic patterns of all kind of traffic classes-evenly. We have evaluated this against the reference schemes. For the above mentioned two categories, we carried out the analysis on a realistic topology (Sprint US: node: 44; edge: 106; average node degree: 4.82). Figure 24, 25, 26 demonstrates the results of the efficiency of our three heuristics individually, on different traffic conditions without operator sharing and figure 28 demonstrates the results of the efficiency of our three heuristics individually, on different traffic conditions, with operator sharing and finally figure 28 demonstrates the results of the efficiency of our three heuristics algorithms combined, on different traffic conditions, with operator sharing only. With the performance gain of our algorithms due to operators sharing in hand, we proceed to evaluate the third criteria: (ii) Efficiency of the algorithms with operator sharing only on different topologies.

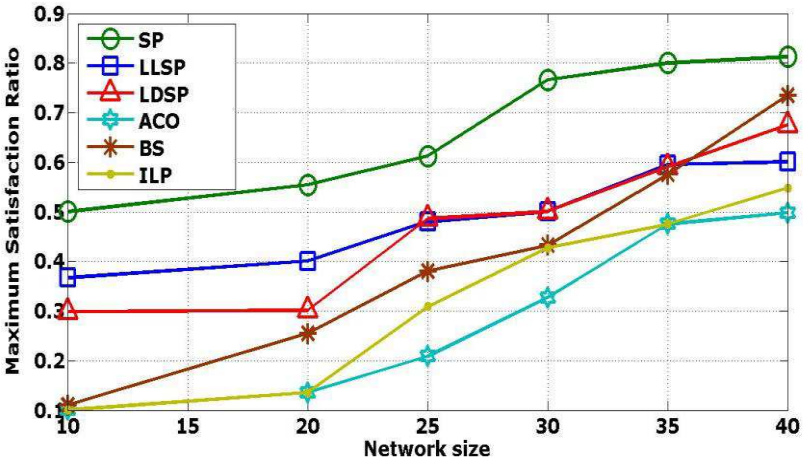
Experiments were carried out on an Intel Pentium Core 2 Duo 3 GHz, 4GB RAM machine. We generated three traffic demands (standard OC1:51.85Mb/s, OC12:622.08Mb/s and OC48:2.488Gb/s) between each node-pair since it is a way of distinguishing more types of traffic classes and each demand has a random bandwidth between 1 and 2.4Gb/s. All links have 337Mb/s ((622.08/2) + (51.85/2)) link bandwidth. End-user demands were generated according to Poisson process and link failures were generated randomly. On a general note, the 50ms restoration latency and 50% restoration capacity overhead associated with SONET BLSR rings

are benchmark figures and thus the QoS parameter Δ is preset to 50ms. The underlying solver for the ILP formulations was CPLEX 9.1 [88].

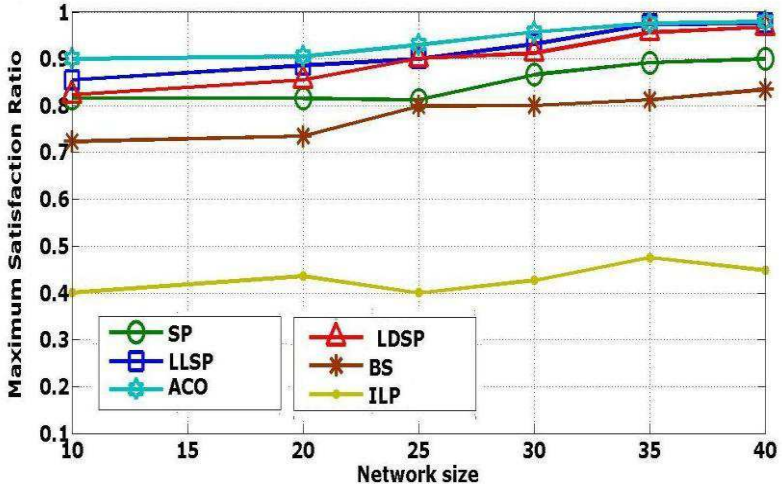
5.6.1.1. Efficiency of the Three Heuristics Individually on Different Traffic Conditions- With and Without Operator Sharing

Here, we differentiate between the two scenarios i.e. with and without operator sharing, by changing only the value of threshold of the links of the topology. That is, we tune only the Shareability Index by setting $\theta_{ij} = 0.50$ (50% allowed range) to indicate that the MNOs allow the others to share up to 50% of their link bandwidth. By setting $\theta_{ij} = 0$, it is implied that there is no link bandwidth sharing.

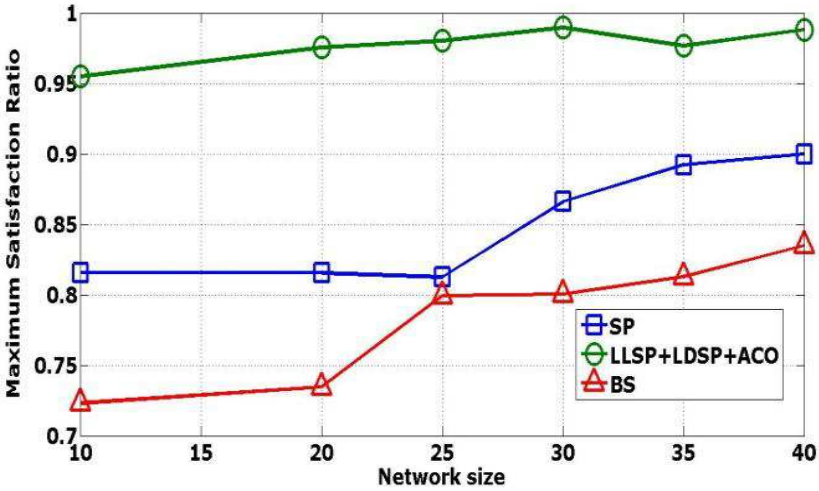
Maximum Satisfaction Ratio (MSR): It is a measure of the number of connection requests accepted against the total number of connection requests. The main measure here is to compare the performance of our approaches individually against reference approaches when the MNOs share and when they do not. Overall, we observe that the number of connections accepted is more likely to be favorable when the MNOs share compared to when they do not share. This is predominant as the network size increases; fundamentally because of the properties of our algorithms to find more feasible paths in larger networks. The reference shortest path routing algorithm almost always performs well, in the situation when MNOs do not share. Our algorithms LLSP and LDSP perform inferior to the SP routing algorithm, when MNOs do not share but the performance gets augmented when the MNOs share. This is mainly due to the fact that SP routing algorithm best fits in a case when the network links are not very congested and that there is always sufficient capacity available; while on the contrary LLSP and LDSP are particularly meant to select paths, even under congested situations. Furthermore, since LLSP and LDSP address the traffic classes which does not demand paths with more capacity, they find it very feasible to choose abundant paths with less capacity than SP or BS - meaning that LLSP and LDSP succeeds as much as SP routing algorithm in re-routing delay sensitive traffic. Adding to this, the MSR for ACO is the lowest when the MNOs do not allow the others to share. This is because, ACO looks for the most optimal path with more capacity to re-route bandwidth consuming traffic. By our approach, ACO shows very high MSR, meaning that even if there is high traffic demand spikes/more congestion due to link failures in the network, it can be efficiently tackled by our approach and thereby the overall demand request is met better, thus maximizing the end-customer satisfaction ratio.



(a)



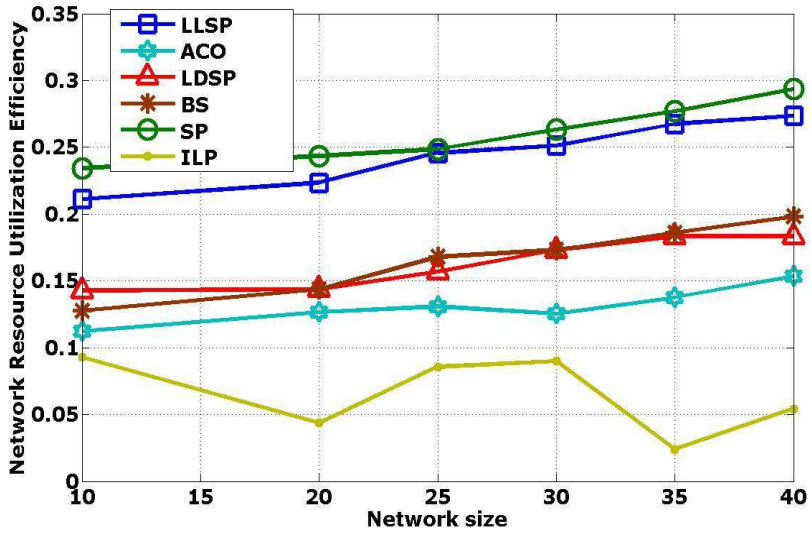
(b)



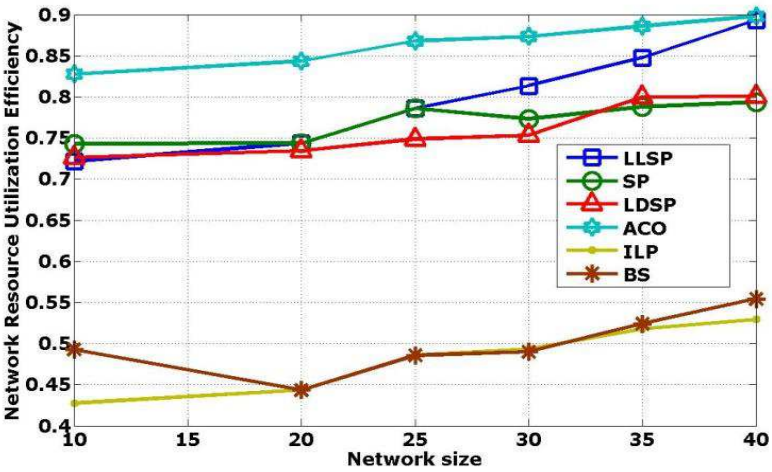
(c)

Figure 24: Illustration of Maximum satisfaction Ratio (MSR) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology).

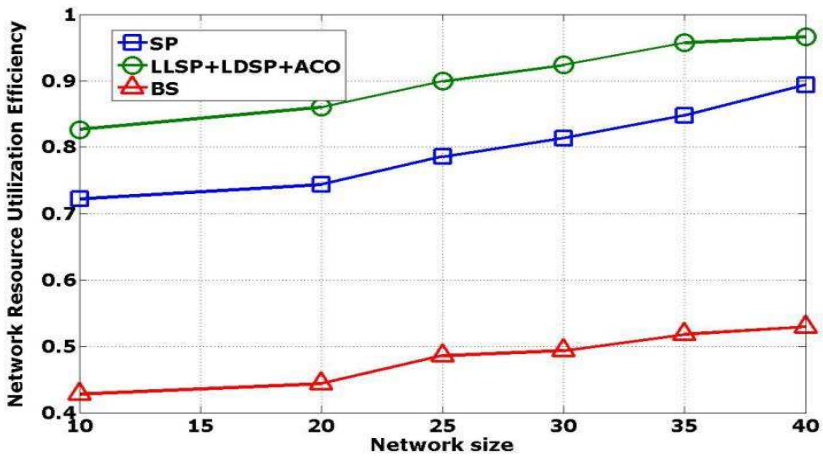
Network Resource Utilization (NRU) Efficiency: Network resource utilization efficiency is defined as the ratio of the link bandwidth which is utilized to the total bandwidth provisioned [14]. For a case with sharing, NRU efficiency value indicates how efficiently the total available network resources are utilized (which is actually utilized for protection and restoration and/or tackling overloaded situations). Precisely, NRU efficiency can give an estimate of the efficiency of our algorithms with respect to effectiveness of resource usage. High NRU value indicates better resource optimization. Overall, our results demonstrate that the value of NRU is better with sharing than without, specifically, as the node size increases. What this means to us, is that, by our approach, we could achieve efficient network resource utilization, meaning that, over-provisioning for backup path could be eliminated. The fact that our scheme utilizes network resources according to the traffic class greatly contributes to the better efficiency, particularly because high bandwidth traffic connections may be carried much efficiently on the available bandwidth while meeting their availability requirements. This is clear while one observe ACO whose utilization is doubled while MNOs share, which is the highest. This is because link bandwidth occupancy of ACO in order to guarantee connection availability requirements is higher and thus it utilizes every available bandwidth. Thus, all available resources are more efficiently consumed. Similarly, NRU for LLSP and LDSP, if not the best, is also good, in-par with SP routing algorithm, even when the network size is large - when shared. To summarize, our approach tries to achieve better capacity utilization so that no un-used resource remains "wasted" to achieve connection-availability guarantee.



(a)



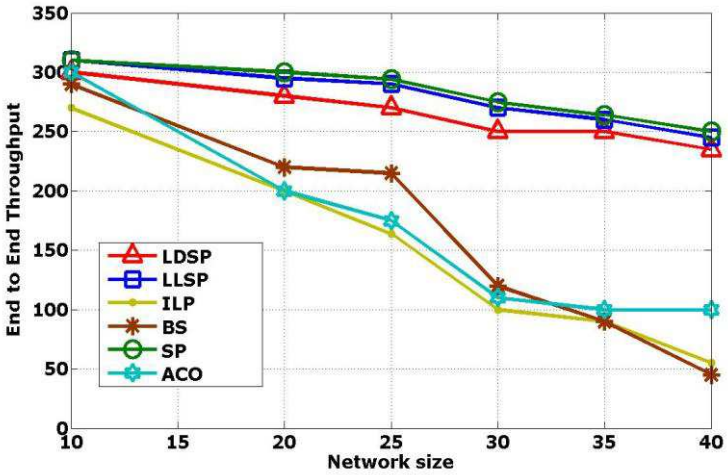
(b)



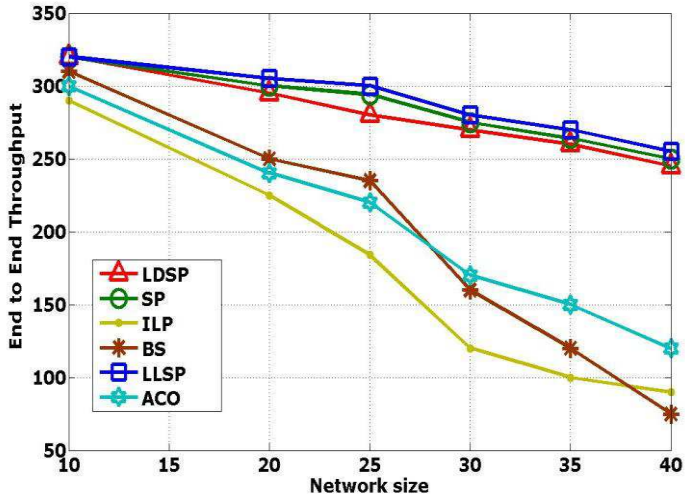
(c)

Figure 25: Illustration of Network Resource Utilization (NRU) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology).

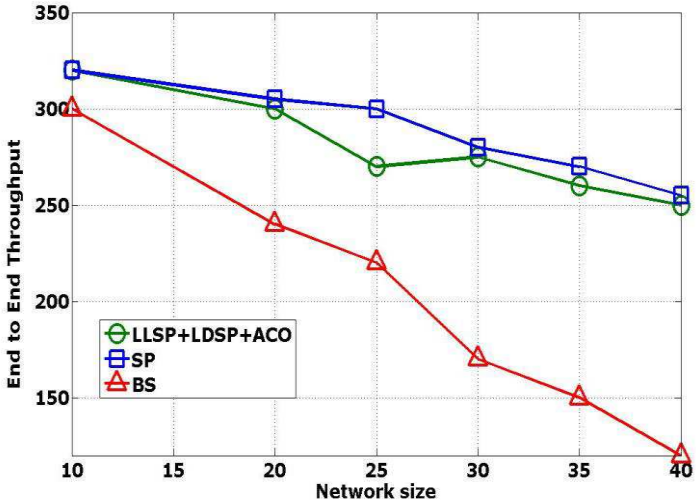
End-to-End Throughput(EET): This metric allows us to determine the efficiency of the path computation algorithms. That is, the end-to-end throughput of the network topology with and without sharing, will enable us to understand the complexity of our path computation algorithms, thereby affecting the overall network throughput. Fundamentally, an end-to-end path with more links will lead to poor performances because it is more likely that allocating sufficient resources to an end-to-end path may not succeed [15]. Also, due to the delay associated with a path with more links, the allocated resource may not be available until the end of a connection request. Consequently, we observe that LLSP performs better than LDSP and both LLSP and LDSP perform much better than ACO when MNOs share, essentially due to the fact that ACO looks for paths with more link capacity rather than simply selecting paths of shorter length.



(a)



(b)



(c)

Figure 26: Illustration of End-to-end Throughput (EET) for ILP and three heuristics individually for different traffic conditions- (a) without MNOs sharing, (b) with sharing, (c) three heuristics combined with sharing (on Sprint U.S. topology).

5.6.2. Efficiency of the Algorithms with Operator Sharing Only - on Different Topologies

Motivated by our earlier results from the above section, now we go forward to present the efficiency of our framework on four different topologies and determine the best topology that can maximally benefit MNOs if they conclude on backhaul resource sharing. This will allow us to quantify the network resource utilization that can be achieved for a particular topology, not just for a particular flow. Now we recall that the centre of our earlier work was heavily quantified, based on a new key metric that we defined as Shareability Index (θ_{ij}). This metric characterizes the extent to which available capacity on a link is shareable among MNOs. In a way, it is representative of a specific topology's survivability with respect to the utilization range of the available capacity. We now tune the accuracy of this metric using four different topologies under a range of failure probabilities and present our results. The end result, therefore, accurately predicts the survivability of a given network topology, with reduced redundancy. To do this, we vary the value of θ_{ij} between 0 (0% allowed range- implying no network resource sharing between MNOs) and 0.50 (50% allowed range- implying sharing half of the available network resources in each link), in the topologies where we have carried out the experiments. Table IV summarizes the different topologies that were used for the simulation, each exhibiting its own characteristics, such as - mesh, ring, grid and star. To measure the impact of our algorithms on them, we compare our results against the Shortest Path Routing (SPR) and Beam Search Algorithm (BS) as reference schemes.

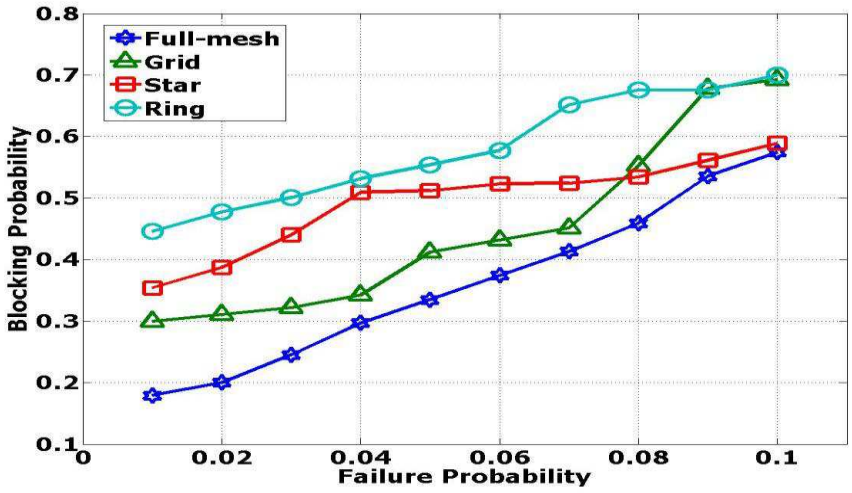
TABLE IV. NETWORK TOPOLOGIES CHARACTERISTICS

Network Type	Network Characteristics		
	# of Nodes	# of Links	Average Node Degree
Full-Mesh	20	190	19.00
Manhattan Grid	25	40	3.20
Ring	25	25	2.00
Star	25	24	1.92

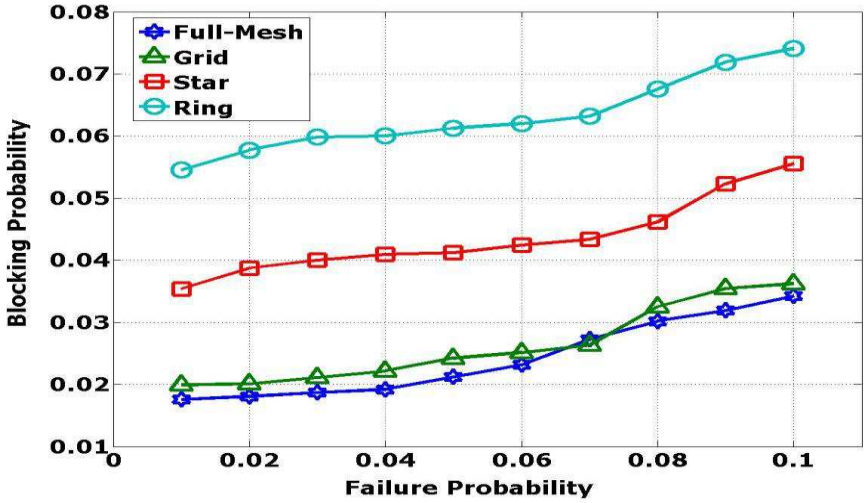
5.6.3. Influence of Topologies

In this section, we present numerical illustrations towards the realization of our scheme. Here the metric that was considered for the evaluation is Blocking Probability (BP). BP is defined as a measure of the number of connection requests rejected against the total number of connection requests. Our methodology for evaluations is described as follows: As a first step, we focus on determining the topology that yields the best performance for the proposed OpenRoutes

restoration scheme. To do so, we evaluate and compare the performance of all the four topologies by combining the three heuristics (LLSP+LDSP+ACO) for the two cases: (i) when the MNOs do not share $(\theta_{ij} = 0)$and (ii) when the MNOs share$(\theta_{ij} = 0.5)$, in figure 27 (a) and figure 27 (b).



(a)



(b)

Figure 27: Illustration of blocking probability for various topologies when all the three heuristics (LLSP+LDSP+ACO) are combined for (a) $\theta_{ij} = 0$ (no resource sharing) (b)$\theta_{ij} = 0.5$ (50% resource sharing).

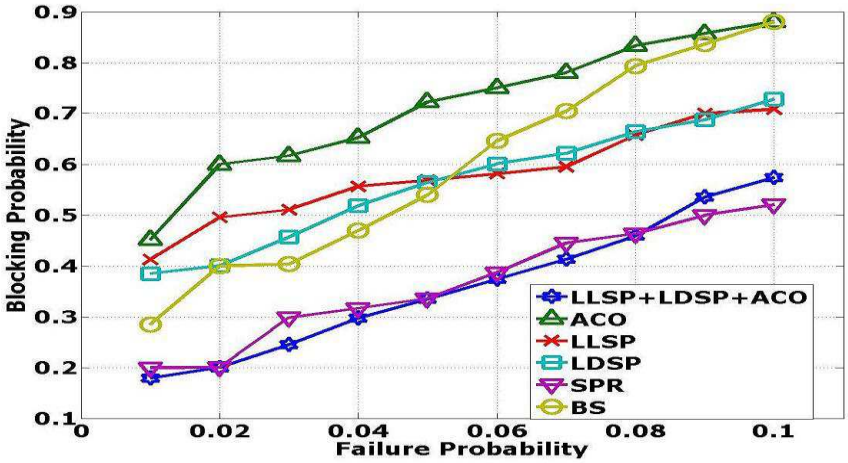
The performances of all three heuristics when combined yield the best results on the full-mesh topology than any other topologies in consideration. To give them a ranking, full-mesh performs the best, followed by grid, then star, then ring. Our justification to this is that it is due to the density of this 'mesh-like' topology which is larger than star or ring network topology. As the density decreases, it may no longer be possible for some pairs of intermediate nodes to communicate over short paths. Hence a decrease in density is typically accompanied by an increase in network diameter, which results in larger length, resulting in poor performance. Furthermore, unlike each of the other topologies in consideration such as grid, star and ring,

messages sent on a full-mesh network, where every node in the topology is connected to every other node, can take any of several possible paths from source to destination, thus maximally benefitting from our restoration heuristics. On the other hand, considering the case of ring, this shows the least performance because a failure in any link disconnects the entire loop and thus the entire path is not available for the failed connections to traverse-through. Nevertheless, it has to be noted that the performance of all the topologies is better for $\theta_{ij} = 0.5$ than $\theta_{ij} = 0$. (Detailed analysis on the same is in the section below). Nonetheless, through our results, we are able to demonstrate that the survivability of disrupted connections due to resource sharing will have much higher availability in the presence of any number of failures (single or double link failures), if the contribution of the reconfiguration time from primary path to backup path towards unavailability is disregarded [since it is relatively small (on the order of tens of milliseconds) with respect to the manual failure repair time (on the order of hours) and the connection's holding time (on the order of weeks or months).

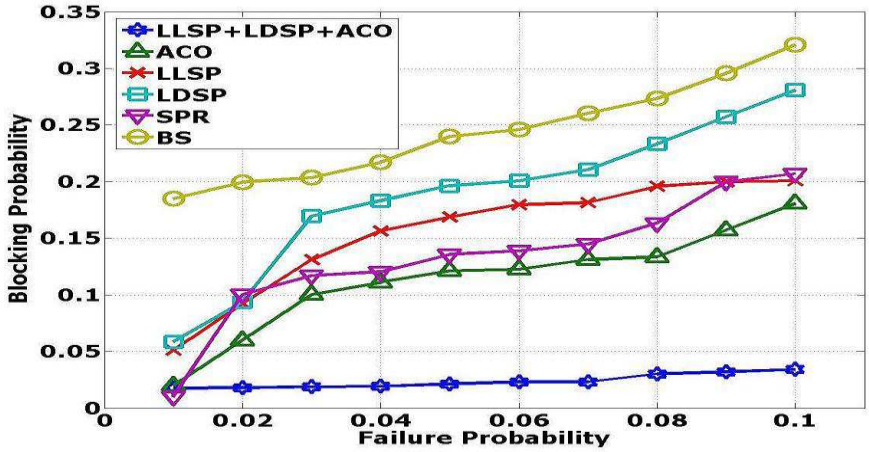
5.6.4. Influence of Sharing

Having determined the best topology, we now illustrate the performance of our three heuristics (LLSP, LDSP, ACO) individually against the reference approaches and then combine all three heuristics into one (LLSP+LDSP+ACO) and compare against the reference approaches for the two cases- (i) when the MNOs do not share $(\theta_{ij} = 0)$and (ii) when the MNOs share $(\theta_{ij} = 0.5)$. Figure 27 illustrates the performances for the Full-mesh topology alone which performs the best as ascertained by our earlier results. Observing from Figure 28, we can conclude that the total number of connections rejected when the MNOs share (Figure 28(b)) is lesser compared to when they do not share (Figure 28(a)). Taking a closer look at the obtained results precisely indicate the following observations. The reference shortest path routing (SPR) algorithm almost always performs well, be it in the case when the MNOs do not share or when they share. However, there is a slight difference in performance observed looking closely. Our algorithms LLSP and LDSP perform inferior to the SPR routing algorithm, when MNOs do not share but the performance gets augmented atleast by 50% when the MNOs share and gets in-par with the performance of the SPR algorithm. This is mainly due to the fact that SPR routing algorithm best fits in the case when the network links are not very congested (congested in the sense that there is no failure and hence no congestion encountered) and that there is always sufficient capacity available. As stated earlier, since LLSP and LDSP address the traffic classes which does not demand paths with more capacity, they find it very feasible to choose abundant paths with less capacity compared to the classic SPR - meaning that LLSP and LDSP succeeds as much as SPR routing algorithm in re-routing delay sensitive traffic. Moving forward, the performance of ACO shows a huge variation unlike the other two heuristics (LLSP, LDSP), when the MNOs share and when they do not share. Especially, the BP is the highest when the MNOs do not allow the others to share. This

is because, ACO heuristics looks for optimal paths especially with more capacity to re-route bandwidth consuming traffic. Having said that, ACO performance is the best when there is resource sharing, implying that more paths with enough capacity to re-route bandwidth consuming traffic can be easily found in the case when the MNOs share. Adding to this, the performance when all three heuristics are combined is notably remarkable, seemingly much better than the reference schemes, when the MNOs share and it is notably not affected by the size of the network or the failure probability. This is because our approaches fundamentally makes sure that the overall congestion due to link failures is reduced as much as possible by "intelligently" using the unused resources of the network. Our simulation results show that, for sharing constraints those are not strict, our proposed heuristics approaches return solutions close to the optimum making their application for multi-constrained routing problems very promising.



(a)



(b)

Figure 28: Illustration of blocking probability (a) for $\theta_{ij} = 0$ (no resource sharing) (b) for $\theta_{ij} = 0.5$ (50% resource sharing) on a Full-mesh topology.

5.7. Concluding Discussions

The problem of QoS-based routing in multi-domain heterogeneous networks is increasingly important as the use of broadband services that span multiple public operator boundaries grows. There is a necessity to separate global routing in two levels, inter-domain and intra-domain routing in order to allow different operators use their own routing algorithms inside their premises. This idea is followed in two different QoS-based routing mechanisms. The one is triggered on-demand, meaning that the whole process starts when there is a user connection request between two access points with specific QoS characteristics. The other has a part running as a background process regardless any user request that pre-calculates routes according to pre-defined service categories and QoS criteria, and uses them for an incoming connection request. Both mechanisms have benefits and drawbacks. The former is time consuming for an incoming request the latter needs great storage capacities. Depending on the network's nature, the most appropriate approach can be selected.

Our work here presents a novel fault restoration framework which can cost-effectively provide protection and restoration for the MNOs, allowing them with a parameterized objective function to choose the desired paths based on traffic patterns of their end-customers. True, there is a trade-off between resource utilization, computational delay and cost here. Nevertheless, since the shared capacity of another MNO is not used under normal no-failure conditions except by low priority pre-emptible traffic, the objective of minimizing restoration capacity overhead in the network translates to higher network utilization. Also, our approach here is to define which type of traffic needs to be protected all the time thus allowing the MNOs to protect and improve the availability of their revenue generating services to ensure high-quality, uninterrupted user experience, increasing the link capacity offering more data services.

Furthermore, insisting that topologies remain an important part of network design theory, we extended our analysis for four different synthetic topologies, each exhibiting different characteristics. Based on our results, we could conclude that it is most beneficial when two (or more) MNOs with already existing mesh topologies decide to cooperate and share their backhaul resources, in order to maximize their network resource utilization or in other words to minimize the disrupted connections resulting due to failure situations. Regardless, through our results, we have demonstrated that the management of resources can yield notably different performances leading to different restoration behaviors for different network topologies.

*"One cannot really argue with a mathematical theorem." – **Stephen Hawking, Theoretical Physicist, Cosmologist.***

Chapter 6

Divide and Share: Multi-operator Greedy Routing Based on Sharing with Constraints

Understanding the performance difference between the static and the dynamic bandwidth allocation schemes is important for traffic control and management. In static link sharing system, a fixed bandwidth share of the link capacity is assigned, irrespective of whether it is active or not. On the other hand, dynamic link sharing refers to the process of dynamically allocating bandwidth based on the instantaneous utilization of the link. Henceforth, dynamic link sharing provides a novel quality of service (QoS) framework broadband wired/wireless networks. In this chapter we analyze the link capacity requirements for microwave backhaul architecture when two different Mobile Network Operators (MNOs) decide to dynamically "divide and share" their primary resource (working path) as an alternative for investing in a backup path, in order to tackle the problem of provisioning additional resources within their backhaul. To examine and to develop practicable performance bounds on resource sharing, we make an estimation of the resource utilization and derive integer linear programming (ILP) counterparts. Given the complexities of solving ILP, we also propose heuristic-based resource provisioning algorithm which allows MNOs to share their primary resource with (an)other MNO(s), without having to sacrifice their own traffic demand requirements. Because our model uses preference orderings of outcomes to establish equilibria for computing both primary bandwidth capacity and backup bandwidth capacity, it allows for a quick exploration of the limits regarding resource sharing. Illustrative numerical results show the effectiveness of our resource provisioning approach in terms of network resource utilization and connection blocking probability.

6.1. Introductory Statements

6.1.1. Problem Formulation

While 'OpenRoutes' specifically targeted on routing disrupted connections across the available paths of multiple MNO backhaul networks based on their respective traffic class, in this chapter we analyze the capacity constraints of a single link when two different Mobile Network Operators (MNOs) decide to "divide and share" it. The above statement can be scrutinized and approached through the following questions:

- When multiple MNOs decide to share their existing working paths (as an alternative for investing in back up paths), how to deal with the resource allocation of a single link which is already occupied by a sharing MNO that does not own it?

- How to explicitly provide control of the shared percentage of capacity of a link when the MNO who built it, needs it. i.e., which operator gets preemption priority in case of congestion on the sharing MNO?

6.1.2. Motivation and Concept Visualization

As stated in the earlier chapters, classical methods to bring down the impact of failures in backhaul networks include pre-allocated backup bandwidth when the primary bandwidth is provisioned. Initially backup paths were configured to recover working paths from failures, but are not used under normal conditions. At later points in time, this unused backup capacity was suggested to be used for supporting extra traffic besides serving as working path under failure situations, which is preempted in case of a working path failure [89], [90]. And, this was termed as Backup Bandwidth Sharing (BBW). It thus became a common practice to share one or more common links among primary and backup paths as long as a connection's availability is satisfied, especially when these links have high reliability. Consequently it lead to the improvement of network capacity utilization. In order to efficiently utilize the resource of the backup path, researches led to the consideration of sharing the same backup resource such that traffic from multiple working paths could be re-routed, as long as they are mutually diverse. This was termed as Shared Protection Path (SPP). Sharing highly-reliable links between primary and backup paths greatly reduces backup bandwidth overhead in a network while still satisfying stringent availability requirements of connections. Specifically, the SPP scheme has received much research attention, as it provides the best balance between availability, recovery time, and resource utilization [91], [92]. The most desirable property of SPP is its resource efficiency resulting from backup resource sharing. Consequently, how to increase backup resource sharing

based on different cost models is of particular interest and has been reported in [93]-[97]. Since backup resource sharing depends on the routes of working paths, most of existing work computes a backup path after the working path is determined. Besides, there have been exclusive attention paid in the literature to evaluate the behavior of wireless backhaul and mesh networks when their capacity increases and have been intensively studied in the recent years with a specific focus on capacity or other QoS parameters and installation costs. Conversely, many researches have focused on minimizing the cost of setting up additional backup resource, such as by minimizing the link or node failures, backbone construction or monitoring in sensor and ad-hoc networks. While the above stated literature research focus on optimal backup resource provisioning taking into the effects of cost investments, there have been a wide spectrum of research efforts studying the problem of re-routing the traffic and bandwidth allocation through the backup path in different contexts such as optical networks, ATM networks, MPLS networks, IP networks, and application-layer overlay networks. Within this scope, the main technical challenge is to find the right tradeoff among robustness, efficiency, and fast restoration in the specific context. Almost all of these proposals and solutions consider single fault situations in the primary path with the assumption that any failure could be repaired before the next failure occurs. Literature studies on the dual failure scenarios [98] have revealed that the current SPP sharing schemes with 100% restoration for single fault could in average recover about 60-70% failures in dual faults situations but it can be as low as 20%. The expansion of networks and increased durations of applications demand future networks to posses a 100% restorability even for dual faults.

Nonetheless, all these research activities definitely have paved a way towards minimizing the loss of data due to link failures by providing an additional backup path. Even though solutions such as SPP proved a point towards a shared form of resource provisioning, the necessity to design an additional backup path was inevitable, since this shared backup path also comes with an extra cost. Thus, it is quite consensual that there is still much room for the conceptualization of more sophisticated solutions in this research area while one should focus on a system-wide approach to reach a global cost expenditures minimum for network operators.

Our goal, however, is to provide the same kind of protection with reduced cost by mutually using the existing available paths. With this goal, we target to achieve optimal sharing between two different network operators who agrees upon the upper and lower bounds of the capacity limits for sharing the resources; because increasing the amount of sharing will naturally increase the risk that might create an inter-relatedness of one or more MNOs. High inter-relatedness could lead to under-utilization or over-utilization of the network resources by their partner. If one partner over-utilizes the sharing commitments, then the position of the other partner would be weakened. Another barrier for the MNOs is the fact that sharing can lead to loss of non-optimal

long term capacity provisioning decisions. Therefore, we center our focus towards the "optimum configuration choice" for backhaul resource provisioning between the MNOs agreeing to share their primary resource (working path), so that the overall bandwidth reservation for the backup path would be minimal, thus minimizing the total cost for additional backup resource. Within this context, we tackle the problem of dealing with a complex decision for setting the maximum and minimum bounds in link capacity that can be shared and utilized between the MNOs' who agree to share. This decision consists in determining the optimal configuration of total link bandwidth capacity to handle the additional traffic demand due to a new connection request which arrives from the sharing MNO. To examine and to develop practicable performance bounds on resource sharing, we make an estimation of the resource utilization and derive integer linear programming (ILP) counterparts. Given the complexities of solving ILP, we also propose heuristic-based resource provisioning algorithm which allows MNOs to share their primary resource with (an)other MNO(s), without having to sacrifice their own traffic demand requirements. Because our model uses preference orderings of outcomes to establish equilibria for computing both primary link capacity and backup link capacity, it allows for a quick exploration of the limits regarding resource sharing. This can help both the MNOs and the regulators to evaluate the strategic decision regarding (backhaul) resource sharing in a typical oligopoly telecom market.

6.1.3. Current Contributions and Significance of our Results

Unlike most previous works, we present a framework in this chapter to sustain availability requirements cost effectively. We propose a protection-differentiated availability-guaranteed provisioning algorithm to support connections with stringent availability requirements. Our algorithm enables service providers to share their backhaul resource with one another deciding the degree of backup sharing to target connection availabilities. To the best of our knowledge, this is the first study to investigate the effects of multiple backup paths and link sharing between primary and backup paths for high-availability-targeting and service differentiated provisioning, in dynamic traffic environment. We investigate the optimal spare capacity placement problem based on ILP and heuristic based approaches.

Original contributions can be summarized as below:

- Optimization of resources when one MNO decides to share their primary resource with another MNO which would serve as backup resource, without jeopardizing their own quality-of-service (QoS) requirements.

- A systematic optimistic methodology to efficiently define the capacity bounds in its

ability to offer a high quality of experience (QoE) for subscribers, i.e. to define the upper and the lower bounds of the traffic through another MNOs' backhaul network for each connection going through a failed link.

6.2. Issues Affecting Availability in Shared Backup Bandwidth Allocation

A protection scheme that evolves when two or more network operators join hands to set-up one complete backhaul architecture enabling more protection, has much more complications than a classical architectural evolution involving only one party. To make our proposed solution reasonably modest, we also point out the issues and the policies that have to be born in mind strongly that will affect the availability of connections when two or more different network operators share their backhaul.

• Static Bandwidth Allocation Versus Dynamic Bandwidth Allocation

According to our scheme, connections are carried by primary path $\mathbb{P}$ of one operator and protected by a link-disjoint backup path **B** (which is the primary path of another operator here). There are two ways by which backup sharing could be performed: allowing a fixed bandwidth resource sharing or allowing the operators to dynamically share their bandwidth. In the first case, backup bandwidth is fixed to certain threshold or a capacity limit on each of the operators' backhaul on each link, allowing backup bandwidth to be chosen from a pre-reserved backup bandwidth pool when failure occurs. While in the second case, depending upon the current availability operators' choose to "give" their bandwidth. In addition to this, the reserved bandwidth on each network operators' link of **B** can be utilized by the operator who owns it, as long as SLA constraints are satisfied.

• Reverting Versus Non-reverting

Connection t's traffic will be switched to **B** when a failure occurs on $\mathbb{P}$. After the failure is repaired, connection t's traffic can be switched back to $\mathbb{P}$, an approach which is called reverting; or it can stay on for the remaining service time (or till **B** fails), an approach which is called non-reverting. Both the reverting and non-reverting strategies have their pros and cons. For example, traffic may be disturbed twice in the reverting strategy, which may be undesirable for some services. In the non-reverting strategy, the backup paths for the connections in S_t may need to be rearranged since some of the shared backup bandwidth on parts of their backup paths has been taken by t when t is switched to its backup path. These connections can become vulnerable during their backup-recomputation and backup-resource reservation processes; and,

furthermore, their successful backup rearrangement is not guaranteed; so, non-reverting may result in unpreferred service degradation. A network operator may choose policies based on operational cost and service characteristics. The reverting model may sometimes be preferable since it provides simplicity in network control and management. We assume a reverting model in our analysis. The concept of stub release refers to the release of capacity along the surviving upstream and downstream portions of a failed primary path, and making those capacity available for the restoration process. Since we only consider to restore a connection using the pre-planned backup path and assume a reverting model, stub release is not relevant for this modeling study. Stub release will become important for dynamic provisioning where connections come and go.

• **Active Recovery Versus Lazy Recovery**

In the reverting model, after traffic is reverted back to $\mathbb{P}$, the shared backup resources will be released. Similarly, when backup resources are fixed from a failure, they are also "up and free", which means that the backup resources are not in failing states (up) or being used by any connection (free). In both of the two cases, the fixed or released backup resources can be actively used to recover the connections in S_t that are experiencing failure and waiting for their backup resources to be fixed or released. We call this mechanism active recovery. On the contrary, if the backup resources wait to be activated when the next failure arrives, these currently failed connections cannot be recovered even though their backup is up and free now. This mechanism is called lazy recovery. In active recovery, the backup resources released by a connection may be able to recover more than one connection as may traverse multiple links. Obviously, backup resources are utilized more intelligently in the active-recovery model so we assume an active-recovery system in our study. If active recovery is employed, another problem will arise, i.e., if there are multiple failed connections waiting for the backup resources, which connection should be chosen to recover next? Connections can be recovered in the exact order of their failure sequence, i.e., earliest failure recovered first. We call this a resource-locked system in the sense that a failed connection will "lock" all the up and free backup wavelengths it needs and wait for others to be fixed or released. And we further assume that the locked backup resources can only be released when the primary path of the failed connection is fixed.

6.3. Divide and Share Optimization

6.3.1. General Problem Statement

In this section, we introduce Integer Linear Programming (ILP) based mathematical formulations to the optimization problem of determining the upper and lower bounds for

bandwidth resource utilization when two different MNOs decide to "divide and share" their backhaul resources with each other, as a means for backup resource. We target to optimize the minimum and maximum possible degrees of resource sharing respectively. These bounds will allow a MNO to quickly determine the amount of backup resource sharing that is acceptable, given the prevailing conditions in the network. We first define the notations and then formally state the problem to be addressed.

Formal Notations: The physical backhaul network topology is represented as a weighted bidirectional graph G = (V, E, A, λ) where V= {n} is the set of nodes, $E = \{l_{ij} = 1\}$ represents the set of all microwave links with the end points (i, j) between source s and destination d, such that $(i, j)\varepsilon V$ and $ij\varepsilon\ E$. Therefore, the total number of links that constitutes the backhaul network topology becomes $\sum_{ij\varepsilon E} l_{ij}$. The availability denoted by A: E → (0, 1) is called point-wise availability, instantaneous availability, or transient availability of each microwave link where (0, 1) denotes the set of positive real numbers between 0 and 1. Here, A_{ij} denotes the total availability of the microwave link (i, j). Therefore, α_{ij} represents the availability parameter of the microwave link such that $\alpha_{ij} = -log\ A_{ij}$. With this, now we introduce α_D which guarantees minimum required availability to satisfy the "required traffic demand[11]" of the donor. Therefore, $\alpha_D = -log\ A_D$.

Furthermore, t = *(s, d, SLA)* is an incoming connection request between source s and destination d on the link (i, j), whose Service Level Agreement (SLA) defines the type of traffic demand that needs more protection than another traffic demand that can have a lower level of protection. Now, the k-th connection request for the donor is denoted as $C_{ijk,D}$ and for the recipient is denoted as $C_{ijk,R}$. $\lambda : E \rightarrow Z+$ specifies bandwidth on each microwave link (where Z+ denotes the set of positive integers) and, λ_{ij} be the total available bandwidth of the link (i, j) between source s and destination d. $\mathbb{P}_{ij}$ is a portion (subset) of λ_{ij} which is reserved for the donor. This bandwidth serves as the primary resource (working path) for the donor. The set of connections $\{t_1, t_2, \dots t_k, \dots t_n\}$ on $\mathbb{P}_{ij}$ is denoted by flow $\mathbb{S}$. Now $\mathbf{B}_{ij}$ is the backup bandwidth that can be utilized by the recipient on λ_{ij} and flow $\mathbb{W}$ represents the set of connections on $\boldsymbol{B}_{ij}$. This causes $\mathbb{P}_{ij}$ equal to λ_{ij} when $\mathbf{B}_{ij}$ is not in utilization. The above defined parameters are pictorially depicted in figure 29.

11 MNOs decide and define what their "required traffic demand" is. It could be satisfying a set of flows consisting of high revenue generating premium customers and/or delay sensitive voice call users etc.

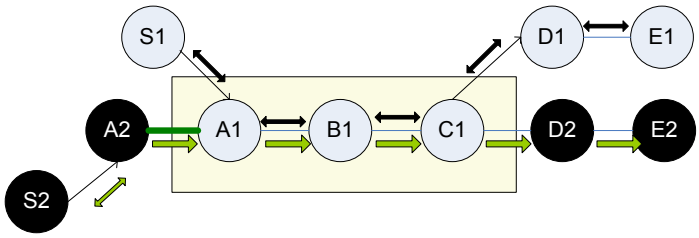


Figure 29: Traffic flow design with infrastructure sharing under faulty conditions with arrow on the bottom indicating traffic from the recipient and arrows on the top indicates the traffic of the donor.

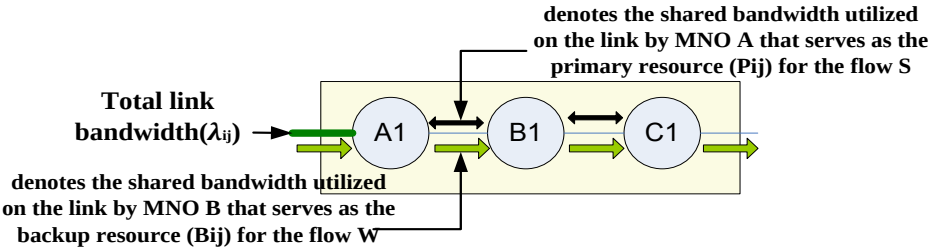


Figure 30: Backhaul link bandwidth allocation through sharing.

Let b be the Blocking Ratio (BR) assuming that not every connection request can be accommodated due to the unavailability of resources and/or constraints (which is detailed later) that are not satisfied. Therefore, the number of connections accepted successfully for the donor can be calculated as:

$$BR_{Donor} = b.\sum_{\mathbb{S}}\sum_{ij\in E} C_{ijk,D} \tag{1}$$

and similarly for the recipient can be calculated as:

$$BR_{Recipient} = b.\sum_{\mathbb{W}}\sum_{ij\in E} C_{ijk,R} \tag{2}$$

Additionally, we classify a hypothetical description to sustain availability requirements cost effectively, i.e. the additional capacity required by the donor to support the recipient traffic contributes significantly to its cost. Given that A_{ij} as the availability of the microwave link (i, j), we associate the cost $\mathbb{C}_{ij}$ as a function of A_{ij}, For more details on this, please refer [reference]. i.e.,

$$\mathbb{C}_{ij} = -\log A_{ij};\ \text{i.e.}\ \mathbb{C}_{ij} = \alpha_{ij} \tag{3}$$

$\mathbb{C}_{ij}$ = Total cost for additional backup resource for transporting data of the recipient on the donor's backhaul during link failures and/or network congestions.

$$\delta(V_h, V_d) = |P_s(V_h, V_d)| \tag{4}$$

6.3.2. ILP based Optimization for Link Bandwidth Allocation through Sharing

Optimal backup bandwidth allocation through infrastructure sharing seeks to find a stable equilibria point such that the bandwidth resource of the donor is not "eaten-up" by the recipient when used as backup path and at the same time we need to consider how to route the flows of the donor and the flows of the recipient together because primary and backup path pairs need to be routed simultaneously to achieve optimal performance for both of them. Therefore, we formulate the optimal backup bandwidth allocation as the following optimization problem, where optimization must be made so that the overall bandwidth reservation for the shared backup path is kept minimal while not impacting the "required traffic demand" of the donor. Our model is built on the central idea of sharing capacity, where we allocate backup capacity to a recipient based on capacity allocated to individual set of traffic demands of the donor. The effect on the ILP is that the binary variables are essentially converted into integer flow variables (requiring more than a simple relaxation of these variables).

Problem Definitions:

1) Compute resource for the flow $\mathbb{S}$ on λ_{ij} such that the bandwidth reserved $(\mathbb{P}_{ij})$ on the link (i, j) as the primary path of the donor satisfies the "required traffic demand".

2) Compute resource for the flow $\mathbb{W}$ on λ_{ij} such that the backup bandwidth reserved $(\boldsymbol{B}_{ij})$ on the same link (i, j) utilizes without exceeding the limits agreed in the SLA between MNOs.

Variables: Here $\mathbb{P}_{ij}^{C_{ijk,D}}$ and $B_{ij}^{C_{ijk,R}}$ are the variables, because this optimization problem concerns with allocating the backup path bandwidth on the primary path bandwidth. $\mathbb{P}_{ij}^{C_{ijk,D}} = 1$, if the flow $\mathbb{S} = \{t_1, t_2, \dots t_k, \dots t_n\}$ successfully traverses through the link (i, j); otherwise $\mathbb{P}_{ij}^{C_{ijk,D}} = 0$. $B_{ij}^{C_{ijk,R}} = 1$, if the flow $\mathbb{W}$ is successfully re-routed through the link (i, j); othewise $B_{ij}^{C_{ijk,R}} = 0$.

Objective:

$$\textbf{Mininimze} \left(\left(\sum_{\mathbb{W}} \mathbf{B}_{ij}^{C_{ijk,R}} . \varepsilon \right) + \left(\sum_{\mathbb{S}} \mathbb{P}_{ij}^{C_{ijk,D}} . \alpha_{ij} \right) \right), \forall\, ij \in E \tag{4}$$

subject to:

- Flow constraints.

$$\sum_{j:ij \in E} \mathbb{P}_{ij}^{C_{ijk,D}} - \sum_{i:\in E} \mathbb{P}_{ji}^{C_{ijk,D}} = \begin{cases} 1, & i = s \\ -1, & i = d \\ 0, & otherwise \end{cases} \quad \forall \mathbb{S} \tag{5}$$

$$\sum_{j:ij\in E} \mathbf{B}_{ij}^{C_{ijk,R}} - \sum_{i:ji\in E} \mathbf{B}_{ji}^{C_{ijk,R}} = \begin{cases} 1, & i = s \\ -1, & i = d \\ 0\,, & otherwise \end{cases} \quad \forall \mathbb{W} \tag{6}$$

- Demand constraints.

$$\sum_{\mathbb{S}} \mathbb{P}_{ij}^{C_{ijk,D}} = D_{ij}^{C_{ijk,D}}, \qquad \forall\, ij \in E \tag{7}$$

$$\sum_{\mathbb{W}} \mathbf{B}_{ij}^{C_{ijk,R}} . D_{ij}^{C_{ijk,R}} \leq \sum_{\mathbb{S}} \mathbb{P}_{ij}^{C_{ijk,D}} . D_{ij}^{C_{ijk,D}}, \quad \forall\, ij \in E \tag{8}$$

- Availability constraint.

$$\sum_{ij\in E} \mathbb{P}_{ij}^{C_{ijk,D}} . \alpha_{ij} \leq \alpha_D \qquad \forall \mathbb{S} \tag{9}$$

- Bandwidth constraints.
  - Primary Bandwidth constraints for the donor

$$\sum_{ij\in E} \mathbb{P}_{ij}^{C_{ijk,D}} \leq \mathbb{P}_{ij} . \lambda_{ij} \qquad \forall \mathbb{S} \tag{10}$$

  - Backup Bandwidth constraints for the recipient

$$\sum_{ij\in E} \mathbf{B}_{ij}^{C_{ijk,R}} \leq \mathbb{P}_{ij} \qquad \forall \mathbb{W} \tag{11}$$

$$\mathbb{P}_{ij}^{C_{ijk,D}}, \mathbf{B}_{ij}^{C_{ijk,R}}\ \varepsilon\ \{0,1\}, \text{such that } ij \in E \tag{12}$$

The objective function illustrated above in (4) tries to maximize the availability of the bandwidth reserved for the flows of the donor and at the same time, minimizes bandwidth resource utilization for the flows of the recipient, where ε is a small value that we have assigned arbitrarily, so that satisfying the "required traffic demand" of the donor is of higher priority. Equation (5) gives the flow balance for the primary path for the set of flows $\mathbb{S}$ that already exists in the bandwidth W_{ij} and (6) gives flow balance for the backup path for the set of flows $\mathbb{W}$ that has to be routed through the reserved backup bandwidth along the microwave link (i, j), guaranteeing that the traffic demand requirements for the donor and the recipient are satisfied respectively. In the rest of chapter, we will refer to (5) as the primary flow constraint and (6) as the backup flow constraint. By (7), we ensure that there is enough bandwidth resource for the donor to accommodate its "required traffic demand $D_{ij}^{C_{ijk,D}}$" for the set of connections $\mathbb{S}$ before it allows the recipient to share. Only when (7) is fulfilled, the recipient is permitted to take hold of its part

of the bandwidth resource if and only if the demand of the recipient is no greater than the donor. This is ensured by (8). Furthermore, in (9), we impose that the availability of a connection on the primary path should not be downgraded than the minimum required availability to satisfy the "required traffic demand" of the donor. Now, considering the problem of dividing and sharing the bandwidth resource between the MNOs as a means for backup, in typical real world situations, the bandwidth that is reserved for the connections of the recipient as the backup path are not utilized as much as the bandwidth reserved for the donor as the primary path. Therefore, the above defined optimization problem in (4) is relaxed by decoupling the bandwidth reserved for the recipient as the backup path (B_{ij}) on the link (i, j) from the bandwidth reserved for the donor as the primary path ($\mathbb{P}_{ij}$) on the link (i, j) as in (10) and (11). In (10), we assume that initially all of the bandwidth on link (i, j) (i.e. $\mathbb{P}_{ij}.\lambda_{ij}$) can be utilized for the provisioning for the primary bandwidth for the donor. A general static connection-provisioning problem can also consider optimizing the bandwidth on the primary path to avoid over-utilizing or congesting links. (11) ensures that the bandwidth that is reserved for the backup for the recipient does not exceed the bandwidth reserved for the donor. To obtain a linear program, we relax the last constraint to $\mathbb{P}_{ij}^{C_{ijk,D}}, B_{ij}^{C_{ijk,R}} \in \{0,1\}$ in (12). Therefore, the optimal solution to a LP relaxation of an ILP problem gives us a bound on the optimal objective function value. For maximization problems, the optimal relaxed objective function value is an upper bound on the optimal integer value. For minimization problems, the optimal relaxed objective function value is a lower bound on the optimal integer value.

6.3.3. Heuristics based Approach for Link Bandwidth Allocation through Sharing

The above ILP formulations of section IV can be solved only for smaller node sizes. The complexity of an ILP formulation is the product of the number of equations by the number of variables, such as our case too. Due to the complexity that ILP solvers face while solving even mid-sized networks with a large number of binary variables, in what follows next, we resort to heuristics.

6.3.3.1. Algorithm for Link Bandwidth Allocation through Sharing

Based on our architectural design, we propose an algorithm that we term as Divide and Share by Infrastructure Sharing (DASIS) Algorithm. The specificity of this algorithm is to allow (backhaul) link bandwidth sharing among MNOs excluding the need for an additional backup path, in addition to be able to satisfy the "required traffic demand" for the donor. The idea of our algorithm is that the bandwidth resource of the donor is re-evaluated constantly, so that the

existing traffic demand is not jeopardized. During this re-evaluation, the donor's network resources are constantly computed for the backup bandwidth reservation to determine if it is efficient enough to maximize the network resource utilization subject to: Availability constraint, SLA constraint and Bandwidth Constraint. Algorithm 1 describes this. To interpret the algorithm below easily, we assume that there is a link failure in MNO B (as in figure 29). Therefore, working path of MNO B (W2) becomes unavailable and the traffic is re-routed through working path of MNO A (W1).

ALGORITHM 1 DIVIDE AND SHARE BY INFRASTRCUTURE SHARING (DASIS) ALGORITHM

INPUT: Network topology *G = (V, E, A, λ)*; Connection request $C_{ijk,R}$.

OUTPUT: New backup-path W with a backup bandwidth B_{ij} is established satisfying the connection $C_{ijk,R}$'s constraints; or refuse $C_{ijk,R}$ if no such path(s) is found.

STEP 1) Compute the minimum required bandwidth $\mathbb{P}_{ij}$ on λ_{ij} from s to d on W1 for the donor.

STEP 2) Set the initial backup bandwidth B_{ij}on λ_{ij} for the recipient as null.

STEP 3) Compute the backup bandwidth B_{ij} that has to be reserved on W_{ij} from s to d on W1 based on the following three constraints:

> **STEP 3.A) Availability constraints:** Compute the availability of W1 and check if the k-th connection request $C_{ijk,R}$ is satisfied according to $0 < \mathcal{B}_{C_{ijk,R}} \leq B_{ij}$ such that the set of flows $\mathbb{W}$ utilizing B_{ij} of the recipient are re-routed successfully and go to Step 3.b. Refuse connection $C_{ijk,R}$ if availability constraints are not satisfied and /or path W1 is not found.
>
> **STEP 3.B) SLA constraints:** If $B_{ij} \leq$ SLA agreed between the donor and the recipient, set W1 as the working path for the recipient and go to Step 3.c. Refuse connection $C_{ijk,R}$ if SLA constraints are not satisfied and /or path W1 is not found.
>
> **STEP 3.C) Bandwidth constraints:** Now check whether the bandwidth availability requirement for the donor is also still satisfied, i.e. $B_{ij} \leq \mathcal{B}_{C_{ijk,D}} \leq \mathbb{P}_{ij}$ and go to Step 4. Refuse connection $C_{ijk,R}$ if bandwidth constraints are not satisfied and /or path W1 is not found.

STEP 4) Connection $C_{ijk,R}$ is accepted and a new backup-path W with a backup bandwidth B_{ij} is established for the recipient on the donor's backhaul.

STEP 5) Update network resource information accordingly so that the total available bandwidth is divided and shared appropriately.

Using Algorithm 1, the degree of sharing is controlled stringently such that network resources are shared and utilized more intelligently and efficiently, nevertheless to say that the flow connections of the donor are sustained to be able to meet the demand requirements. In practice, we do not execute these three constraints step by step but mix them together. Trap situations might result when a connection is refused if the algorithm fails due to limited bandwidth resources on the donor.

6.3.3.2. Description of the Algorithm

From the previous discussions in section III, it is made clear that the requested bandwidth for the backup path should be allocated along the primary path. Thus for any link with end points (i, j), the amount of bandwidth reserved for the donor is the sum of the requested bandwidth of individual connections in $\mathbb{S}$ whose primary paths use that link. This is denoted as:

$$\mathbb{P}_{ij} = \sum_{\mathbb{S} \in \mathbb{P}_{ij}} \mathcal{B}_{C_{ijk,D}} \tag{13}$$

where, $\mathcal{B}_{C_{ijk,D}}$ denotes requested bandwidth of an individual connection $C_{ijk,D}$ of the donor. Thus, we first determine the minimal bandwidth for the donor which can satisfy the "required traffic demand". To do this, we first set an initial high value, and start to decrease this value one by one until when all the connections can be set up in the optimization. The process is repeated until some connections cannot be set up. This value is fixed as the value in previous loop. Here, no connections are blocked since all the connections can be carried satisfactorily. In particular, across any link (i, j), we allocate the minimum required bandwidth for the set of flows $\mathbb{S}$ on the primary path through which the minimum demand $D_{ij}^{C_{ijk,D}}$ is satisfied. We define this as the *Minimum Required Primary path Bandwidth (MRPB).* Formally it is written as,

$$\mathbb{P}_{ij}^{MRPB} = \min_{ij \in E \setminus D_{ij}^{C_{ijk,D}}} \sum_{\mathbb{S} \in \left((\lambda_{ij} \cap \mathbb{P}_{ij}) U \, \boldsymbol{B}'_{ij}\right)} \mathcal{B}_{C_{ijk,D}} \tag{14}$$

At the same time, we enforce a lower bound on bandwidth allocation for backup path since allocating more bandwidth for the backup may interrupt the bandwidth reserved for the primary path. For this, we consider the baseline approach in which no backup path bandwidth is allocated initially. We define this as the *Zero Backup path Bandwidth (ZBB)*.

$$\boldsymbol{B}_{ij}^{ZBB} = 0 \tag{15}$$

So the goal of the backup path bandwidth allocation algorithm is to determine B_{ij}, the amount of bandwidth that needs to be reserved on link (i, j) for the backup path across this link. Similar to primary path bandwidth allocation, a naive approach for backup path bandwidth allocation is to reserve the requested bandwidth of each flow along the backup path. We define this as the *Minimum Required Backup path Bandwidth (MRBB)* across link (i, j) which is the sum of the requested bandwidth of those flows whose backup paths use this link. Formally it is given as,

$$\boldsymbol{B}_{ij}^{MRBB} = \sum_{\mathbb{W} \in \boldsymbol{B}_{ij}} \mathcal{B}_{C_{ijk,R}} \tag{16}$$

Finally, we enforce the maximum bound for the bandwidth allocation for the backup path on this link. This bound is necessary so that the bandwidth reserved for the backup neither affects the availability requirements nor ignores the SLA constraints nor affects the bandwidth for the "required traffic demand" of the donor. We define this as the *Maximum Backup path Bandwidth Allocation (MBBA)*.

$$\boldsymbol{B}_{ij}^{MBBA} = \max_{ij \in E \setminus D_{ij}^{C_{ijk,D}}} \sum_{\mathbb{W} \in \left(\left(\lambda_{ij} U \left(\mathbb{P}_{ij} \cap \boldsymbol{B}_{ij}\right)\right)\right.} \mathcal{B}_{C_{ijk,R}} \tag{17}$$

To implement MRPB, we need to guarantee that every node has the information of the requested bandwidth $\mathcal{B}_{C_{ijk,D}}$. We can use any signaling protocol that can reserve the requested bandwidth for the donor. To implement MRBB for the new connection $C_{ijk,R}$ from a recipient to use any link (i, j), this signaling protocol indicates each node along the primary path about the requested backup bandwidth. To avoid the expense of maintaining per-flow state, we can take advantage of the algorithm for the partial information scenario proposed in [13]. However, description of how the signaling protocol works in detail is beyond the scope of this chapter.

Remark 1: In [15], a clear evaluation on the relationship between the degrees to which the resources can be shared and the availability offered by any protection scheme resulting out of sharing is made. The authors stated that ability of connection to restore from failure is affected by the degree of sharing and hence they had proposed techniques to optimize the capacity requirements for protection scheme with explicit limits on the sharing degree. However, in our approach (i.e., Algorithm 1), we do not place explicit limits on the sharing degree. Instead, the degree is automatically controlled by the allocation of backup capacity based on capacity allocated to individual set of traffic demands of the donor, which provides more flexibility.

Remark 2: The authors of [97] elaborate about computing a separate share of resource along a link (i, j) for a connection t=(s, d, SLA), where they aim at determining the bandwidth

assignment and the traffic flows that minimize the total bandwidth cost, but we feel that our optimization here are certainly more customized for the current problem of sharing between different MNOs.

Remark 3: The computational complexity involved for our algorithm is similar to that of a standard shortest-path routing algorithm, i.e., O(L + NlogN), given that L is the size of E and N is the size of V.

Thus, the adaptation of our approach enables to cautiously control the total capacity allocated to the backup paths without affecting the bandwidth requirements for the donor. The backup capacity optimized indirectly depends upon the availability of the primary path, which directly depends upon the cost C_{ij}. This encourages MNOs to divide and share their resources to reduce the total cost of setting up an entire backhaul network.

6.3.3.3. Competitive Differentiation

Our approach here is to define which type of traffic needs to be protected all the time, and which can have a lower level of protection rather to protect all traffic at all costs, i.e. a trade-off among resource utilization, availability and the cost. The priority for differentiation in traffic that flows through another MNOs' backhaul is decided by the MNOs themselves. True, the above scenario does not offer a 100% protection scheme like in the SDH world. It does however offer 100% protection level for premium (i.e. revenue generating) traffic during partial network downtime, while leaving some headroom for low priority service so as to avoid starvation. At any other time, the network can utilize all the available bandwidth, providing higher capacities at a much better cost-per-bit ratio than SDH. Taking advantage of the now available granularity features, e.g. using OpenFlow, MNOs can "split" their capacity according to service types, i.e., a 200Mbps link can be utilized as follows: 50Mbps high-priority real-time services at 99.999%; 100Mbps data services at 99.99% and 50Mbps for low-priority traffic at 99.9%. From a first glance it may seem like we have reduced availability, but in truth, the system ensures that premium types of service never fail and have a guaranteed bandwidth regardless of any other traffic. Thus, MNOs protect and improve the availability of their revenue generating services to ensure high-quality, uninterrupted user experience, and increase link capacity to offer more data services.

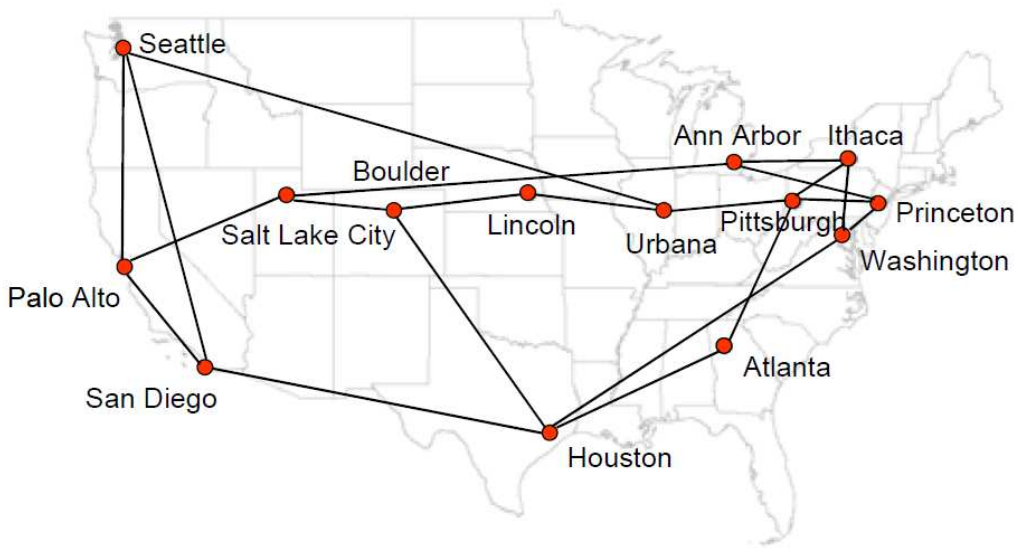
6.4. Illustrative Numerical Evaluation

6.4.1. Experimental Set-up and Computational Considerations

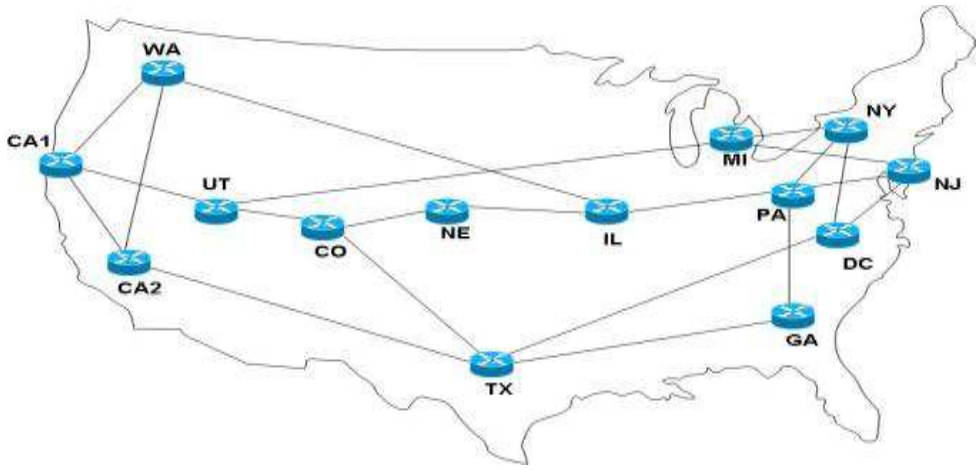
In this section, we present simulation results to evaluate the performance of shared backup path

routing and bandwidth resource allocation algorithm that we proposed. Numerical evaluations comparing the performance of ILP-based approach and heuristic-based approach of the proposed method are presented. Our algorithms are based on fixed, shortest path routing. In order to get an overall picture of the attainable performance gain of our framework, we simulated for various network sizes of 5, 6, 8, 10, 14 (the choice is mainly for evaluation purposes and not for any specific reason of the node sizes) NSFNET network (14-node NSFNET topology is shown in Fig. 4) on Intel Pentium Core 2 Duo 3 GHz, 4GB RAM machine. For a particular network topology, we generated 3 traffic demands (standard OC3, OC 12 and OC48) between each node-pair since it is a way of distinguishing more types of traffic classes. Each demand had a random bandwidth from 1 to 200 Mbit/s. The underlying solver for the ILP was LP Solve [88].

Due to the limited access to the information of link failure patterns in the real networks, we use an exponential physical link failure model in our simulations. We assume that link failures are not permanent but can be fixed by some means. With the exponential link failure model, we assume that both up-times and down-times of a physical link follow exponential distributions. We randomly assign failure probabilities to physical links uniformly and independently. Then we generate physical link failures at random following the exponential link failure model discussed below. To make the failure probability of a physical link be pp, the rate of down-times should be μ (1-p/ p) if the rate of up-times is μ. For dynamic traffic, the arrival of traffic to the network follows a Poisson distribution with a rate of λ connection requests per unit time and a connection-holding time that is exponentially distributed with a mean value of μ. An arrival request is equally likely to originate from and be destined to any node in the network. The network load is given by λ/μ. We use GT-ITM to generate the network topology for our simulations.



(a)



(b)

Figure 31: Illustration of 14-Node NSFNET topology.

6.4.2. Performance Comparison between ILP and Heuristics.

Bandwidth Utilization versus Number of Nodes: Network resource utilization efficiency is defined as the ratio of the bandwidth reserved for the backup connections to the bandwidth reserved for primary connections [99]. It is a measure that exhibits the additional resource overhead (RO) utilized for backup. Better backup-sharing optimization is achieved when the resource overhead is lower. Thereby, the objective here to estimate the usuage of the backup path bandwidth of the recipient on the primary path of the donor.

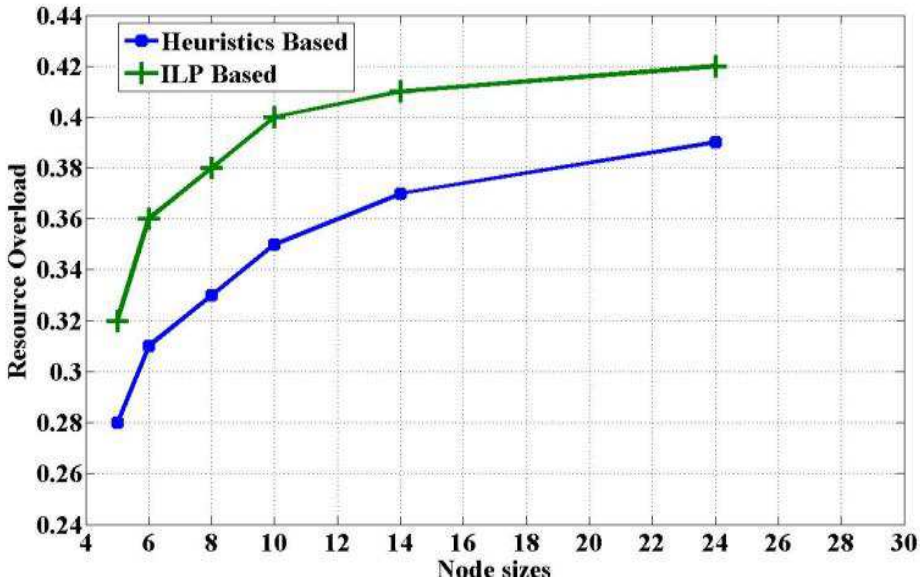


Figure 32: Illustration of Resource Overhead versus Number of Nodes.

Figure 32 demonstrates resource overhead for the ILP-based and the heuristics-based approaches for different node sizes. From the results, it can be noticed that, as the node size

increases, the resource overhead value decreases because of our approach. What this means to us, is that, by our approach, we could possibly achieve less resource overhead, meaning that, the occupancy of the backup bandwidth on the primary bandwidth gradually decreases for large network sizes, which gives more freedom for the donor to provision more resources for their own demands. Furthermore, it can also be seen that the RO due the ILP-based approach has higher values than those of the heuristics-based approach due to computational complexity.

Blocking Probability versus Number of Nodes: The blocking probability is a measure of the number of connection requests rejected against the total number of connection requests. The main measure here is to compare the performance of the ILP-based approach and the heuristic–based approach. The number of connections provisioned is calculated by simulating at least 10,000 connection requests, under dynamic traffic. Figure 33 demonstrates the number of connections that are provisioned with ILP and heuristic based approaches for different node sizes. We find that a connection is less likely to be blocked by in ILP than in heuristics.

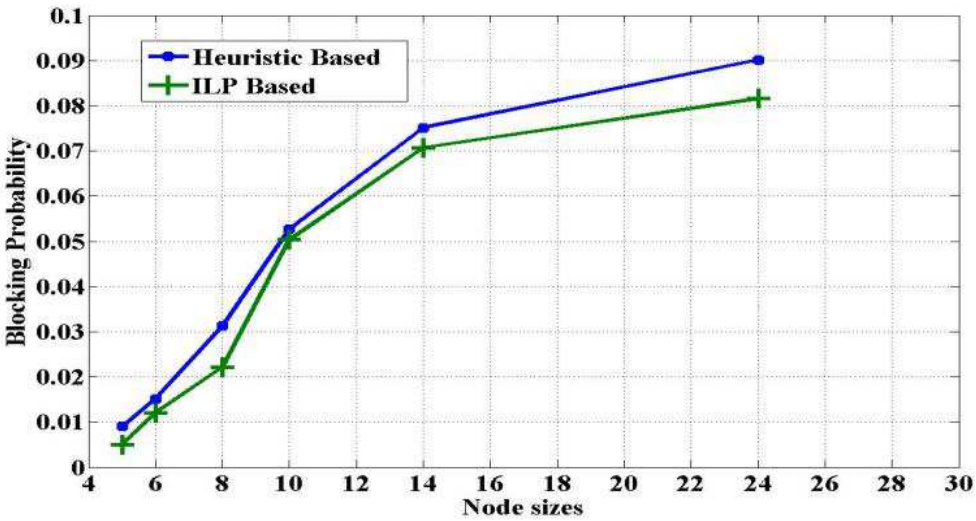


Figure 33: Illustration of Blocking probability versus Number of Nodes.

Our justification for this is that in ILP routing is not limited by candidate routes, since our heuristics are based on shortest path routing. Also, from figure 33, we could observe that ILP has overall lower blocking probability compared to heuristics-based approach.

Cost versus Number of Nodes: As we observe from the results, as the node size increases, the cost for provisioning additional backup resource decreases for the heuristics as well the ILP. It can also be seen that the performance of heuristics is almost the same as compared to the ILP for smaller network sizes (for N=5, N=6 etc) while the performance improves and gets better than those of ILP for larger networks (N=14, N=22 etc). What is illustrious here, this efficiency that is achieved is without any additional cost at all for backup resource.

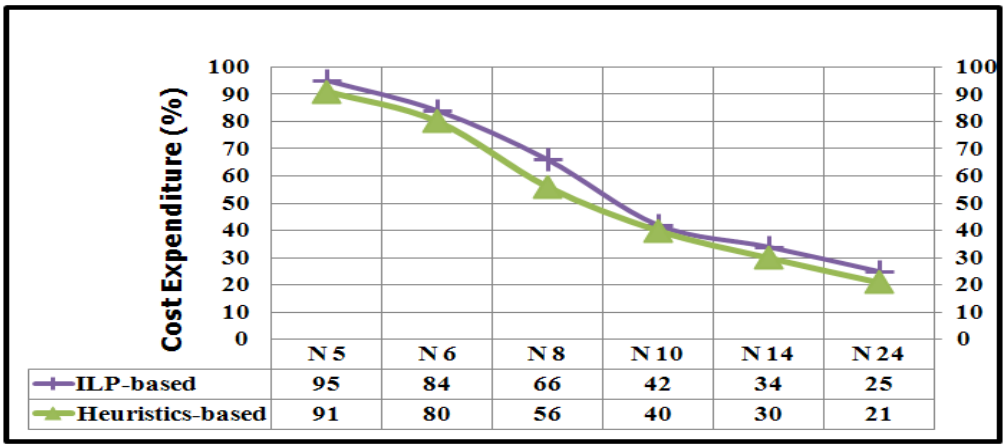


Figure 34: Illustration of Cost versus Number of Nodes.

Overall Performance Evaluation Remarks: Overall, we observe that the performance of resource sharing by the heuristic and the ILP approaches improves as the size of the network increases. From our experience, we reason out that ILP solvers have a difficult time solving our model which has binary variables in abundance. On a conclusive basis, we could say that the ILP-approach necessitates more resources (link bandwidth) to produce similar performances as that of the heuristics.

6.5. Concluding Discussions

As the mobile communications sector continues its relentless expansion with more subscribers and more advanced services generating ever-greater volumes of traffic, MNOs must invest in their infrastructure to provide the bandwidth to meet the demand. Network congestion or mobbing and traffic overloading is resource-sharing problem, which will upswing whenever resources are not enough to meet users demands. As discussed in this chapter, we have presented a novel resource sharing framework which can cost-effectively provide protection services by guaranteeing the service demands without jeopardizing minimum required demands for the MNOs.

We have introduced mathematical formulations and proposed resource provisioning algorithm for this problem. Our framework here is ILP-based and heuristic-based provisioning approach to tackle the problem of assigning bandwidth between MNOs for reliable wireless backhaul networks. While the initial results are encouraging, there are exceptions as well. One such potential disadvantage is the complexity due to the dynamic nature of the supported customer base, the required memory and execution time of our method grows exponentially. Consequently, by the time the optimization results are available, the environment may have changed. Our response to this is to implement methods to shorten the modeling cycle time orderings of outcomes to establish equilibria.

*"We especially need imagination in science. It is not all mathematics, nor all logic, but it is somewhat beauty and poetry." – **Maria Montessori, Italian Physician and Educator.***

Chapter 7

X-Control: A Quasi-Distributed Fault Restoration Mechanism Using Logically Centralized Controllers

Thus far, we have discussed on how backhaul network resources could be shared among multiple MNOs. To tackle the management complexity of a backhaul network that comprises of several MNOs/ISPs 'heterogeneous' network equipments, an alternative approach involves centralized management and network-wide control using logically centralized controllers - accountable for collecting, computing, and maintaining the state required by the individual network equipments, to operate coherently. While such physical centralization is good as a first order evaluation example, practical deployment of such architectural design to various application scenarios, such as ours, may be restricted by questions about the overall scalability, restoration latency, convergence delay of the physically centralized controller. With this background, here we illustrate the survivability of backhaul networks with reduced amount of physical redundancy, by effectively managing geographically distributed backhaul network equipments which belong to different MNOs using 'logically-centralized' physically-distributed controllers, while meeting strict constraints on network availability and reliability.

7.1. Introductory Statements

7.1.1. Concept Visualization

Network Resilience, as in [100], which ensures quick recovery and thus continuous availability, is considered as an important factor in assessing a network design. Among others, one naive solution to guarantee uninterrupted availability is to over-provision the network links, sometimes termed as Redundancy. Through our earlier chapters, we argued over the necessity for every independent Mobile Network Operator (MNO) within a geography to build permanent backup paths (redundant paths) – because the capacity which is allocated for the backup path is not always actively filled-in as much as the capacity allocated for the primary path. Our arguments led to a novel design in which two or more MNOs share each other's unused network resources mutually (links/bandwidth capacities), up to a certain extent without exceeding their limits on resource sharing, thereby saving on over-provisioning costs. With this background, here we illustrate the survivability of backhaul networks with reduced amount of physical redundancy, by effectively managing geographically distributed backhaul network equipments which belong to different MNOs using 'logically-centralized' physically-distributed controllers, while meeting strict constraints on network availability and reliability. Therefore, as a first step towards this illustration, it thus becomes inevitable to demonstrate the reliability of 'logically-centralized' physically-distributed controllers placed across the geography. Today, the reliability of Software Defined Networking (SDN) control networks has been gaining much attention in research in the recent past, with works such as [101]-[103]. However, there has been no general analytical framework to model network resilience under shortest path routing policy and single link failure in a logically centralized architecture, strictly speaking, the SDN architecture.

7.1.2. Motivation

Logically centralized network-wide control enables data-plane and control-plane separation in communication networks. This approach lays the foundation for a range of industrial products and academic contributions such as: BGP Route Reflectors [104], RCP [105], MPLS Path Computation Elements with Label-Switched Routers [106], enterprise wireless controllers with CAPWAP access points [107], 4D planes [108], Ethane [109], and recently Software-Defined Networks (SDN) that enables OpenFlow-based switches and controllers [110]. While the above stated decoupled architectures proposes a logically centralized control plane, until now the investigations of such design have been limited to physical centralization [111], [112] where 'one centralized controller' acquires the required network information, executes the essential algorithms for computing the network state, and communicates this state information to the data forwarding elements i.e., switches and routers. While such physical centralization is good as

a first order evaluation example, practical deployment of such architectural design to various application scenarios, such as ours, may be restricted by questions about the overall scalability, restoration latency, convergence delay of the physically centralized controller. Although a very few recent works [113], [114] have explored the scalability of the centralized controllers and their placement, the results of these research works are restricted towards the investigation of the controllers' scalability and its placement within one network domain, i.e. every controller has the (complete) view of only one topology, i.e., a single network. That being said, in this chapter, we propose a quasi-distributed fault restoration mechanism for backhaul networks. Within the scope of our research, our contributions in this work exclusively focus on:

- Illustrating a restoration architectural design paradigm of a communication network by adapting the logically centralized approach and more specifically towards a Quasi-Distributed approach. For reasons which are made clear later, we call the resulting scheme as Cross-Control (*X-Control*).

- Consequently, our scheme has been developed and evaluated with proof of correctness specifically including (i) an extensive stochastic model which characterizes our problem as a multi-constrained optimization problem (ii) completely new Integer Linear Programming (ILP) formulations based on the model definitions (iii) an efficient greedy heuristics based on convex combination technique [115] to solve the formulated ILP model (iv) performance evaluation on real network topologies.

7.2. Towards A Quasi-Distributed Fault Restoration

As stated before, Network resilience ensures that the network recovers quickly and smoothly from one or a series of failures/disruptions. Network resilience could be maximized by minimizing the convergence delay after a link/ node failure, thereby ensuring maximum uptime. Hence, network resilience is fundamentally limited by convergence delay bounds. Minimizing convergence delay will reduce the amount of time for the routing to stabilize, after any topology change. Founded on this fundamental definition, in this chapter, we present a general analytical framework to maximize network resilience in SDN based architectures. The complexity here lies in the convergence on failure procedure which requires exchange of information among network elements (controllers-to-controllers as well as controllers-to-nodes) within the limits of the convergence delay bounds. Such exchange necessitates each controller to take part in negotiating 'the global optimal solution'. Typically to define optimality here, we converge on the objective of maximizing network resilience, which narrows-down to solving a multi-constrained optimization problem. As a consequence, here we look at minimizing the convergence delay (i) first by placing controllers at 'close proximity' (near) faulty locations, thus rapidly detecting a

topology change (ii) and then by optimizing 'the total cost' in information exchange between network elements, in the event of topology changes. Our approach takes into account important factors such as network connectivity, failure locations, and routing message processing delay, following a change in the network topology or policy.

7.2.1. Cross-Controller Network Design: When Controllers Talk!

Before we dive into characterizing the overall optimization procedures, we begin with a flavor of the Quasi-Distributed Fault Restoration Mechanism here, demonstrating through real topologies with the illustration of Cross-Controllers (Figure 35). In Figure 35, all links in Red color represent Internet2 L1 topology (let's say, A) and all links in Green color represent TeliaSonera US L1 topology (let's say, B). Nodes C_A and C_B represent the 'restoration controllers' of A and B, which are placed at Kansas (geographical centre for now for illustration purpose). Each controller maintains a database (such as MIB [13] for instance) containing network graphs and re-routing algorithms. Each controller updates this database periodically and independently via the states collected from their respective physical network domain (e.g., through port counters or flow-level statistics gathering). The specificity of this design is now notably distinguished by connecting the restoration controllers C_A and C_B (via a proxy controller) [12]. It allows C_A and C_B to synchronize themselves in order to disseminate their domain state. A direct implication of this design is that every controller locally stores the complete view (full reachability information) about its own topology, but synchronizes to access partial view (relevant information) about other MNOs topology information. We call this Inter-Domain Synchronization (IDS) [13]. The extent to which the topology information is synchronized translates to the specific functionality of the centralized control plane, for which it is intended. Therefore MNOs are not required to disclose their entire topology information always, i.e., under normal operation, C_A manages the set of nodes of the topology of A though they are also reachable by C_B and C_B manages the set of nodes of the topology of B though they are also reachable by C_A. In this scenario, we assume a routing policy that takes local decisions at each restoration controller based on the available information, without exchanging any more messages than what is needed to disseminate the information about the event. We recall that shortest path routing exhibits this property as each entity takes local decisions without negotiating the possible choices with other entities. Our approach, as termed as quasi-distributed scheme, as evident as it is, employs the advantages of both the distributed and the centralized approaches. We call such a design as *Cross-Controller design*.

[12] The (optional) proxy controller links multiple MNO controllers and serves as a backup agent by providing fan-out capabilities to minimize network load.

[13] Chapter 8 exclusively deals with Inter Domain Synchronization (IDS).

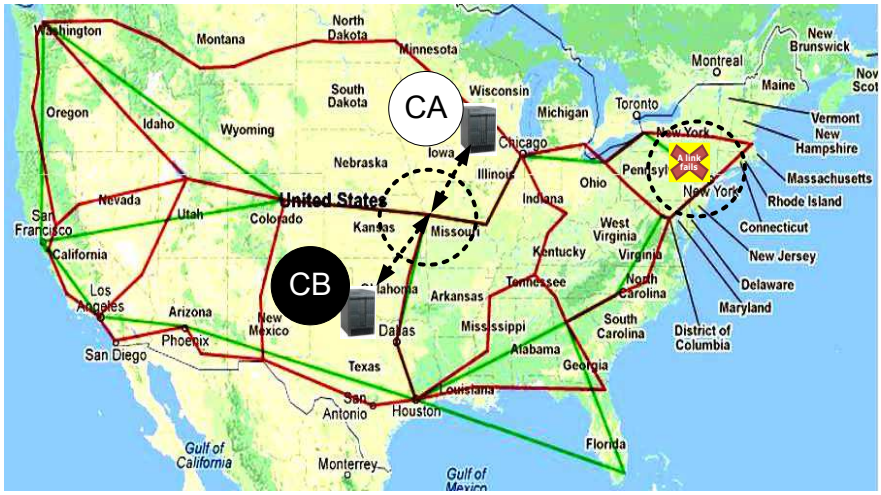


Figure 35: An illustrative example outlining Quasi-Distributed Fault Restoration Mechanism for the U.S. Two MNOs share their resource (links/bandwidth capacity) by discreetly sharing their topology information using cross-controllers, making a 'resilient' topology, thus avoiding the need for redundancy in the already existing topology. Multiple stand-by controllers can takeover in case of failure of the controller itself.

Having introduced the basics, moving forward, now we get to the bottom of the details. To start with, for instance, let's say the green link of B between New York city and Philadelphia is not available– due to bad weather/ bomb-blast (we recall 9/11, Hurricane Katrina 2005, etc) at that particular geographical zone. Traditionally, the information of the failed link is propagated through flooding. Naturally flooding linearly scales with the distance of the longest loop free path. On the contrary, in this approach, rather than being flooded, each controller works collaboratively with other controller(s) in order to accomplish the overall network-wide control to compute end-to-end available paths, in response to individual failure events. Here, all routes between node(s) and its respective controller(s) use the available shortest path connections between nodes. Precisely, upon a failure (link/node) at NewYork city, the information goes to the respective controller C_B , which will detect a topology change based on link status and reachability information by Link State Advertisement (LSA) packets and therefore starts synchronizing with C_A negotiating for new end-to-end available routes. C_A will in turn, calculate the active routes from all the routes within its own topology and informs about the available routes to C_B. C_B chooses the path with the lowest max link utilization on which to assign the next arriving flow, sends the updated routing tables to the affected nodes at NewYork city, updates the forwarding tables and establishes new routes. Therefore the incoming traffic will be re-routed through the new available routes and reaches the core network of B. This we define as Reactive Forwarding or Flow-Driven Forwarding, where the controller updates the forwarding tables and installs new routes into the nodes, upon a topology change. Network is said to be converged when none of the forwarding tables are 'volatile' after a duration. This duration is quantified as some time interval, based on the expected maximum time to stabilize, after a

topology change, defined as Convergence Delay and this process is defined as Network Convergence, the process of synchronizing forwarding tables of 'network elements' after a topology change.

7.3. On Characterizing Topology Changes

TABLE V. LIST OF NOTATIONS AND SYMBOLS USED IN THE MODEL

Notations	Implications
$G = (V, C, E, D, L)$	Weighted bi-directional graph denoting the backhaul.
$V = (v_1, v_{2,}, \dots v_n)$	Set of vertices of the graph containing the nodes, $\forall v \in V(G)$ (microwave towers, edge routers, switches, gateways, PoP etc)
$C = \{c_1, c_{2,}, \dots c_k\}$	Set of restoration controllers for centralized management of each MNO topology, $\forall c \in C(G)$.
$E \supseteq \{E_{ij}^{v}, E_{ij}^{c}, E_{ij}^{vc}\}$	Set of edges of the graph that includes the set of all possible link properties, $\forall e \in E(G)$.
$E_{ij}^{v} = \{e_{ij}, i, j, \in V\}$	Subset of $E(G)$ that includes direct links e_{ij}between any two distinct vertices i, j of the graph, $\forall v \in V(G)$.
$E_{ij}^{c} = \{e_{ij}, i, j, \in C\}$	Subset of $E(G)$ that includes direct links e_{ij}between any two distinct controllers i, j of the graph, $c \in C(G)$.
$E_{ij}^{vc} = \{e_{ij}, i, j, \in V \in C\}$	Subset of $E(G)$ that includes links e_{ij} between a controller and a node i, j of the graph, $\forall G$.
$D: E \rightarrow R+$	Delay function which assigns a non-negative weight to each link e denoted by a weight vector $\vec{w}(e) = (w_1^e, w_2^e, \dots, w_z^e)$, where edge weights represent propagation latencies, $\forall e \in E(G)$.
$L = \{l_1, l_2, \dots l_m\}$	Set of faulty locations in the backhaul topology, $\forall\, ij \in E(G), (i, j) \in V(G)$ and $l \in L(G)$.
$\mathcal{F}_L^t, \gamma_{ij,c}^t$	Binary variable denoting (i) a topology change triggered by a fault (ii) the existence of a controller near a fault.

A topology change could be characterized as a stochastic variable with a probability density function $f(t)$ that is proportional to the cumulative failure rate $F(t)$ of a location defined over the time from $t = 0$ to $t = \infty$. Therefore, now we introduce our model definitions to quantify the distribution of faults. We define a faulty location as a potentially defective stochastic spatial location experiencing disruptions resulting from one or a series of link and/or node failures due to the absence of sufficient redundancy. Thus, the failure rate of a location l_i denoted as $\lambda(t)$, describes the frequency with which faults occur at that particular location per unit time. With this, we define $\lambda(t)$ of a location l_i at any time instant t, defined as,

$$\lambda(t) = \lim_{\tau \to 0} \frac{1}{\tau} \left(\frac{F(t+\tau) - F(t)}{R(t)} \right) \tag{1}$$

where, $R(t)$ denotes the system reliability function defined as the probability that the time to failure of the system (the lifetime of the system, denoted as T) is beyond some specified time t represented as $Pr(T > t)$ and F(t) denotes the probability that a randomly selected unit will fail

by time t at a particular location represented as $\Pr(T \leq t)$ and τ denotes the time increment during which the failure exists. For the purposes of this research, we define the failure rate of a location as the derivative of the cumulative failures with respect to 'distance' i.e., the failure rate is defined as the number of failures per unit distance (δ). The cumulative failure data consists of a discrete set of data points, inhibiting the calculation of the exact derivative per (2), given below as:

$$Failure\ Rate, \lambda(\delta) :\Leftrightarrow \lim_{\Delta distance \to 0} \left(\frac{\Delta failures}{\Delta distance} \right) \tag{2}$$

Note that (2) strictly agrees with (1) if reliability R(t) is 1, and time is replaced by distance. With the above definition of failure rate, we now introduce our first binary variable, $\mathcal{F}_z^t$, to quantify a topology change due to a faulty location l_i from the set $L = \{l_1, l_2, \dots l_m\}$ in the graph at time instant t defined as:

$$\mathcal{F}_L^t = \begin{cases} 1, if\ \exists\ f(t) := \frac{d}{dt} F(t), \forall F(t) = 1 - \left(e^{-\int_0^t \lambda(\delta) dt} \right) \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad Otherwise \end{cases} \tag{3}$$

7.3.1. On Modeling Network Convergence

We now proceed to the next goal to optimize the 'total cost' in information exchange among the network elements in the event of topology changes. Here we approach this goal by systematically characterizing a key metric that we define as Intra-Domain Orientation (IDO). It indicates the controller-to-node connectivity within each MNO topology, i.e., to optimally place a controller near a faulty location that causes a topology change. For instance, in backhaul networks, the 'last -miles' and the 'middle-miles' experience very high and high failure rates, respectively. So, it makes it more serviceable to deploy a controller near these spots than someplace. Placing a controller closer to a faulty location results in faster 'reaction time' than placing a controller several hops away from the faulty location [116]. Hence, we proceed to optimally map the set of controllers $C = \{c_1, c_{2,}, \dots c_k\}$ near a set of nodes $V = \{v_1, v_{2,}, \dots v_n\}$ present at the faulty locations $L = \{l_1, l_2, \dots l_m\}$. We begin by placing a controller from a faulty location based on propagation latencies τ_d between a controller c_i and a node v_i. By adding the individual edge weights $\vec{w}(e)$ of each link from a faulty location, the end-to-end propagation latencies of each path can be determined. Formally, it is:

$$\tau_d = \sum_{e \in E} w_i^e, \forall\ i \in (1, 2, \dots z) \tag{4}$$

where z is number of links in each path. The minimum value of propagation latency (τ_d) corresponds to the optimal distance to place a controller from the faulty location. We call this as

the *Optimal Controller Delay (OCDe),* denoted by Δ. Formally,

$$\Delta \coloneqq \{\min\{\tau_d\} \mid \tau_d \in \{\tau_{d1}, \tau_{d2}, \dots \tau_{d\mathcal{K}-1}, \tau_{d\mathcal{K}}\}\} \tag{5}$$

where, $\mathcal{K}$ is the total number of paths of the topology which has atleast one fault. Equation (5) models the propagation delay between controller c_i and a node v_i. With this, we introduce our second binary variable to determine if there exists atleast one controller near a faulty location on link (i, j)εV and ijε E at time instant t, defined as:

$$\gamma_{ij,c}^{t} = \begin{cases} 1, if \ \exists \ \Delta \sum_{l \in L} \mathcal{F}_L^t \leq \min\{\tau_d\} \\ 0, Otherwise \end{cases} \tag{6}$$

Having clearly delimited ourselves with our definitions, we now formalize on the definition of Convergence Delay $\mathcal{D}$ given as per (7), which indicates the maximum time taken for a network to stabilize after a single topology change:

$$\mathcal{D} \coloneqq 2.(E[\max\ (\Delta)\ \max\ (\mathbb{C})]) = 2.E[\max\ (\Delta)].E[\max\ (\mathbb{C})] \tag{7}$$

where, $E[max\ (\Delta)\ ]$ and $E[max\ (\mathbb{C})\ ]$ are the expectation $E(\cdot)$ of the maximum propagation delay values between node-to-controller and controller-to-controller respectively. The implicit implication is that the convergence delay is generically proportional to the network diameter and that the proportionality constants Δ and ℂ may include queuing and transmission delays, as well as propagation delay, especially when multi-hop paths are used. The total delay is twice and hence '2'. The values of Δ and ℂ is protocol specific and can be assumed uniform over the small region of a given network size.

7.4. On Optimizing Quasi-Distributed Fault Restoration Using ILP Based Formulations

Objective: Let $C = \{c_1, c_2, \dots c_k\}$ denote the set of k controllers to be positioned in each MNO network topology. Let $L = \{l_1, l_2, \dots l_m\}$ be the set of possible faulty locations. Given a pattern of failure rates for fault locations extracted from section II, our goal is to choose controller locations that minimize the total convergence delay after a topology change, under shortest path routing policy and link/node failure, at time instant t, thus maximizing the overall network resilience.

Variables: $\gamma_{ij,c}^{t}$ is the decision variable in this optimization problem. $\gamma_{ij,c}^{t} = 1$ if there is atleast a controller c_i allocated near a fault location l_i; else $\gamma_{ij,c}^{t} = 0$.

Thus, our ILP model can be formulated as:

$$\textbf{Minimize}\left(\left(\sum_{c\in C}\gamma_{ij,c}^{t}\right)\right) \tag{8}$$

subject to:

$$\sum_{l\in L}\mathcal{F}_{L}^{t}=1,\ \forall\ ij\in E,(i,j)\in V,L=\{l_1,l_2,\dots l_m\}\in G \tag{9}$$

$$\sum_{ij\in E}\gamma_{ij,c}^{t}>0,\ \forall\ ij\in E\ ,(i,j)\in V,C=\{c_1,c_{2,},\dots c_k\}\in G \tag{10}$$

$$\sum_{l\in L}\gamma_{ij,c}^{t}+\sum_{l\in L}\gamma_{ji,c}^{t}\ \leq 1,\quad \forall\ C=\ \{c_1,c_{2,},\dots c_k\}\in G \tag{11}$$

$$\sum_{l\in L}\gamma_{ij,c}^{t}+\sum_{l\in L}\gamma_{ji,c}^{t}\ \leq\sum_{l\in L}\mathcal{F}_{L}^{t}\ ,\quad \forall\ C=\ \{c_1,c_{2,},\dots c_k\},L=\{l_1,l_2,\dots l_m\}\in G \tag{12}$$

$$\sum_{l\in L}\sum_{c\in C}\mathcal{D}\leq\mathbb{B},\forall C=\ \{c_1,c_{2,},\dots c_k\}\ ,L=\{l_1,l_2,\dots l_m\}\in G \tag{13}$$

$$\gamma_{ij,c}^{t}\in\{0,1\},\forall\ ij\in E,(i,j)\in V,C=(c_1,..,c_k)\in G \tag{14}$$

The above illustrated equation in (8) defines the ILP objective function aiming to maximize the overall network resilience by minimizing fail-over convergence delay bounds. This objective ILP formulation is subjected to: (i) constraints which are required to ensure that the controllers' placement does not contradict apriori with faulty locations; (ii) the propagation latencies that must be satisfied to ensure that the controllers' placement does not violate the convergence delay bounds. That stated, by constraint (9), we detect a topology change in response to a fault. This is an important fundamental pre-requisite, as $\gamma_{ij,c}^{t}=\ 1$ if and only if $\mathcal{F}_{L}^{t}=1$. $\mathcal{F}_{\mathrm{L}}^{\mathrm{t}}=0$ implies that the solution set does not contain the most optimal set of controllers. By constraint (10), we ensure that atleast one controller is assigned at 'close proximity' to every faulty location. Constraint (11) ensures loop-free re-routing, i.e., during the time of re-convergence, temporary micro-loops may exist in the topology due to inconsistency of forwarding tables of various network elements. This behavior is hard-to-ignore with respect to link-state algorithms, because controllers closer to faulty locations tend to update the forwarding tables earlier than the other controllers. Enhanced Interior Gateway Routing Protocol (EIGRP), which is loop-free at any moment during re-convergence, is the only routing protocol that lacks this property, thanks to the explicit termination of the diffusing computations. It is worth mentioning that for the link

state-protocols, there are improvements to the forwarding tables update procedures by which such micro-loops with link-state routing can be eliminated. Finally (12) restricts that a faulty location is not served by more than just one controller. Now moving forward to delay computation constraints, by constraint (13), we ensure that the convergence delay is restrained minimum. The intended meaning of equation (13) is therefore, to avoid feasible solutions containing cycles with delay bounds larger than $\mathcal{D}$ bounded by a constant $\mathbb{B}$, where Land C stands, respectively, for the set of links and controllers, in that instance. Eventually equation (14) indicates that $\gamma_{ij,c}^{t}$ is a binary variable. Thus our ILP formulation outputs a set of k controllers, those which satisfy the constraints, to be placed near every faulty location.

7.5. On Greedy Heuristics Based On Convex Combination

The above ILP formulations tries to assign controllers based on the failure rate probability of faulty locations defined over the time from t = 0 to t = ∞. Although this sort of ILP formulation gives optimal solution, in practice, systems under consideration (here, backhaul networks) can be highly non-linear and extremely unpredictable. It is also possible that the performance functions of these systems are non-differentiable, implicit, non-linear, noisy, and cannot even be characterized from past statistical data. Computation of failure probabilities under such conditions of these sophisticated failure domains thus generally necessitates significant computational efforts and more resources (here, restoration controllers) in order to obtain results with high confidence levels, especially in case of rare-event analysis. This might indirectly result in slightly higher cost investments for MNOs since they have to assign controllers to every individual faulty location, those which are identified through our ILP model definitions. Therefore, to even out this, after a thorough analysis of existing approaches such as greedy, clustering, min-min, max-min algorithms, we consider a simple greedy heuristics, which employs convex combination technique. For the sake of brevity, we do not get into comprehensive specifics on convex combination. Nonetheless, briefly, P is a convex combination of a set of points $\{a, b, c\} \in R^n$ if and only if the set of all convex combinations of points $\{a, b, c\} \in R^n$ is the line segment connecting those three points. We can formally define the line segment between $\{a, b, c\} \in R^n$ as:

$$P \coloneqq \{(1 - x^2)a + (1 - x)b + xc \mid 0 \leq x \leq 1\} \tag{15}$$

That is, the formulated ILP model assigns one controller near 'every' faulty location. Our heuristic seeks to minimize the total number of controllers among m controllers, starting within each subnet. The algorithm removes the set of controllers within each subnet and allocates them based on the convex combination technique, together with preserving the OCDe (Δ) obtained in (5), because these metrics consider the nodes within a latency bound. Notice that this is a greedy

strategy. This process is repeated until we obtain a feasible solution, i.e., a partition with N groups of controllers, with N ≪ m, that guarantees the required availability for each MNO. For clear and better visualization, the above stated is pictorially illustrated in figure 36 and our algorithm is in Algorithm 1.

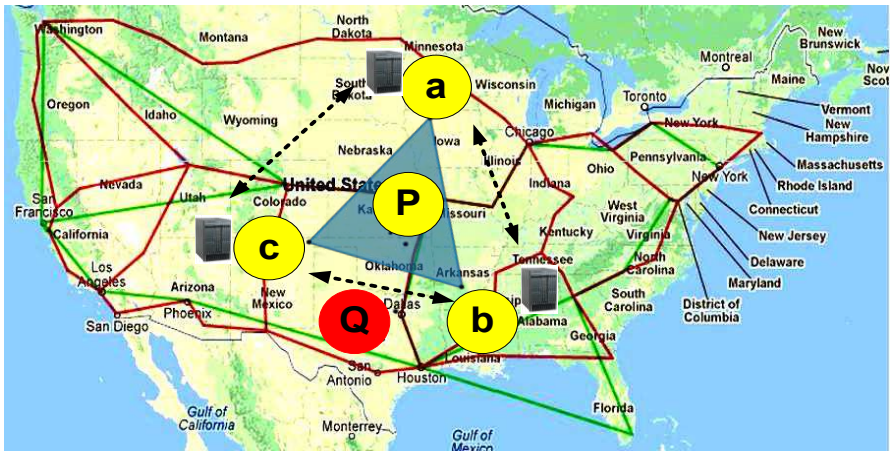


Figure 36: An illustration of convex combination technique for controller placement. Given three faulty locations a, b, c in a plane as shown, the point P is a convex combination of the three faulty locations, while Q is not.

ALGORITHM 1 CONVEX COMBINATION BASED GREEDY HEURISTICS

Begin

Until each subnet contains exactly one controller, ***Do***

Identify controllers from set $C = \{c_1, c_2, \dots c_k\}$, $\forall\ \delta$ is the minimum.

Assign controllers from new set $C_{New} = \{c_1, c_2, \dots c_i\}$to different and empty subnets, where $C_{New} \subseteq \{c_1, c_2, \dots c_k\}$

Discard assigned controllers from the set $C_{New} = \{c_1, c_2, \dots c_i\}$.

If only one subnet is remaining ***then***

Assign c_i to this subnet

Discard controller c_i from set $C_{New} = \{c_1, c_2, \dots c_i\}$.

End Until

End

7.6. Illustrative Numerical Evaluations

7.6.1. Optimal Locations for Logically-centralized Physically-distributed Controllers

Our key figure of merit to evaluate the performance here is the restoration latency values. Restoration latency indicates the average time taken for a connection to be re-routed successfully

across another backup path after a failure. It indirectly refers to the response time of the network. In our scenario, it is an indicator of the convergence delay response time between controller(s) and the nodes, which enables to determine the optimal locations for controller placements. We carried out our evaluations on two different topologies and the characteristics of these two topologies are in Table VI (Figure 37).

TABLE VI. NETWORK TOPOLOGIES CHARACTERISTICS

Network Type (Nick Name)	**Network Characteristics**				
	# of nodes	**# of links**	**Average node degree**	**Mean # of hops for working paths**	**Mean # of hops for backup paths**
Internet2 L1 (A)	57	65	2.18	8.60	15.10
TeliaSonera US L1 (B)	21	25	2.74	3.0	5.8

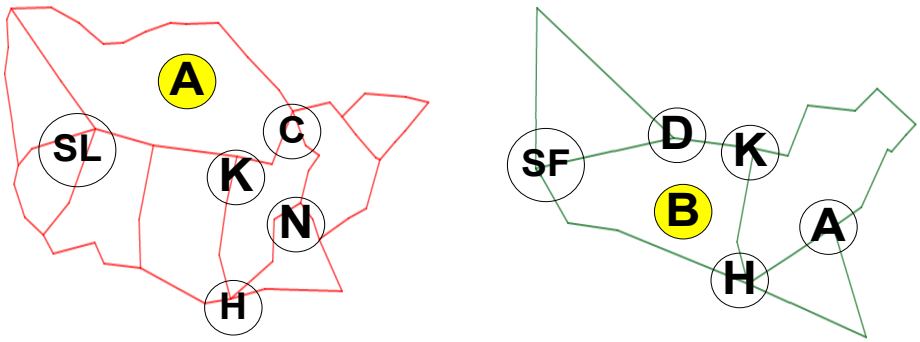
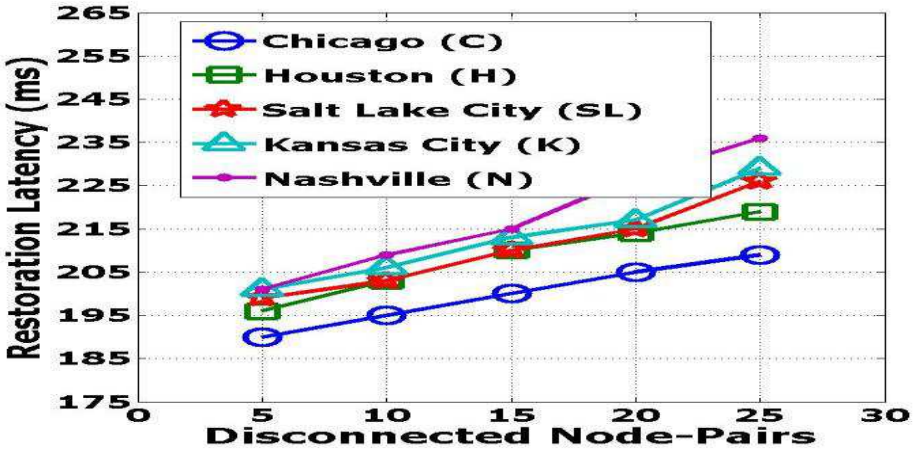


Figure 37: Topology (A) and topology (B) used in the simulations.

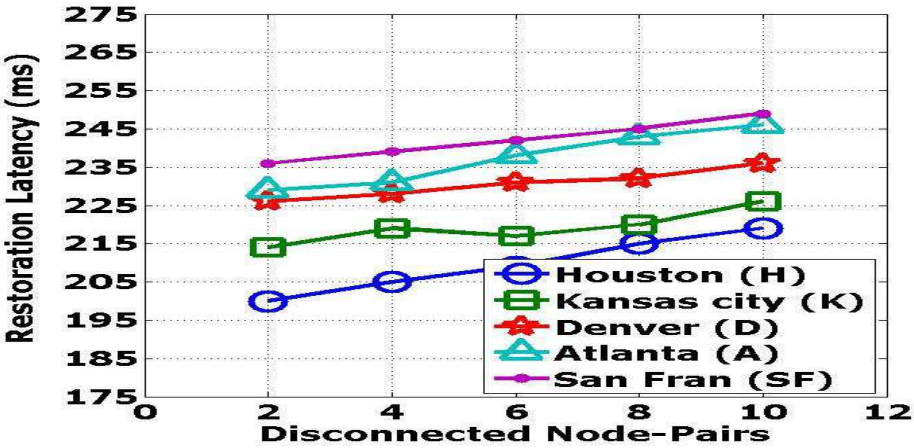
As a first step, we separately simulated multiple node failures for each topology and we calculated the number of interrupted connections that each failure caused. This is done by simulating at least 10000 to 20000 connection requests, for different network loads. Based on this, we identify the best possible controller locations based on our approach methodology (starting from equation (1) till (15)). Adding to this, the 200ms-250ms restoration latency for mesh topologies were set as benchmark figures for comparison purpose, since these two topologies are 'mesh-like' topologies, exhibiting the same characteristics and accordingly the QoS parameter $\mathbb{B}$ in (13) is changed and repeated during each simulation.

The objective here is to determine the most optimal controller locations with respect to the disconnected node-pairs that are caused by any given number of failures. Figure 42(a) and 42(b) illustrate the restoration latency values for (A) and (B) respectively. Overall, we observe that our results comply strictly with the benchmark figures. Furthermore, as expected, the values of restoration latency increase as the number of disconnected node-pair increases. Specifically, Figure 38(a) shows the worst-case restoration latency against the average number of interrupted

connections between each node-pair for five best controller locations for (A). By accounting the least favorable value (highest value) of restoration latency for the maximum number of disconnected pairs when the controller is placed at different locations, Chicago (C) came out to be the first best location for controller placement for (A) that could minimize the worse-case latency, then Houston (H) and then Salt Lake City (SL). For operator (B), Houston (H) was the best controller location that could minimize the worse-case latency, then Kansas City (K) and then Denver (D), shown in figure 38(b).



(a)

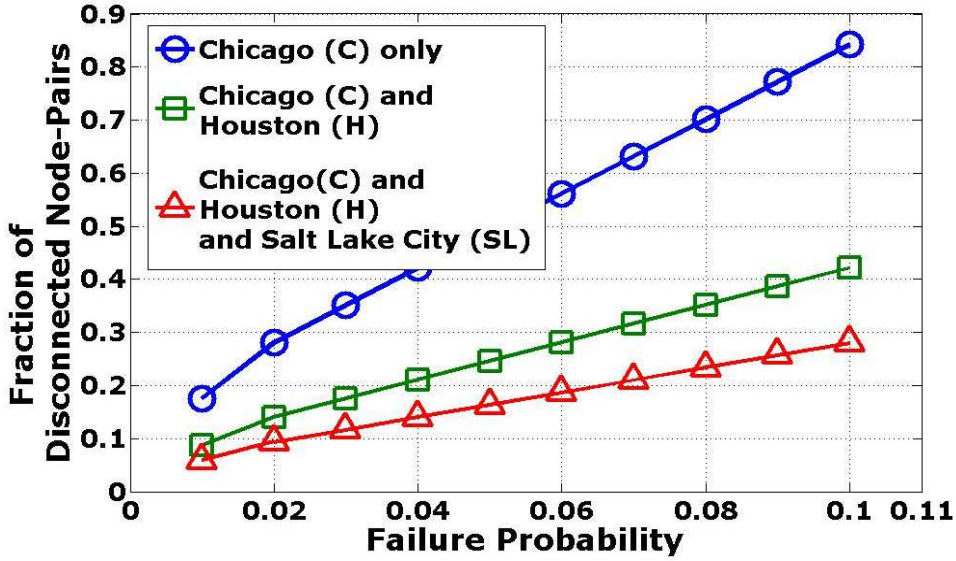


(b)

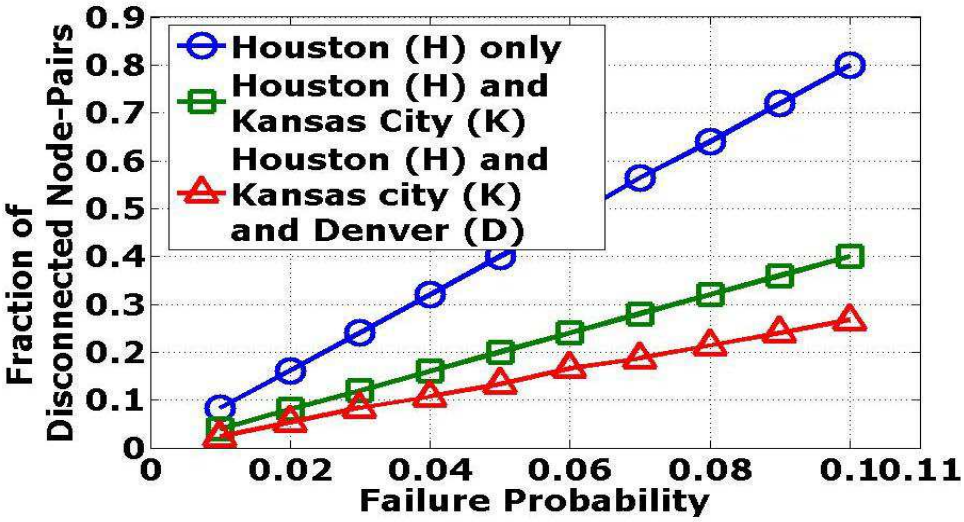
Figure 38: An illustration of restoration latency due to optimal controller placements for A and B for various disconnected node-pairs.

Thus having determined the optimal controller locations, we now cross-verify, if the pre-determined controller locations have an effect in reducing the number of disconnected node-pairs. To do this, we picked the best three locations from figure 38(a) and 38(b), which fell within the convergence delay bounds and placed controllers there, one after another incrementally. We simulated multiple failures and observed the results, for both the topologies. As we observe in figure 39(a) and 39(b), there is definitely a decrease in the number of disconnected node-pairs,

for both the topologies. More precisely, when multiple (three) controllers are used collaboratively for each topology, the number of disconnected node-pairs can be almost eliminated. Here, if ∝ is the number of total number of node-pairs and β is the total disconnected node-pairs, then β / ∝ is the fraction of disconnected node pairs in figure 39(a) and 39(b).



(a)



(b)

Figure 39: An illustration of multiple controller placements for A and B.

7.7. Concluding Discussions

In this chapter, we proposed an analytical framework to model network resilience under shortest path routing policy and single link failure in a logically centralized architecture, strictly speaking, the SDN architecture, adapted within the context of mobile backhaul network

architecture. Our approach enables us to obtain previously unavailable analytical results, including the delay bounds of path fail-over for the SDN architecture and its convergence enhancements. Our analysis shows that fail-over delay bounds in SDN architecture are mainly determined by two factors: (1) the distance between the failure location and the placement of controllers, and (2) the length of the longest alternate path to reach the controllers after the failure. These two factors are captured formally by our analysis and can explain why existing convergence enhancements often provide only limited improvements in fail-over events in SDN architecture. Explicitly modeling message processing delay reveals insights into the impacts of connectivity richness (i.e., node degree and total number of links in the network), and also the effectiveness of different enhancements. These new results enable one to better understand and compare the behavior of various controller placement algorithms proposed so far, under different topology, network sizes, and different message delays. Furthermore, using our approach, network operators can easily add more controllers to handle more flow initiation events while keeping the flow setup latency minimal. We note that, since in our approach, controllers' operations do not depend on other controllers, they continue to operate even under heavy synchronization load. However, as the load increases, the window of inconsistency among controllers grows (i.e., the time it takes to have the views converge).

For the sake of simulations and evaluation purposes here, we demonstrated by using the already existing network topologies with backup paths, eliminated those backup metrics and proved our theory. Nonetheless, in real world scenarios where there are already backup paths set up the network operators, it is unrealistic and impractical to go back to the past and eliminate the already existing backup paths. Instead, MNOs can take advantage of the proposed scheme to avoid over-provisioning in the future, because, as evident as it is, it will not be cost-efficient anymore to extend the network resources in the same ratio than the traffic demand.

*"Programming is one of the most difficult branches of applied mathematics; the poorer mathematicians had better remain pure mathematicians." – **Edsger Dijkstra, Computer Scientist, Inventor of Shortest Path Algorithm.***

Chapter 8

Stitch-n-Sync: Discreetly Disclosing Topology Information Using Logically Centralized Controllers

From the above discussions, one recurring question is on the complexity to decide what MNOs should reveal and what not to reveal, i.e. competitive MNOs are typically long-known for their shrewdness to conceal their underlying network topology information. Having said this, we propose a quasi-distributed topology information sharing framework for network operators based on logically centralized controllers. Through our approach, we present a topology information sharing scheme in which two or more MNOs can cooperatively and more importantly-discreetly, reveal their topology information for the sake of utilizing the unused available resources of each other, at times of network failure situations. Our approach has been formulated and developed based on a novel key metric to 'tune' the amount of information sharing. Based on extensive simulations, we then investigate the impacts of network topology information sharing on the network capacity. The overall feasibility is illustrated through significant numerical results.

8.1. Introductory Statements

The topology of a network specifies the location of the underlying network elements such as links, nodes (routers, switches, gateways, etc.) of a network. In practice, it is the topological structure of a network and often depicted physically or logically. While physical topology refers to the placement of the network's various components, including device location and cable installation, logical topology shows how data flows within a network, regardless of its physical design. The Internet consists of a collection of more than 21000 domains called Autonomous Systems (AS) operated mostly under different authorities (operators/providers) that although co-operate over different geographical areas, they compete in a country or other area. Today BGP is the de facto standard for exchanging reachability information over the domain boundaries and for inter-domain routing. The GMPLS controlled optical beared networks are expected to have similar architecture, however, more information has to be carried for TE, resilience and QoS purposes. Therefore, extensions of BGP and of PNNI as well as the PCE have been proposed.

Still in all cases emerges the question of 'Protection Shareability', as introduced in the first chapter. For dedicated protection it is enough to know the topology of the network to be able to calculate disjoint paths. However, to be able to perform sharing of protection resources (shared protection) it is not enough to know the topology, but it is mandatory to know exact working and protection path pairs for all the demands, since protection paths can share a certain resource only if there is no such a pair of working paths that contain any element from the same Shared Risk Group (SRG). This can be checked within a domain where the full topology and link-state information is flooded, however, over the domain boundaries for security and scalability reasons no such information is being spread.

Mobile Network Operators (MNOs), with their intimate knowledge of their physical network topology, often consider revealing details of such network information to be strictly confidential and legally privileged. We respectfully challenge this paradigm of 'topology hiding' in this chapter by consequently proposing, designing and evaluating our approach on discreetly disclosing topology information among multiple MNOs, using logically centralized controllers, to improve Network Survivability, thus not having to excessively invest in the backhaul.

8.1.1. Current contributions and Organization of the Chapter

To do so, our proposal in this article, is to effectively manage geographically distributed backhaul network elements which belong to different MNOs using 'logically-centralized' physically-distributed controllers, while meeting strict constraints on network availability and reliability. With this introduction, our contributions in this work focus on:

- Illustrating a novel 'multi-topology shared' architectural design paradigm of a communication network by adapting the logically centralized approach and very specifically towards a Quasi-Distributed approach. More significantly, our approach exploits the recently emerging SDN/OpenFlow approach on maximizing the network survivability through bilateral cooperation between several MNOs, elaborately described by a real world use case scenario –Detailed in Section II.

- Subsequently, we formulated and developed a key metric that is based on mathematical modeling to characterize our problem as an optimization problem - Detailed in Section III.

- Based on the model definitions, we proceed forward to define and elaborate on our Integer Linear Programming (ILP) formulations - Detailed in Section IV.

- Performance evaluation on real network topologies illustrates the numerical results showing its support to the theory and proof of correctness - Detailed in Section V.

8.2. Towards A Multi-Topology Shared Architecture

8.2.1. Discreetly Disclosing Topology Information: Stitch n Sync!

Before characterizing the overall optimization procedures, we recapture our Cross-Controllers framework from our earlier chapter, demonstrating through real topologies with the illustration of Quasi-Distributed Topology Information Sharing (Figure 40). In Figure 40, all links in Red color represent Internet2 L1 topology (let's say, A) and all links in Green color represent TeliaSonera US L1 topology (let's say, B). Nodes C_A and C_B represent the 'restoration controllers' of A and B, which are placed at Kansas (geographical centre for now for illustration purpose). Each controller maintains a database (such as MIB [117] for instance) containing network graphs and re-routing algorithms. Each controller updates this database periodically and independently via the states collected from their respective physical network domain (e.g., through port counters or flow-level statistics gathering). The specificity of this design is now notably distinguished by connecting the restoration controllers C_A and C_B (via a proxy controller)[14]. It allows C_A and C_B to synchronize between themselves in order to disseminate their domain state.

14 The (optional) proxy controller links multiple MNO controllers and serves as a backup agent by providing fan-out capabilities to minimize network load.

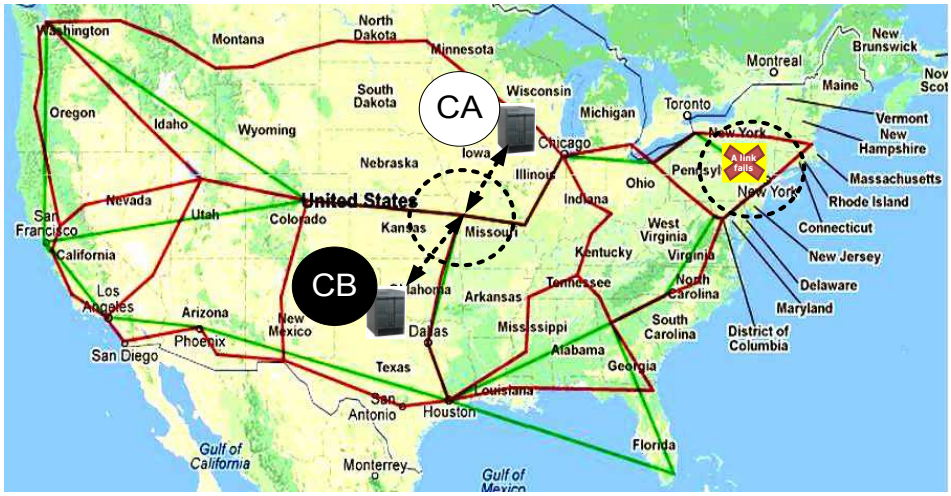


Figure 40: An illustrative example outlining Quasi-Distributed Topology Information Sharing framework for the U.S. Two MNOs share their resource (links/bandwidth capacity) by discreetly sharing their topology information using cross-controllers, making a 'resilient' topology, thus avoiding the need for redundancy in the already existing topology. Multiple stand-by controllers can takeover in case of failure of the controller itself. Best viewed in Color.

A direct implication of this design is that every controller locally stores the complete view (full reachability information) about its own topology, but synchronizes to access partial view (relevant information only) about other MNOs topology information. We define this as Inter-Domain Synchronization (IDS), which is the main scope of this chapter. The extent to which the topology information is synchronized translates to the specific functionality of the centralized control plane, for which it is intended. Therefore MNOs are not required to disclose their entire topology information always, i.e., under normal operation, C_A manages the set of nodes of the topology of A though they are also reachable by C_B and C_B manages the set of nodes of the topology of B though they are also reachable by C_A. Our approach, as termed as quasi-distributed scheme, as evident as it is, employs the advantages of both the distributed and the centralized approaches.

8.2.2. Challenges Posed by Sharing between Multiple Operators/ Domains

Practically all the networks consist of horizontally interconnected parts where these parts are defined for administrative or routing purposes [118]. These domains are typically operated by different operators/providers. A thorough explanation of how routing works over this horizontal structure can be found in [119]. Analogously, not only the IP (Internet Protocol) networks have this structure, but also the current and future optical beared multi-layer networks. Partitioned networks consisting of multiple domains have both advantages and drawbacks. The advantage is the scalability, where each node has to know everything about the domain it belongs to however

it has a simplified view of all the other domains. For this reason less information has to be flooded, processed, stored and used while routing, therefore it improves the scalability. On the other hand, the drawbacks are the inaccurate view of the topology as well as the lack of information for disjoint routing [120]. Also in contrast to BGP that floods only reachability information, but no link state information, such routing is required that can support Quality of Service (QoS) guarantees and meet TE (Traffic Engineering) and resilience objectives [120],[121]. Therefore, extensions of BGP and of PNNI as well as the PCE [122] have been proposed. In [123] and [124] the effects of the delay while flooding information and the period and trigger threshold for starting information flooding in multi-domain networks are investigated. In [125] a game theory based approach is proposed to analyse what effects the pricing policy of certain operators has onto the blocking and income of other operators in a multi-provider/operator environment. In [126] the cases when different multi-domain resilience strategies are to be employed are classified. In [127] the use of p-cycles in a multi-domain network are investigated and different approaches evaluated and compared. In [128] two European multi-domain networks, a hierarchical and a non-hierarchical, are defined and evaluated from routing and protection points of view. When assuming a multi-domain environment we consider two levels, the lower one that is within each domain and the upper one where each domain is represented as a node only or as a simplified graph with parameters characterising the connections between its own border nodes, while the links that interconnect these domains play the main role. Here we discuss two techniques to be employed on this two-level representation, which we define as *Inter-Domain Synchronization (IDS)*.

8.3. On Maximizing Network Survivability

On discussing this, the complexity lies in the Inter-Domain Synchronization (IDS) procedure which requires exchange of information among controllers-to-controllers within the limits of the convergence delay bounds. Such exchange necessitates each controller to take part in negotiating 'the global optimal solution'. Typically to define optimality here, we converge on the objective of maximizing network survivability, which narrows-down to solving a multi-constrained optimization problem. As a consequence, here we look at maximizing network survivability by optimizing 'the total cost' in information exchange between controllers-to-controllers, in the event of topology changes triggered upon a failure/disaster. The appropriateness of optimally sharing physically distributed control plane state information, designed in a way to work collaboratively as if it were centralized, to maximize the overall network survivability, in such a shared topology, is the subject of this research. Diving deep, here the key objective is to evaluate the performance of a network when the underlying distributed control plane state is characterized by a topology change based on the distribution of faults.

TABLE VII. LIST OF NOTATIONS AND SYMBOLS USED IN THE MODEL

Notations	Implications
$G = (V, C, E, D, L)$	Weighted bi-directional graph denoting the backhaul.
$V = (v_1, v_{2,} \dots v_n)$	Set of vertices of the graph containing the nodes, $\forall v \in V(G)$ (microwave towers, edge routers, switches, gateways, PoP etc)
$C = \{c_1, c_{2,} \dots c_k\}$	Set of restoration controllers for centralized management of each MNO topology, $\forall c \in C(G)$.
$E \supseteq \{E_{ij}^{v}, E_{ij}^{c}, E_{ij}^{vc}\}$	Set of edges of the graph that includes the set of all possible link properties, $\forall e \in E(G)$.
$E_{ij}^{v} = \{e_{ij}, i, j, \in V\}$	Subset of $E(G)$ that includes direct links e_{ij}between any two distinct vertices i, j of the graph, $\forall v \in V(G)$.
$E_{ij}^{c} = \{e_{ij}, i, j, \in C\}$	Subset of $E(G)$ that includes direct links e_{ij}between any two distinct controllers i, j of the graph, $c \in C(G)$.
$E_{ij}^{vc} = \{e_{ij}, i, j, \in V \in C\}$	Subset of $E(G)$ that includes links e_{ij} between a controller and a node i, j of the graph, $\forall G$.
$\mathcal{T}$	Synchronization time that refers to the collaboration among the controllers of several MNOs.
$L = \{l_1, l_2, \dots l_m\}$	Set of faulty locations in the backhaul topology, $\forall\, ij \in E(G), (i, j) \in V(G)$ and $l \in L(G)$.
$\mathcal{R}_c^t$	Binary variable denoting the logical portioning between controllers of MNOs.

8.3.1. On Modeling Inter-Domain Synchronization (IDS)

Here we formally define Inter-Domain Synchronization (IDS). We characterize IDS by the following measure that we term as Sync Index ($\mathcal{R}_c^t$) . Synchronization ($\mathcal{T}$) refers to the collaboration among the controllers of several MNOs and hence Sync Index is a measure that limits the synchronization of topology-information-exchange by the controllers of several MNOs. An all-to-all synchronization between several controllers may be triggered over a time period ranging between $\mathcal{T}_{min}$ and $\mathcal{T}_{max}$. This bound in the time period corresponds to a synchronization session, which enables the network designer/manager to modify (make one or more partial changes) synchronization capabilities based on the specific applications and/or services, etc. using any protocol over any topology. For instance, for the scenario illustrated in section II.B, i.e., for fault restoration and routing control, by simply exchanging information only about available links and utilization states (not the entire topology!), it is quite sufficient for the controllers to update the forwarding tables and perform the shortest-path 're-routing'. On the other hand, such level of information exchange alone may not be sufficient for computing different possible control plane tasks such as flow-based control, traffic differentiation, bandwidth shaping, etc. These may necessitate different levels of topology-information-sharing among the controllers required for their respective control-plane operations. Henceforth, here we remark that while the objective of this research work exclusively focuses on improving/augmenting survivability with minimal inter-domain information exchanges, this level of other MNOs topology information cannot influence all the tasks that may involve the

centralized control plane and therefore the applicability of this topology-sharing strategy may extend beyond multi-constrained route optimization problems. Instead of hard coding the maximum topological information in the design, we allow for more variation and leave the actual split of encoding the topological information to the network manager/designer, who anticipates better in determining the optimal topological information to be synchronized among the controllers, depending on whether the chosen synchronization period is sufficient to meet the requirements of the control plane task.

Nevertheless, to ascertain that there is atleast the minimal logical portioning among controllers of different MNOs, i.e. the selected controller has the access to full reachability information about its own topology, and has access to atleast relevant information about other MNOs' topologies, we define:

$$\mathcal{R}_c^t = \begin{cases} 1, if\ \exists\, \mathcal{T}: (\mathcal{T}_{min} \leq \mathcal{T} < \mathcal{T}_{max}), \forall e \in E(G): \{E_{ij}^c\} \neq \emptyset \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad Otherwise \end{cases} \tag{1}$$

8.4. On Optimizing Quasi-Distributed Topology Sharing Using ILP Based Formulations

In this section, we introduce Integer Linear Programming (ILP) based mathematical formulations to optimize, respectively, the minimum and maximum possible degrees of synchronization among the controllers.

Objective: Let $C = \{c_1, c_2, \ldots c_k\}$ denote the set of k controllers positioned in each MNO network topology at faulty locations $L = \{l_1, l_2, \ldots l_m\}$ which are pre-determined from the past experience, measurements and statistics. Given a pattern of failure rates for fault locations, our goal is to maximize the overall network survivability through logical portioning of centralized controllers after a topology change, under shortest path routing policy and link/node failure, at time instant t.

Variable: $\mathcal{R}_c^t$ is the decision variable in this optimization problem. $\mathcal{R}_c^t = 1$ when there is atleast minimal inter-domain information exchanges between controllers of different MNO topology, else $\mathcal{R}_c^t = 0$. Thus, our ILP model can be formulated as:

$$\textbf{Minimize}: \left(\left(\boldsymbol{\varepsilon} \sum_{\substack{c \in C \\ e \in E}} \mathcal{R}_c^t \right) \right) \tag{2}$$

The above illustrated equation in (1) defines the ILP objective function aiming to maximize the

overall network survivability by cross-controlling information exchanges between controllers of different MNO topologies. Here ε is assigned arbitrarily in the range (0; 1) that allows the network designer/ manager for the optimal topological information to be synchronized among the other controllers as per their Service Level Agreements (SLAs). This objective ILP formulation is now subjected to the following constraints defined in equation (3), (4) and (5).

$$\sum_{l \in L} \sum_{c \in C} \mathcal{T} \leq \mathbb{C}, \forall C = \{c_1, c_{2,}, \dots c_k\}, L = \{l_1, l_2, \dots l_m\} \in G \tag{3}$$

By constraint (3), we ensure that the synchronization delay between controllers-to-controllers is constrained to a minimum. The intended meaning of equation (3) is therefore, our optimization framework permits the feasibility for MNOs to scale the network with additional controllers to handle more flow initiation events while keeping the flow setup latency minimal. The sync index with delay bounds larger than $\mathcal{T}$ is bounded by a constant $\mathbb{C}$, where $\mathbb{C}$ is set approximately equal to $\mathcal{T}_{\max}$ on most occasions, decided by the network manager.

$$\sum_{c \in C} \mathcal{R}_c^t = 1, \ \forall\, ij \in E, (i,j) \in V, C = \{c_1, c_{2,}, \dots c_k\} \in G \tag{4}$$

Equation (4) ensures that there 'exists' logical portioning between controllers of different MNO topologies. This is an important pre-requisite for our research objective, as when $\mathcal{R}_c^t = 0$, it practically might turn-out impossible for the network to recover because there would not be any more synchronization among the controllers.

$$\mathcal{R}_c^t \in \{0,1\}, \forall\, ij \in E, (i,j) \in V, C = (c_1, .., c_k) \in G \tag{5}$$

Eventually equation (5) indicates that $\mathcal{R}_c^t$ is a binary variable. Thus our optimization framework outputs the most appropriate synchronization time bounds those which satisfy the constraints, satisfying the essential control plane tasks.

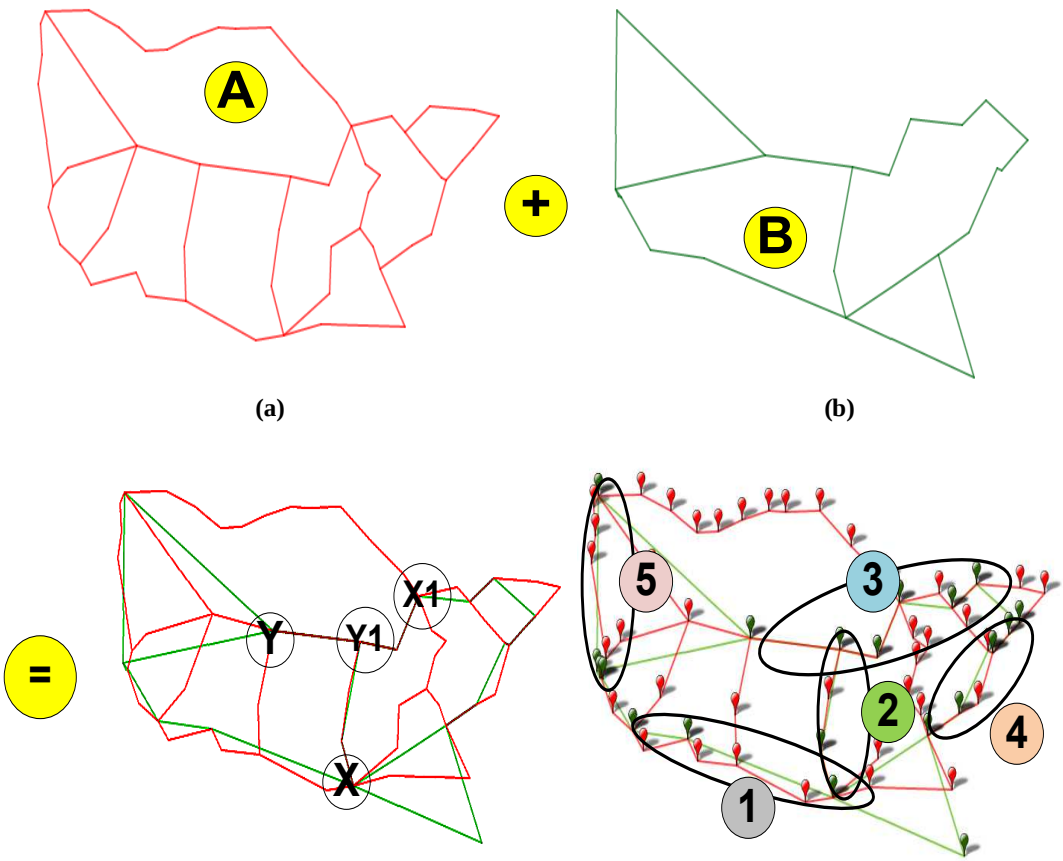


Figure 41: An illustration of merging or 'stitching' two different MNO topologies (a) and (b) into one single topology (c), in which controllers were placed in order to reduce the cost of over-provisioning in already existing networks with special mention on overlapping links and nodes at five different locations (d).

8.5. Illustrative Numerical Evaluations

Moving forward, we present our numerical results here. We reiterate that the spotlight of this research fundamentally targets on demonstrating the survivability of backhaul networks using 'logically-centralized' physically-distributed controllers with reduced amount of physical redundancy. Emphasizing on this fact, we carried out our analysis on the same two real topologies which we used for illustration in section II (Fig.40, also Fig. 41(a) and 41(b)). The choice of these two topologies is mainly due to the fact that these two operators have already expressed their interests towards a logically centralized architecture and further our results should motivate in a different direction. Table II summarizes the characteristics of these two topologies. Simulations were carried out on an Intel Pentium Core 2 Duo 3 GHz, 4GB RAM machine, with GLPK solver [129] used as the underlying ILP formulations solver and ns-3 for SDN-OpenFlow based simulations. Each link has a link bandwidth of 622.08Mb/s (OC12) between each node-pair. Multiple link failures were simulated for at least 10000 to 20000 connection requests, for different network loads.

TABLE VIII. NETWORK TOPOLOGIES CHARACTERISTICS

Network Type (Nick Name)	Network Characteristics				
	# of nodes	# of links	Average node degree	Mean # of hops for working paths	Mean # of hops for backup paths
Internet2 L1 (A)	57	65	2.18	8.60	15.10
TeliaSonera US L1 (B)	21	25	2.74	3.0	5.8

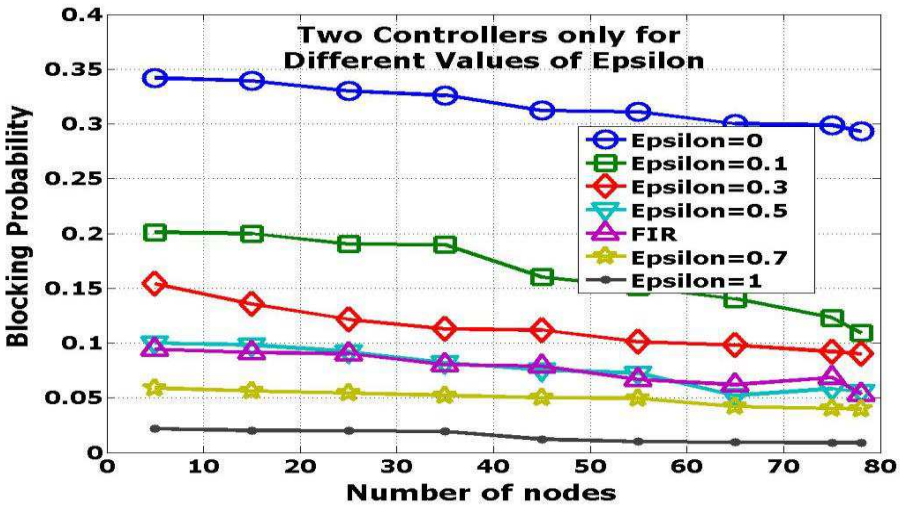
8.5.1. Efficiency of Logically-centralized Physically-Distributed Approach - With and without controller Collaboration

In this section, we illustrate on synchronizing information between controllers of different operators and how our Sync Index helps operators to improve their network survivability with reduced redundancy. To do this, we adopted to a different new approach. We simulated a network topology which was created by merging or 'stitching' the two topologies into one single topology (Figure 41(c)). By this way, nodes and links of the primary path of both operators which overlap were considered as 'backup' for each of the them mutually and already existing backup paths for each operator were eliminated (thereby avoiding the over-provisioning costs), i.e., the mean number of hops for backup paths for A and B from Table VIII was set to 0. Precisely, both operators have common set of links/nodes at five different locations that can be shared and utilized mutually, i.e., [1,2,3,4,5] (Please refer Figure 41(d)). Thus, we now evaluate the effectiveness of our approach with respect to the following three performance metrics: *(i) Blocking Probability, (ii) Average Link Utilization efficiency and (iii) Overall Network Throughput*. For the purpose of simulation, we placed the controllers, first at positions X(A) and Y(B) together - X(A) indicating one of the most optimal controller locations for (A) and Y(B) indicating one of the most optimal controller locations for (B) (2 controllers in total). Then we extended to 4 controllers with X (A), X1(A) and Y (B), Y1 (B) working collaboratively (4 controllers in total). The question on how these locations were determined as the most optimal controller locations was tackled already by few recent works such as [102], [103] and we reused the results of these research adapted to our topologies, since this is not the scope of this work.

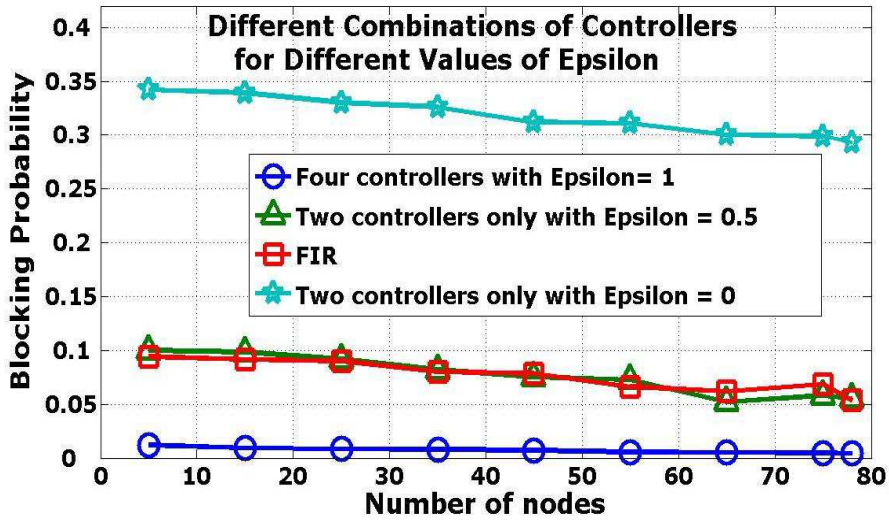
We differentiate between with and without controller collaboration by altering the value of ε in (2), i.e., we vary the Sync Index from $\varepsilon = 0$ (no collaboration among the controllers of different operators and thus no synchronization of topology information) until $\varepsilon = 1$ (indicating complete collaboration between controllers of different operators). Furthermore, on a general note we point-out that as this work is entirely unique and due to the lack of extensive specific works to relate with, we compare our approach with [130]. Here the authors analyzed the

problem of distributed path selection for restorable connections in a GMPLS shared mesh restoration architecture and propose a distributed restoration path selection algorithm in a GMPLS shared mesh restoration architecture, called Full Information Restoration (FIR), that uses signaling protocol extensions to distribute and collect additional link state information.

Blocking Probability (BP): It is a measure of the number of connection requests rejected against the total number of connection requests due to insufficient resources in the network. Figure 42(a) visualizes the performance of BP with only two controllers X(A) and Y(B) for different ε values. From the initial observations, we can distinctly see that a connection is less likely to be blocked due to our scheme (even with minimum logical portioning among two controllers, $\varepsilon = 0.5$) than the reference scheme (FIR), without secondary backup paths. Moving forward, overall we can observe that the controllers are able to gain more control over resources for higher values of ε. Precisely, there is a big shift from $\varepsilon = 0$ to $\varepsilon = 0.1$, i.e., from no sharing to atleast some sharing. Poor results for $\varepsilon = 0$ implies that the controllers can not discover more available paths for failed connections due to the lack of topology information sharing among them. We also observe that BP values gradually get reduced for higher values of ε, i.e., higher is the value of ε, lower is the blocking probability. This is due to the fact when ε increases, it makes it more feasible for the controllers to discover more resources (more feasible paths) for a failed connection, meaning faster restoration is achieved by our quasi-distributed approach leading to very few dropped connections. Another remark observing the results is that the performance gets better with larger node sizes. Moving to figure 42(b), we observe that this figure of merit shows much better performance when more than one controller is used for each individual operator, i.e., significant improvement is seen with four controllers with $\varepsilon = 1$, where there is very neglible blocking probability. This very good performance is mainly due to the high 'visibility' of resources that controllers can choose from both the topologies. We recall that ε allows network designer/manager for more variation in topology information sharing. Undoubtedly, higher the value of ε, higher is the network resource sharing.



(a)

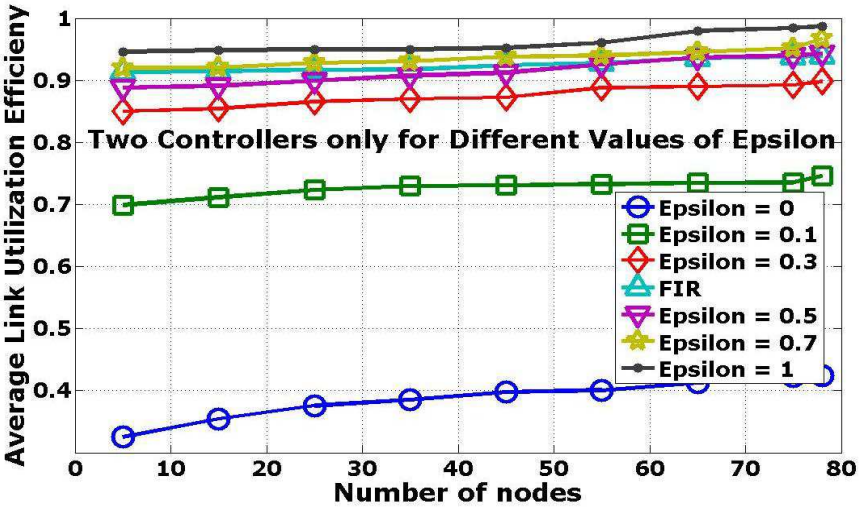


(b)

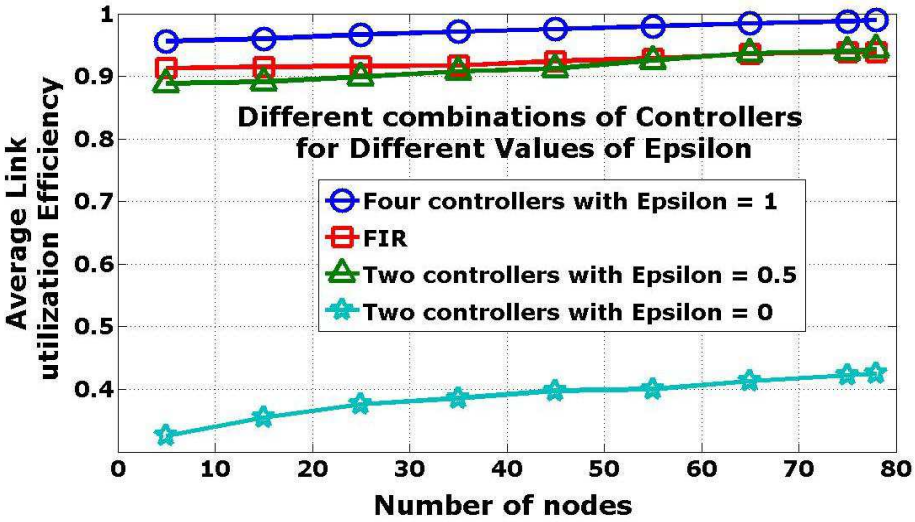
Figure 42: An illustration of Blocking Probability.

Average Link Utilization (ALU) Efficiency: The next metric, Average Link Utilization (ALU) values are shown in figure 43(a) and 43(b). Link utilization efficiency is a measure of the ratio of the link bandwidth which is utilized to the total bandwidth provisioned. Precisely from figure 43(a), for a case with higher ε, ALU efficiency value reaches as high as 98%, with two controllers and almost 99% with four controllers in figure 43(b), indicating how efficiently the total available network resources are utilized (which is actually utilized for protection and restoration). Furthermore, ALU efficiency gives an estimate of the efficiency of our quasi-distributed restoration approach with respect to effectiveness of resource usage. High ALU value indicates better resource optimization. Overall, our results demonstrate that the value of ALU is better with collaboration than without, specifically, as the node size increases. What this means to us, is that, by our approach, we could achieve utmost 99% efficient network resource utilization by re-using the existing paths, meaning that, over-provisioning for backup path could be eliminated. Similarly, from fig. 43(a), for $\varepsilon = 0.1, 0.3, 0.5, 0.7$ if not the best, is also good, more

than 75% minimum, in-par with FIR, especially when the network size is large. That is, even with the minimal logical portioning between controllers, the ability to find feasible paths within two (or more) independent topologies results in atleast 75% resource utilization. In theory, higher the resource utilization implies better network efficiency. Finally, to summarize, our approach tries to achieve better capacity utilization so that no unused resource remains "wasted" to achieve connection-availability guarantee.



(a)

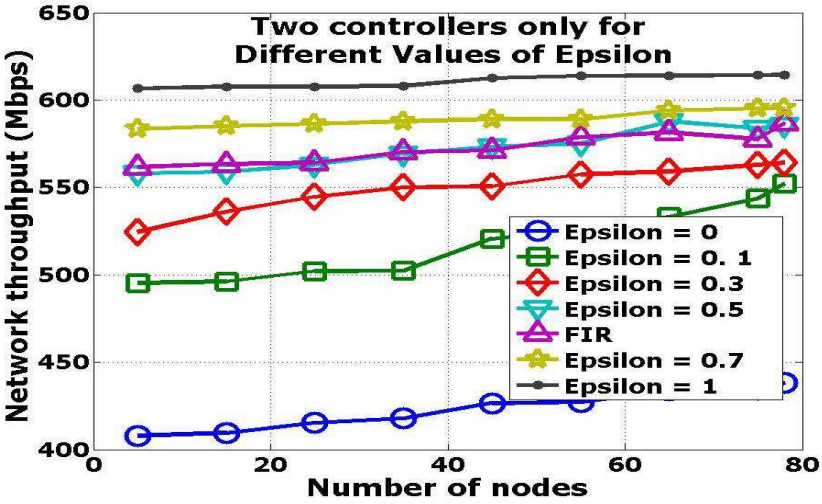


(b)

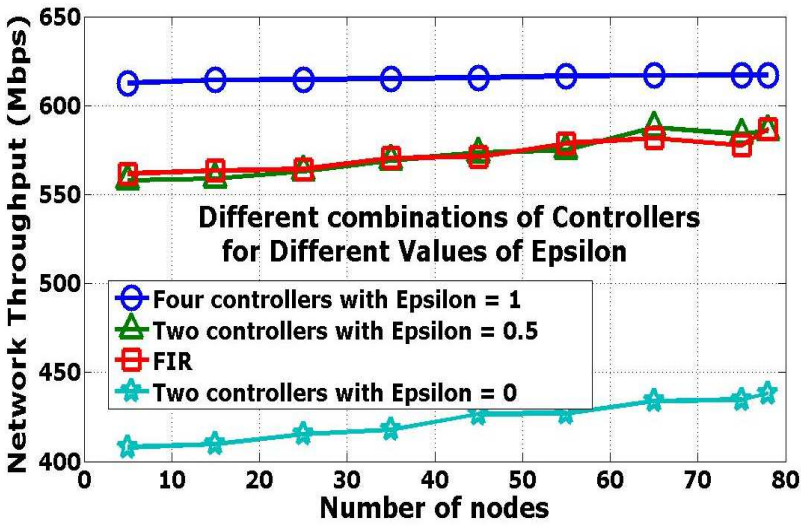
Figure 43: An illustration of Average Link utilization.

Overall Network Throughput (ONT): Last but not least, this metric allows us to determine the overall efficiency of our restoration strategy based on topology information sharing. That is, the end-to-end throughput of the network topology with and without controller collaboration will enable us to understand the complexity of our optimization framework, thereby affecting the overall network throughput. Consequently, we observe that atleast 99% of throughput is obtained when four controllers work collaboratively, essentially due to the fact that controllers

are able to discover more paths with more link capacity rather than simply selecting paths of shorter length. Furthermore, it is quite fairly understandable that the overall ONT performance values indicate positive behavior similar to BP and ALU, seen in figure 44(a) and 44(b). Furthermore, NT increases with larger ε, implying higher is the network resource sharing, higher is the network throughput. The fact that our scheme utilizes the available network resources greatly contributes to the better efficiency, particularly because every failed connection may be carried much efficiently on the available bandwidth. Thus, all available resources are more efficiently consumed.



(a)



(b)

Figure 44: An illustration of Overall Network Throughput.

8.6. Related Works

To the best of our knowledge, this is the first work that describes an optimization framework to share the underlying network topology information between several MNOs for the sake of

protection and restoration. Nonetheless, the work has several other inspirations fundamentally ranging from shared back up path protection schemes to distributed path selection schemes until the recent distributed control plane architectures in SDN/OpenFlow-based networks. To point-out a few high-impact works, in [131], [132], the behavior of wireless backhaul and mesh networks when their capacity increases have been paid exclusive attention. Consequently, how to increase backup resource sharing based on different cost models is of particular interest and has been reported in [133]-[136]. Also, literature studies such as [137]-[138] have focused on the problem of routing primary paths and backup paths for optimal efficiency. On the other hand, distributed control plane architectures in SDN/OpenFlow framework is fairly new and only a very few recent works [139], [140] have explored the scalability of the centralized controllers. However, the results of these research works are restricted towards the investigation of the controllers' scalability within one network domain, i.e. every controller has the (complete) view of only one topology, i.e., a single network. With these, it becomes self-explanatory that our work significantly differs from the rest.

8.7. Concluding Discussions

Cooperative communications among network operators can significantly enhance transmission reliability and bandwidth efficiency in wireless networks. However, many upper layer aspects of cooperative communications merit further research. In this chapter, we call for a novel fault restoration architectural design based on logically centralized controllers which allows several other operators to maintain a map of forwarding devices to controllers and discreetly share their own topology information and therefore their resources (links/ bandwidth capacity), to dynamically setup end-to-end paths across multiple backhaul networks. We investigate its impacts on network topology sharing and network capacity sharing, which is determined by considerable aspects, such as physical layer capacity, synchronization among the domains etc. The topology sharing framework is then formulated as a discrete optimization problem with simulation results presented to show the effectiveness of the proposed scheme. Simulation results have shown that our approach has significant impacts on the network redundancy. With extensive performance evaluations uncovered in this work, we believe the present approach has considerable potential beyond the context considered here in this work, especially on addressing technical interdependencies resulting from sharing, providing a better Quality of Experience (QoE) for the end-users. In future work, we will consider the adaptations needed to meet other factors such as shared risk link groups into the model to allow analysis of complex real world network design issues as well as we will also carry out simulations to see the performance of our metric by merging more than just two topologies.

Part IV

Performance Evaluation of SDN/OpenFlow Architecture

"The nice thing about standards is that there are so many to choose from."
– Andrew S. Tannenbaum, Computer Scientist.

Chapter 9

Can SDN/OpenFlow be Adapted for Mobile Backhaul Networks?

This part of the dissertation deals with illustrating the feasibility of mobile backhaul network sharing via an open network approach, based on OpenFlow. We evaluate the practical feasibility of our proposed architectural designs adapted within the context of Software Defined Networking (SDN)/OpenFlow. By demonstrating the feasibility of adapting the existing OpenFlow mechanism to mobile backhaul network architecture, we seek to define how far it can be gone within the sharing scenarios, where the key lock is to define flexible and extensible policies that can be modified dynamically. Here, we look at several costs of the original OpenFlow model – virtualization properties, statistics collection etc. –from the perspectives both of an abstract distributed system design, and of a real-world switch implementation. We carried out experiments and discuss our experimental results to visualize the effect of performance by considering OpenFlow based backhaul networks to evaluate their effect on the network performance.

9.1. Introductory Statements

In the discussions that followed about backhaul network sharing, we presented our overview in Chapter 1 that SDN/OpenFlow is currently seen as one of the promising approaches that may pave the way towards that goal. With this view, we present our performance results supporting our claim and related discussions in this chapter. Currently, first OpenFlow implementations from hardware vendors are available and being deployed in networks. As a result, we can expect a growing number of works conducting experiments in OpenFlow-enabled networks. Here, OpenFlow serves as the basis for the evaluation of new virtualization techniques or new routing protocols for several use-case scenarios. However, the basic technology itself, i.e., the use of an OpenFlow controller to modify the flow table of an Ethernet router via a secure channel, is still new and few performance evaluations of the OpenFlow architecture exist. Understanding the performance and limitations of the basic OpenFlow concept is a pre-requisite for using it for any practical deployment to different application scenarios, such as ours. This may be restricted by questions about the control-plane scaling implications of such an approach, overall data plane performance, as well as the performance of OpenFlow switch and the OpenFlow controller itself. Therefore, we aim to provide the performance of an OpenFlow system in this chapter, with adequate results within the scope of our research.

Here, the research results are aimed at measuring the performance and researching different functionalities of OpenFlow protocol to determine the overall practicability of our proposals. The conducted research is a result of four weeks dedicated work and the results are verified by simulations and measurement experiments with the Open vSwitch software version 1.2.2, which has its own typical implementation of OpenFlow switch and an OpenFlow controller; precisely we consider NOX version 0.9 as the baseline for our performance study since it has been previously used in different papers [141]-[143]. The experiments presented in this chapter were performed around late 2011 and around mid 2012. Ever since then, there has been significant changes in the versions of OpenFlow switch (both in hardware implementations as well as software implementations) and OpenFlow controllers and have different performance characteristics. Nevertheless, we emphasize that our goal in this chapter is to show that SDN/OpenFlow can be optimized to be adapted within the mobile backhaul network architecture and how our proposed algorithms and architectures can be best fit-in.

The performance results capture several performance metrics, amongst others the throughput and latency of OpenFlow in comparison to standard switching and routing throughput analysis of the OpenFlow protocol, delay experienced by packets that have to be processed by the controller in contrast to be processed just by the switch, as well as the probability to drop packets if the controller is under high load. Based on our results, we derive conclusions about the

importance of the performance of the OpenFlow protocol in different realistic scenarios, and its effect on the traffic flowing through the OpenFlow-enabled switch.

9.2. Background and Concept Visualization

To better understand the results of the OpenFlow performance evaluation, we first give a brief overview of Software Defined Networking (SDN) and OpenFlow. Software-Defined Networking (SDN) is an emerging next-generation networking technology that is widely used in computer communications, data-center communications etc. The fundamental idea lies in decoupling the control and data planes in network switches and routers, thus enabling optimization of routing and switching equipment. SDN follows a stacked architecture with a southbound interface defined by the OpenFlow protocol that enables the interaction between the control and data planes, and a northbound API that presents a network abstraction interface to the applications and management systems residing at the top.

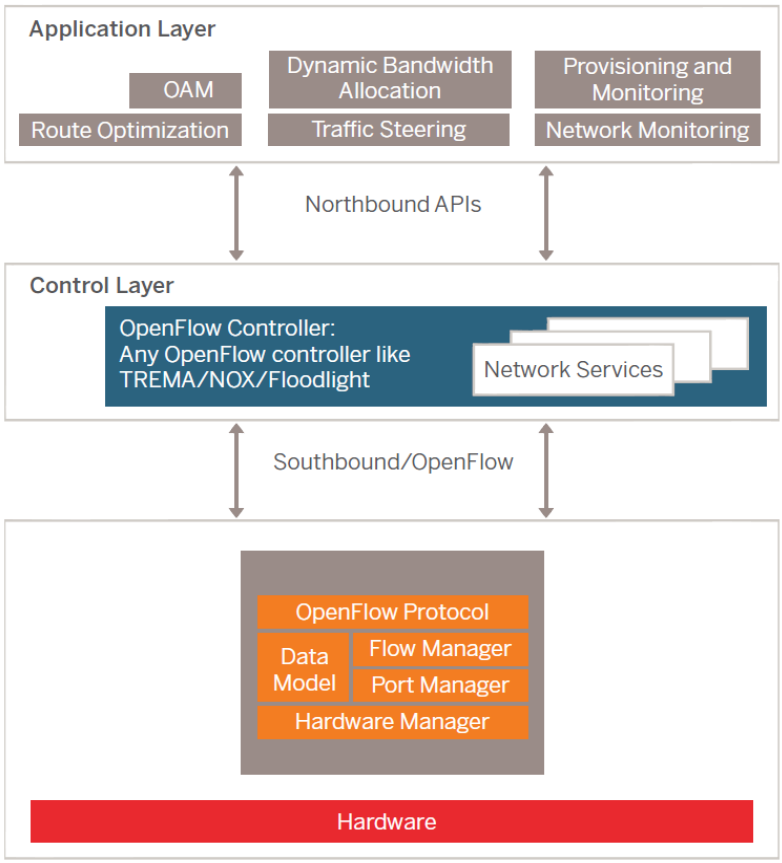


Figure 45: Illustration of architectural Flow diagram of Software Defined Networking (SDN).

With this, OpenFlow was first proposed in [144] as a way to enable researchers to conduct experiments in production networks. However, its advantages lead to its use beyond research, e.g. in the context of network virtualization, network optimization, traffic prioritization. At its

core, OpenFlow offers a higher flexibility in the routing of network flows and the freedom to change the behavior of a part of the network without influencing other traffic. It achieves this by separating the control plane in network switches from the data plane, and allowing for a separate controller entity that may change the forwarding rules in modern switches. This enables the implementation of, e.g., virtual networks, user mobility, or new network and transport layer protocols. We give a brief overview on the functionality of OpenFlow below; nevertheless more details on OpenFlow can be found in the OpenFlow specification [145].

9.2.1. OpenFlow Architecture in brief

The fundamental concept behind OpenFlow is that it allows the path of network packets through the network of switches to be determined by software running on a separate server. This separation of the control from the forwarding allows for more sophisticated traffic management than feasible today using Access Control Lists (ACLs) and routing protocols. It works by standardizing the interface between control and data planes and defines atomic behaviors for packet handing within each switching element. The control plane is then moved off-box into a centralized server called the OpenFlow Controller, thus enabling users to program their own network behaviors by injecting their own control programs into the controller.

OpenFlow switches: An OpenFlow switch has a flow table that stores an ordered list of rules for processing packets. Each rule consists of a pattern (matching on packet header fields), actions (such as forwarding, dropping, flooding, or modifying the packets, or sending them to the controller), a priority (to distinguish between rules with overlapping patterns), and a timeout (indicating whether/when the rule expires). A pattern can require an "exact match" on all relevant header fields (i.e., a microflow rule), or have "don't care" bits in some fields (i.e., a wildcard rule). For each rule, the switch maintains traffic counters that measure the number of bytes and packets processed so far. When a packet arrives, a switch selects the highest-priority matching rule, updates the traffic counters, and performs the specified action(s). Switches also generate events, such as a "join" event upon joining the network, or "port change" events when links go up or down.

Centralized controller: An OpenFlow network has a centralized programming model, where one (or a few) software controllers manage the underlying switches. The controller (un)installs rules in the switches, reads traffic statistics collected by the switches, and responds to network events. A controller application defines a handler for each event (e.g., packet arrival, rule timeout, and switch join), which may install new rules or issue new requests for traffic statistics. A common idiom for controller applications is to respond to a packet arrival by installing a rule for handling subsequent packets directly in the data plane. Sending packets to the controller

introduces overhead and delay, so most applications try to minimize the fraction of traffic that must go to the controller. These controller applications are general-purpose programs that can perform arbitrary computation and maintain arbitrary state.

FlowVisor [146] is a specialized OpenFlow controller that uses the OpenFlow protocol to control the underlying physical network. It acts as a transparent proxy between OpenFlow-enabled network devices and OpenFlow controllers, using the OpenFlow protocol to communicate with both the controllers and network devices, which are e-Node Bs in our scenario. FlowVisor can logically slice an OpenFlow network and allow multiple controllers to concurrently mange different subsets or different slices of the network resources. Slices can defined by any combination of ten packet header fields, including physical layer (switch ports), link layer (src/dst mac addresses, ether type), network layer (src/dst IP address, IP protocol), and transport layer (src/dst UDP/TCP ports or ICMP code). FlowVisor slices can also be defined with negation ("all packets but TCP packets with dst port 80"), unions ("ethertype is ARP or IP dst address is 255.255.255.255"), or intersections ("netblock 192.168.0.0/16 and IP protocol is TCP"). In this way, much like a Hypervisor that acts in a standard machine virtualization, FlowVisor intercepts all control messages to and from the data path and then checks severely and re-writes them to ensure isolation.

In an OpenFlow network, when a packet arrives at a switch that does not match any cache flow entries of the switch, the switch generates a message to the controller asking what to do with the packet that has been received of this form. The FlowVisor intercepts this message and makes a policy check to determine which controller is responsible for this packet. This policy check is what we define a slicing definition, i.e. when an OpenFlow switch connects to a FlowVisor, the FlowVisor receives all the slices configured to the OpenFlow switch based on the MAC address. The message is then forwarded to the appropriate controller associated with the slice which makes the forwarding decision. Once the decision is made, the controller sends a corresponding new forwarding rule back down to the switch. The FlowVisor again intercepts the rule and does another policy check, this time, to ensure that the new rule does not infringe on the traffic from other slices. Once the rules are approved by the FlowVisor, it is forwarded onto the switch, cached and then the packet is forwarded on appropriately. Any new packets arriving further, upon matching the cache entry are then forwarded without going through this process again. Thus, all OpenFlow messages, both from switch to the controller and vice versa, are sent through FlowVisor. More explanations about the working of OpenFlow are enumerated in [145].

The fundamental motivation for the choice of SDN/OpenFlow is the underlying fact that the operators want to control their own part of their networks even though they share their network with another operator. Due to the particular ability of OpenFlow protocol to endow software

defined networking by providing an architecture for monitoring the network and also by providing the ability to configure the network in a positively controlled system, it is conceptualized as the best choice for our proposed architecture. With the current state of the art, to the best of our knowledge, not a single traditional network monitoring and management tool offers this capability. Besides, network operators can define flows and determine what paths those flows take through a network, regardless of the underlying hardware (where in most cases the vendors are different when two different operators share the network). Presented below are our arguments towards realizing our solutions adapted within the scope of SDN/OpenFlow:

Route Optimization: One of our arguments dealt with calculating routes across multiple MNOs. Legacy networks are inflexible in that all traffic targeting the same destination is sent along a pre-determined path. Paths are calculated on a local basis, and thus the network may not be utilized to its full potential. Each device in the network may have separate management and configuration processes, which can put a huge burden on the administrator as the network grows in size and complexity. As mentioned before, with SDN, a single controller can configure and manage the entire network for each operator, and network elements can be configured to precisely control how the network operates and handles the traffic. This introduces greater flexibility into the network, simplifies management, and reduces maintenance and trouble-shooting. It allows network control applications to be rolled out as efficient as possible.

Dynamic Bandwidth Allocation: We targeted on how to allocate bandwidth dynamically across links of multiple MNOs when they decide to 'divide and share' their bandwidth. Although a variety of mechanisms are available today to tackle link congestion (e.g. MPLS-TE), there is no mechanism that enables the differentiation of the traffic between two different operators when the network is sliced across dimensions such as topology, bandwidth and forwarding table entries. With OpenFlow, a centralized controller with global knowledge of the network across the dimensions of topology, bandwidth could make better utilization of network resource. We leverage recent work on FlowVisor, a slicing mechanism for OpenFlow-based networks. FlowVisor enables network slicing by providing virtualized views of network resources, and can be used with QoS controller to provide more strict isolation between network slices in congestion. From figure 46, when the traffic is re-routed through the sharing operators' backhaul, the physical equipment i.e. access nodes are sliced into two. By this, it is implied that it enforces a policy where there are only two operators who share the same network resources.

According to this, the entire backhaul network resource is divided into two slices by the FlowVisor policy; one for operator A and one for operator B. Each operator operates and controls its own controller(s). Thus, FlowVisor policy slices the network so that operator A's sees traffic from users that have opted-in to his slice. Operators A's slice controller does not know the

network has been sliced, so it does not realize it but only sees a subset of only its own traffic. When operator A's controller sends a flow entry to the e-Node Bs, FlowVisor intercepts it, examines operator A's slice policy, and rewrites the entry to include only traffic from the allowed source. Hence the operator A's controller is controlling only the flows it is allowed to, without knowing that the FlowVisor is slicing the network underneath. Similarly, messages that are originating from the e-Node Bs are only forwarded to respective controllers whose flowspace match the message. That is, it will only be forwarded to operator A if the new flow is traffic from a user of operator A that has opted-in to his slice. Thus, FlowVisor enforces transparency and isolation between slices by inspecting, rewriting, and policing OpenFlow messages as they pass. Depending on the resource allocation policy, message type, destination, and content, the FlowVisor will forward a given message unchanged, translate it to a suitable message and forward, or "bounce" the message back to its sender in the form of an OpenFlow error message.

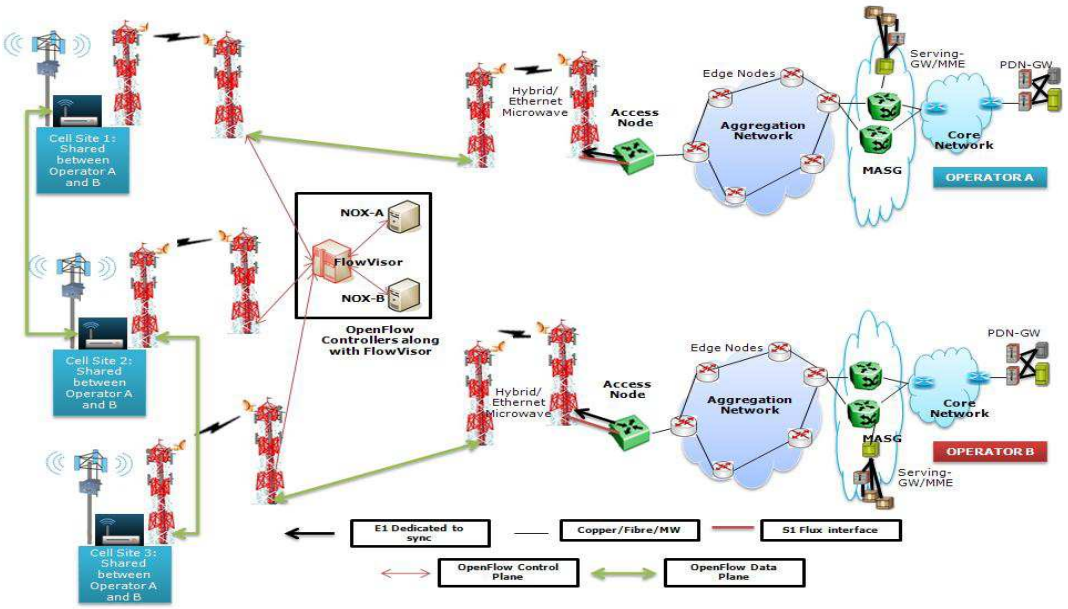


Figure 46: Access Network sharing between operators using Virtualization (Thanks to OpenFlow FlowVisor)

For a message sent from slice controller to e-Node B, FlowVisor ensures that the message acts only on traffic within the resources assigned to the slice. For a message in the opposite direction (e-Node B to controller), the FlowVisor examines the message content to infer the corresponding slice(s) to which the message should be forwarded. Slice controllers only receive messages that are relevant to their network slice. Thus, from a slice controller's perspective, FlowVisor appears as an e-Node B (or a network of e-Node Bs); from an e-Node B's perspective, FlowVisor appears as a controller. This is one use case by which we trying to elaborate that it is possible to efficiently slice a network according to the needs of the operators.

Choice of Virtualization: Realizing network virtualization technique to the LTE/EPC mobile network architecture means to virtualize the infrastructure of the LTE system. This includes e-Node Bs, routers and even ethernet links and let multiple mobile network operators share a common infrastructure that already exists, by creating their own virtualized network depending on their requirements. From our research prospective, there are primarily two different scopes of virtualization that are foreseen for the LTE/EPC mobile architecture. The first one falls under the scope of virtualization of the air interface between the UE and the e-Node Bs and the second one is to virtualize the physical nodes from the e-Node Bs extending to the backhaul. In [147], the authors carried out virtualization of air interface between the UE and the e-Node Bs by running Hypervisor on the physical e-Node Bs. The simulation results proved that based on the contract configurations and the traffic load of each virtual operator, when the air interface resources are shared among the operators, the overall resource utilization is enhanced and the performance of both network and end-user is better. Although the simulation results are quite specific, the basic findings are representative and show the advantages of applying network virtualization to the LTE/EPC architecture. Their results also demonstrated that the sharing operators benefitted from virtualization mainly by being able to cut costs and providing better performance for the users.

Forecasting such results as the possibility of opening the market to new players especially Greenfield operators that can serve a specific role and have small numbers of users, here, we propose a solution that is based upon virtualization of the physical nodes of the LTE/EPC architecture which particularly includes the e-Node Bs. Each e-Node B is virtually sliced and the resources of physical e-Node Bs owned by an operator are allowed to be controlled remotely by the sharing operator also. Current access network sharing techniques discussed in chapter 2 are based on VLANs [148], a common network slicing technique. However, from our research results, we could not be convinced with the advantages that VLANs are offering at the moment. In enterprise and data center networks, VLAN technology is commonplace and continues to evolve. VLANs like IEEE 802.1Q operate mainly on the link layer, subdividing a switched Local Area Network (LAN) into several distinct groups either by assigning the different ports of a switch to different VLANs or by tagging link layer frames with VLAN identifiers and then routing accordingly. When two operators decide to share the same e-Node B with the current VLAN techniques, the operators partition the network by switch port and all traffic is mapped to a VLAN by input port or explicit tag. Nevertheless, these types of partitioning by the VLANs are considered as coarse-grained type of network slicing that complicates IP mobility or wireless handover. On the other hand, in the backbone networks, virtualization in the form of different protocol families utilizing a single Multi Protocol Label Switching (MPLS) core network, Virtual Private Networks (VPN) (both layer-2 and layer-3) and tunneling technologies (e.g., IPSec) are widely used and allow some degree of sharing of common physical infrastructures. However,

such virtualization approaches are focusing on the virtualization of links and does not allow for traffic differentiation. Accordingly, our solution is based on the idea of having a dedicated OpenFlow network which implements FlowVisor based isolation, which deals with the virtualization of a whole network infrastructure with the ability to control the traffic remotely.

We exploit the capability of FlowVisor based virtualization for virtualizing LTE/EPC architecture because it gives the possibility to slice or virtualize bandwidth, traffic, topology of any given network. After virtualization, each operator gets its own portion on a link. As mentioned before, one of the current technologies that is widely used in today's networks as well as a proposed solution for LTE network sharing scenario is based on VLANs. However, VLANs differ from FlowVisor in that rather than virtualizing the network control layer generally, they virtualize a specific forwarding algorithm (L2 learning). FlowVisor, on the other hand, not only supports a much more flexible method of defining networks over set of flows called flow space, it provides a model for virtualizing any forwarding logic which conforms to the basic flow model. Taking advantage of FlowVisor's flexible and fine-grained network slicing technique, with additional capability of hosting multiple OpenFlow controllers with one controller per slice, making sure that a controller can observe and control its own slice, while isolating one slice from another, we chose to visualize our proposed solution on network infrastructure sharing based on it.

Network Management: The basal motivation to consider OpenFlow to tackle link congestion (caused due to link/node failures or traffic peak) was due to the limitations faced by today's routers that arise from the basic assumptions of IP routing, which summarizes to the idea that core routers treat IP traffic as connectionless datagrams, not as streams of data similar to virtual circuits in ATM or Frame Relay. The only mechanism available in today's purely IP-based networks that optimizes the utilization of redundant links in the network core and influences the paths that the traffic is taking based on the actual network load is Multi-Protocol Label Switching Traffic Engineering (MPLS TE).

- **Reintroducing virtual circuits to the IP core:** MPLS-TE was not connected to QoS for a long time. While alternate traffic-engineered (TE) label switch paths (LSPs) across the network could be provisioned and even specify how much bandwidth each path would need, the bandwidth limitations or preferential treatments of provisioned LSPs were not enforced automatically. MPLS TE was configured independently from the IP QoS or MPLS QoS, in that their interoperability was totally dependent on a good network design.

- **Automatic bandwidth adjustment simplifies MPLS TE provisioning:** Most large service providers have experienced the pain of provisioning numerous MPLS TE LSPs

across the core network (configured as MPLS TE tunnels on the edge routers). Ideally, a pair of LSPs is needed between each pair of edge devices or between each pair of Penultimate Hop Popping (POPs). The number of MPLS TE tunnels thus grows with the square of the number of edge points in the network. The autotunnel mesh groups significantly simplify MPLS-TE provisioning because the tunnels between members of the mesh group are established automatically. Allocating correct bandwidth to each MPLS-TE LSP provisioned across the network core became easier with the automatic bandwidth adjustment (autobandwidth) feature, which measures the actual long-term utilization of an LSP and adjusts its bandwidth allocation in real time. With edge problems solved, focusing on the network core, unless there is fortunate enough very high-bandwidth core links, it is inevitable to face link congestion. The bottom line is that it is best to alleviate these issues before they arise. Most modern routers and layer-3 switches perform forwarding decisions independently from the QoS decisions. For example, when a core link becomes congested, a router continues forwarding packets onto the congested link even though there might be a longer or slower but less congested alternate path through the network. The core MPLS QoS mechanisms (queuing and selective dropping) can try to cope with the congestion, but they are effectively a zero-sum effort. Obviously, we need something more than standard IP routing and QoS. Routers should be aware of the bigger picture and use the network resources more intelligently, doubtless to adopt OpenFlow.

Fault Notification: The classical solutions for fault detection and notification involve a router to identify the failure and establish an alternate route every time a failure is identified. Considering SDN architecture, it is the capability of OpenFlow controller (e.g. NOX) to take control of how traffic flows through a network out of the hands of the infrastructure, i.e. the switches and routers that could allow operators to craft policies that find paths with available bandwidth, less latency or congestion, and fewer hops. Nevertheless, OpenFlow implementation offers two kinds of functionalities. Accordingly in the following section, we analyze both of it and we envision our solution to tackle link failures in mobile backhaul networks.

- **Notification by the OpenFlow controller- Fail–Closed mode:** As briefed earlier, in SDN the switches and the routers do not have the intelligence to re-route the traffic to a new path without the updates from the controller. Whenever the connection between the switch and the controller fails, the switch does not take any actions, it simply waits for the controller to establish a new connection. The controller identifies a failed link (by constantly sending *packet_out* OpenFlow messages and receiving *packet-in* OpenFlow messages from the switches) and updates flow table entries in all the relevant switches that are connected to it. Therefore, until the controller sends an update, packets that

travel on the failed link will be dropped. Therefore, it is crucial to prevent any traffic from entering the failed link to preserve the processing resources of the network. Besides, in a mobile communication network, it is practically impossible for a centralized controller to reach all of the innumerous switches and routers (say e-Node Bs) and detect failures. Especially for our proposed architecture that takes in account wireless backhaul network sharing between operators, each operator owns and controls different sets of switches that may be controlled by different controllers. If a link fails in such scenarios and the controllers make conflicting decisions in establishing new routes, it could lead to infinite loops that continue to route within the backhaul network causing enormous amount of unnecessary control-plane traffic in the network. The whole idea of incorporating SDN for wireless backhaul sharing is to considerably reduce the network traffic. Hence it is important to take precautions to prevent any loops in the network that could be formed by a failed link.

- **Notification by the OpenFlow switch- Fail-Open mode:** While the above mentioned solution for handling and resolving link failures using controller action proves to create undesired effects on the network, the second functionality is the fail–open mode. In fail–open mode, whenever the connection between the switch and the controller fails, the switch becomes proactive and tries to reach the controller periodically (by sending packet-in OpenFlow messages) until the controller becomes available.

The above mentioned functionality proves practically feasible, since the network does not get flooded by unwanted control-plane traffic from the centralized controller. This also reduces the resource utilization of the centralized controller that has to reach several switches constantly within the large network. We consider this to be predominantly suitable solution to tackle link failure situation within mobile backhaul architecture. Nevertheless, in this case, the switch that is disconnected from the controller starts flooding the network. This still would result in more control-plane traffic being circulated in the network. In [149], authors have proposed a mechanism where, link failure detection packets such Bi-Directional Forwarding (BFD) packets are periodically sent out on links such as via the MPLS-TE profile to peer OpenFlow switches. Link failure detection packets are received from the peer OpenFlow switches on the links and monitored. A link failure is detected if no incoming link failure detection packets are received on a link for a periodical interval. In the event of link failure, traffic is re-directed from the failed link to a back-up link. Though this approach seems to be convincing, it necessitates the need for a protocol such as the BFD to be run in each switch/router entity and also the need for MPLS-TE. Henceforth, we propose our own technique to tackle congestion due to link failures, to make this feature fully practically applicable for wireless backhaul networks of cellular operators.

Our approach does not necessitate the additional use for a protocol such as the BFD to be run on each entity, rather it takes advantage of the built-in capability of each device to ping each other by a simple Echo request message. Especially with the LTE architecture introducing the new X2 interface connecting each LTE nodes, it is thus possible for each node to check its connectivity with its neighbors. We briefly illustrate the step-by-step procedure for the detection of link failure below:

1. Every e-Node B keeps sending Echo request message to its neighbor through the X2 interface.

2. When Echo response message is not received, the e-Node B creates an error message, indicating about the link failure and sends it across the interface that it does not receive a response.

3. Therefore, the neighboring e-Nodes that receive the error message stops forwarding any further traffic across the direction of failed link.

4. Neighboring e-Node Bs that had received the error message also notifies the controller about the failed link.

5. When informed of a failed link, the controller then flushes all the flow entries at those switch which use the failed link.

6. When a new packet from each of these affected flows arrives at the switch, the packet will be forwarded to the controller which will then establish a set of flow entries along a new path thus avoiding the failed link.

To explain this simply, let's look at figure 47, where the point A1 and A2 are the last-mile links of two operators that are connected using an additional link and B1 and B2 are the access nodes which essentially are a part of middle-mile. C1 and C2 further represents the aggregation nodes and D1 and D2 denotes the core network such as the Service Gateway (S-GW) and Packet Data Network Gateway (PDN-GW) and finally E1 and E2 represents the Internet. OpenFlow enabled switches between A1 and C1 are controlled by the controller of operator A and between A2 and C2 are controlled by the controller of operator B.

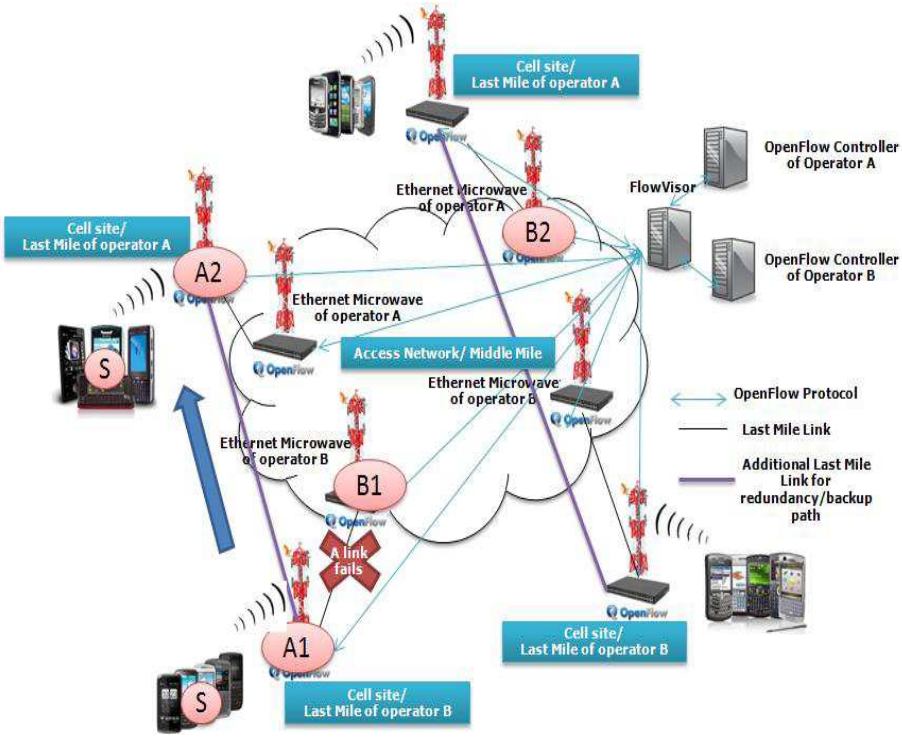


Figure 47: Illustration of recovery from link congestion through backhaul sharing.

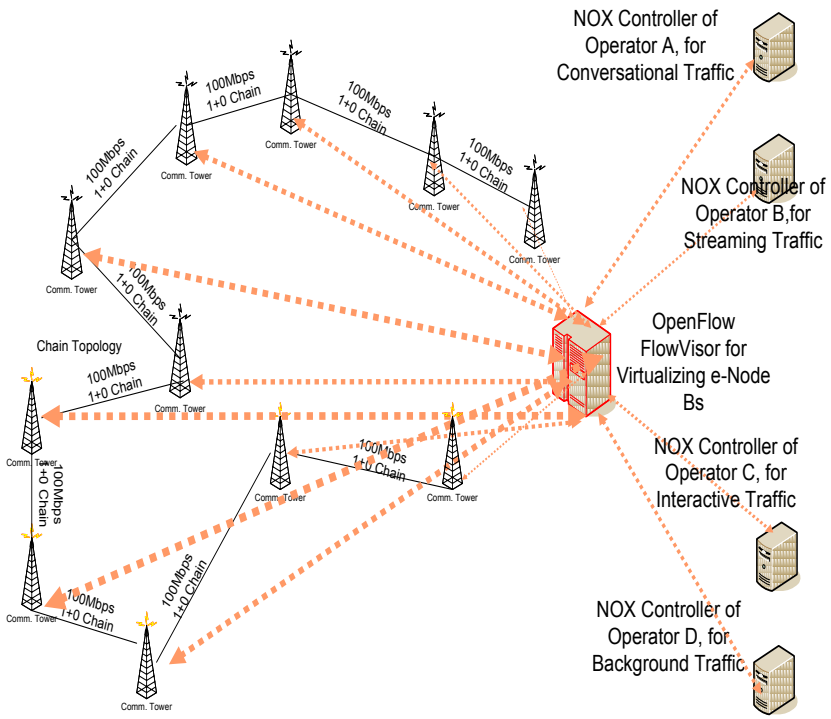
From figure 47, it is possible for B1 to check whether all of its links are up and working. If B1 could inform its neighbors A1 and C1 of the failed link, it is possible to prevent the packets from A1 from being dropped. Furthermore, when A1 informs the controller of the broken link, a new route could be given by the controller immediately since the controller is topology aware. In addition, this also prevents B1, C1 and D1 to constantly flood the controller.

9.3. Resource Sharing Strategies: Illustrative Examples

Network infrastructure sharing should enable the operators to be able to share the network resources that are already available, without having to invest any further, just by making "slight" modifications to the existing system. This "slight" modification should not result in any additional cost more than it would result in establishing a separate network infrastructure. Our primary solution focuses on the sharing strategies extending to the backhaul where the resources from the e-Node Bs until the mobile core network are shared and controlled by operators who have concluded on a sharing agreement. Now, according to our proposal, each operator will be able to share sufficient amount of its own resource with the other operator(s) who is sharing the infrastructure for the purpose of load sharing as well as to tackle network failure situations of their own network.

Here the network resources are divided into four different slices. That is each e-Node B is sliced into four for the four different classes of traffic- one optimized for conversational traffic which

requires constant bit rate, like voice traffic, one optimized for streaming which is best supported as a variable bit rate service such as audio or video streaming, one optimized for interactive which uses the available bit rate and the last one for background which uses unspecified bit rate like web applications. These four different types of traffic correspond to four different virtual mobile network operators and this is enforced as a policy in the FlowVisor. Figure 48 shows an example topology that could represent real world OpenFlow mobile network architecture based on our proposal. In Figure 48, each e-node B in the topology is the connected to a common FlowVisor over a single network path which acts as proxy between the e-node Bs and four different NOX controllers, each operated and controlled by four different operators according to the specified traffic class. Thus, FlowVisor slices every e-Node B of our network and creates multiple logical copies of the same physical network. As explained above, when a controller sends a flow entry to the e-Node B, FlowVisor intercepts it, examines the respective slice policy and rewrites the entry to include only traffic from the allowed source. Thus the bandwidth allocated for each e-Node Bs to carry the traffic towards the core network are isolated virtually and shared among the operators. Thus, operators will be able to control and monitor the resources of a physical e-Node B without really having to take control over it.



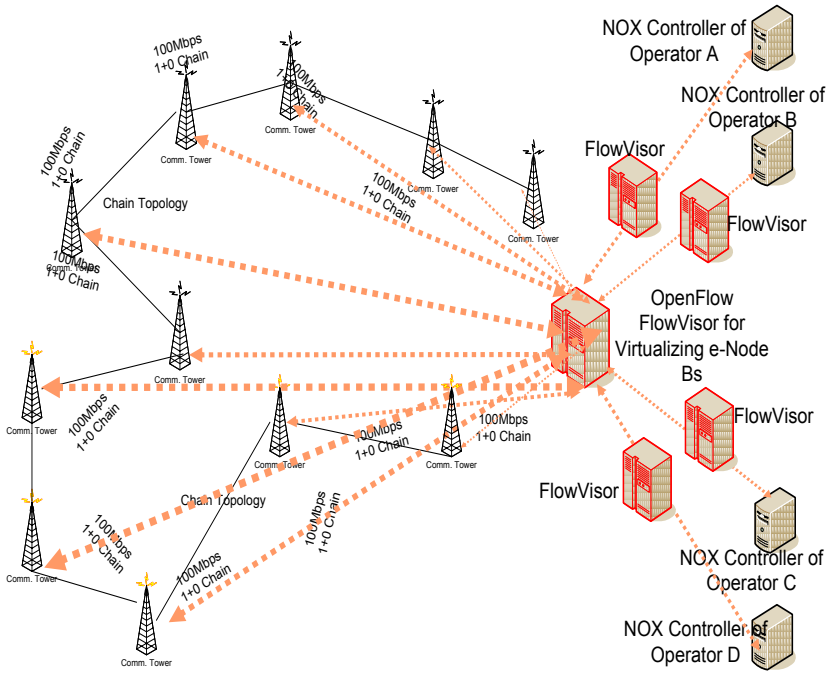


Figure 48: Backhaul Network sharing strategies between operators using Virtualization based on traffic needs.

The main advantage of this solution are

- Enormous cost reduction: If all the four operators (as in our case) decide to share the cost for deploying the network infrastructure, CAPEX will be greatly reduced for each of them individually.
- Efficient resource utilization: The operators get to optimize their traffic according to the available bandwidth. With our solution we could achieve more optimized use of the available bandwidth according to need of the applications.
- Technically simple solution: Since, the operators do not have to modify the e-Node Bs, it allows for more simplified modification at any time just in the controllers.
- The operators do not have to take care or even pay attention to the traffic of the sharing operator that flows through their own backhaul network infrastructure after the provisioning.
- The operators have the liberty to choose to prioritize the type of traffic that he would want to flow in the sharing backhaul bandwidth. Even better is, the operator can nonetheless care about the traffic priorities and just re-route a part of its own traffic in the shared bandwidth.

9.4. Performance Evaluation

Therefore, here, the properties, features, and limitations of OpenFlow enabled devices when illustrated within the context of LTE/EPC architecture are clearly described. The mobile network architecture model was prototypically simplified and simulated by employing the currently available virtualization technique, FlowVisor [5] proposed by the OpenFlow group consortium, since our proposal is based on adapting OpenFlow protocol to the LTE/EPC architecture and the performances were evaluated with comparative results. This chapter is a proof of concept experimentation to validate the virtualization behavior of FlowVisor on mobile network architecture. Here we evaluate the performance of a network based on OpenFlow protocols on the virtualization of the e-Node Bs for different traffic classes and allocating one slice per operator depending upon their traffic needs and evaluate how the available bandwidth is isolated efficiently depending upon the traffic. The most interesting feature of networks based on FlowVisor virtualization technique is that, it gives the operators, the possibility to slice or virtualize bandwidth, traffic, topology of any given network to give each slice its own fraction on a link to the sharing operator.

9.4.1. Quantitative analysis on Virtualization Capabilities

The first part of the simulations was to prove that the efficiency of OpenFlow protocol compared to standard layer 2 switching is better, since a part of our argument also involves proving that the current access network sharing techniques for e-Node B based on VLAN could be replaced by OpenFlow architecture. In order to prove the validity of our proposal, we evaluated the performance of OpenFlow protocol against the standard VLANs. As a result of it, we tried to perform the three tests each separately in linux PC.

The aim of this test is to evaluate the performance gains that could be achieved from virtualizing the LTE/EPC nodes based on OpenFlow implementation exploiting the FlowVisor's bandwidth isolation properties. The fundamental idea is to prove that the network resource that is allocated to a certain physical equipment, which is e-Node B in our case, will be fairly shared among each and every operator who concluded on a sharing agreement based on traffic needs. To demonstrate this, we experimented by considering a simple topology which consists of one OpenFlow Switch connected to four hosts, one FlowVisor Controller and two NOX controllers defining two slices, one is for TCP traffic and the other slice is for UDP traffic. The demonstrated test setup uses two physical machines- one running FlowVisor 0.7.2. configuration the other one runs Mininet simulation tool [150] that helps to populate OpenFlow switches connected to hosts and NOX controllers, running on a virtual LINUX Ubuntu 10.10 as the default OS. Mininet uses the software-based switch type of OpenFlow protocol that use UNIX/Linux systems to implement the entire OpenFlow switch functions. We carried out two sets of experiments. The

first one is when the OpenFlow switch is directly connected to the NOX controllers and the second by connecting the switch to FlowVisor, which is inturn connected to the NOX controller. In both the experiments, there are four hosts each connected to two OpenFlow switches on which we carried out TCP and UDP tests using iperf. For the first experiment without FlowVisor connected, when iperf was carried out simultaneously for TCP and UDP traffic on the host machines, we observed that the UDP traffic consumes nearly all the bandwidth and the TCP traffic was only given a part of the bandwidth which averages to 12.28Mbytes of the 1G available link bandwidth. This, in reality means that one operator gets to enjoy more bandwidth than the other when they are sharing a common link. For the second test, where FlowVisor is connected and iperf was carried out simultaneously for TCP and UDP traffic on the host machines, the TCP traffic was able to gain control of the bandwidth ranging to a value of 716Mbytes of the 1G available link bandwidth. This concludes our solution based on FlowVisor isolation where every operator depending upon the contract signed for the specific kind of traffic, will be given a fair share of the network resource. Thus, the FlowVisor does the task of isolating the bandwidth and traffic among the different operators who agreed on sharing. Hence, we could conclude that by adapting FlowVisor based bandwidth isolation features for network infrastructure sharing in LTE/EPC networks, each operator could have its fair share of bandwidth depending upon the traffic needs. Primarily, our emphasis is that with this kind of virtualization technique based on adopting OpenFlow, the configuration of the e-Node B's themselves need not have to be modified in order to change properties of the network infrastructure that is being shared. Also, this scenario allows examination of several aspects of virtualization of e-Node Bs. First, it can be shown that it is possible to migrate one physical network infrastructure entirely into a number of isolated networks just by adding different slice definition in the FlowVisor, without really making many modifications to the existing design of the e-Node Bs. Second, it is possible to share several e-Node Bs in parallel among different operators, sporting different attributes like incorporating different traffic properties for the respective virtually isolated e-Node Bs of the operator. Third, changes within one network can be achieved dynamic during run-time, without any disruption of service in any other virtual e-Node B of another sharing operator. And finally, operators get to control their part of the network without having to be interfered by the sharing operator.

9.4.2. Quantitative analysis on Network Management Capabilities

As a starting point to evaluate our proposal, it thus becomes necessary to compare OpenFlow with the existing network management protocols. Therefore, in this section we discuss our experimental results to visualize the effect of performance by considering IP, MPLS and OpenFlow based backbone networks to evaluate their effect on the network performance.

9.4.2.1. Experimental Setup

To test the performance of forwarding among the various technologies and to be fair with the testing scenarios, we set up a small network of Linux kernel–based software switches. First, to test the performance metrics of MPLS, we thus adopted to the most significant approach of the MPLS-for-Linux project [151] to produce our test results. It supports MPLS integration into 2.6.18.1 Linux kernel. This project implements the basic MPLS stack for the Linux kernel, with the necessary forwarding functions. In this context, the IETF proposes two different approaches for deploying MPLS-based VPNs. Layer 2 VPNs, where layer 2 frames are directly forwarded from source to destination sites using MPLS as the signaling and management plane and Layer 3 VPNs, where IP is the common layer between sites and MPLS is used in the backbone for a more efficient IP packet forwarding. For our evaluation, we considered connections between MPLS systems to be 'native', with no underlying transport protocol. Second, to test the performance metrics of IP-Routing, we enabled the ip_forwarding feature to set the layer-3 of the Linux kernel by querying the sysctl kernel value net.ipv4.ip_forward to see if forwarding is enabled or not. Third, to test the performance metrics of OpenFlow protocol, we used the software based OpenFlow switch (version v1.0). Using the OpenFlow tool DataPathControl (dpctl), we configured two ports enabling these interfaces to act as an OpenFlow switch. Also we added a simple rule in the flow table to forward input packets with a certain destination or source IP address to the output port (interface).

For network testing, a traffic generation and analysis tool is required. The tool should enable analysis of all traffic scenarios including well-behaved traffic such as TCP and real-time traffic such as UDP. Many tools are available online, such as TTCP, Netperf, JTG, Ethereal, Iperf, etc. For testing our network we use Iperf, which can measure maximum TCP bandwidth, allowing tuning of various parameters and UDP characteristics. Iperf also reports bandwidth, delay jitter, datagram loss. Iperf can run as a separate instance, or one can have multiple instances of Iperf to generate and capture individual flows at source and destination respectively.

9.4.3. Performance Metrics and Analysis

9.4.3.1. Throughput Analysis

Throughput of any network depends upon its link speed and mainly dependent on the nature of the forwarding technology behind it that is used to transmit the data.

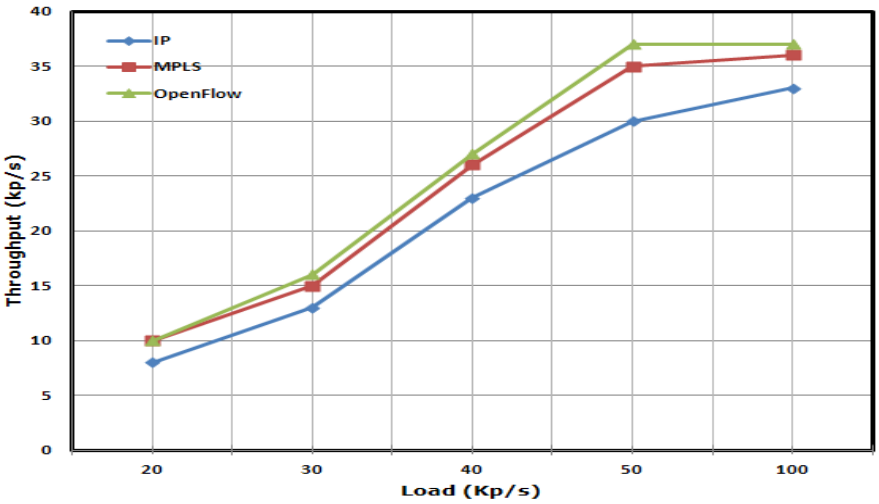


Figure 49: Performance comparison for Throughput.

From figure 49, it is evident that there is a linear increase with the throughput as load increases up to a certain point. However, after this point, the values of throughput does not vary very rapidly as initially in cases of OpenFlow and MPLS but there is an observable decrease in the case of IP. This is as a result of the connectionless nature of IP protocol that results in heavy packet drop that may be because of congestion. On the other hand, OpenFlow and MPLS based networks establish a virtual path that is defined for each packet in the network cores. In particular, OpenFlow protocol that runs on top of TCP, which is a connection-oriented protocol with congestion avoidance intelligence, produces the best result. Besides, after certain point, when the load increases even further, it appears that OpenFlow and MPLS's performance are almost the same. This is due to the effect of the flow table entries of OpenFlow, since OpenFlow's performance also depends upon the size of the flow table.

9.4.3.2.Delay Analysis

Figure 50 clearly indicates the performance comparison carried out with respect to delay. Although, initially the delay among each of the technologies vary very slightly for small loads, with increase of loads, the delay of IP is quite intolerable. To reason it, it is the absence of virtual connection that amounts for the relatively larger delay in IP based cores especially when compared with OpenFlow. On the other-hand, MPLS falls between these two although its behavior is similar to that of OpenFlow. There is an initial delay with OpenFlow since the controller takes time to setup the path. At the later point, since the path is already established, high delay values are not observed.

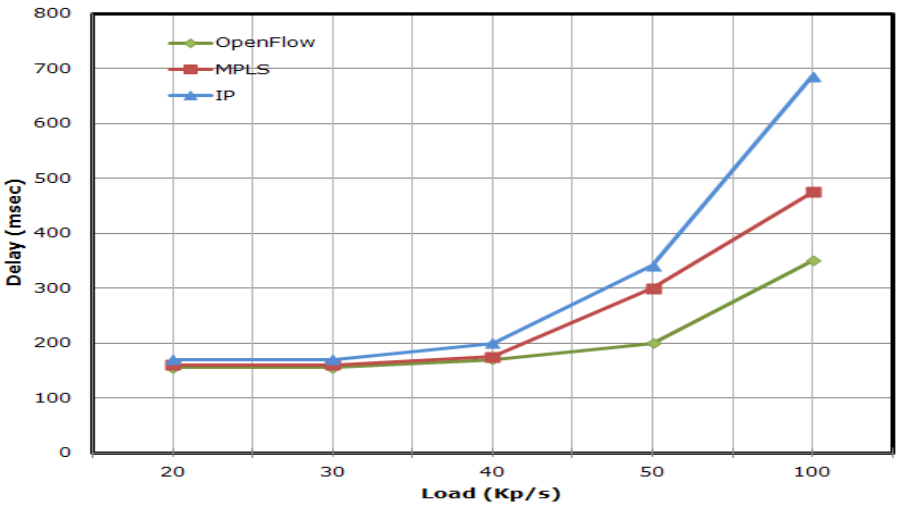


Figure 50: Performance comparison for Delay.

9.4.3.3. Network Utilization Efficiency

This is one of the key metrics to check the efficiency of the technology. This weighs how efficiently the technology makes use of the available resources such as bandwidth etc. The general trend of the utilization is to linearly increase with load till the point of saturation is reached. Note that IP relatively makes good use of the available bandwidth although it produces lower throughput. This is because number of packets is large in case of IP compared to other two technologies because of no prior path establishment time. Moreover, IP router needs extra bandwidth in order to run routing algorithm several times to predict the best available path. Relatively less utilization of OpenFlow and MPLS does not mean inefficiency. Instead it will benefit at the time of congestion and overloading situations.

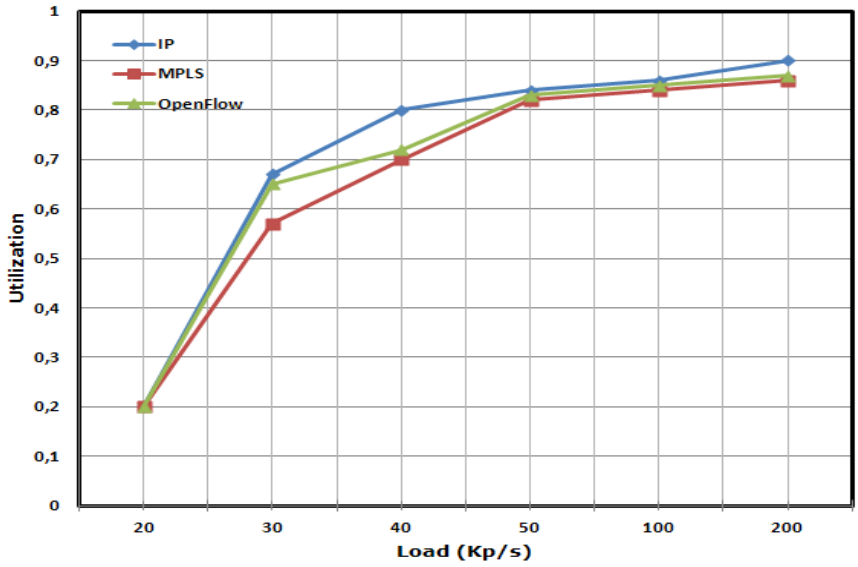


Figure 51: Performance comparison for Network Utilization.

9.4.3.4. Normalized Received Traffic

In figure 52, as we observe the effect of connectionless and connection oriented features of IP and other two technologies respectively, connectionless behavior of IP leads to decreased utilization at the time of congestion (e.g. at 50kpps). However, it is not always the case i.e. IP device tries to avoid congestion by running congestion avoidance mechanism which most of the time works efficiently. It is therefore evident from figure 52 that there is only one particular short interval of time where the received traffic normalized by sent traffic is significantly low.

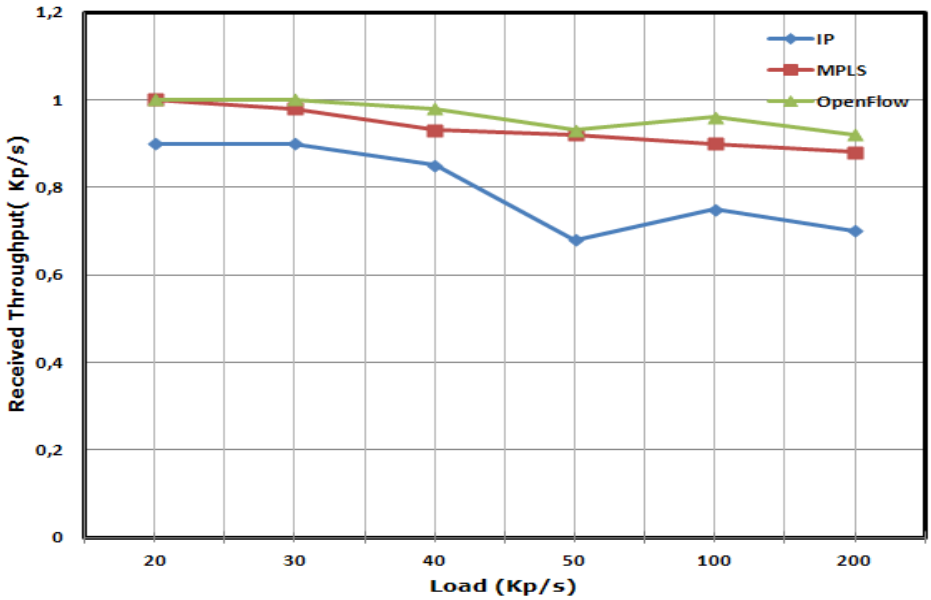


Figure 52: Performance comparison for Received Throughput.

Furthermore, we also observe that there is a gradual decrease in the received traffic common to all network cores with the increase in offered load. Our hypothesis for this is that it could be due capacity limit, network environment and some other reasons e.g. poor performance at physical layer, the performance of the test bed set up etc. A further examination on this is needed. However, it is important to mention that the current IP based network cores do not depict such a poor performance on account of improved IPv6 architecture and some other technology advancement which we did not include in our simulation. Our comparative results here take into account IPv4 versus OpenFlow and MPLS because we also do not consider the recent improvements made in OpenFlow and MPLS.

9.5. Concluding Discussions

4G network sharing strategies are highly sensitive to operators' business goals and to regulations where they provide services. One of the most important considerations that is taken into account in mobile network sharing strategy is to have maximum flexibility to accommodate the shifting

relationships between business goals and regulations as new wireless devices drive change in the market. We presented our idea to tackle congestion in communication links due to traffic overload and/or network failure situations as a means to dynamically create private, resource isolated, customizable, end-to-end mobile networks. We believe that the SDN/OpenFlow architecture and control plane separation will open new mutual beneficial interaction between network operators that can create new capabilities at the packet-circuit interface.

We believe that OpenFlow opens a door to a new world of virtualization thereby enabling to utilize shared network access. It can be an enabler to network virtualization and service virtualization programmability within the context of mobile network architecture. Network & service virtualization for increasing the ARPU while cutting down CapEx, OpEx can increase revenue opportunities for network service providers. As a part of our proposal towards network infrastructure sharing within the context of LTE/EPC, we have demonstrated in this chapter, the adaptability of OpenFlow protocols incorporating the basic additional features to be inculcated into the architecture. With the first phase of results here, we could conclude that network infrastructure sharing by means of virtualization could open new doors not only towards cost reduction but also gives the operators the flexibility they want in terms of traffic prioritization. It allows virtualization of an existing network infrastructure, to start at least between four operators in parallel thus enabling dynamic modification of the properties of one network operator giving fair resource allocation to operators.

With such convincing results, our next phase of results extended to prove that with such virtualization technique adapting OpenFlow mechanisms, eases the design of sophisticated network management solutions on top of virtualized networks (e.g. resilient networks). One of these capabilities has been demonstrated here as a networking application that uses them to provide application-aware aggregation and traffic engineering. From an operational perspective this approach allows network resources to be considered a flexible pool of assets which can be dynamically utilized as needed. Besides everything else, we envision the SDN as a significant approach to enable new service abstractions especially where network operators need to interact with the network more closely, or customize network behavior.

Scalability and redundancy are possible by making a controller stateless, allowing simple load-balancing over multiple separate devices. If we are successful in deploying OpenFlow networks in the existing mobile network infrastructure, it will lead to a new generation of control software, allowing operators to re-use controllers.

Part V

Substitution Networks

*"The Internet is becoming the town square for the global village of tomorrow." – **Bill Gates, Programmer, Inventor and Philanthropist.***

Chapter 10

Substitution Networks Based on SDN- A Radical View

A Substitution Network (SN) is a rapidly deployable temporary wireless network that should be dynamically integrated within an existing base network. They back-up the base network in order to meet temporary network overloaded conditions to keep providing services and to ensure the network connectivity, which could not be achieved by the base network alone. Within this context, in this chapter, we propose a solution considering SNs as a means for provisioning backup path for Mobile Network Operators (MNOs backhaul to overcome network overload due to excessive wireless data traffic. Our approach considers Software Defined Networking (SDN) technology due to its flexibility to integrate diverse future generations of switches as well as its centralized approach for decoupling control-plane and data-plane. Our solution is based on exploring the OpenFlow protocol. Based on our experimental results, we demonstrate the feasibility of our proposal, which allows verifying the effectiveness of adopting SNs based on SDN. Here, our approach is considered in the context of emerging economies, since, from past research, studies have shown that OPEX/CAPEX may not have the same impact in emerging countries as they have in developed countries.

10.1. Introductory Statements

Due to the continuous network and service evolution in wireless communications, future wireless ecosystem calls-for re-designing backhaul solutions to provide efficient and ubiquitous broadband wireless access to current and future Internet-based applications and to evolve seamlessly into the future "pure" packet network architecture. Data consumption has risen dramatically across the globe following the widespread availability of machine-to-machine communications, Wireless Sensor and Actuator Networks (WSAN), 3G and 4G-LTE which are being deployed worldwide. Focusing towards the emerging markets such as the BRICS (Brazil, Russia, India, China, South Africa) economies and the Sub-Saharan African countries, in the light of the various challenges for the Mobile Network Operators (MNOs), traffic growth and the pressure to continuously deploy new services due to the gradual migration from 2G to 3G and further to 4G, raise one of the greatest challenges to support the backhaul capacity requirement. Furthermore, unlike in developed economies, there is generally no fixed line infrastructure to support this ever-rising traffic increase which creates a problem for backhauling.

Within this challenging context of addressing the problem of increased backhaul capacity, in a very competitive market in emerging economies, we propose in this chapter a new architecture based on Substitution Networks (SNs). In simple words, a SN could be defined as any form of temporary wireless network that has rapid deployment capability to back-up a base network [152], [153]. SN is a new research area that is motivated by significant challenges among various disciplines such as wireless mesh networks, wireless sensor networks etc. However, its application towards fully demonstrating its behavior to practical technical systems such as the wireless mobile backhaul is very limited until today. Nevertheless, SN is foreseen to play a major role in future communication systems due to its simple but efficient design objective. While SNs are envisioned are to be highly autonomous, encompassing self-configuration, self-optimization and self-healing in a massively distributed environment, we claim that the non-centralized nature of SNs makes them sensitive to guarantee the required quality of service (QoS) to a wide variety of users, since in such networks, issues such as bandwidth management are expected to be transparent to the end-users. In addition, the requirement for bringing-in variety of vendor switches renders the networks increasingly complex, and therefore, more difficult to monitor, control, configure and manage.

Hence, this led to the necessity for a solution to deploy SNs through a centralized scheme, which is incidentally made possible by SDN, whose applicability and performance we study in this chapter. That said, with this in mind, here in this article, we propose a new network design through which we appropriately suggest adopting SDN technology to SN. We incorporate SDN to tackle the problem of a centralized control of multiple diverse vendor equipments and thus we

adopt OpenFlow to demonstrate the feasibility of our proposed network design. Moreover, through this solution, we demonstrate the possibility to adjust the bandwidth on a set of links and switches dynamically according to the traffic needs of individual end-users, which guarantees the required QoS. We believe that our proposal to incorporate SDN into SN will appeal to Internet Service Providers as well as the MNOs to solve the problem of network overload produced by varying user traffic demand at different periods of time.

10.2. Problem Characterization: Background and Existing Solutions

Problem 1: Network Overload. Network overload is a situation that generates an unexpected amount of traffic which exceeds the regular network capacity. This can be caused by a variety of factors, from too much traffic at one point in time to excessive traffic generated (i) under emergency situations like flood, earthquake, national emergency or other "chaotic" situations (ii) and in case of any other public social events. Thousands of cell sites installed throughout the country may determine the reach of the MNO, but it can not accommodate for the capacity increase in the backhaul to guarantee the required QoS to end-users. In order to prevent overload and the resulting network congestion, network traffic must be managed through a variety of methods. Bandwidth management [154], [155] and traffic shaping [156], [157] help stabilize network usage.

Problem 2: Cost of Resilience. Besides these technological advancements, setting up back-up paths is considered as another solution [158], [159] as shown in figure 53. Back-up paths are usually set up permanently across the locations where MNOs had predicted from previous statistical analysis that there could be network congestion or traffic spike under certain period of time. This typically involves over provisioning the core network and when the network gets overloaded, the exceeding traffic is re-routed through the back up networks; thereby avoiding congestion. Back-up paths are generally fixed paths and are not capable of being moved to another location whenever required. While setting up the back-up paths seem to be a feasible solution in developed countries, it may not have the same impact with regard to emerging countries due to the extremely high operational expenditures (OPEX) and capital expenditure (CAPEX).

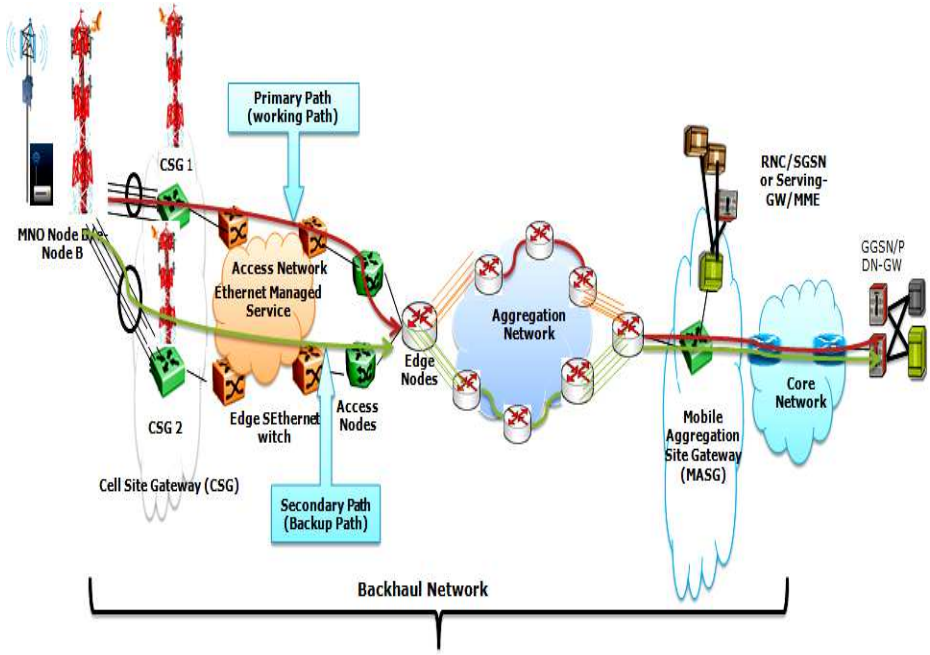


Figure 53: Figure illustrating backup path protection in wireless microwave backhaul in 3G/4G.

Problem 3: Reach of Service over Speed. Among others, one of the major focuses of the Telecom regulators all over the world is a system that enables people to get what they want and pay accordingly, i.e. the delivery of "unprecedented" broadband speeds should not be the guiding principle; rather what is important is to make sure that there is robust Internet connectivity in every nook-and-corner that gives atleast the minimum broadband coverage with minimum QoS as-and-when new Internet applications widely penetrate the related markets. This, in the first place, includes taking broadband coverage to rural and remote locations to prevent the tangible risk that some people and businesses may be left behind because of the inadequate access to the internet and all its benefits. Due to the cost involved in cell-site acquisition, Operation and Maintenance (O&M) etc. MNOs are reluctant to extend their broadband coverage to such rural and remote customers, unhesitatingly.

Problem 4: Heterogeneity. Today's communication network consists of heterogeneous networking vendor equipments and device models such as Cisco, Juniper, Ericsson, Nokia Siemens Networks, Alcatel Lucent etc. and hundreds of in-house developed applications not only based on different operating systems but also different versions of the same management protocol itself. These are deployed globally in hundreds of sites along the end-to-end wireless architecture (access/backhaul/core). They support tens of thousands of users, using a variety of network topologies and access mechanisms to provide connectivity. To complicate matters, with the proliferation of new technologies such as from 2G to 3G and now to 4G, networks are becoming more and more complex with different generations of technologies coexisting within the same network. This intensifies maintenance and network management, driving up OPEX.

10.3. Approaching the Problem through Substitution Networks (SNs)

Under these circumstances, solutions based on adaptive networks and low cost infrastructures are of major interest due to limited budget in emerging economies (also in developed economies for cost-sparring reasons), so that the services could be provisioned dynamically according to variable conditions. Therefore, the aforementioned factors lead to the consideration of an alternative approach called Substitution Networks.

10.3.1. Inspirations for Substitution Networks (SNs)

Our work here derives from a long line of related research [160]-[162] that inspired us towards the concept of SN to specify high-level policies at a logically centralized controller, which are then enforced across the network without the tedious concern of manually crafting switch-by-switch configurations. Distributed wireless sensor and actuator networks (WSANs) [163] that perform distributed sensing and acting tasks with the help of a controller that is responsible for monitoring and managing the overall network through communications with sensors and actuators is seen as another potential motivation towards our concept. There are three essential components in WSANs: sensors, actuators and a controller. Sensors observe information about the physical world, while actuators make decisions and perform appropriate actions upon the environments. The controller is responsible for monitoring and managing the overall network through communications with sensors and actuators. After sensors in the sensor/actuator field detect a phenomenon, they transmit their readings in one of the two following forms. They either transmit their readings to the resource-rich actuator nodes which can process all incoming data and initiate appropriate actions, or sensors route data hop by hop upto the sink which issues action commands to actuators. The former case is termed as Automated Architecture due to the nonexistence of central controller (human interaction) while the latter one is termed as Semi-Automated Architecture since the sink (central controller) collects data and coordinates the acting process.

The choice of centralized versus distributed approaches for WSANs has been in discussion [164], [165] and on a conclusive basis, we can infer that the pros of the semi-automated (centralized) architecture is to have a single view for taking the right decision versus the distributed architecture that takes decisions on partial knowledge and that may suffer from instability (in case of contradictory decisions taken by adjacent actuators). This may lead to an inefficient multi-actor global behavior. The cons are that centralized approach does not scale. Congestion is a consequence of scalability. Nevertheless, the problems of delay and potential congestion issues can be significantly mitigated, since the links close to the sink are those which are likely to

exhibit the best quality (since they are close to the core network) with low latency and congestion, as opposed to those close to the actuators (since they will be close to the last mile in our target scenarios). Though it seems that the use of a centralized approach necessitates more hops, the extra hops alleviate the significant source of congestion and delay. With this motivation, we go forward to visualize our concept.

10.3.2. Substitution Networks (SNs) in Wireless Backhaul Networks

Within our context of wireless backhaul networks, a Substitution Network (SN) refers to network elements (NEs) (which could refer to elements of the access network, namely Node B or e-Node B or microwave backhaul equipped in a vehicle such as truck or car like Cell-on-Wheels (CoW)/Cell-on-Light Truck (CoLT) [166] as in figure 55) that are used for emergency services or temporary events) that can move or can be moved, and can be dynamically integrated into the base network. Accordingly, we propose SNs for different scenarios of network operation, e.g. during initial roll-out to carry-out radio planning or during early phases of operation where planned shutdown for maintenance is foreseen, or operation of a mature network with high load. In general, SN relies on Self Organizing Networks (SON) use cases which are related to self-configuration and coverage. These properties are the most important in the earlier phases, whereas quality and capacity-based use cases will be in the focus later. Hence, SNs do not apply only for overload traffic conditions but also to situations when a network is anticipated to be shutdown for maintenance reasons.

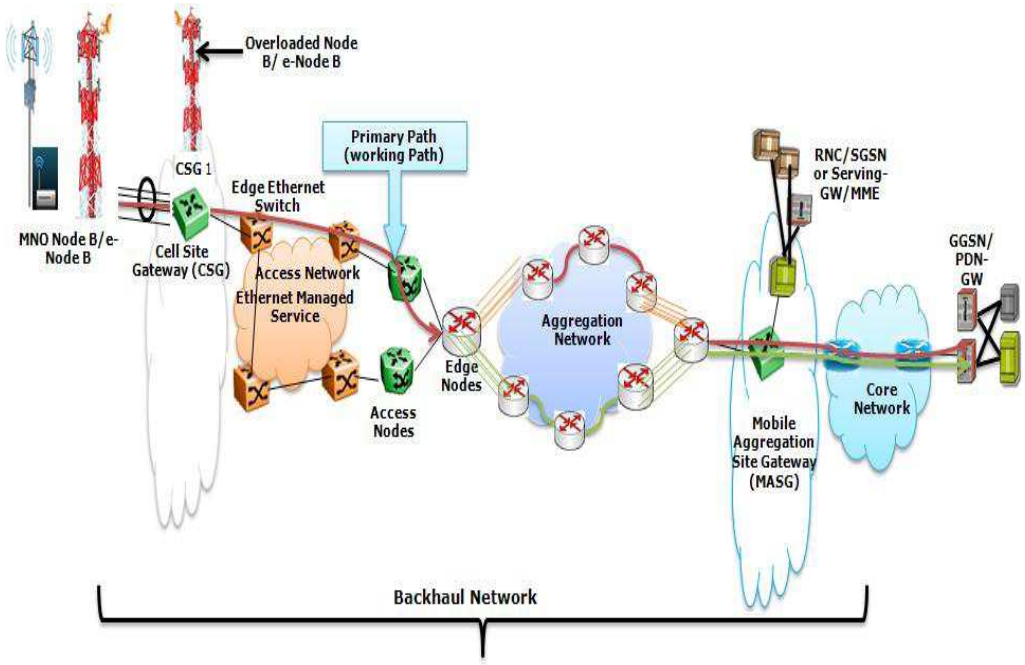


Figure 54: Architectural design illustrating the elimination of back-up path.

Now focusing towards emerging countries, the major concern is that the Mean-Time-To-Repair (MTTR) values are usually too high (in terms of days, sometimes weeks [167]) due to inadequate logistics facilities. With a rapid SN in-place, this could be considerably reduced to few hours. Adding to this, SN also allows reducing OPEX by optimized use of the existing NEs and physical resources, and prolonging equipment lifetime. Therefore the same coverage, capacity, and quality can be obtained with less investment in NEs, or those performance measures can be improved, thus allowing increased capacity, higher subscriber loyalty, and reduced failure events. This, therefore, can be of great interest for emerging countries where the cost of setting up a back-up network, only to handle additional traffic at peak hours or protect the last-mile link (which do not have double backup protection at all) is a real issue in terms of cost and technical complexity involved.

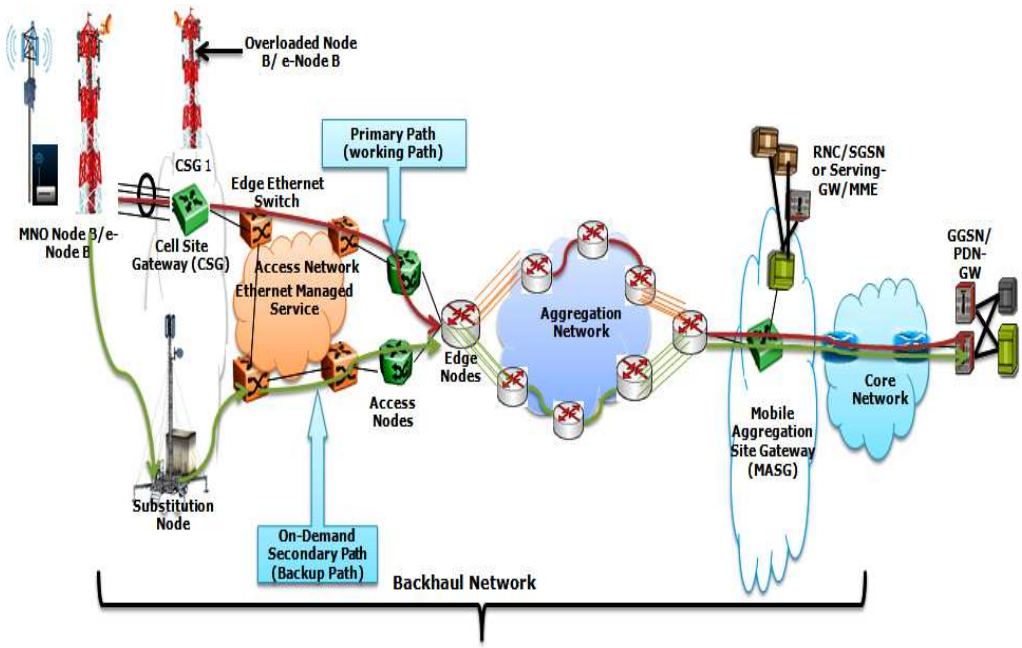


Figure 55: Architectural design illustrating the integration of Substitution Node.

10.3.3. Shortcomings of Substitution Networks (SNs) that Hinder a Wide Adoption into Wireless Backhaul Networks

Now, the question that arises is whether SNs can be generally exploited to a larger scale for solving some of the aforementioned pending problems for future networks. This question leads to a variety of open research challenges. Solutions to these challenges are pivotal in either leveraging the possible advantages of SNs, but could also turn out to be a heavy burden for both MNOs and end-users. The goal is clearly set: after purposefully introducing the SN either automatically or semi-automatically, the beneficial features often identified as the so-called self-properties should clearly out-weight the detrimental aspects, such as un-controllability,

undesired instability or unpredictability. In this context, we do not consider mobility of the SN as a constraint; rather, we claim that the concept of controlled mobility may be based on operation research mechanisms that use empirical network monitoring statistics from the past for determining/predicting traffic load at a given period of time (e.g., every evening) and a given appropriate location. In any cases, this is the network traffic monitoring unit that accordingly decides the location of the SNs as well as the amount of time that the SN has to be present. Even if they are less reactive than traditional resilience mechanisms in case of unpredictable failures, they provide the same level of quality for scheduled management operations that take place largely more often than failures.

As previously mentioned, a SN is a spontaneous system made up of independent interacting entities often acting on simple rules. By independent, we imply that these systems do not necessarily have to comply with any standardized protocols and or any standardized vendor equipments. That does not make it easier to define the rules (protocols/algorithm) of the entities that are in-place in order to achieve a desired (emergent) behavior to back-up an existing network, so that a highly fault-tolerant and efficient network emerges with respect to pre-defined performance metrics. On the other hand, within the scope of microwave backhaul networks of MNOs, as mobile telecom market becomes more competitive, MNOs are increasingly at odds about the balance between choosing the NEs from "one" unique vendor alone and the cost associated with the equipment of that vendor. Adding to this, NE vendors, on the other hand, want to deliver standardized functionalities which are implemented in proprietary algorithms. This creates a dead-end to integrate SNs, specifically to mobile backhaul. In addition, but specific to SNs, if we want to integrate a SN into different networks at different periods of time, we need uniformity in management, or the SN has to evolve in order to produce the desired effect within the integrated network. Using open standards enables a variety of independent third-party tools to be applied to configuration, testing and troubleshooting. However, each NE has a limited amount of processing capacity and memory for storing and retrieving the data that travels over the network. When the amount of data on the network is excessive, the extra data can not be processed and has to be re-sent or dropped. This should be possible for the MNO, not as a burden of manual human intervention, but should be carried out autonomously. Thus, it is essential to design, optimize, and control complex backhaul architecture in a structured and centralized way together with the integration of an external node, i.e. the SN.

10.3.4. Towards a Centralized Approach for Substitution Networks (SNs)

This necessitates for an approach which is not inherently centralized to handle the additional

burden of carrying out the data processing but also to co-operate with other NEs, since NEs are not necessarily based on a standardized implementation. A first critical issue is about integrating the SN into a base network automatically once it reaches the "spot". To do this, the SN has to discover the existing topology, configure resources, and integrate new resources at data, control and management levels, and release resources where they are not utilized anymore. There is no debate this can be best implemented in a distributed way within the SN and the base network. However, considering an environment such as the wireless mobile backhaul network, several independent SON functionalities coexist in the network and act on different algorithms. This may be conflicting sometimes. Indeed, these autonomic functionalities should ideally act in a coordinated manner to fulfill a common objective defined by the operator policy. Besides, in a distributed environment, the upper bound for communicating between any two nodes scales linearly with the longest loop free path. This could be sometimes higher than the time taken by a NE to reach a centralized controller. Furthermore, the fact that a real system might have only partial or error-prone knowledge of the existing neighbors and might not be able to detect all existing collisions adds whole new aspects to the problem. A specific centralized solution can locate a specific SON functionality in the NEs and can be further differentiated into the distributed case, where the SON functionality of multiple NEs need to collaborate and into the localized case, where the problem can be solved by a single NE without the need to communicate or coordinate. A centralized solution could address these needs by enabling a tight integration between an MNO's planning systems while maintaining the flexibility for MNO to adapt planning and visualizing diagnostics in a heterogeneous, multi-provider and multi-technology environment. This simplifies support of multi-vendor SON in a single geographic area. Since SNs within the scope of microwave backhaul are highly difficult to manage due to heterogeneity of networks, spontaneous set-up and negotiate the required QoS among the interconnected devices, we envision the centralized-based solution is cost-effective, suitable for different application scenarios, and simplifies O&M relatively.

10.4. Concept Visualization

10.4.1. The Application of the Approach to the Problem: OpenFlow

OpenFlow is a framework that is an implementation of SDN technology where policies are imposed by logically-centralized software, rather than by switch hardware or firmware. Thus, the OpenFlow protocol allows different vendor switches to be programmed without exposing the internal functionalities of the switches. A very brief description of the OpenFlow network functioning is elaborated below, within the context of this chapter, for the ease of understanding of our proposed solution.

Understanding Flow Table: Since the control plane and the data plane are separated, the data path of an OpenFlow switch presents a clean flow table. Each flow table entry contains a set of packet fields to match (Figure 56), and an action (such as send-out-port, modify-field, encapsulate and forward to the controller or drop). These actions associated with each flow table entry tell the OpenFlow switch how to process the flow. Ingress flows installed in an OpenFlow switch are stored in flow tables.

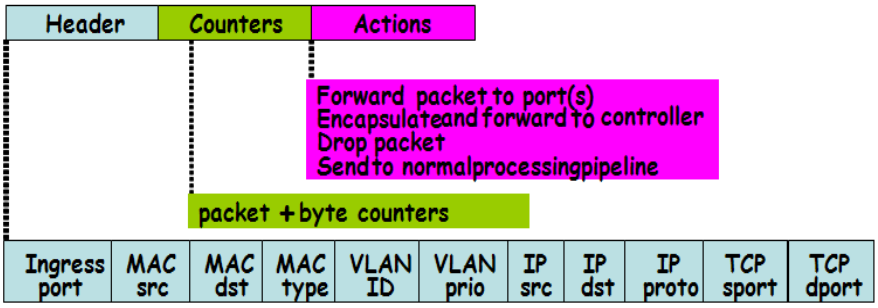


Figure 56: Figure illustrating OpenFlow Fields that are used to match against flow table entries to match different actions to be performed by the switch upon receiving a packet. This header represents OpenFlow version 1.0.0.

Matching Flow Entries: When an OpenFlow switch receives a packet for the first time, for which it has no matching flow entries, it sends this packet to the controller. The controller then makes a decision on how to handle this packet. It can drop the packet, or it can add a flow entry directing the switch on how to forward similar packets in the future. OpenFlow switches use these flow entries that they have received from their controller to make forwarding decisions. In total the OpenFlow 1.0.0 specification includes 12 fields that can be matched upon as in the Fig. 4. A "microflow" rule (a microflow is equivalent to a specific end-to-end connection) matches on all fields of an incoming packet, whereas a "wildcard" rule can have "don't care" bits in some fields, meaning that a packet need not necessarily have to match all of the 12 fields in the OpenFlow table entry. Rules can be installed with a timeout that triggers the switch to delete the rule after a fixed time interval (a hard timeout) or a specified period of inactivity (a soft timeout). In addition, the switch counts the number of bytes and packets matching each rule, and the controller can poll these counter values.

Specifying Flows: A flow can be created for a specific stream of traffic by matching the fields in the flow table entry to that ingress flow. This means that the input port, source and destination MAC address, IP address, TCP/UDP port, etc. must all match with that flow. These flows are stored in a 'hash' table because the 12-tuple is hashed and then stored as an index in a table for fast lookups. If one or more of the fields are wild-carded, i.e. can match with any value, the flow is usually stored in a 'linear' table, to be looked at after the 'hash' table in a linear fashion. The hashes of the exact flows are typically stored in Static RAM (S RAM) on the switch. This memory allows for an indexed table of the hashes and a fast lookup procedure by the switch.

This is done by matching against certain header fields while wildcarding others. Flows that do not match one of these "flow spec" categories are treated as best-effort.

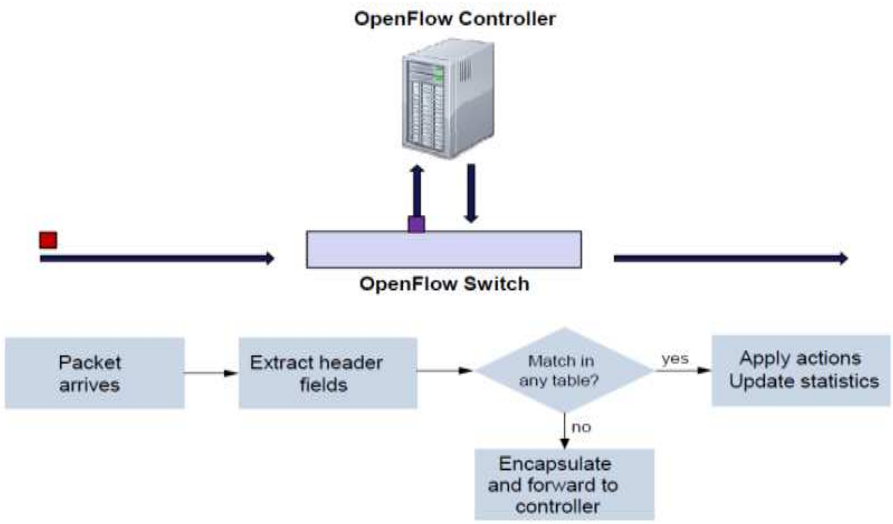


Figure 57: Flow diagram of Open Flow packets.

Thus, by specifying a standard interface (the OpenFlow Protocol) through which entries in the flow table can be defined externally, the OpenFlow Switch avoids the need to program the switch. While each vendor's flow-table is different, it will be interesting to identify a common set of functions that run in multiple switches and routers. OpenFlow exploits this common set of functions and thus provides an open protocol to program the flow table in different switches and routers. For high-performance and low-cost, the data-path must have a carefully prescribed degree of flexibility. This means forgoing the ability to specify arbitrary handling of each packet and seeking a more limited, but still useful, range of actions. Because OpenFlow connections are explicit, Network-as-a-Service is more secure and potentially provide improved QoS. This is because policies that set routes for packets can use application and even user priority to determine how traffic is allocated to resources, thus setting performance levels. Clearly, this property supports our approach.

10.4.2. Substitution Networks (SNs) based on Software Defined Networking (SDN)

Taking Control of the Control-plane Traffic: As detailed previously, the split architecture in SDN technology assumes a logically centralized controller, which is physically separated from data plane forwarding switches. Thus, when the control plane is decoupled from the data plane, the traditional mechanisms that were commonly adopted to integrate a new node into an exiting network topology also changes. This means, since the control plane and the data plane of the OpenFlow are logically separated, any disruption in the control plane that incurs due to

deployment of a temporary SN should not necessarily affect the existing communication sessions in the data plane. This is predominantly the desired effect when we introduce SN into a base network at times of network overload. With this we propose a solution based on the centralized SDN approach. Without emphasizing a separate centralized controller to integrate SON functionalities only for the SNs ignoring the base-network, our proposal include controlling the base network together with the SN in a joint fashion. This is done judiciously by incorporating OpenFlow protocol within the backhaul of the wireless networks. Figure 55 and 58 illustrates the proposed network design.

Support for Flow-level Management for Backhaul Bandwidth: Flow-based switches, such as those enabled by the Open-Flow protocol, support fine-grained, flow-level control of Ethernet switching. Such control is desirable because it enables (1) correct enforcement of flexible policies without having the need to craft switch-by-switch configurations, (2) visibility over all flows, allowing for near optimal management of network traffic, and (3) simple and future-proof switch design. This facilitates the deployment and the re-deployment of SNs, which is a critical part of the adaptation of the SNs to wireless mobile backhaul networks, because the protocols employed depend on the traffic patterns in the networks. A problem to tackle here is to provide an updated view of the traffic inside both the base and the substitution networks and to deliver this information to each NE (base or SN). OpenFlow will work best where traffic is made up of a modest number of predictable flows. That way, once the switches/routers learn the traffic rules from the controller, little additional interaction with the controller is needed. In the context of the control of base-to-substitution or substitution-to-base traffic within a wireless mobile backhaul, OpenFlow is particularly adapted to tackle this situation. This would apply to SN resources that would become under the control of the base network controller. With this approach the MNO does not need to have any prior reservation of network resources of the base network at any point in time and the integration of SN resources takes place dynamically. Our architecture does not include the flow concept inside the SN. In our architecture, the flow concept ends at the Bridge Router level, before entering into the SN. This is due to the computation time and memory constraints of the SN. Furthermore, even within SNs in a distributed case, OpenFlow could be expected to manage traffic within each distributed NE. In addition, OpenFlow can provide optimal admission control and flow-routing in support of QoS policies globally, in cases where a hop-by-hop QoS mechanism cannot always provide global optimality. However, this does not mean that all flow setups should be mediated by a central controller. For instance, the controller can define flow categories that demand per-flow vetting which are required to guarantee particular QoS levels (e.g., "all flows to or from the specific e-Node B MAC or IP address"). Thus, only the flows that require guarantees actually need to be approved individually at setup time. Other flows can be categorically treated as best-effort traffic.

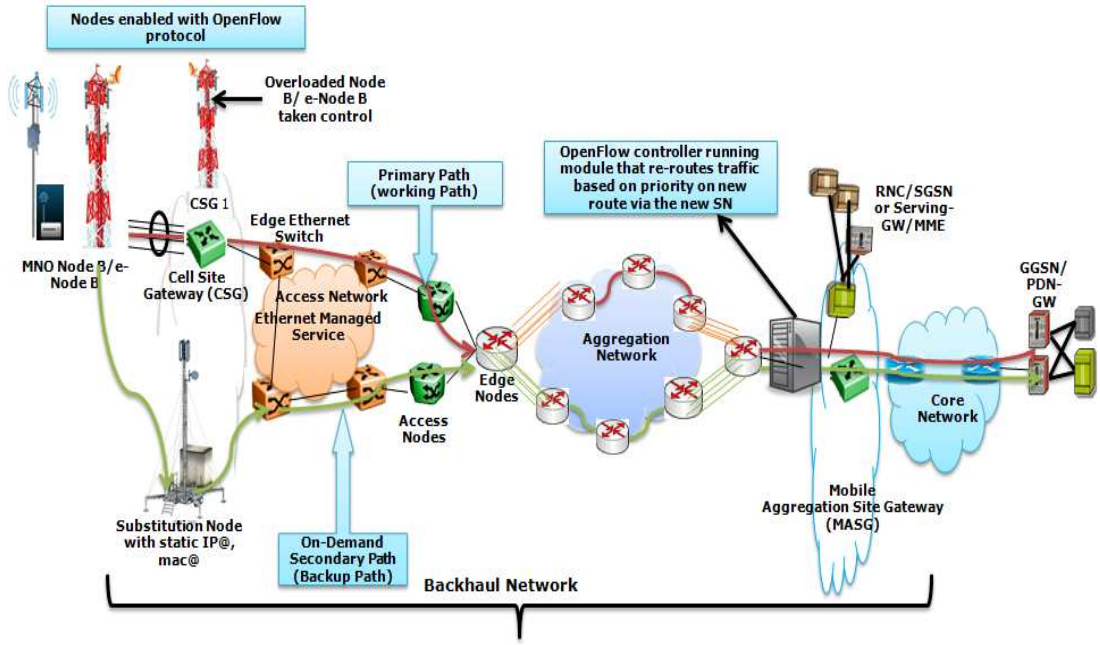


Figure 58: Architectural design illustrating Substitution Networks based on SDN.

In summary, we believe that the benefits of the centralized control in OpenFlow can be maintained by individually approving some flows, but categorically approving others. We conclude that some use of a centralized controller is necessary to build a power-proportional, energy and memory efficient, high-performance SNs.

10.5. Experimental Evaluations

In this section, we put forward our experimental results that were carried out on OpenFlow software-based implementation. Here, we have evaluated our approach that guarantees the required performance in terms of bandwidth management to satisfy QoS to every user within a network, irrespective of the "chaotic" situation, typically an overloaded network situation.

10.5.1. Design and Implementation

Our method outlines a bandwidth management framework based on OpenFlow. Briefly, when the centralized controller detects the OpenFlow enabled SN, it creates a new path via the SN and re-routes the traffic, thus guaranteeing the QoS to end-users. Thus, OpenFlow enabled SN uses the flow entries they have received from the controller to make forwarding decisions.

Topology Discovery and Traffic Re-route: For a SN to be integrated into an overloaded base network, the SN should be first detected by the controller. According to OpenFlow specification v1.0.0, an OpenFlow switch must be able to establish the communication at a user-configurable (but otherwise fixed) IP address, using a user-specified port with a controller. Henceforth, we set

the controller's IP address and port when starting the OpenFlow enabled SN. Then the controller and the SN will establish a TCP or TLS connection and *OFPT_HELLO* messages will be sent to each side of the connection. Now the controller knows that there is a new OpenFlow enabled node (SN) integrated into the network. Then the controller will let the SN itself to send out LLDP packets at a regular intervals to the controller, with each LLDP stamped with the sender's (here SN) datapath ID and outgoing port. If one outgoing port is linked to another switch, the LLDP packet will be sent to the controller by that switch and controller now knows the topology. The advantage of this sort of topology discovery scheme is that discovery packets sent by the SN can be appropriately prioritized so they get-through even on heavily loaded links.

Learning Switch: In order to setup paths, we use a simple learning switch application. This application associates MAC addresses to ports and installs respective flow entries on all OpenFlow-enabled nodes. The OpenFlow-enabled nodes will examine each packet and learn the source-port mapping. Thereafter, the source, i.e., MAC address, will be associated with the port. If the destination of the packet is already associated with some port, the packet will be sent to the given port, else it will be flooded on all ports of the switch. That is, once the SN is detected by controller, it results in the following:

a) The controller flushes all the exiting flow entries in all OpenFlow switches and now wildcards each flow entry based on source IP address and Ethernet address.

b) Accordingly, certain flows (based on source IP/MAC address) are now forwarded to the SN.

c) From this point, all of the data traffic from the base network starts to flow through the SN reducing the traffic load. However, at this point in time, the OpenFlow enabled SN is not aware of what to do with this first stream of packets that has just arrived from the base network. Hence it encapsulates and forwards the packet to the controller through a *packet_in* message (The message that a switch sends to the controller to inform it about an unknown flow is called a *packet_in* event message).

d) The controller now makes a decision on how to handle this traffic stream and forwards it to the SN by the *packet_out* message.

e) Accordingly, in this case specific to our situation, we choose to re-route the low-priority traffic through SN that can tolerate delay, while allowing the high priority traffic to continue to flow through the base network without any disruption. This is done by wildcarding the source IP address field of each low-priority user group traffic flow to be forwarded to the SN.

f) From then onwards, all the high priority traffic (delay-sensitive traffic, real-time traffic, premium customers, corporate customers) continues to flow through the base network, taking maximum advantage of the "now" available bandwidth and the low priority traffic (best effort traffic) is re-routed through the SN.

It is worth mentioning that that the bandwidth consumed for path setup is negligible. Thus, our evaluation results would still apply, even if we install all paths proactively. As mentioned earlier, in our approach mobility is not taken as a constraint, rather, it is assumed that the SN is brought in-place/ retained very close to the spots where there is usually traffic spikes (based on previous statistics). What we accomplish here distinctly due to the adaptation of OpenFlow is that, in general scenario, it is the network administrators who manually configure the SN when it is brought in-place as well as the traffic of the base network that has to re-routed every time when the SN integrated. But, with OpenFlow, the controller automatically takes care of re-routing the specific traffic flows by matching the fields of that flows, thereby retaining the required performance of the whole network. To maximize flexibility, the slice specifications can be applied to individual flows, aggregate traffic of certain flows, or even combination of them based on customer's requirements. The re-routing algorithm, implemented in the controller is the most important mechanism when considering the congestion control issue within our scenario. It decides (by prior configurations) which flows may be served through the base network and which should be re-routed through the SN. The pseudo-code below describes the view of the network resources from a base node perspective after a SN is integrated.

ALGORITHM 1 ALGORITHM TO GUARANTEE BANDWIDTH MANAGEMENT FROM AN OPENFLOW ENABLED BASE NODE PERSPECTIVE

```
1  : for each flow entry ∉ Flow Table do
2  : Send packet_out openflow message
3  :  If  packet_out message then
4  :          //no Optimization needed
5  :          Start Time Out to Increase
6  :     else if  Reject  then
7  :        if  maximum available bandwidth not reached then
8  :              Change Bandwidth  parameters
                        (increase data rate)
9  :              go to 1:
10 :        end if
11 :     end if
13 : if  Time Out to Increase  then
14 :     if  maximum available  Bandwidth reached  then
15 :        Change Bandwidth parameters
                  (deccrease data rate)
16 :        go to 1:
17 :     end if
18 :  end if
```

Most previous research works propose numerous queuing algorithms to guarantee QoS [168]-[170] by retaining certain flows and dropping the rest. These algorithms engage differently; however, the outcome of their functioning is almost identical. These algorithms implicitly give priority to the packets of flows whose peak rate is less than the current fair rate. The flows with rates less than the current fair rate are assigned high priority. This way, streaming flows with peak rates less than the current fair rate are subjects to the buffer-less multiplexing and, therefore, perceive low delays and losses [170]. However, our solution takes into account to route every flow within the network. Thus, it allows for fair access to the resources without any intervention form the user or the network administrator. To effectively manage the performance of a network, the controller needs to know about the current loads on most network elements. Maximizing some performance objectives may also require timely statistics on some flows in the network. (This assumes that we want to exploit statistical multiplexing gain, rather than strictly

controlling flow admission to prevent oversubscription.) However, load-balancing does not require the controller to be aware of the initial setup of every flow.

10.5.2. Evaluation and Results

Setup: In our experiments, we emulated an OpenFlow network using Mininet hosted on a physical machine to generate the network topology, just as in figure 58. The controller that we utilized for our experiments is the standard NOX controller (destiny branch).

Results: As a first step, we measure the latency by the controller to add a new flow entry directing the SN on how to forward the ingress flows. That is, when the SN establishes a connection with a controller, it sends to the controller, the first stream of packets which is receives and then the controller sends our *packet_out* messages. We measure this time to see how long it takes for the flows to be installed so that there is eventual forwarding without any disruption. To do so, we utilized a host machine with two Ethernet interfaces running OpenFlow v1.0.0, one connected to a switch port and one to the management port. The interface connected to the switch port starts to send unknown flows and listens on the control channel port for incoming packet_in messages. Based on the RFC2544, experiments with different frame sizes were conducted on latency test. The experiments were carried out five times for each packet size ranging from 60 bytes to 1024 bytes. The values are indicated in Table IX and the variance of the latency is depicted in figure 59.

TABLE IX. AVERAGE LATENCY VALUES FOR 5 TRAILS FOR MEASURING THE TIME TAKEN TO INSTALL FLOW ENTRIES

Time (seconds)	**15**	**30**	**45**	**60**	**75**
Packet size (bytes)	**64**	**128**	**256**	**512**	**1024**
Latency (µs) Trail 1	4	6	8	8	15
Latency (µs) Trail 2	3	7	9	8	14
Latency (µs) Trail 3	4	5	8	11	13
Latency (µs) Trail 4	5	5	8	10	15
Latency (µs) Trail 5	4	7	10	9	13

From figure 59, it is very convincing to observe that latency time that is taken by an OpenFlow controller to install the first flow entries. As we described before, once the first flow entries are in-place in the flow table of an OpenFlow-enabled node, the node can forward similar packets in the future. Ignoring the time that is taken to move the SN to the spot (or if the SN has been already placed close to the spot because of the previous statistics), the time that is taken to configure flow entries in the flow table is totally negligible, which is only of the order of few microseconds. However, here we like to remark that the placement (location) of the controller has some significant role to play with this latency time that is measured. In [103], authors have

measured the reaction-time requirements for the controller placement problem, by placing the controller in different locations in the country and presented the time to reach a controller.

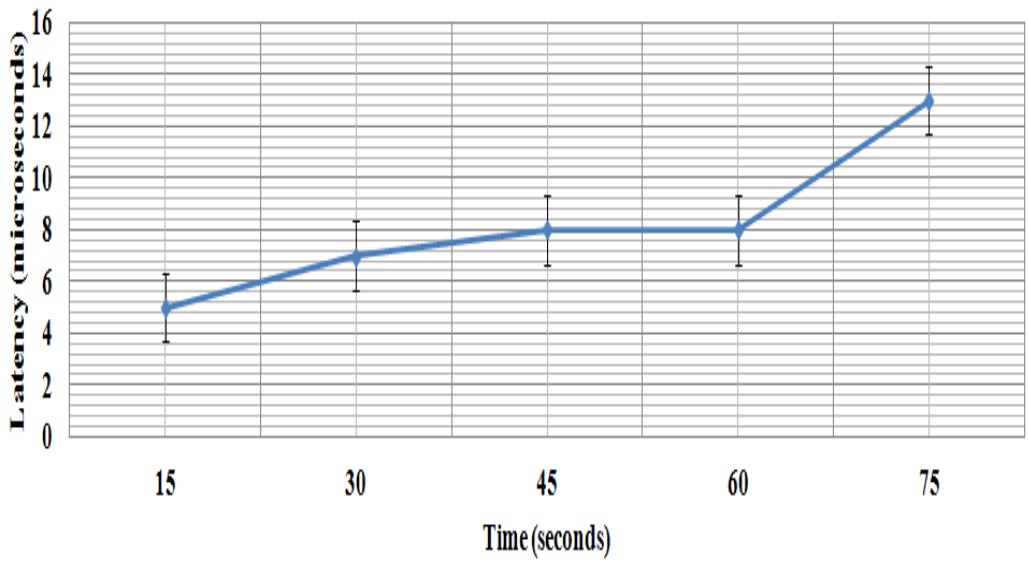


Figure 59: Average latency to install flows on an OpenFlow switch.

Next, through our experiments we aim to study average packet loss though a link, with and without the SN. That is, our aim is to observe through our experiments the decrease in the load on a node, say X, due to the integration of a new node, say Y, which is the SN. We classified two different sets of traffic based on IP source address. That means, any flow with a certain source IP address, when it matches the "IP src" field of the node X continues to flow through it and the rest is re-routed through node Y. Each connected end-hosts runs UDP traffic. Our experiments were carried out as described in section 10.1. Figure 60 shows the bandwidth consumption of the node X, before and after node Y in introduced. It is interesting to see the influence of the new node Y on the bandwidth of the node X. To do this, we carried out experiments based on the steps described in section 5.1. Following this, we specified link bandwidth capacity on each link between the nodes that was created using the Mininet emulator. Each connected end-hosts runs UDP traffic. We overloaded the link more than our specified link capacity with and without the SN. Figure 60 shows the packet loss on the link before and after the SN was introduced. It is interesting to see the influence of the new node on the packet loss parameter values. As expected, there is significant packet loss without the SN, which is avoided when the SN is introduced.

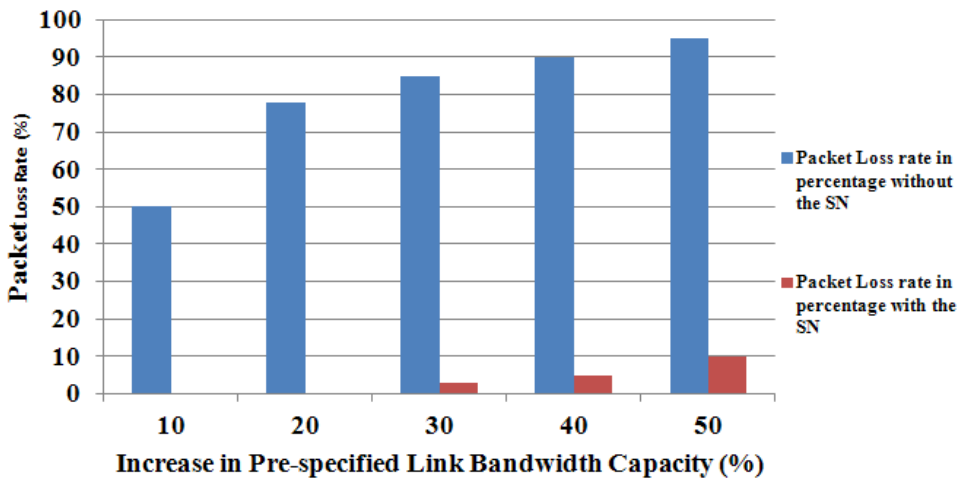


Figure 60: Packet Loss Rate on a link before and after introducing SN.

10.6. Discussions and Conclusions

Our approach here that embraces SDN and SN is completely a very new area of research. Instead of utilizing SNs that were classically considered to recover from failure, we propose to use them to increase efficiency with respect to desired performance metrics. This enables networks to evolve, e.g. to improve over time and to converge to a stable state that can be respected as a (local) optimum of the performance objective(s). It is unrealistic to simply reuse the homogeneous performance-related system design evaluation assumptions to illustrate a comparative evaluation or a quantification of the savings in terms of resource utilization or energy efficiency with any existing approach.

Nevertheless, our past experience with OpenFlow [29] gives a good hold on this technology, atleast to some extent. Apart from the technical performance improvement, our approach depends very much on the economics, and cost models. Obviously it is hard to derive a final quantitative metric to capture all these aspects, in particular as the costs are confidential and highly dependent on the deployment scenario, region, strategy and work flows. Nevertheless some factors impacting the benefits can be quantified better, in particular the performance improvement (with respect to availability and Mean Time Between Failures (MTBF) and Mean Time To Repair) for a large base of end-users. We have discussed the performances as approximations to the real performance functions due to the fact that not all functions in a centralized scenario with possibly acting nodes can be optimized. We demonstrated the feasibility of the approach for wireless backhaul networks, where a topology is desired in which communication/routing cost is minimal.

*"I think and think for months and years. Ninety-nine times, the conclusion is false. The hundredth time I am right." – **Albert Einstein, Theoretical Physicist.***

Chapter 11

Concluding Discussions - Recovery without Redundancy is possible!

What happens to end-users when backhaul networks fail (link failures and/or node failures)?

In today's' wireless communication network, microwave radio links are considered as one of the key technologies to build backhaul networks and a preferred choice over leased lines and fiber optics for many reasons especially in Europe and Africa. But, the downside of such backhaul architecture is generally link failures resulting in network traffic congestion. Various techniques have been proposed to protect connections against potential network failures. So, what happens to end-users when backhaul networks fail (link failures and/or node failures)? From the end-user perspective, there are several scenarios:

- In the best one, the network traffic from the end-users are seamlessly re-routed across the backhaul network of other 'functioning' locations, with minimal or no disruption in service. No harm, no foul.

- In other cases, especially when multiple failures occur simultaneously at multiple locations, end-users may experience problems. They may be unable to access the network, their calls may drop or not complete, or they may experience quality problems such as garbled voice quality or reduced Internet data speeds. It's important to note these problems may affect end-users on nearby locations because of the additional unexpected traffic re-route as well as those on the failed locations.

With the world increasingly dependent on mobile communications, any interruption to service inconveniences end-users. But, on the other hand, what is the consequence of backhaul network failures to service providers and network operators? In a dynamic, 'resilient' network where network operators hand off end-users easily to other locations, the answers are not straightforward.

A link/node failure means end-users are having problems at that particular location. This is true whether an outage is due to a single isolated failed tower or due to a cluster of 10, 20, or 30 towers failing simultaneously (multiple towers may fail together if a shared resource, such as a power source or backhaul link goes down or when towers in close proximity are hit by the same local weather event.) Therefore, it goes without saying that it can negatively affect businesses for service providers and network operators. So when network equipments of the backhaul fail, whether it's a single link failing or a cluster of nodes and links failing simultaneously, network operators work tirelessly to quickly restore service to minimize the impact on end-users. While redundancy may insulate customers from the effects of an outage, it is considered as a solution which is cost inefficient, because, we argue that permanently provisioning a secondary backup

path (redundancy) (i) incurs an additional cost investment which is as similar in magnitude as the initial "huge" cost investments that is incurred for setting up the primary path, (ii) even though backup paths may serve as an additional carrier to carry the extra traffic load of the primary working path under link/node failure conditions and/or network overloaded situations, this may not be the most optimal solution, because, in typical real world conditions, the capacity which is allocated for the secondary path is not *always* actively filled-in as much as the capacity allocated for the primary path.

Therefore within this context, focusing towards the backhaul networks of mobile network operators, we summarize the following problems:

Problem 1: How to avoid link failures that are inevitable at the "last-mile" of the backhaul since there is no enough redundancy?

Problem 2: How to improve the availability of backhaul architecture of mobile network operators without redundancy?

Problem 3: How to avoid the backhaul bottleneck in case of link failures?

It was the aim of this dissertation thesis to answer these questions relating to tackling backhaul network failures, without over-provisioning. Thus, in this dissertation thesis, we describe architectures and algorithms that accomplish these goals. As with any scientific work, it has brought up more questions than it has solved, some of which are illustrated in the latter part of this chapter. Before that, however, the contributions of the thesis are glued together to give a better picture of the choice of research conducted.

With this as starting point, in this dissertation thesis, emphasizing on these pitfalls, we necessitated the idea of "re-designing" backup path provisioning scheme, which not only should result in investing less for redundancy but also should satisfy the mere availability requirements for the MNOs. Our arguments lead to a design consideration in which the primary resource (working path) of one MNO could be re-provisioned as the backup resource (backup path) for another MNO - exclusively at times when a link fails, when resource utilization exceeds a threshold and/or when the network state changes to achieve better resource utilization, for any one of the MNOs, by connecting both of the MNOs last mile links. Since the evolved architecture is a ring topology, MNOs who agreed to share and build the backhaul topology together, need not invest for another additional secondary link to include redundancy across their own chain topology. What is described above is pictorially depicted in figure 61.

As depicted in figure 61, there are two operators who share the backhaul links. The one at the top of the figure is the topology of operator A. The one below with circles is the topology of another operator B who agrees to share the backhaul links. When the last miles of two operators are connected by just another additional link, we observe that the ring topology network that originates provides more protection including the last miles compared to a microwave chain topology. It is therefore evident, that our protection scheme will help improve a connection's availability since traffic on the failed primary path (which could be any one of the Operator's backhaul) will be quickly switched to the backup path (which is the backhaul of the sharing operator). Our work is particularly applicable to Tier I, Tier II MNOs, ISPs and large geographically distributed backhaul networks operators, where persistent and scalable network-wide control of a large number of heterogeneous network equipments becomes inevitable.

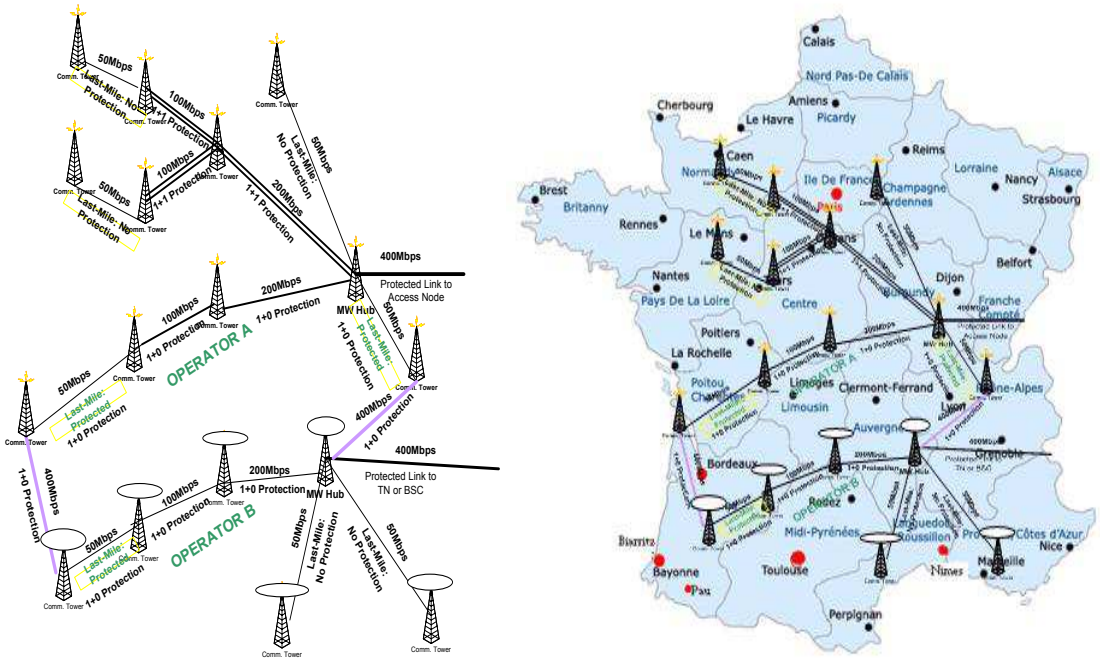


Figure 61: An illustrative example network topology portraying resilience design flow using infrastructure sharing within the country France. Two MNOs: one at the top (north), another in south (with circles) are joined by just another additional link (green colour thick link), making a 'resilient' ring topology.

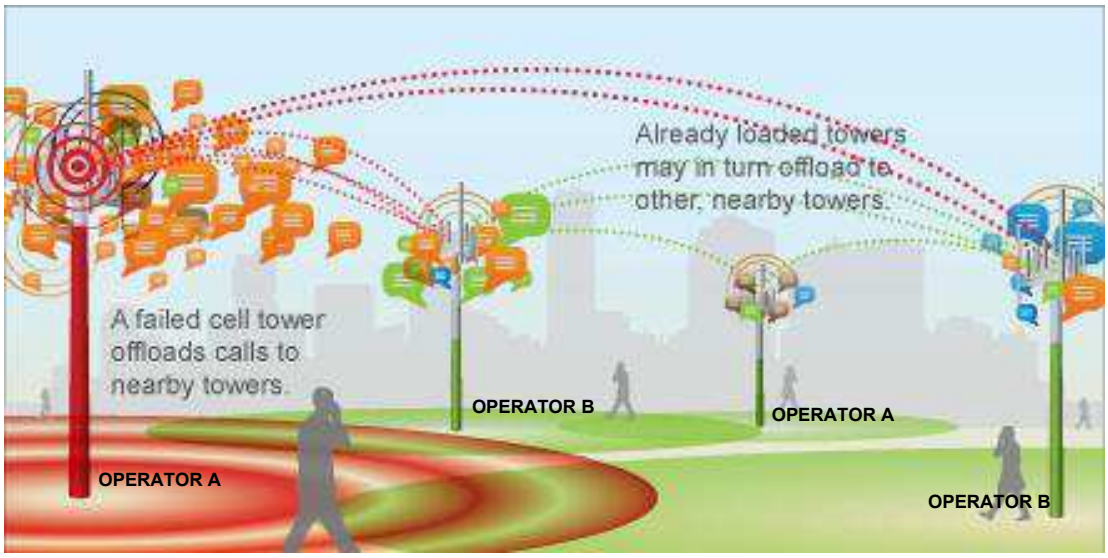


Figure 62: Traffic re-route resulting from backhaul network sharing due to a link/node failure in the backhaul between several mobile network operators.

Within this context, this dissertation thesis has addressed the following:

<u>Part II: Theory and Modeling</u>

- Proposed a novel architectural design for increasing reliability and reducing network costs of building backhaul networks. This new concept that we have termed as Resiliency, Reliability, Redundancy by Infrastructure Sharing (3RIS) provides a solution to improve reliability without additional cost investments, by sharing another operator's microwave backhaul. We evaluated our results by **a simple 2-path parallel system using State Space Markov Chain model**.

- Proposed a 'measurement-driven' approach that adopts the concept **Multi-State System (MSS) approach using Discrete-state Continuous-time Markov chain model**, to ensure robust operation of networked systems under unexpected conditions such as natural/unnatural disasters which has been analytically developed. 'Measurement' in the sense that the values used for the calculation were based on real-world network failure values from a typical Tier-I MNO (who shall remain anonymous for the sake of confidentiality).

- Illustrated a flexible re-routing scheme for this architectural design, where backup capacity can traverse via physically separate routes of another MNOs backhaul. Through this work, we were able to affirm that the problem to interrupt both the primary path and the backup path of different MNOs simultaneously, is therefore not likely at all. Following this, we developed a **path-based proactive analytical model for recovery**

and re-routing based on probability theory that enables to understand how the user traffic is re-routed around a failing network component, when MNOs share their backhaul link-bandwidth together. We call this as ROFL (Restoration of Failures through Link-Bandwidth Sharing).

Part III: Optimization Techniques for Network Survivability

- Consequently, we developed 'OpenRoutes', a simple and systematic model illustration that exemplifies an entirely different **approach to compute alternative disjoint paths with optimal capacity**, in a wireless backhaul network that has emerged out of sharing between different MNOs, without affecting any of the other MNOs' existing traffic flows. The objective of our approach has been formulated using Integer Linear Programming (ILP), based on our model definitions. Since such ILP formulations are very complex to solve for medium/large networks, in what follows then, we appeal for three simple yet efficient heuristic algorithms.

- Followed by this is **to optimize the resources when one MNO decides to share their primary resource with another MNO** which would serve as backup resource, without jeopardizing their own quality-of-service (QoS) requirements, i.e. we developed a systematic optimistic methodology to efficiently define the capacity bounds in its ability to offer a high quality of experience (QoE) for subscribers, i.e. to define the upper and the lower bounds of the traffic through another MNOs' backhaul network for each connection going through a failed link.

- The next step is to **seamlessly adapt our solutions for the Software Defined Networking (SDN) architecture**. Following this, we illustrated a novel 'multi-topology shared' architectural design paradigm of a communication network by adapting the logically centralized approach and very specifically towards a Quasi-Distributed approach. More significantly, our approach exploits the recently emerging SDN/OpenFlow approach [1] on maximizing the network survivability through bilateral cooperation between several MNOs, elaborately described by a real world use case scenario.

- Within this scope, we illustrated a restoration architectural design paradigm of a communication network by adapting the logically centralized approach and more specifically towards a Quasi-Distributed approach. For reasons which are made clear later, we call the resulting scheme as Cross-Control (X-Control).

Part IV: Performance Evaluation of SDN/OpenFlow Architecture

- This part of the dissertation deals with **illustrating the feasibility of mobile backhaul network sharing via an open network approach, based on OpenFlow**. We evaluate the practical feasibility of our proposed architectural designs adapted within the context of Software Defined Networking (SDN)/OpenFlow. By demonstrating the feasibility of adapting the existing OpenFlow mechanism to mobile backhaul network architecture, we seek to define how far it can be gone within the sharing scenarios, where the key lock is to define flexible and extensible policies that can be modified dynamically.

Part V: Substitution Networks- A Radical View

- Within this context, we proposed a solution considering **Substitution Networks (SNs) as a means for provisioning backup path for Mobile Network Operators (MNOs) backhaul** to overcome network overload due to excessive wireless data traffic. Our approach considers Software Defined Networking (SDN) technology due to its flexibility to integrate diverse future generations of switches as well as its centralized approach for decoupling control-plane and data-plane. We demonstrated the possibility to adjust the bandwidth on a set of links and switches dynamically according to the traffic needs of individual end-users, which guarantees the required Quality of Service (QoS).

Research and Deployment Challenges

As detailed in this dissertation thesis, the rollout of low-cost backhaul deployment strategies, especially based on emerging technologies such as the Software Defined Networking (SDN)/OpenFlow, may at first suggest divergent set of requirements that will be difficult to address with a common approach to backhaul transport, especially considering multiple operator environment.

On one hand, backhaul requirements have been consistent between the two evolutions strategies (MPLS-TP and IP/MPLS) described in the initial chapters (Chapter 1). This convergence of requirements is due to the fact that regardless of the starting point, all operators have the same end objective which is a LTE based network for mobile broadband.

On the other hand, SDN, which is based on the elements of the control-plane decoupled from the data-plane in management and virtualization is a new dimension to the design space which is constantly evolving with considerable scope for improvement and further development. The

transfer of research results and concepts to real-world networks imposes additional constraints and requirements undeniably. With this thought, in this section, we give an overview on the research challenges and the complications that MNOs could encounter while incorporating SDN technology into mobile backhaul networks.

On a general perspective, OpenFlow based SDN approach certainly calls-forth for challenges that include minimization of overhead, stability, and scalability issues, considering the centralized approach. Scaling the centralized controller has been the topic of recent proposals [26]-[28]. Within a mobile communication environment, we find that the network elements such as the Node B or e-Node Bs themselves can be a bottleneck in flow setup more than the controller itself. Even though, approaches such as ours, where aggressive use of OpenFlow flow-match wildcards or hash-based routing (such as ECMP) reduces control-plane load (detailed in Chapter 10), this prevents the controller from effectively managing traffic. Furthermore, we consider that SDN excessively couples central control and complete topology visibility. When considering mobile networks, disclosing the network topology has never received compelling recognition from the MNOs, to preserve confidentiality. However, as one of our contributions, Chapter 8 opens the first step towards topology visibility from a theoretical point of view.

While destination-based, shortest path forwarding state can be calculated in a distributed fashion (Chapter 7), SDN is built on a long reflection on the best way to meet data-forwarding. That means there is a lot more states in the OpenFlow datapath beyond that used for standard forwarding (filters, tagging, policy routing, QoS policy, etc.). And there are a lot more desired uses for networks than simple destination-based forwarding. We see it as a minimalist solution, enhancing the service building potential of the current Internet as well as mobile networks which remains resolutely located at the edge. The intention is also to make the network more cost effective by allowing closer control of provisioning and more precise capacity planning. We hope this dissertation thesis will stimulate further research. Our own work is currently in several directions. We are continuing the performance evaluation reported in [29] paying special attention to the calibration of measurement based admission control. We are also seeking more efficient algorithms for realizing the admission control and Packet Fair Queuing (PFQ) mechanisms to facilitate implementation. Adding to these, what is needed is a way of somehow merging OpenFlow with traditional IP networking at the edge of the backhaul, if a large base of users is visibly beyond the scope of an explicitly-managed connection. There are proposals already in play to interwork OpenFlow and MPLS (from Ericsson) to generate a new kind of IP network that offers a combination of open connectivity and policy-managed connectivity.

And here is where the technology and business refuses to go hand-in-hand. Sure, it appears possible and yes there is at least one widely publicized production WAN deployment (Stanford

campus network deployment) where the network switching devices receive their FIB state from a centralized SDN application using OpenFlow. But one must realize that to fully replace all the required features and functionality of MPLS, OpenFlow and SDN will need to evolve to offer those same features and functions. Would adding those features and functions make OpenFlow and SDN as complex in the future as MPLS is today? If so, what will the industry have gained? So, would we be just moving the complexity problem somewhere else? On the other hand, trying to scale a solution using classic OpenFlow almost certainly won't work. To begin with, the use of n-tuples (say per-flow, or even per host/destination pair) will most likely result in table space exhaustion. Even with very large tables (hundreds of thousands) the solution is unlikely to be suitable.

Further, to efficiently use the fabric, multipathing should be done per flow. It's highly unlikely (in my experience) that having the controller participate in flow setup will have the desired performance and scale characteristics. Therefore the multipathing should be done in the fabric (which is possible in a later version of OpenFlow like 1.1 and 1.2). Given these constraints, an SDN approach would probably look a lot like a traditional routing protocol. That is, the resulting state would most likely be destination IP prefixes (so we can take advantage of aggregation and reduce the table requirements by a factor of N over source-destination pairs). Further, multipathing, and link failure detection would have to be done on the switch.

Software defined networking (SDN) has so far been used predominantly to optimise datacentre resources in the cloud. But it has also been much discussed in the telco sphere and operators have tested SDN applications for operational network elements. The application of SDN to transport and backhaul optimisation is so recent that there is little hard evidence to support SDN business cases for service providers. However, research released suggests that SDN can almost halve a perceived "backhaul shortfall" and save operators just under $5bn in capital expenses by 2017. A Strategy Analytics report published last year found a $9.2bn gap in expected demand and expected availability of backhaul capacity. As mobile data traffic grows, the investment required to meet users' expectations of customer experience escalates. A capacity shortfall in backhaul networks has already begun to build and that backhaul gap may reach 16Pb (petabytes) globally by 2017, Strategy Analytics said. In a follow-up report published on behalf of Tellabs today, Strategy Analytics predicts that SDN can save mobile operators more than $4bn in capital expenses by 2017. Savings stem from five key SDN applications for mobile backhaul networks and can help close almost half of the gap identified in Strategy Analytics' earlier report by delivering network load sharing and dynamic resources allocation. Further new SDN control and resource management will dramatically lower Network Operations Backhaul Expense (OPEX).

As an overall conclusion, related network evolution steps considering SDN/OpenFlow will be common and the difference will lie in whether all operators will experience all of the transformation stages or whether some can accelerate or side step one or two of the stages. Dominant operators with the legacy infrastructure have the most complex task ahead of them. The challenge lies in the complexity of managing the transition to packet backhaul whilst maintaining existing high quality of legacy services. For many years to come Backhaul will have to accommodate not only HSPA+ and LTE but also to simultaneously provide transport solution for a full range of legacy RAN transport technologies. With today's hybrid approaches packet data traffic is either carried encapsulated into TDM transport or alternatively it is transported separately over a public internet. Hybrid approaches of tomorrow will reverse the hierarchy by carrying TDM traffic encapsulated over packet based transport. And eventually 2G networks will be turned off allowing for the pure packet transport network for Mobile Broadband.

Bibliography

1. Lee, Kyunghan, et al. "Mobile data offloading: how much can WiFi deliver?." Proceedings of the 6th International COnference on emerging Networking EXperiments and Technologies, ACM, 2010.
2. Available online: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html
3. Jorswieck, E.A., Badia, L., Fahldieck, T., Gesbert, D., Gustafsson, S., Haardt, M., Ho, K.M., Karipidis, E., Kortke, A., Larsson, E.G., Mark, H., Nawrocki, M., Piesiewicz, R., Romer, F., Schubert, M., Sykora, J., Trommelen, F., Van den Ende, B., Zorzi, M: Resource Sharing in Wireless Networks: The SAPHYRE Approach. In: Future Network and Mobile Summit 2010 Conference Proceedings, Cunningham, P. and Cunningham, M (Eds), IIMC International Information Management Corporation, 2010, ISBN: 978-1-905824-16-8.
4. Digital World Forum, Low cost broadband access and infrastructure, http://digitalworld.ercim.eu/wp3.html.
5. Boudec, J.Y.L.: Rate adaptation, congestion control and fairness: A tutorial. Technical report, Tutorial, Ecole Polytechnique Federale de Lausanne (EPFL), 2003.
6. Kelly, F., Maulloo, A., Tan, D.: Rate control for communication networks: Shadow prices, proportional fairness and stability. In: Journal of Operations Research Society, vol. 49, p. 237252, March 1998.
7. Peters, H. J. M. : Axiomatic Bargaining Game Theory. In: Kluwer Academic Publishers, 1992.
8. Busi, N., Manfredini, C., Montresor, A., Zavattaro, G., Department of Science and technology, University of Bologne : Towards Data driven coordination Infrastructure for Peer-Peer systems.
9. Barcelo, J., Infante, J., Oliver, M., Department of Information and Communication Technologies, Universitat Pompeu Fabra, Carrer Tanger 122-140, 08018 Barcelona, Catalunya, Spain.: Wireless Open Access Networks: State-of-the-art and Technological Opportunities.
10. Meddour, D.E., Rasheed, T., Gourhant, Y.: On the role of infrastructure sharing for mobile network operators in emerging markets. In: Computer Networks, Volume 55, Issue 7, Recent Advances in Network Convergence, 16 May 2011, Pages 1576-1591, ISSN 1389-1286, DOI: 10.1016/j.comnet.2011.01.023.(http://www.sciencedirect.com/science/article/B6VRG-528P8FF-1/2/0c4d37bd3af22ca654537ade6eebc362)
11. 3GPP Release 6 Technical Specification Group: Network sharing; Architecture and functional description. [TS 23.251].
12. 3GPP Techincal Report [TR 22.951]: Service aspects and requirements for network sharing.
13. 3GPP Technical Specification [TS 36.300]: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2.
14. Frisanco, T., Tafertshofer, P., Lurin, P., Ang, R.: Infrastructure Sharing for Mobile Network Operators From a Deployment and Operations View. In: Network IEEE Operations and Management Symposium, 2008, NOMS 2008.
15. Bhatia, S.,, Motiwala, M., Muhlbauer, W., Valancius, V., Bavier, A., Feamster, N., Peterson, L., Rexford, J.: Hosting virtual networks on commodity hardware. Georgia Tech. University.,Tech. Rep. GT-CS-07-10, January 2008.
16. Kohler, E., Morris, R., Chen, B., Jahnotti, J., Kasshoek, M.F.: The Click Modular Router. In: ACM Transaction on Computer Systems, vol. 18, no. 3, 2000, pp. 263–297.
17. VROUT: http://nrg.cs.ucl.ac.uk/vrouter
18. VMware Server, http://www.vmware.com/products/server/
19. Cisco VN-Link: Virtualization-Aware Networking, white paper. http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns892/ns894/white_paper_c11-525307_ps9902_Products_White_Paper.html
20. GENI Planning Group: GENI: Conceptual Design, Project Execution Plan. In: GENI Design Document 06-07, January 2006. http://www.geni.net/GDD/GDD-06-07.pdf
21. GENI: Global Environment for Network Innovations. http://www.geni.net/
22. Bavier, A., Bowman, M., Culler, D., Chun, B., Karlin, S., Muir, S., Peterson, L., Roscoe, T., Spalink, T., Wawrzoniak, M.: Operating System Support for Planetary-Scale Network Services, Mar. 2004.
23. Bavier, A., Feamster, N., Huang, M., Peterson, L., Rexford, J.: In VINI Veritas: Realistic and Controlled Network Experimentation. In: ACM SIGCOMM'06, Sept. 2006.
24. Feamster, N., Gao, L., Rexford, J.: How to lease the Internet in your spare time. In: ACM SIGCOMM Computer Communications Review, Vol. 37, No.1, January 2007.
25. Zhu, Y., Zhang-Shen, R., Rangarajan, S., Rexford, J.: Cabernet: Connectivity architecture for better network services. In: Workshop on Rearchitecting the Internet, Dec. 2008.
26. Niebert N, Baucke S, El-Khayat I, et al.: The way 4WARD to the creation of a Future Internet. In: ICT Mobile Summit, Stockholm, June 2008.
27. 4WARD project page at www.4ward-project.eu
28. AKARI Architecture Conceptual Design for New Generation Network [translated version 1.1] (http://akari-project.nict.go.jp/eng/conceptdesign/AKARI_fulltext_e_translated_version_1_1.pdf)
29. Asia Future Internet (AsiaFI) (www.asiafi.net)
30. S. Rai and B. Mukherjee, "IP Resilience within an Autonomous System: Current Approaches, Challenges, and Future Directions," *IEEE Communications Magazine*, Oct. 2005.
31. M. Menth, R. Martin, M. Hartmann and U. Spoerlein, "Efficiency of Routing and Resilience Mechanisms in Packet-Switched Communication Networks," *European Transactions on Telecommunications*, vol. 21 Issue 2, 2010.
32. H. Lehpamer, *Microwave Transmission Networks*, 2nd ed.: McGraw-Hill Professional, 2010.
33. C. Ou, J. Zhang, L. H. Sahasrabuddhe, and B. Mukherjee, "New and improved approaches for shared-path protection in WDM mesh networks," *Lightwave Technologies*, vol. 22, pp. 1223–1232, 2004.
34. R. Muñoz, R. Casellas, and R. Martinez, "An experimental signalling enhancement to efficiently encompass WCC and backup sharing in GMPLS-enabled wavelength-routed networks," *in Proc. IEEE ICC' 08*, 2008, pp. 5401–5406.
35. K. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications: Continuous Markov Chain Models*, 2nd ed.: John Wiley & Sons, 2009.

36. M. Rausand and A. Høyland , *System Reliability Theory: Models, Statistical Methods, and Applications*, 3rd ed.: Wiley, Nov. 2003.
37. ReliaSoft Publishing, *System Analysis Reference: Reliability, Availability and Optimization* , 2003.
38. S. Distefano and L. Xing, *"*A New Modeling Approach: Dynamic Reliability Block Diagrams,*" in Proc. 52nd Ann. Reliability and Maintainability Symp. (RAMS '06),* Jan. 2006.
39. *International Telecommunications Union Telecommunication Standardization Sector Recommendations E.800*, ITU-T, 1994.
40. A. Lisnianski and G. Levitin, Multi-state system reliability: Assessment, optimization and applications: World-Scientific, Singapore: 2003.
41. R. Howard, Dynamic Programming and Markov Processes. Cambridge, Massachusetts: MIT Press , 1997.
42. T. Aven and U. Jensen, Stochastic Models in Reliability. NY: Springer,1999.
43. S.V. Amari and R.B. Misra, "Dynamic reliability analysis of coherent multi-state systems", IEEE Transactions on Reliability, Vol. 46, pp. 460–461, 1997.
44. J. Xue and K. Yang, " Dynamic reliability analysis of coherent multi-state systems" in IEEE Transactions on Reliability ,Vol. 44, pp. 683–688, 1995.
45. P.Hoang,, Hand Book of Reliability Engineering. Springer, New York: pp: 61-87. 2003.
46. N. McKeown, T. Anderson., H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: Enabling innovation in campus networks,"ACM SIGCOMM CCR, April 2008.
47. M. Kodialam and T. V. Lakshman,"Dynamic routing of bandwidth guaranteed tunnels with restoration," in Proc. of IEEE INFOCOM, March 2000.
48. P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 2000.
49. J. Doucette, M. Clouqueur and W. D. Grover, "On the availability and capacity requirements of shared backup path-protected mesh networks," SPIE Optical Networks Mag., Nov. 2003.
50. Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," in Proc. of IEEE INFOCOM, vol. 2, pp. 699–708, Apr. 2001.
51. X. Su and C. Su, "An online distributed protection algorithm in WDM networks,"in Proc. of IEEE ICC, vol. 5, pp. 1571–1575, June 2001.
52. K. Murakami and H. S. Kim, "Virtual path routing for survivable ATM networks," IEEE Trans. on Networking, Vol. 4(1), February 1996.
53. C. Su and X. Su, "Protection path routing on WDM networks," in Proc. of OFC, vol. 2, Mar. 2001.
54. A. Kumar, M. Marathe, S. Parthasarathy, and A. Srinivasan, "Algorithmic aspects of capacity in wireless networks," in Proc. of ACM SIGMETRICS, vol. 33, no. 1, pp. 133-144, June 2005.
55. Y. Liu, D. Tipper and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," in Proc. of IEEE INFOCOM, vol. 2, pp. 699–708, 2001.
56. G. Li, D. Wang, C. Kalmanek and R. Doverspike, "Efficient distributed path selection for shared restoration connections," in Proc. of IEEE INFOCOM, pp. 140–149, 2002.
57. S. Ramamurthy and B. Mukherjee. "Survivable WDM mesh networks. Part I Protection," in Proc. of IEEE INFOCOM, April 2009.
58. T.Chang, D. Pendarakis and Z.Liu, "Cost-effective configuration of content resiliency services under correlated failures," in Proc. of DSN 2006, pp.536-548, 2006.
59. C. Su and X. Su, "Protection path routing on WDM networks," in Proc. of OFC, vol. 2, Mar. 2001.
60. M. Kodialam and T. V. Lakshman,"Dynamic routing of bandwidth guaranteed tunnels with restoration," in Proc. of IEEE INFOCOM, March 2000.
61. J. P. Rohrer, A. Jabbar and J.P. Sterbenz,"Path diversification: A multipath resilience mechanism," in Proc. of IEEE DRCN, Oct .2009.
62. J. W. Suurballe and R. E. Tarjan, "A quick method for finding shortest pairs of disjoint paths," Networks, vol. 14, 1986.
63. E. F. Moore, The shortest path through a maze. Bell Labs,1959.
64. R. W. Floyd, "Algorithm 97: Shortest path," ACM Communications, vol. 5, no. 6, p. 345, 1962.
65. L. Ford, "Network flow theory," 1956.
66. W. D. Grover and D. Stamatelakis, "Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-plaining network restoration," in Proc. IEEE ICC, 1998, pp. 537–543.
67. H. Huang and J. Copeland, "Multi-domain Mesh Optical Network Protection using Hamiltonian cycles," in Proc. High Perf. Switching and Routing, Workshop on Merging Opt. and IP Technol., May 2002, pp. 26–29.
68. Y. Xiong and L. Mason, "Restoration Strategies and Spare Capacity Requirements in Self Healing ATM Networks," IEEE/ACM Trans. Netw., vol. 7, no. 1, pp. 98–110, Feb. 1999.
69. B. G. Jozsa and D. Orincsay, "Shared backup path optimization in telecommunication networks," in Proc. of Dynamic of Reliable Com. Netw., DRCN'2001, Oct. 2001, pp. 251–257.
70. M. Kodialam and T. Lakshman, "Dynamic Routing of Restorable Bandwidth-Guaranteed Tunnels Using Aggregated Network Resource Usage Information," IEEE/ACM Trans. on Netw., vol. 11, no. 3, pp. 399–410, 2003.
71. J. Tapolcai and T. Cinkler, "On-line Routing Algorithm with Shared Protection in WDM Networks," in Proc. Opt. Netw. Design and Modeling, Budapest, Hungary, Feb. 2003, pp. 351–364.
72. D. Xu, C. Chunming, and Y.Xiong, "An Ultra-Fast Shared Path Protection Scheme Distributed Partial Information Management, Part II," in Proc. 10th IEEE Intl. Conf. in Netw. Protocols, France, Nov. 2002, pp. 344–353.
73. S. Sengupta and R. Ramamurthy, "From Network Design for Dynamic Provisioning and Restoration in Optical Cross-Connect Mesh Networks: An Architectural and Algorithmic Overview," IEEE Network, vol. 15, no. 4, pp. 46–54, Jul.-Aug. 2001.
74. J.-F. Labourdette, "Shared mesh restoration in optical networks," in Proc. Opt. Fiber Com. Conf. (OFC), vol. 1, Feb. 2004, pp. 23–27.

75. C. Assi, W. Huo, A. Shami, and N. Ghani, “Analysis of Capacity Reprovisioning in Optical Mesh Networks,” IEEE Com. Letters, vol. 9, no. 7, pp. 658–660, Jul. 2005
76. E. W. Dijkstra, “A note on two problems in connection with graphs,” Numerische Mathematik, vol. 1, pp. 269–271, 1959.
77. M.Dorigo and D.C.Gianni,"Ant colony optimization: a new meta-heuristic."In Proc. of IEEE CEC, vol. 2, 1999.
78. Y.J.Yen, Finding the k shortest loopless paths in a network. Management Science, 17(11), 712-716. 1971.
79. A.R. Rutenbar, Simulated annealing algorithms: An overview, IEEE Circuits and Devices Magazine, 5(1), 19-26., 1989.
80. M. Gendreau, A. Hertz and G. Laporte, A tabu search heuristic for the vehicle routing problem. Management science, 1276-1290. 1994
81. C.M.Fonseca and P.J.Fleming, “Genetic algorithms for multiobjective optimization: Formulation, discussion and generalization,” In Proc. of the fifth international conference on genetic algorithms, June 1993
82. S.Subhash, M.Waldvogel, and P.Warkhede. Profile-based routing: A new framework for MPLS traffic engineering. Quality of future Internet Services. Springer Berlin/Heidelberg, 2001.
83. D.O.Awduche and J.Agogbua. Requirements for traffic engineering over MPLS.1999.
84. Awduche, D. O. (1999). MPLS and traffic engineering in IP networks. Communications Magazine, IEEE, 37(12), 42-47.
85. R. Sherwood, G. Gibb, K.K. Yap, G. Appenzeller, N. McKeown, G. Parulkar and M. Casado, “Can the production network be the test-bed?”, in Proc. of OSDI 2010, pp. 1-6, 2010.
86. N. McKeown, T. Anderson., H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, “OpenFlow: Enabling innovation in campus networks,”ACM SIGCOMM CCR, April 2008.
87. K.H.Kim and K.Y.Kim, Routing straddle carriers for the loading operation of containers using a beam search algorithm. Computers & Industrial Engineering, 36(1), 109-136, 1999.
88. ILOG, CPLEX Optimizer 9.1, www.ilog.com.
89. G. Li, D. Wang, C. Kalmanek, and R. Doverspike, “Efficient distributed path selection for shared restoration connections,” in Proc. of IEEE INFOCOM, pp. 140–149, June 2002.
90. Y. Liu, D. Tipper, and P. Siripongwutikorn, “Approximating optimal spare capacity allocation by successive survivable routing,” in Proc. of IEEE INFOCOM, vol. 2, pp. 699–708, Apr. 2001.
91. C. Su and X. Su, “Protection path routing on WDM networks,” in Proc. of OFC, vol. 2, Mar. 2001.
92. X. Su and C. Su, “An online distributed protection algorithm in WDM networks,”in Proc. of IEEE ICC, vol. 5, pp. 1571–1575, June 2001.
93. G. Mohan, C. S. R. Murthy, and A. K. Somani, “Efficient algorithms for routing dependable connections in WDM optical networks,” IEEE/ACM Trans. Networking, vol. 9, pp. 553–566, Oct. 2001.
94. J. Zhang, H. Wu, Q. Zhang, and B. Li, “Joint routing and scheduling in multi-radio multi-channel multi-hop wireless networks," in Proc. of IEEE BROADNETS, pp. 678-687, 2005.
95. K. Murakami and H. S. Kim, “Virtual path routing for survivable ATM networks,” IEEE Trans. on Networking, Vol. 4(1), February 1996.
96. M. Kodialam and T. V. Lakshman,“Dynamic routing of bandwidth guaranteed tunnels with restoration,” in Proc. of IEEE INFOCOM, March 2000.
97. G.Classen, D.Coudert, A.M.C.A.Koster, and N. Nepomuceno, "Bandwidth assignment for reliable fixed broadband wireless networks," in Proc. of IEEE WoWMoM, pp.1 - 6, 2011.
98. Schupke, Dominic A., and Robert Prinz. "Performance of path protection and rerouting for WDM networks subject to dual failures." *Optical Fiber Communication Conference*. Optical Society of America, 2003.
99. G.Li, D.Wang, C.Kalmenak and R. Doverspike, “Efficient distributed path selection for shared restoration connections,” in Proc. of IEEE INFOCOM, pp: 140-149, june 2002.
100. W.Najjar and J-L. Gaudiot, “Network resilience: A measure of network fault tolerance,” IEEE Transactions on Computers, Vol.39, 1990.
101. A. Tootoonchian,and Y.Ganjali. "HyperFlow: A distributed control plane for OpenFlow," in Proc.UNISEX INM/WREN '10, 2010.
102. H. Iqbal,and T. Znati, “Distributed control plane for 4D architecture,” in Proc. of IEEE GLOBECOM'07, 2007.
103. B.Heller, R.Sherwood, and N.McKeown, “The controller placement problem,” in Proc..of ACM SIGCOMM workshop HotSDN’12 , 2012.
104. BGP Route Reflection: http://tools.ietf.org/html/rfc4456.
105. M. Caesar, et al, “Design and implementation of a routing control platform (RCP),” In Proc. of USENIX NSDI, 2005.
106. Path Computation Clients (PCC): Path Computation Element (PCE) Requirements for MPLS-TE: http://tools.ietf.org/html/rfc5862.
107. Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification: http://tools.ietf.org/html/rfc5415.
108. A. Greenberg, et al.,“A clean slate 4D approach to network control and management," ACM SIGCOMM CCR, Vol. 35,No.5, pp- 41-54, 2005
109. M. Casado, et al.,“Ethane: Taking control of the enterprise,” ACM SIGCOMM CCR. Vol. 37. No. 4. 2007.
110. N. McKeown, et al., “OpenFlow: Enabling innovation in campus networks." ACM SIGCOMM CCR Vol. 38, No. 2, pp-69-74, 2008.
111. H. Yan, et al. “Tesseract:A 4D network control plane.” in Proc. of USENIX NSDI ’07, April 2007 .
112. A. Greenberg, et al., “Refactoring network control and management: A case for the 4D architecture,” Carnegie Mellon University, Tech. Rep. CMU-CS-05-117, Sept 2005.
113. H. Iqbal,and T. Znati, “Distributed control plane for 4D architecture,” in Proc. of IEEE GLOBECOM'07, 2007.
114. B.Heller, R.Sherwood, and N.McKeown, “The controller placement problem,” in Proc..of ACM SIGCOMM workshop HotSDN’12 , 2012.
115. J.Halpern, “Finding minimal center-median convex combination (cent-dian) of a graph,” Management Science Vol.24.5, pp-535-544, 1978.
116. M.Castro, et al. "Exploiting network proximity in distributed hash tables." In Proc. of FuDiCo. 2002.
117. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP): http://tools.ietf.org/html/rfc3418
118. S. Hares, D. Katz: Administrative Domains and Routing Domains, A Model for Routing in the Internet, RFC 1136, December 1989 (www.ietf.org/rfc/rfcl 136.txt).

119. B. Halabi, D. Mc Pherson: Internet Routing Architectures, (2nd Edition), Cisco Press, January 2000.

120. M. Yannuzzi, X. Masip-Bruin, S. Sainchez, J. Domingo-Pascual, A. Orda, A. Sprintson: On the Challenges of Establishing Disjoint QoS IP/MPLS Paths Aross Multiple Domains, IEEE Communications Magazine, vol. 44, no. 12, pp. 60-66, December 2006, (www.comsoc.org/livepubs/cil/public/2006/Dec).
121. X. Masip-Bruin, et al.: The EuQoS System: A Solution for QoS Routing in Heterogeneous Networks, IEEE Communications Magazine, vol. 45, no. 2, pp. 96-103, February 2007, (www.comsoc.org/livepubs/ci /public/2007/Feb).
122. A. Farrel, J.-P. Vasseur, J. Ash: A Path Computation Element (PCE)-Based Architecture, RFC, 4655, August 2006, (www.ietf.org/rfc/rfc4655.txt).
123. J. Szigeti, J. Tapolcai, T. Cinkler, T. Henk, Gy. Sallai: Stalled Information based Routing in Multidomain Multilayer Networks, NETWORKS 2004, 11th International Telecommunication Network Planning Symposium, Vienna, Austria, June 2004.
124. J. Szigeti, I. Ballok, T. Cinkler: Efficiency of Information Update Strategies for Automatically Switched Multi-Domain Optical Networks, IEEE ICTON 2005, 7th International Conference on Transparent Optical Networks, Barcelona, Spain, July 3-7,2005, (www.itl.waw.pl/icton/).
125. K. Loja, J. Szigeti, T. Cinkler: Inter-Domain Routing in Multi-Provider Optical Networks: Game Theory and Simulations, EuroNGI, Thefirst Conference on Traffic Engineeringfor the Next Generation Internet, Rome, 18-20 April 2005 (www.eurongi.org/ngi2005).
126. D. Larrabeiti, R. Romeral, I. Soto, M. Uruefnal, T. Cinkler, J. Szigeti, J. Tapolcai: Multi-Domain Issues of Resilience, IEEE ICTON 2005, 7th International Conference on Transparent Optical Networks, Barcelona, Spain, July 3-7, 2005, (www.itl.waw.pl/icton/).
127. A. Farkas, J. Szigeti, T. Cinkler: p-Cycle Based Protection Scheme for Multi-Domain Networks, DRCN 2005, The 5th International Workshop on Design ofReliable Communication Networks, Ischia, Italy, October 16-19, 2005, (www.drcn.org).
128. D. Mesko, G. Viola, T. Cinkler: A Hierarchical and a Non-Hierarchical European Multi-Domain Reference network: Routing and Protection, Networks2006, Nov 6-9, 2006, NewDelhi, India, (www.networks2006.de).
129. GLPK (GNU Linear Programming Kit), Reference Manual, Free Software Foundation, Inc, 2006.
130. G. Li, D. Wang, C. Kalmanek and R.Doverspike. "Efficient distributed restoration path selection for shared mesh restoration," IEEE/ACM Transactions on Networking, Vol. 5, pp- 761-771, 2003.
131. P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388-404, 2000.
132. A. Kumar, M. Marathe, S. Parthasarathy, and A. Srinivasan, "Algorithmic aspects of capacity in wireless networks," in Proc. of ACM SIGMETRICS'05,pp. 133-144, June 2005
133. G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed path selection for shared restoration connections," in Proc. of IEEE INFOCOM'02, pp. 140–149, June 2002.
134. Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," in Proc. of IEEE INFOCOM, vol. 2, pp. 699–708, Apr. 2001.
135. C. Su and X. Su, "Protection path routing on WDM networks," in Proc. of OFC, vol. 2, Mar. 2001.
136. X. Su and C. Su, "An online distributed protection algorithm in WDM networks,"in Proc. of IEEE ICC, vol. 5, pp. 1571–1575, June 2001.
137. J. Zhang, H. Wu, Q. Zhang, and B. Li, "Joint routing and scheduling in multi-radio multi-channel multi-hop wireless networks," in Proc. of IEEE BROADNETS'05, pp. 678-687, 2005.
138. K. Murakami and H. S. Kim, "Virtual path routing for survivable ATM networks," IEEE Trans. on Networking, Vol. 4(1), February 1996.
139. H. Iqbal,and T. Znati, "Distributed control plane for 4D architecture," in Proc. of IEEE GLOBECOM'07, 2007
140. A. Tootoonchian, and Y. Ganjali, "HyperFlow: A distributed control plane for OpenFlow," in Proc. of USENIX INMC'10, 2010.
141. A. Tavakoli, M. Casado, T. Kopenen and S. Shenker, "Applying nox to the datacenter", In Proceedings of HotNets-VIII (2009)
142. M. Yu, J .Rexford, M. J. Freedman and J. Wang, "Scalable flow-based networking with difane", In Proceedings of the ACM SIGCOMM 2010 (2010), ACM, pp. 351–362.
143. A. R. Curtis, J.C. Mogul, J. Tourilhes, P. Yalagandula, P. Sharma and Sujatha Banerjee, "Devoflow: scaling flow management for high-performance networks", In Proceedings of the ACM SIGCOMM 2011 (2011), ACM
144. N. McKeown, T. Anderson., H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: Enabling innovation in campus networks,"ACM SIGCOMM CCR, April 2008.
145. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf
146. R. Sherwood et al. "Carving research slices out of your production networks with OpenFlow." ACM SIGCOMM CCR 40.1 (2010).
147. Zaki, Y., Zhao, L., Goerg, C., Timm-Giel,A.: LTE Wireless Virtualization and Spectrum Management. In: IEEE Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP.
148. Virtual Bridged Local Area Networks, IEEE Standard 802.1Q. http://standards..ieee.org/getieee802/download/802.1Q-2003.pdf, May 2003. Accessed 17 Dec, 2008.
149. E.Bellagamba, J.Kempf, P.Skoldstrom, Link Failure detection and Traffic Redirection in an OpenFlow Network, United States Patent Application Publication Pub. No. US2011/0286324, Nov.2011.
150. http://yuba.stanford.edu/foswiki/bin/view/OpenFlow/Mininet
151. http://mpls-linux.sourceforge.net
152. Razafindralambo, et al.: Promoting Quality of Service in Substitution Networks with Controlled Mobility. In: 10th International Conference on Ad Hoc Networks and Wireless (2011).
153. Miranda, K., Natalizio, E., Razafindralambo, T..: On the Impact of Router's Mobility on Substitution Networks. In: Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paris, France (2011).
154. Tong, S., Yang, O.W.W.: Bandwidth Management for Supporting Differentiated Service Aware Traffic Engineering. In: IEEE Transactions on Parallel and Distributed Systems, pp: 1320- 1331, vol. 18, (2007).
155. Shankaraiah, Venkataram, P.: Bandwidth management in a hybrid wireless network: For superstore applications. In: ICCS, pp. 517- 521 (2010).

156. Georgiadis, L., Guerin, R., Peris, V., Sivarajan, K.N.: Efficient Network QoS Provisioning Based on Per Node Traffic Shaping. In: IEEE/ACM Transactions on Networking, pp. 482- 501, Vol. 4, (1996).
157. Frank, Y.Li., Stol, N.: QoS Provisioning Using Traffic Shaping and Policing in 3rd-generation Wireless Networks. In: IEEE Wireless Communications and Networking Conference, WCNC 2002, pp. 139 – 143, vol.1 (2002).
158. Chang, T., Pendarakis, D., Liu, Z.: Cost-Effective Configuration of Content Resiliency Services Under Correlated Failures. In: DSN 2006, pp.536-548, (2006).
159. Venmani D.P., Gourhant, Y., Zeghlache, D.: 3RIS for 4G: A New Approach for Increasing Availability and Reducing Costs for LTE Networks. In: ICACT, pp.1025-1030, (2012).
160. Gude, N., Koponen, T., Pettit, J., Pfaf, B., Casado, M., McKeown, K., Shenker. S.: NOX: Towards an Operating System for Networks. In: SIGCOMM CCR, (2008).
161. Tavakoli, A., Casado, M., Koponen, T., Shenker. S.: Applying NOX to the Datacenter. In: HotNets, (2009).
162. Greenberg, A., et al.: A Clean Slate 4D Approach to Network Control and Management. In: SIGCOMM CCR, 35:41-54, 2005.
163. Amirijoo, M., Litjens, R., Spaey, R., Döttling, M., Jansen, T., Scully, N., Türke, U.: Use Cases, Requirements and Assessment Criteria for Future Self-Organising Radio Access Networks. In: Third International Workshop on Self-Organizing Systems, IWSOS (2008).
164. Ian, F. A., Ismail, H.K.: Wireless Sensor and Actor Networks: Research Challenges. In: Elsevier Journal of Ad hoc networks, (2004).
165. Tommaso, M., Dario, P., Vehbi, C.G., Ian F.A.: A Distributed Coordination Framework for Wireless Sensor and Actor Networks. In: 6th ACM international symposium on Mobile ad hoc networking and computing, pp.99 - 110, (2005).
166. Car-On-Wheels: http://en.wikipedia.org/wiki/Cell_on_wheels.
167. Venmani, D.P., Gourhant, Y., Zeghlache, D.: Preliminary Analysis of 4G-LTE Mobile Network Sharing for Improving Resiliency and Operator Differentiation. In: First International Conference on e-Technologies and Networks for Development (ICeND 2011) in LNCCIS pp. 73–93, Springer-Verlag Berlin Heidelberg (2011).
168. Bonald,T., Oueslati,S., Roberts.J.: IP traffic and QoS control: Towards a Flow-Aware Architecture. In: World Telecom Conference, Paris (2002).
169. Roberts,J.: Internet Traffic, QoS and Pricing: In: IEEE Communication Letters, vol. 92, no. 9, Sept. (2004).
170. Jajszczyk, A., Wojcik, R.: Emergency Calls in Flow-Aware Networks. In: IEEE Communications Letters, vol. 11, Page(s): 753- 755, (2007).