



HAL
open science

Metric-based Rate Control for Transport Protocols in Multi-hop Wireless Networks

Le Minh Duong

► **To cite this version:**

Le Minh Duong. Metric-based Rate Control for Transport Protocols in Multi-hop Wireless Networks. Other [cond-mat.other]. Université Paris Sud - Paris XI; Université de Technologie de Hanoi. Vietnam, 2012. English. NNT : 2012PA112136 . tel-00726025

HAL Id: tel-00726025

<https://theses.hal.science/tel-00726025>

Submitted on 28 Aug 2012

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.

Metric-based Rate Control for Transport Protocol in Multi-hop Wireless Networks

Le Minh DUONG



Comprendre le monde,
construire l'avenir®

UNIVERSITE PARIS-SUD
ECOLE DOCTORALE: STITS
Laboratoire des signaux et systèmes (L2S)
DISCIPLINE: PHYSIQUE

Directeur de thèse:	Véronique VEQUE, Professeur, Université Paris-Sud
Co-directeur de thèse:	Dai Tho NGUYEN, Chercheur, UET-VNUH, Vietnam
Co-directeur de thèse:	Lynda ZITOUNE, Chercheur, ESIEE-Paris
Composition du jury:	
Président du jury:	Jalel BEN-OTHTMAN, Professeur, Université de Paris 13
Rapporteurs:	Thierry GAYRAUD, Professeur, Université de Toulouse Yacine GHAMRI-DOUDANE, HDR, ENSIIE
Examineurs:	Cong Duc PHAM, Professeur, Université de PAU

Thèse de Doctorat

Juillet 2012

Abstract

In recent years, Multi-hop Wireless Networks (MHWNs) have experienced an explosion of deployment due to the increasing demand for continuous connectivity regardless of the physical location. Internet predominant transport protocols, i.e. Transmission Control Protocol (TCP), face performance degradation in MHWNs because of the high loss and link failure rates. Several solutions have been proposed which are based on network state estimation or use information from MAC layer (called metrics) in a cross-layer manner to better comprehend the network state. The first part of this thesis provides a survey and comprehensive definition of common metrics from Physical, MAC, Network and Transport layers and thus provides a multi-criteria and hierarchical classification. After that, the effectiveness in reflecting network information of MAC metrics is also investigated in a systematic way by simulating various network situations and measuring the MAC metrics. Thus, the good MAC metric for congestion control which is coupled with the network contention level and the medium induced losses will be found out. From the results of the effectiveness study, new rate control schemes for transport protocols are proposed which adapt efficiently the source bit rate depending on the network condition provided by some MAC metrics. Through an extensive set of simulations, the performance of the proposed rate control schemes in MHWNs is investigated thoroughly with several network situations.

Acknowledgements

First and foremost, I want to give many thanks to my supervisor, Prof. Véronique VEQUE, for the continuous encouragement and guiding. She has been very nice to me from the first day I arrived in France. She not only taught me how to conduct high quality research, but also supported me in the daily life. She has always showed her faith in me, even in the not-so-happy times of my work. It is lucky to work with a supervisor like Prof. Véronique VEQUE. A big thanks also to Mr. Dai Tho NGUYEN, my co-supervisor, for supporting my work during the time in Vietnam. Many thanks for Lynda, my second co-supervisor, for her enthusiasm in our work. In more than three years of my PhD, I have received much help from my colleges in the research team “Réseaux et Télécoms”. Thank Anthony for his kindly support whenever I needed some advices. Thank Stéphane for his encouragement and teaching me french. Thank Tuan for his sharing in my work and daily life.

Many thanks also for all of my friends. They made my time in France full of joy, surprises and warmth. I want to give specially thanks Mr. Anh Quoc LE QUANG, the one who has helped me much like a big brother in France. Finally, I really want to say “thanks a lot” to my parents and my little brother for their unlimited support in my life and my work. They are the greatest encouragement whenever I come up against difficulties, and are the first ones I want to share my successes. This thesis is dedicated to them.

Contents

List of Figures	vii
List of Tables	ix
Glossary	xi
1 Introduction	1
2 Background study	3
2.1 Multi-hop Wireless Networks	3
2.1.1 Introduction	3
2.1.2 Architecture and applications of MHWNs	4
2.1.3 MHNW challenges	5
2.2 Technologies for Multi-hop Wireless Networks	5
2.2.1 Bluetooth	7
2.2.2 Wireless Local Area Networks	7
2.2.3 Worldwide inter-operability for Microwave Access	9
2.2.4 Long Term Evolution	9
2.3 IETF Transport Protocols	10
2.3.1 Transmission Control Protocol	10
2.3.2 User Datagram Protocol	11
2.3.3 TCP-Friendly Rate Control	12
2.3.4 Datagram Congestion Control Protocol	13
2.4 Transport Protocols over Multi-hop Wireless Networks	14
2.4.1 The Challenges in MHWNs	14
2.4.2 The Improvement Approaches of Transport Protocols in MHWNs	16
2.4.3 Cross-layer between Transport and Link layers	17
2.5 Summary	19
3 Metric classification in Wireless Networks	21
3.1 Metrics of PHY layer	22
3.2 Metrics of MAC layer	24
3.2.1 The 802.11 MIB	24
3.2.2 Channel access related metrics	25
3.2.3 Channel load related metrics	27
3.3 Metrics of Network layer	29
3.3.1 Medium transmission related metrics	31
3.3.2 Inter-flow interference related metrics	32

CONTENTS

3.3.3	Intra-flow interference related metrics	33
3.3.4	Multi-Purpose metrics	34
3.4	Metrics of Transport layer	37
3.4.1	Throughput Related Metrics	38
3.4.2	Reliability Related Metrics	39
3.4.3	Packet Delay Related Metrics	40
3.5	Classification table	43
3.6	Summary	43
4	Effectiveness of MAC metrics to reflect network condition	45
4.1	New MAC metrics	45
4.1.1	The Average Transmission Attempt	46
4.1.2	The Average Transmission Time	46
4.1.3	The Medium Access Delay	47
4.2	Metric effectiveness	49
4.3	Effectiveness evaluation	49
4.4	Confidence Interval	50
4.5	Simulation and Results	50
4.5.1	Simulation scenarios	50
4.5.1.1	General configuration	50
4.5.1.2	Scenario 1: Effect of traffic load	51
4.5.1.3	Scenario 2: Effect of channel random error	53
4.5.2	Results and discussion	53
4.5.2.1	Results for scenario 1	53
4.5.2.2	Results for scenario 2	64
4.6	Summary	65
5	Medium Access Delay aware Rate Control for Transport Protocol	67
5.1	The design of Medium Access Delay aware Rate Control	68
5.1.1	General idea	68
5.1.2	Intermediate nodes	69
5.1.3	MAD-TP receiver	69
5.1.4	MAD-TP sender	70
5.1.5	MAD-TP packet formats	71
5.2	Performance evaluation	73
5.2.1	The threshold MAD_{TH}	73
5.2.2	Simulation scenarios	74
5.2.2.1	Scenario 1	74
5.2.2.2	Scenario 2	74
5.2.2.3	Scenario 3	75
5.2.2.4	Scenario 4	76
5.2.3	Results and discussion	76
5.2.3.1	Chain topology	76
5.2.3.2	Grid topology	81
5.2.3.3	Random topology	85
5.3	Summary	86

6	Metric-based Rate Control for Transport Protocol	89
6.1	Network Contention Detection with <i>MAD</i> Gradient	89
6.2	Effective Bandwidth Estimation with <i>ATT</i>	92
6.3	IMAD-TP: Improvement for MAD-TP	93
6.3.1	Intermediate nodes	93
6.3.2	IMAD-TP receiver	93
6.3.3	IMAD-TP sender	94
6.4	Performance evaluation	95
6.4.1	Simulation scenarios	95
6.4.2	Results and discussion	95
6.4.2.1	Chain topology	95
6.4.2.2	Grid topology	98
6.4.2.3	Random topology	103
6.5	Summary	105
7	Conclusions and Future Research	107
7.1	Concluding Remarks	107
7.2	Future Research	108
A	Version française	109
A.1	Introduction	109
A.2	Une classification des métriques cross-layer par couche	111
A.3	Fidélité de différentes métriques MAC à refléter les conditions réseau . .	114
A.4	Un nouveau protocole de transport “rate-based” utilisant la métrique MAD	119
A.5	Contrôle de débit basé sur métrique pour protocole de transport	123
A.5.1	Résultats des simulations	126
A.6	Conclusion	127
	References	129

CONTENTS

List of Figures

2.1	IEEE 802.11 basic medium access mechanism and data delivery procedure	8
3.1	Simple model for IEEE 802.11 service time [1]	26
4.1	$T_{contention}$ in IEEE 802.11 DCF	47
4.2	Topology for scenario 1.3	52
4.3	Scenario 1.1: one flow with different source rates	54
4.4	Scenario 1.2: one flow with sudden change in traffic rate	55
4.5	Scenario 1.3: flow 1's rate is 1Mbps	56
4.6	Scenario 1.3: flow 1's rate is 1.25Mbps	57
4.7	Scenario 2.1: traffic rate 1Mbps	61
4.8	Scenario 2.1: traffic rate 2Mbps	62
4.9	Scenario 2.2: 1 connection with rate = 0.5Mbps and BER=10e-6	63
5.1	MAD-TP packet formats	72
5.2	Grid 8x8 topology	75
5.3	Chain topology with 1 connection and precomputed path	77
5.4	Chain topology with 1 connection and routing protocol AODV	78
5.5	Chain topology with 8 hops and 4 connections with precomputed path	79
5.6	Chain topology with 8 hops and 4 connections with routing protocol AODV	80
5.7	Grid topology with precomputed path: the performance	81
5.8	Grid topology with precomputed path: the fairness	82
5.9	Grid topology with routing protocol AODV: the performance	83
5.10	Grid topology with routing protocol AODV: the fairness	84
5.11	Random topology with routing protocol AODV: the performance	85

LIST OF FIGURES

5.12	Random topology with routing protocol AODV: the fairness	86
6.1	MAD gradient with different offered load	91
6.2	ACK packet structure of IMAD-TP	94
6.3	Chain topology with 1 connection and precomputed path	95
6.4	Chain topology with 1 connection and routing protocol AODV	96
6.5	Chain topology with 8 hops and 4 connections with precomputed path .	97
6.6	Chain topology with 8 hops and 4 connections with routing protocol AODV	98
6.7	Grid topology with precomputed path: the performance	99
6.8	Grid topology with precomputed path: the fairness	100
6.9	Grid topology with routing protocol AODV: the performance	101
6.10	Grid topology with routing protocol AODV: the fairness	102
6.11	Random topology with routing protocol AODV: the performance	103
6.12	Random topology with routing protocol AODV: the fairness	104
A.1	Modèle du temps de service IEEE 802.11 [1]	116
A.2	Chain topology with 1 connection and routing protocol AODV	122
A.3	Chain topology with 1 connection and routing protocol AODV	127

List of Tables

2.1	Mobile Ad hoc Network Applications [2]	6
2.2	IEEE 802.11 standards	7
2.3	Cross-layer proposal classification table	20
3.1	Constants in Airtime [3]	27
3.2	MAC metric table	30
3.3	Routing metric table	37
3.4	Metric patterns for network events	42
3.5	Transport metric table	42
3.6	Metric classification table	44
4.1	General configuration for simulation	51
4.2	General scenario setting	51
A.1	Metric classification table	115

GLOSSARY

Glossary

3GPP	3rd Generation Partnership Project
4G	Fourth Generation
AC	Access Category
ACK	ACKnowledgement
ADSN	ACK Duplication Sequence Number
AIFS	Arbitration Inter-Frame Space
AODV	Ad hoc On-Demand Distance Vector
AP	Access Point
ATA	Average Transmission Attempt
ATT	Average Transmission Time
BAN	Body Area Network
BDP	Bandwidth Delay Product
BER	Bit Error Rate
BSR	Backoff Stage Ratio
BSS	Basic Service Set
CBR	Constant Bit Rate
CCID	Congestion Control Identification
CINR	Carrier to Interference Plus Noise Ratio
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DARPA	Defense Advanced Research Projects Agency
DCCP	Datagram Congestion Control Protocol
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DNS	Domain Name System
DOOR	Detection of Out-of-Order and Response
DSSS	Direct-Sequence Spread Spectrum
E2E	End-to-End
ECN	Explicit Congestion Notification
EDCA	Enhanced Distributed Channel Access

GLOSSARY

ELFN	Explicit Link Failure Notification
ETT	Expected Transmission Time
ETX	Expected Transmission Count
FIFO	First In First Out
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMT-Advanced	International Mobile Telecommunications-Advanced
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LATP	Link Adaptive Transport Protocol
LPR	Low-cost Packet Radio
LTE	Long Term Evolution
MAD	Medium Access Delay
MAN	Metropolitan Area Network
MANET	Mobile Ad hoc Network
MHWN	Multi-hop Wireless Network
MIMO	Multi-Input Multi-Output
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OOO	Out-of-Order
P2P	Peer-to-Peer
PAN	Personal Area Network
PCF	Point Coordination Function
PF	Persistence Factor
PLR	Packet Loss Ratio
PN	Personal Network
POR	Packet Out-of-order delivery Ratio
QoS	Quality of Service
QSTA	QoS Station
RFC	Request For Comments
ROTT	Relative One-way Trip Time
RSSI	Received Signal Strength Indication
RTO	Retransmission Timeout
RTS/CTS	Ready To Send/Clear To Send
RTT	Round Trip Time

SC-FDMA	Single-Carrier Frequency-Division Multiple Access
SIFS	Short Interframe Space
SIG	Special Interest Group
SINR	Signal to Interference Plus Noise Ratio
SNR	Signal to Noise Ratio
SURAN	Survivable Radio Network
TCP	Transmission Control Protocol
TDD	Time-Division Duplex
TFRC	TCP-Friendly Rate Control
TI	Tactical Internet
TPSN	TCP Packet Sequence Number
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VANET	Vehicular Ad hoc Network
VCRH	Variance of Contention RTT per Hop
VoIP	Voice over IP
WAN	Wide Area Network
WiMAX	Worldwide Inter-operability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

GLOSSARY

Chapter 1

Introduction

In the past decade, we have been witnessing the proliferation of wireless devices as well as the user demand for ubiquitous computing. Wireless communications are becoming more and more popular among enterprise and home users and, are foreseen to play a key role in future communication systems. The primary advantages of wireless networks in comparison with their wired counterparts include flexible mobility management, faster and cheaper deployment, and ultimately easier maintenance. The Multi-hop Wireless Network is a network of nodes (e.g. computers) connected by wireless communication links. In this network, there are one or more intermediate nodes along the path that receive and forward packets for the other via wireless links. Therefore, as a subset of wireless networks, Multi-hop Wireless Networks inherit also these advantages. The number of applications for Multi-hop Wireless Networks grows up drastically in recent years.

The emergence of Multi-hop Wireless Networks has led to significant interest in multi-hop networking research. The primary research issue receiving a lot of attention is the performance of Internet widely used transport protocols, i.e. Transmission Control Protocol, over Multi-hop Wireless Networks. Generally, these transport protocols were firstly designed to work in wired line networks with the assumption that the network introduces a high bandwidth and very low channel error rate. However, the wireless medium and multi-hop characteristics of Multi-hop Wireless Networks exhibit a low shared bandwidth and a richer set of packet losses such as medium access contention drops, random channel errors and route failures which should be treated properly. Thus, these transport protocols suffer from performance degradation when they operate over Multi-hop Wireless Networks. Several solutions with different approaches have been proposed in order to improve the performance of transport protocols in Multi-hop Wireless Networks.

This dissertation concentrates on the cross layer improvement for rate-based transport protocols like TCP-Friendly Rate Control over Multi-hop Wireless Networks. Rate-based protocols are suitable for real-time streaming applications which are strictly constrained by low packet loss rate and small end-to-end delay. Nevertheless, these criteria are severely violated in Multi-hop Wireless Networks. Taking into consideration all the above factors, the aim of our work is to propose rate control schemes based on cross layer information which introduces reasonable packet loss rate and end-to-end

1. INTRODUCTION

delay for real-time streaming application in Multi-hop Wireless Networks. The performance of the proposed schemes is investigated thoroughly and in comparison with that of TCP-Friendly Rate Control. Various evaluation of throughput, packet loss rate, end-to-end delay and fairness are used to present the efficiency of the proposed algorithms in Multi-hop Wireless Networks.

The contributions of the thesis are summarized as follows:

- A metric classification. This is a multi-criteria and hierarchical classification which provides a survey and comprehensive definition of common metrics from Physical, MAC, Network and Transport layers. As metrics provide information about the state of the network, their role is very important in the cross layer approach. This classification thus furnishes an insight into the usage of metrics and then, some suggestions will be induced.
- A comparative study on the effectiveness of MAC metrics over Multi-hop Wireless Networks. The function of a MAC metric is to reflect effectively the problems at MAC level such as contention level or collision loss. This study introduces some novel MAC metrics and then provides several experiments to compare the effectiveness between these new metrics and some other typical ones. The results show that our novel metrics can be used as the effective and accurate indicators of MAC events.
- Rate control schemes for transport protocols in Multi-hop Wireless Networks. The design of these schemes is based on the information about the network states provided by MAC metrics in a cross layer manner. The first scheme uses one of our novel MAC metrics to predict the contention level along the connection path and then adjusts the sending rate accordingly. The second scheme uses two MAC metrics to obtain either the network contention level and the optimal effective bandwidth of the connection path. These schemes prevent the transport protocols from overloading the network, thus keep the network operating in an optimal point with low packet loss rate and small end-to-end delay.

The remainder of the thesis is as follows. Chapter 2 provides a review of the related literature. The metric classification is presented in Chapter 3. Chapter 4 is a comparative study on the effectiveness of MAC metrics over Multi-hop Wireless Networks. In Chapter 5 and Chapter 6, the designs of the rate control schemes are explained and their simulation evaluations are also presented. Finally, Chapter 7 concludes the thesis and provides some future research perspectives.

Chapter 2

Background study

In this chapter, a full review of the Multi-hop Wireless Network and the challenges for transport protocols over this kind of network is given. The overview of Multi-hop Wireless Networks is introduced at first. In this overview, the definition, the architecture and the characteristics of a Multi-hop Wireless Network are provided. After that, some common commercial wireless technologies which can be used to deploy Multi-hop Wireless Networks are also described. Among them, the technology based on IEEE 802.11 standard family is paid more attention since it is the technology on which this thesis concentrates. As the focus of this thesis is on the issue of transport protocols over Multi-hop Wireless Networks, this chapter gives a brief review for some commonly-used transport protocols, and the challenges with which they have to deal when they are naturally used in this kind of network. This chapter then provides a brief description of the improvement approaches for the above issue and gives some insights into the cross-layer approach.

2.1 Multi-hop Wireless Networks

2.1.1 Introduction

A Multi-hop Wireless Network (MHWN) is a network of nodes (e.g. computers) connected by wireless communication links. Due to the limited transmission range of the radio, many nodes may not be able to communicate directly to each other. Therefore, in MHWNs, there are one or more intermediate nodes along the path that receive and forward packets for the other via wireless links [4] [5] [6]. This is different with cellular networks and wireless local area networks (WLANs) where wireless communication only performs on the last link between a base station and the wireless terminal such as laptops or mobile-phones. MHWNs have several advantages compared to WLANs. MHWNs can extend the coverage of a network and improve connectivity in a cost-efficient way without a wide deployment of cables. MHWNs may reduce energy consumption since transmission over multiple short links may consume less power than that over one long range one-hop link. Moreover, there may exist several paths between nodes in a Multi-hop Wireless Network which improves the robustness of the network.

2. BACKGROUND STUDY

Historically, the DARPA Packet Radio Network (PRNet in 1972) [7] can be considered as the first concept of multi-hop (or ad hoc) networking. PRNet introduced a distributed architecture which allows to support the dynamic sharing of the broadcast radio channel. The advantages such as flexibility, mobility, resilience and independence of fixed infrastructure inspired from the design concept of PRNet attracted much attention of military and academic research domains. In 1983, DARPA developed Survivable Radio Networks (SURAN) as the evolution of PRNet [7]. SURAN was designed to address the issues of network scalability, security, processing capability and energy management. In the 1980s and early 1990s, several technologies were designed to improve the radio adaptability, security, and capacity such as Low-cost Packet Radio (LPR) in 1987, DARPA Global Mobile (GloMo) Information Systems program in 1994. In 1997, the US Army implemented the Tactical Internet (TI) which is a large-scale implementation of mobile wireless multi-hop packet radio network [8] [9]. To this end, with the fast growth up of commercial radio technologies and the user demand for ubiquitous computing, the Multi-hop Wireless Networks with its great potential and advantages has been becoming a very vibrant and active research field.

2.1.2 Architecture and applications of MHWNs

The Multi-hop Wireless Network may be referred to different names in different application scenarios. The Wireless Mesh Network (WMN) has been proposed to provide broadband Internet services for civilian users. This kind of network consists of mesh routers and mesh clients, where mesh routers are almost stationary and form the backbone of the network and communicate with mesh clients through wireless links [5]. Heterogeneous network technologies can be used to form a Wireless Mesh Network, including IEEE 802.11, IEEE 802.16 and cellular networks. Many factors can affect the performance of a Wireless Mesh Network such as the number of channels in use, the network topology, the node mobility and the density, etc.

Another type of Multi-hop Wireless Network is the Mobile Ad hoc Network (MANET) where each node is free to move independently in any direction [4]. The primary consequence of this free movement is that the topology in MANETs will change frequently. The paths between nodes, therefore, are destroyed and established from time to time during the network operation. Thus, the most investigated challenge in MANETs is to maintain routing information at each node.

A variant of MANET is the Vehicular Ad hoc Network (VANET) whose nodes are commonly transport vehicles [10]. The main difference between the two networks is that in VANETs, vehicles move in an organized fashion such as car routes rather than randomly. In Vehicular Ad hoc Networks, the vehicles' movement should follow some certain traffic rules, hence their mobility can be predicted in the short term. VANETs are commonly intended for safety applications and safety traffic where vehicles can inform each other the information of accidents or traffic jams.

Wireless Sensor Networks (WSN) are another emerging technology. In a Wireless Sensor Network, hundreds or thousands of small sensors communicate with each other through wireless links, thus can cover large geographic areas [11] [12]. Sensor data can be read using multi-hop networking between configured sensor nodes. The use of WSNs

2.2 Technologies for Multi-hop Wireless Networks

is to monitor physical and environment conditions, such as temperature, sound, pressure or motion. The operation of sensors are normally based on batteries. Therefore, the key design of applications used in Wireless Sensor Networks is energy efficiency.

Table 2.1 lists some applications of Multi-hop Wireless Networks [2].

2.1.3 MHNW challenges

Although the Multi-hop Wireless Network introduces several salient features, there exists also a number of issues that should be taken into consideration in Multi-hop (Ad hoc) networking [9] [13]. The deployment of Multi-hop Wireless Networks is infrastructure-less and without centralized administration. Every node in the network acts as an independent router which relays packets throughout the network. In MANETs, nodes also can move arbitrarily which in turns make the network topology change frequently. The topology control requires a proper transmission power adjustment scheme with minimal acceptable interference level. Many topology control algorithms such as location based, energy based, direction based, and critical neighbor based have been developed for this kind of networks [14] [15].

In MHWNs, each node may be equipped with one or more radio interfaces which may differ in transmission capability and frequency bands. The operation of the nodes in the networks is normally based on power limited batteries. Thus, designing routing algorithms in MHWNs is also a challenge as it is constrained by frequent mobility induced disconnection, lower consumption of energy, communications bandwidth, and computing resources.

The performance degradation of transport protocols over MHWNs is also a serious problem [16] [17] [18] [19] [20] [21]. This is mainly caused by the shared nature of wireless medium and a richer set of packet losses in MHWNs.

The security is another critical issue in ad hoc networking. The source of vulnerabilities comes from the shared nature of wireless channel and collaborative multi-hop communications among mobile nodes [22] [23].

In the past years, several wireless technologies have been released which enable to design from small to large scale Multi-hop Wireless Networks. The next section will give a brief introduction to some common commercial wireless technologies which can be used to deploy Multi-hop Wireless Networks.

2.2 Technologies for Multi-hop Wireless Networks

The Multi-hop Ad hoc Networks can be classified into several classes depending on their coverage area: Body Area Network (BAN), Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN) [9] [24] [25] [26]. Each class relies on some underlying wireless technologies. This section provides an overview of some common wireless technologies which are Bluetooth for PAN, IEEE 802.11 for WLAN and also WiMAX and LTE for MAN and WAN.

2. BACKGROUND STUDY

Table 2.1: Mobile Ad hoc Network Applications [2]

Application	Possible scenarios/services
Tactical networks	<ul style="list-style-type: none"> - Military communication and operations - Automated battlefields
Emergency services	<ul style="list-style-type: none"> - Search and rescue operations - Disaster recovery - Replacement of fixed infrastructure in case of environmental disasters - Policing and fire fighting - Supporting doctors and nurses in hospitals
Commercial and civilian environments	<ul style="list-style-type: none"> - E-commerce: electronic payments anytime and anywhere - Business: dynamic database access, mobile offices - Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks - Sports stadiums, trade fairs, shopping malls - Networks of visitors at airports
Home and enterprise networking	<ul style="list-style-type: none"> - Home/office wireless networking - Conferences, meeting rooms - Personal area networks (PAN), Personal networks (PN) - Networks at construction sites
Education	<ul style="list-style-type: none"> - Universities and campus settings - Virtual classrooms - Ad hoc communications during meetings or lectures
Entertainment	<ul style="list-style-type: none"> - Multi-user games - Wireless P2P networking - Outdoor Internet access - Robotic pets - Theme parks
Sensor networks	<ul style="list-style-type: none"> - Home applications: smart sensors and actuators embedded in consumer electronics - Body area networks (BAN) - Data tracking of environmental conditions, animal movements, chemical/biological detection
Context aware services	<ul style="list-style-type: none"> - Follow-on services: call-forwarding, mobile workspace - Information services: location specific services, time dependent services - Infotainment: touristic information
Coverage extension	<ul style="list-style-type: none"> - Extending cellular network access - Linking up with the Internet, intranets, etc.

2.2.1 Bluetooth

Bluetooth [27] is a short-range radio technology that enables wireless connectivity between mobile devices. The design goals for Bluetooth are simple, small size, minimal power consumption, and low price. Bluetooth was first created by telecoms vendor Ericsson in 1994 and is managed by Bluetooth Special Interest Group (SIG) which has more than 14,000 member companies [27]. The current released version is the Bluetooth v4.0. Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. Depending on the equipped radio class, the communication range of Bluetooth is from 1 m up to 100 m. According to the latest report from Bluetooth SIG [27], about 7 billion cumulative Bluetooth products have been in the market by the end of 2011. This number is expected to grow in the next few years thanks to the technology's economic and easy to use features. In fact, Bluetooth is becoming the most economically feasible short-range wireless technology to implement nowadays.

2.2.2 Wireless Local Area Networks

Wireless Local Area Network (WLAN) technology has evolved to extend to existing local wired networks and is based on IEEE 802.11 standards [28] where two or more devices can communicate with each other in a wireless manner. The communication range normally is short, from few meters to hundred meters. To date, there have been four commonly used 802.11 standards which are different in performance, frequency and bandwidth as showed in the Table 2.2 below

Table 2.2: IEEE 802.11 standards

802.11 standard	Frequency band	Bandwidth
802.11a	5 GHz	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	2.4 GHz	5.5, 11 Mbps
802.11g	2.4 GHz	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11n	2.4 GHz, 5 GHz, 2.4 or 5 GHz (selectable), 2.4 and 5 GHz (concurrent)	Up to 450 Mbps

Except for 802.11b which uses Direct-Sequence Spread Spectrum (DSSS), the others use Orthogonal Frequency-Division Multiplexing (OFDM) technique to achieve their high bit rates. All of them use the same medium access mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in order to minimize the collision. Today, the commercial wireless 802.11 products, branded Wi-Fi [29], exist everywhere in our daily life as there has been an explosion of increasing user demand for wireless connectivity for the past 10 years. Some more 802.11 standards are also under development in order to catch the trend of 4G technology.

The IEEE 802.11 wireless LAN standard defines a structure called the basic service set (BSS) containing at least two stations in communication with one another. Two types of BSSs correspond to the two operation modes of WLANs: infrastructure-less

2. BACKGROUND STUDY

(or ad hoc) and infrastructure-based. The first structure is the independent BSS (IBSS) which involves stations communicating directly with one another, with no center administration required. The stations in this structure communicate with other stations in the BSS in an independent (ad hoc) manner. The operation of WLANs in this manner is called infrastructure-less mode. The second type of BSS is somewhat similar to the concept of a cell in cellular systems, corresponding to infrastructure-based operation mode. In this mode, stations within each BSS communicate only with a special station associated with each BSS and called an access point or AP. The AP thus plays the role of a server which relays messages to and from other BSSs. With this design, multiple BSSs may combine to form an extended network, or may be connected to external wired LANs such as Ethernets.

IEEE 802.11 wireless LAN standard defines two medium access schemes for packet transmission: DCF (Distributed Coordination Function) and PCF (Point Coordination Function) [28]. The PCF is implemented on top of DCF and is based on a polling scheme which cyclically polls stations, giving them the opportunity to transmit. Since the PCF cannot be adopted in the ad hoc mode, only DCF is taken into consideration in this thesis.

The DCF provides a contention-free service based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. Two access methods are defined which are the basic access and the four-way handshake RTS/CTS (Ready To Send/Clear To Send) access. The basic access is a simplified version of RTS/CTS which is used for “small size” packets. With rather “large” packet which may have higher probability of transmission collision, the RTS/CTS mechanism of DCF is used to solve the problem as shown in Fig. 2.1.

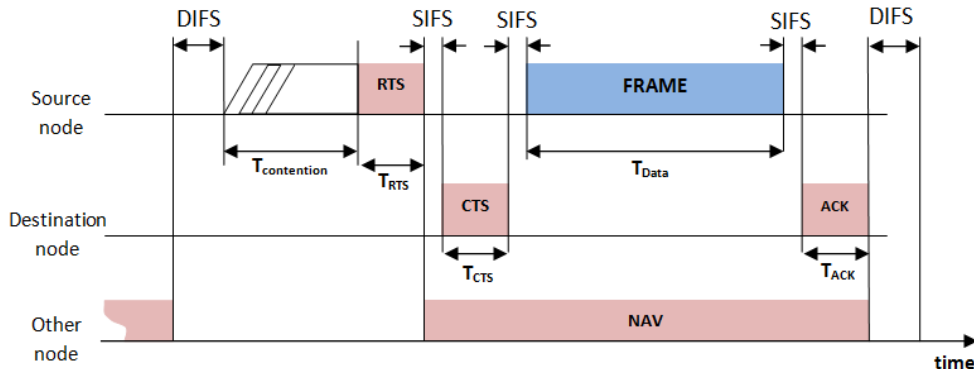


Figure 2.1: IEEE 802.11 basic medium access mechanism and data delivery procedure

In Fig.2.1, T_{RTS} , T_{CTS} , T_{DATA} and T_{ACK} represent respectively the propagation time for RTS, CTS, DATA and ACK packets. NAV is the reserved channel time indicated by RTS or CTS packets. $T_{contention}$ is the contention delay for a transmission opportunity which consists of backoff time and total freeze periods during the backoff stage. $SIFS$ and $DIFS$ are two predefined time intervals in the standard and $SIFS < DIFS$.

A station senses periodically the channel idle to obtain a transmission opportunity. If the channel is idle for $DIFS$ of time, the station invokes backoff mechanism [28] to

2.2 Technologies for Multi-hop Wireless Networks

minimize collision before sending a packet. If the channel becomes busy during backoff stage, the station freezes the backoff process. If the channel is idle and the backoff counter reaches zero, the station starts transmission in basic manner if the packet size is smaller than a `RTSThreshold`. Otherwise, the station exchanges RTS and CTS packets with the destination before sending the data packet while stations in its neighborhood use the two packet to set their Network Allocation Vector which means that an amount of channel time will be reserved. DCF has an ARQ mechanism [28] to enable reliability at MAC. Thus, when receiving a packet correctly, the destination MAC entity waits for an interval of *SIFS* immediately after the reception has completed and transmits a MAC acknowledgement (MACK) back to the source MAC entity to confirm the correct reception. If the source MAC entity does not receive the MACK due to collision or transmission errors, it re-triggers the backoff algorithm after the channel remains idle for an amount of time interval. The packet transmission operation terminates either by the source MAC entity receiving correctly the desired MACK or dropping the packet after the number of failed retransmission attempts exceeds a predefined parameter in the standard called `RetryLimit`.

2.2.3 Worldwide inter-operability for Microwave Access

The Worldwide Inter-operability for Microwave Access, or WiMAX, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard, which is also called WirelessMAN [30]. To this end, two standard specifications for WiMAX have been published, IEEE 802.16-2004 [30] for fixed broadband wireless access and IEEE 802.16-2009 [31] for both fixed and mobile broadband wireless access. WiMAX physical layer is based on OFDM for both downlink and uplink and its data rates can be up to 25 Mbps for downlink and 6.7 Mbps for uplink when operating using a 10 MHz spectrum and TDD (Time-Division Duplex) scheme [32]. Some other salient features of WiMAX are scalable bandwidth and data using OFDMA (Orthogonal Frequency-Division Multiple Access), support for advanced antenna techniques, provision of Quality of Service (QoS), support for mobility and IP-based architecture [32]. As a report of WiMAX Forum in May 2011 [33], there were total of 583 WiMAX deployments in 150 countries with more than 823 million subscribers.

WiMAX is sometimes marked as 4G. However, since its current version does not fulfil the International Mobile Telecommunications-Advanced (IMT-Advanced) requirements [34] for 4G standards, in which the required peak data rates are 100 Mbps for high mobile communication and 1 Gbps for low mobile communication, WiMAX is now referred to as pre-4G technology. Another IMT-Advanced compliant version of WiMAX under development is WirelessMAN-Advanced [34]. This version is based on IEEE 802.16m standard [33].

2.2.4 Long Term Evolution

LTE stands for Long Term Evolution of UMTS (Universal Mobile Telecommunications System), which is a standard for wireless data communications technology developed

2. BACKGROUND STUDY

by the 3rd Generation Partnership Project consortium (3GPP) [35]. The goal of LTE is to provide not only high bit rates, but also less delay for connection establishment and transmission, more flexible spectrum usage, simplified network architecture, more support for mobility and reasonable mobile power consumption. As WiMAX [30], LTE is referred as a pre-4G technology since its shared peak rate capacity is 100 Mbps in the downlink and 50 Mbps in the uplink within a 20 MHz bandwidth [36]. The multiple-access schemes used in LTE are OFDMA for downlink and SC-FDMA (Single-Carrier Frequency-Division Multiple Access) for uplink. The downlink of LTE is also designed to support MIMO (Multi-Input Multi-Output) operation to achieve high peak data rates. The LTE standard was finalized in December 2008 and one year later, the Sweden's telephone company TeliaSonera launched its first LTE service in Stockholm and Oslo. To this end, the commercial LTE service was deployed in many countries all over the world.

In order to fulfil the requirements of IMT-Advanced [34], 3GPP develops an enhanced LTE standard called LTE Advanced with theoretical peak rates of 1 Gbps in downlink and 500 Mbps in uplink. Furthermore, LTE Advanced aims at providing higher efficiency, user fairness, heterogeneous network support and some other performance enhancements [35]. The latest 3GPP specification for LTE Advanced is Release 10 and will continue to be developed in subsequent 3GPP releases.

Among these technologies, Wi-Fi, the trade mark technology of IEEE 802.11-based standards, is becoming one of the most commonly used technology for daily wireless data communication. The Multi-hop Wireless Networks based on IEEE 802.11 standard [28] has drawn much researchers' attention for the past few years.

The objective of the thesis is to improve the transport protocol operation over MHWNs. Hence, a review of the main transport protocols and then their problems over MHWNs will be presented in the next sections.

2.3 IETF Transport Protocols

In general, the Transport protocols provides end-to-end communication services for applications over the network. Their main functions are to encapsulate the applications' data into segments which are suitable for transmission through the network (multiplexing), to manage the transmission operation and to delivery the payload inside the segments to the appropriate applications at the destination host (demultiplexing). The following section will provide an overview of some commonly used transport protocols in the today Internet.

2.3.1 Transmission Control Protocol

Today, TCP is the most commonly used transport protocol in the Internet and carries more than 90% of the traffic and 80% of the total number of the flows in the Internet [37] [38]. Transmission Control Protocol (TCP) provides a connection-oriented, reliable data transmission between the source and the destination. The original specification for TCP is RFC 793 [39], although some errors have been corrected in the later RFCs

[40] [41] [42] [43]. There are several developed versions of TCP, and TCP Reno [40] is the most widely used version in the Internet.

In TCP Congestion Control specification [40] [44], four congestion control mechanisms are defined: slow start, congestion avoidance, fast retransmit and fast recovery. The slow start and congestion avoidance mechanisms are used to control the amount of outstanding data being injected into the network. The congestion window, “cwnd”, represents the number of packets that are allowed to be transmitted without getting acknowledged. TCP connection starts with the slow start phase where the initial cwnd is not more than 2 segments. In this phase, for each received acknowledgment (ACK), the TCP sender increases the cwnd by one segment until it reaches the slow start threshold (ssthresh). After that, the TCP sender enters into the congestion avoidance phase during which the rate increases roughly one segment per Round Trip Time (RTT). The size of cwnd is also limited by the receiver’s advertised window, which is the maximum window size requested from the receiver TCP. The TCP sender stops the congestion avoidance whenever it detects a segment loss either by receiving three duplicate acknowledgements (ACK) or by retransmission timeout (RTO). If the loss is detected, the fast retransmit and fast recovery mechanisms work together to retransmit the lost packet and to reset the threshold ssthresh. The TCP sender then turns back to slow start phase if the loss is detected by RTO, or congestion avoidance phase if the loss is detected by duplicate ACKs.

Although TCP provides mechanisms for flow control, the fairness and effectiveness of sharing a bottleneck is inversely proportional to the number of TCP flows. TCP also suffers from performance degradation when the number of active TCP flows exceeds the network bandwidth-delay product [45]. The TCP congestion control mechanisms do not also consider delay requirement of non-elastic application. To this end, many modifications have been introduced to TCP by both IETF and researchers’ efforts in order to meet the new constraints and requirements for the increasing number of systems and applications in the proliferation of today Internet.

2.3.2 User Datagram Protocol

User Datagram Protocol (UDP), formally defined in RFC 768 [46], is a transport protocol designed for applications having simple exchange such as the Domain Name System (DNS), Voice over IP (VoIP) or streaming media IPTV. UDP is a protocol much simpler than TCP. It is a connectionless protocol as it does not have the connection establishment phase. UDP does not provide reliability transmission since the communication is achieved by transmitting information in one direction from source to the destination. The sending rate of UDP is also not regulated. Instead, its rate depends on the rate at which the application generates data and the bandwidth of the network. Another characteristic is that UDP has only 8 bytes of overhead in every segment while that of TCP is 20 bytes. Reliable protocols like TCP have congestion control mechanism to prevent transmission links from excessive congestion. Nevertheless, this mechanism can have a severe impact on real-time applications such as VoIP or streaming of stored audio and video, which can tolerate some packet loss but is very strict to end-to-end delay. All of the aforementioned features make UDP become so far one of the most widely used transport protocol for multimedia and real-time applications. However, in

2. BACKGROUND STUDY

a network, the lack of congestion control is a potentially serious problem. If there are many users in the network starting streaming with high bit rate, the network will soon be overloaded, routers will have to drop packets and then the quality is not guaranteed.

2.3.3 TCP-Friendly Rate Control

TCP-Friendly Rate Control (TFRC) [47] is a congestion control scheme which is reasonably fair when competing for bandwidth with TCP flows, but has a much lower variation of throughput over time, comparing with TCP. TFRC does not enable reliable and in order data delivery services and is specially designed to carry multimedia streams where a relatively smooth sending rate is of importance. The major difference between TFRC and TCP is the fact that TCP is a complete transport protocol which support features like flow and congestion control as well as connection establishment, while TFRC just takes care of congestion control and is intended to be used by a transport protocol that provides an unreliable data transmission, i.e., Datagram Congestion Control Protocol (DCCP) [48].

Since one of the most important goals of TFRC is reaching TCP-friendly behaviour which means using no more bandwidth than a TCP flow under same conditions in steady state, TFRC utilizes the throughput equation of TCP for its congestion control mechanism [47].

$$R = \frac{S}{RTT\sqrt{\frac{2bp}{3}} + RTO(3\sqrt{\frac{3bp}{8}})p(1 + 32p^2)} \quad (2.1)$$

where R is the TCP's average transmission rate in bytes per second, S is the segment size in bytes, RTT is the round-trip time in seconds; RTO is the TCP retransmission timeout value in seconds, b is the maximum number of packets acknowledged by a single TCP acknowledgement, and p is the packet loss rate. As recommended in [47], one should set $RTO = 4 * RTT$ and $b = 1$. Thus, there are only two parameters RTT and p that influence the transmission rate R .

TFRC uses its sophisticated mechanisms to gather the equation parameters. RTT is measured by sending feedback time stamps to sender. The TFRC sender also attaches its estimated RTT to the data packet transmitted to the receiver in order to help the receiver to calculate the packet loss rate. The packet loss rate estimation is carried out by computing the average loss interval. [47] defines the term "loss event" such that if two packet losses are in the same loss event, the time scale between them is smaller than one RTT . Thus, the packet loss rate is measured via loss intervals by tracking the number of packets between consecutive loss events. TFRC keeps a history of n most recent loss intervals to calculate the average loss interval in such a way that old loss intervals contribution in this average is less. The TFRC specification [47] recommends to use $n = 8$ with their contribution weight from the most recent interval are of $\{1, 1, 1, 1, 0.8, 0.6, 0.4, 0.2\}$ respectively. The loss rate is considered as the inverse of the average loss interval size. Beside packet loss rate p , the receiver also estimates the receiving rate and attaches these two important parameters to the feedback to the sender. The rate calculated by the equation 2.1 and the receiving rate are used to

determine the new sending rate.

The smoothness of the sending rate is maintained by some additional mechanisms which prevent TFRC from responding aggressively to single loss events, and to guarantee that the sending rate adapts quickly to the long intervals that are loss-free.

After starting the connection, TFRC steps directly into a slow-start phase just like TCP in order to increase its rate to reach a fair share of bandwidth. The slow-start phase is ended when the sender receives a report of loss event. TFRC receiver updates the equation parameters and feeds them back to sender at least once per round-trip time RTT and every time a loss starting a new loss event. Hence, the recalculation of the sending rate for TFRC is performed at least once per RTT.

TFRC's main advantage is its stable and smooth sending rate variations. This feature fits in the media application transmission besides being responsive to the co-existing traffic in a TCP-friendly manner. Despite smoother throughput, TFRC responds slower than TCP to the changes in the available bandwidth. Therefore, for applications that simply need to transfer as much data as possible, TFRC is not recommended.

2.3.4 Datagram Congestion Control Protocol

Datagram Congestion Control Protocol (DCCP) [48] is a IETF standardized unreliable transport protocol with end-to-end congestion control. DCCP is intended to use with multimedia applications such as streaming or on-line gaming, where the real-time constraint is most important and packet retransmissions are uninteresting. DCCP aims to be a general-purpose transport-layer protocol with two main functions: (1) The establishment, maintenance and tear-down of an unreliable packet flow; and (2) congestion control of that packet flow. DCCP also provides a standard way to implement congestion control and congestion control negotiations for special applications.

DCCP has several interesting features. First of all, DCCP allows applications choosing from a set of congestion control schemes. Each congestion control scheme has a unique identifier denoted by *CCID*. Currently, two options are available in DCCP specification [48]. The first one is TCP-Like Congestion Control with *CCID* = 2 which halves the congestion window in response to a packet loss, similarly to TCP. Applications using this scheme will respond quickly to the network congestion state, but they suffer from abrupt changes in the sending rate. The second one is TCP-Friendly Congestion Control or TFRC with *CCID* = 3. This scheme maintains a relatively smooth sending rate and long-term fairness with TCP. Like TCP, DCCP has connection setup and teardown phases but provides an unreliable delivery of data flows, with acknowledgements. This acknowledgement contains information about received packets as well as packets which are Explicit Congestion Notification (ECN) marked, corrupted, or dropped at the receiver side. Beside allowing applications choosing congestion control scheme, two DCCP endpoints can also negotiate properties for connection by a reliable procedure. DCCP also introduces a low per-packet overhead, with only 12 bytes generic header for every packet. DCCP enables option mechanism similar to TCP. The options are appended to the end of DCCP header and used for acknowledgement reporting and parameter negotiation.

2. BACKGROUND STUDY

Nowadays, with the sharp increase of the demand for applications such as radio-streaming, IP-TV, VoIP and massive multiplayer online games, the UDP traffic in the Internet has becoming massive which may lead to the unstable operation of the Internet. Even though some applications have their own congestion control mechanism, DCCP with its salient features is one of the best solution for the Internet in this context. In fact, Linux had implemented the first release of DCCP in its kernel version 2.6.14-released in October, 2005.

Generally, all of the aforementioned transport protocols in this section were firstly designed to work in wired line networks. Thus, their operation is based on the assumption that the network introduces a high bandwidth and very low channel error rate. Today, wireless communication is getting very common with the matureness of wireless technologies as well as the fast increasing demand of ubiquitous computing. The Internet predominant transport protocols face the performance degradation challenge when they are naturally used in wireless networks since this kind of network provides a small and shared bandwidth with high channel error rate. The next section will provide insights into this problem.

2.4 Transport Protocols over Multi-hop Wireless Networks

Although the Multi-hop Wireless Network has several advantages, it also introduces a number of characteristics, complexities, and design constraints that are specific to wireless environment and complicated by ad hoc networking. This section presents some remarkable problems for Internet transport protocols when they are used in MHWNs.

2.4.1 The Challenges in MHWNs

Multi-hop Wireless Networks have gained a lot of attention in recent years, both in the industry as well as the research community as these networks are flexible and resilient. The performance of Internet predominant transport protocols, i.e. TCP, in MHWNs has become a popular research domain as a consequence.

The primary problem of congestion control based transport protocols like TCP over Multi-hop Wireless Networks is that they suffer from severe throughput degradation. This comes from the wireless and multi-hop characteristics of such network.

A fundamental issue in MHWNs is that the performance degrades sharply as the number of path hops increases. For example, in a network of nodes with identical and omnidirectional radio ranges, the throughput of a flow is halved with a two hop path compared to that with single hop path. The reason comes from the rule of the wireless medium access scheme that only one of the 2 hops can be active at a time. The works [49] [50] [51] [52] provided the estimation of the per node capacity to be expected in an Wireless Ad hoc Network. In a Wireless Ad hoc Network with a chain of nodes, the overall capacity of the network ranges from 1/7 to 1/4 of the raw channel bandwidth obtained from the radio. In addition, if the nodes are randomly located, the transmission range of nodes is fixed and the transmission rate is W bps, then the per node throughput for a randomly chosen destination is $\Theta\left(\frac{W}{\sqrt{n}\log n}\right)$ bps.

2.4 Transport Protocols over Multi-hop Wireless Networks

Even under optimal circumstances, where nodes' placement, the transmission range and traffic pattern are optimally chosen, the end-to-end throughput available to each node is $\Theta\left(\frac{W}{\sqrt{n}}\right)$ bps. The reason for this limitation of capacity in Wireless Ad hoc Networks is the share nature of wireless medium in wireless environment. This means that each node can not fully utilize all the channel but share it with other nodes lying in its local neighborhood.

In addition to the limited wireless bandwidth, a number of factors in MHWNs further reduce the performance of transport protocols. In wireless environment, the bit error rate (BER) is high because of the fading and interferences in wireless channels and this may cause several packet losses other than dropped by queue overflow. The existing congestion control mechanisms often assume that each packet loss indicates network congestion and triggering the congestion control mechanism affects the throughput and link utilization.

The hidden node and exposed node problems existing in IEEE 802.11 DCF are also the reasons of throughput degradation. The exposed node problem indicates that two nodes lying in the carrier sensing range of each other can not transmit at the same time. Thus, nodes within the transmission range of other nodes are unable to receive a correct RTS or respond with a CTS, which causes these nodes to be penalized by other nodes' transmission. Then the channel resource can not be fully utilized which leads to performance decrease. The hidden node problem mentions that the concurrent transmissions of two nodes not lying in the carrier sensing range of each other may cause a collision at a node which lies in both transmission ranges of each one. Both problems may cause the MAC layer report wrongly to the upper layer that there is a link breakage. Then a route failure event occurs. The network layer has to trigger route recovery mechanism which may cost several seconds. This route recovery period is relatively longer than the time RTO of transport protocols, it will cause the cutting down the sending rate of the traffic source or freeze the operation in a certain time. Hence, the throughput decreases. These two problems are studied thoroughly in [53] [54].

Beside the throughput problem, TCP flows present a severe unfairness in the MHWNs, which is the result of the joint interactions of TCP, MAC layer protocol and queuing type at the router. At the network layer, an unfair packet-dropping scheme, such as FIFO drop tail scheme, causes some flows experiencing more losses than the others. At MAC layer, the Binary Exponential Backoff scheme of DCF favours the latest successful nodes, which occupy the channel persistently and let other flows starve of the resource or even stop transmission completely [53] [55]. The combination of Backoff scheme and collision losses causes severe unfairness issues between congestion control transport flows, i.e. TCP. TCP's timeout and backoff schemes further worsen the unfairness [53] [56].

All of these problems come from the fact that the common Internet protocols were designed to work in wired networks while communication in wireless networks is essentially different with that in wired networks. The time-varying nature of the channel, the impact of interference, the intricacies of MAC protocol scheduling, and the self-interference [53] [57] [58] among packets as they are relayed down multi-hop wireless paths [59] combine to restrict the use of conventional approaches for these protocols.

2. BACKGROUND STUDY

Transport protocols like TCP usually misbehaves in MHWNs by overloading the network which in turn exacerbates the contention problem. As the contention becomes serious, queueing delay, backoff and transmission delays and collision losses increase while the throughput decreases. Thus, to achieve the expected performance of transport protocols in MHWNs is a challenging issue that requires significantly different solutions that are aware of the characteristics of MHWNs. The next section will provide a brief review of the improvement approaches so far.

2.4.2 The Improvement Approaches of Transport Protocols in MHWNs

In the past few years, several improvement schemes have been proposed for transport protocol in Multi-hop Wireless Networks. The first type of approach is that the transport protocols rely on end-to-end information to respond to network events. For example, TCP Detection of Out-of-Order and Response (DOOR) [60] proposed an end-to-end mechanism based on out-of-order (OOO) delivery events. OOO events are interpreted as an indication of route failure. The receiving node can notify the sender about detected out-of-order data packets by two bytes TCP option, called TCP Packet Sequence Number (TPSN). The sender itself may notice ACKs arriving out-of-order by one byte option added to ACKs called ACK Duplication Sequence Number (ADSN). When out-of-order packets are detected, the sender temporarily disables TCP's congestion control mechanisms and instant recovery during congestion avoidance. The expected effect is that after the "wrong" changes to TCP's parameters are reverted, the connection continues to operate as if no route change had occurred.

Fu et al. in [61] proposed an end-to-end approach of combining multiple metrics instead of relying just on a single one, called ADTCP. The authors claimed that the use of metric combination prevents the network indicator measurement from noisiness in ad hoc networks. The receiver uses four metrics: inter-packet delay difference, short-term throughput, out-of-order packet arrivals and packet loss ratio to detect network congestion, route changes and channel errors. The estimated current network states are then fed back to the sender by its feedbacks. The sender then performs appropriate mechanisms accordingly.

In the second type, cross-layer approach, the proposals rely on the information provided by other layers such that upper layer protocols may take into account lower layer information to keep the network load at a reasonable level or in contrast, lower layers may be provided with upper layer information to guarantee the quality of service (QoS) [62] [63] [64] [65]. A transport protocol then can collect information not only from the layer its belongs to, but also from lower layers in order to accurately estimate the network condition, thus better operates in MHWNs.

Holland et al. [17] proposed to use the Explicit Link Failure Notification (ELFN) techniques to improve the TCP performance. In this proposal, the route failure notifications are informed to the transport layer by piggybacking the ELFN message onto a route failure message sent by the routing protocol, or to use "host unreachable" Internet Control Message Protocol (ICMP) message. Upon receiving the ELFN message, the TCP source disable its retransmission timers and enters a "standby" mode. During

2.4 Transport Protocols over Multi-hop Wireless Networks

the standby period, the TCP sender sends probe packets in regular intervals to check if the route is restored. The TCP sender leaves the “standby” mode as soon as it receives the acknowledgement for the probe packet.

ATCP [66] is another proposal which exploits the network layer feedback. The main contribution of ATCP is to handle route failures, longer periods of disconnection and to distinguish congestion-related from other losses. ATCP is implemented as a layer inserted between the TCP and IP layers. ATCP listens to the network state information provided by Explicit Congestion Notification (ECN) [42] and ICMP message, then it puts TCP agent into the appropriate state which are persist, congestion control and retransmit states. If no ECN message is received, then the detected loss is interpreted as channel error induced.

Another common approach for transport protocols in MHWNs, which is the main focus of this thesis, is cross-layer between Transport and Link (MAC) layers. Since end-to-end information is not sufficient enough to solve the problems in Multi-hop Wireless Networks, the proposed schemes in this approach have a common ground that they try to exploit the MAC layer information to have better knowledge about what happens at lower layers [67] [55] [54] [68] [69]. This information is then sent up to transport layer in a cross-layer manner and is used in various ways to improve the transport protocols. The classification of the proposals and their brief description will be explained in the next section.

2.4.3 Cross-layer between Transport and Link layers

As mentioned in the previous section, lower layers’ information is collected to form metrics and then is submitted to the upper layer to improve the operation of transport protocols. In our work, these metrics are classified such that they may fall into following categories: packet delay, traffic load, transmission and retransmission attempt numbers. Two issues should be taken into consideration. The first issue is the MAC metrics used to indicate the network state at lower layers. The more information of lower layers to the transport layer the metric provides, the more efficiently the transport protocol controls the traffic rate. The second issue is the rate control scheme which uses the MAC metrics to improve the performance of transport protocols in MHWNs.

Li et al. [67] propose a mechanism which enables TFRC to estimate the optimal network load level by considering the MAC layer contention. An optimum round-trip time is computed as a total transmission time of every link on the path, in which the link transmission time is estimated depending on a model based on network topology and equivalent loss event rate at MAC. The current RTT is then compared to this optimal value to estimate the contention level and adjust the traffic rate accordingly. However, there is a doubt about the accuracy of the scheme since it assumes that the traffic at each hop is independent, thus the cumulative delay for the Multi-hop network can be the total of all the delays of every hop. In addition, the evaluation results are limited to simple chain topology. We do not know how it works in more complex scenarios such as grid or random topologies.

To obtain the channel utilization information, Zhai et al. [55] collect the *channel busyness ratio* computed at each node and then estimate the network available band-

2. BACKGROUND STUDY

width. The estimated value is attached to every packet so that it can reach to the destination. This information is then used to adjust the traffic pumped into the network. This scheme provides a relative simple method to estimate the available throughput in MHWNs, enables a faire throughput between TCP flows sharing the same bottleneck along the path and increases the overall network throughput. However, beside the MAC channel busyness ratio provided up to Transport layer, the proposed scheme also requires that the MAC layer has to be provided with some transport information such as the packet sending rate. This is inapplicable in the fact. Generally, the higher layer can get information from MAC layer, i.e. using the network card driver, while the MAC layer can not access to header's fields of arrived packets to obtain Transport or Network layers' information. In addition, the channel busyness metric does not deal with the hidden node problem which is very common in MHNW's environment. This metric also requires an assumption that the collision probability $p \leq 0.1$ [55], which occurs in non saturated state, i.e. the average packet queue of each node almost equals 0 [70]. But in fact, the network often operates in saturated state, i.e., each node always has packets in the queue [70], because of the hidden node problem and complex traffic patterns throughout the network.

To overcome these shortcomings, Navaratnam et al. [54] proposed to use a metric named *permissible throughput*, which is the combination of channel busyness ratio and effective throughput computed at each node, to assess the current network capacity in terms of both channel utilization and collision level. Thus, this proposed metric takes into account the hidden node problem. The scheme also provides a relatively smooth rate control which is suitable for real time applications. Nevertheless, the load at each link is contributed by several flows passing across it. So the available bandwidth should be fairly shared between them. But in the proposed Link Adaptive Transport Protocol (LATP), each flow increases its sending rate with an amount of available bandwidth reported by feedback packets. This increase is sometimes too large and the total traffic increase from all of the flows may quickly overload the network.

To derive contention level along the packet path, Hamadani et al. [68] proposed to calculate periodically the MAC service time from all hops along the path. Four congestion control stages have been defined as fast probe, slow probe, light contention and severe contention. The TCP receiver compares the total MAC service time of the path and throughput of two consecutive intervals to determine the current network state. Depending on the comparison result, the proposed congestion control scheme applies one of the four predefined stages to adjust the sending rate. The authors proposed a rather complicated scheme but it seems to be not accurate enough to take into account all network situations.

Zhang et al. [69] split the round trip time RTT into two parts - congestion RTT and contention RTT. The congestion RTT is the end-to-end transfer delay of all the links, while the contention RTT is the total contention delays through the path. They then proposes a MAC metric named VCRH (Variance of Contention RTT per Hop) which depends on the variance of the contention RTT along the path. The TCP protocol uses this metric to control the congestion window *cwnd* such as whenever the sender receives an ACK with VCRH exceeding a threshold, the *cwnd* is decreased instead of an increase. The proposed scheme provides a good early signal of congestion and a simple and steady window adaptation mechanism. However, this metric considers only

the variation of the contention RTT but not the true contention level of the network which sometimes may already be high and not vary largely.

Ma et al. [71] measure the contention level at a node by using a metric called Backoff Stage Ratio (BSR). BSR is the ratio of the number of backoff stages performed after failed transmission and sensing channel busy to the total of that number and those after finishing successful transmissions. The first packet in the queue will be dropped/marked with a probability based on BSR. The packet drop/mark probability is calculated based on the comparison between the average BSR and its two predefined thresholds. The dropped/marked packets will provide an early indication of network congestion, thus improve the TCP performance in MHWNs. This scheme makes use of the ECN-enabled TCP to improve TCP performance. It also uses only local and reliable information in each node, thus reduce the computation overhead. However, this scheme works well only with ECN-enabled transport protocols which are not as common as those without ECN-enabled. Another disadvantage of BSR is that it does not reflect the network situation such that the contention level around a node is also high due to several nodes having packets to transmit, thus increase the backoff freeze time, but may not cause severe collision.

Table 2.3 shows in brief the proposal classification mentioned above.

2.5 Summary

In this chapter, the Multi-hop Wireless Network, its salient features and taxonomy are introduced. Wireless technologies which support multi-hop wireless architecture such as Bluetooth, Wi-Fi, WiMAX and LTE are also presented.

As the thesis concentrates on the performance of transport protocols over MHWNs, this chapter provides a brief review of some commonly used transport protocols such as TCP, UDP, TFRC and DCCP. After that, the performance degradation challenge for transport protocols over MHWNs is investigated. This chapter also provides an overview of improvement approaches for this problem. Among them, the cross layer between Transport and Link (MAC) layers is the approach applied in this thesis. In the cross layer approach, lower layers' information is collected to form metrics and then is submitted to the upper layer to improve the operation of transport protocols. Thus, to clarify the approach of the thesis, a taxonomy of cross layer solutions is made based on metric information.

As metrics provide information about the state of the network, their role is very important in the cross layer approach. Thus, in the next chapter, a multi-criteria and hierarchical classification of the metrics not only collected from MAC layer, but also other layers, i.e. Physical, Network and Transport, will be introduced.

2. BACKGROUND STUDY

Table 2.3: Cross-layer proposal classification table

Classification criteria	Metrics	Control mechanisms	Advantages	Disadvantages
Delay based	<ul style="list-style-type: none"> - [67]: optimal Round-trip time r_{opt} - [68]: contention delay CD - [69]: contention round-trip time RTT_{cont} 	<ul style="list-style-type: none"> - using r_{opt} to estimate the optimal network load level, thus adjust the sending rate accordingly - using the change of CD and throughput to determine the network state and apply the correspond control stage - If $VCRH$ is greater than a predefined threshold, decrease $cwnd$ instead of increase 	<ul style="list-style-type: none"> - rather simple computation for r_{opt} and expected rate - reduce the TCP intra-flow interference - good early congestion indication - a simple and steady window adaptation mechanism 	<ul style="list-style-type: none"> - delay model is not accurate enough - less results - rather complicated scheme - not reflect well the network situations - not reflect the situation where the contention level is already rather high but not vary largely
Load based	<ul style="list-style-type: none"> - [55]: channel busyness ratio r_b - [54]: permissible throughput P 	<ul style="list-style-type: none"> - each flow rate increases or decreases depending on its current load and the available bandwidth estimated by r_b - the smallest P along the path is submitted to the traffic source - if $p > 0$, it is the amount of traffic the sender can pump into network; else the sender decreases rate with a factor 	<ul style="list-style-type: none"> - simple estimation for available bandwidth - increase fairness among flows - take into account the hidden problem - rather smooth rate control 	<ul style="list-style-type: none"> - not take into account the hidden node problem - require transport information present at MAC layer - each flow increases their rate with an amount of the network available bandwidth, thus the aggregate traffic may quickly overload the network
Transmission attempt based	<ul style="list-style-type: none"> - [71]: backoff stage ratio BSR 	<ul style="list-style-type: none"> - the packet is marked/dropped based on BSR, thus ECN-enabled TCP can detect the congestion early 	<ul style="list-style-type: none"> - make use of ECN-enabled TCP - minimum the computation overhead 	<ul style="list-style-type: none"> - do not work with normal TCP - does not fully reflect network contention situation

Chapter 3

Metric classification in Wireless Networks

In Chapter 2, the Multihop Wireless Networks characteristics and the challenges they introduce to upper layers have been investigated. The upper layers' protocols (technology-independent protocols) suffer from performance degradation in this environment. Indeed, the operation of these protocols is based on the intrinsic information taken from the layer to where they belong. This information is used with an assumption that the available network resource is large and the bit error rate (BER) is very low. However, it is not the case in MHWNs where the network resource is limited and the BER is relatively high. Therefore, these technology-independent protocols need to be improved or re-designed in order to operate properly in MHWNs.

There have been several proposed schemes on improving the performance of routing protocols and also on improving TCP operation in MHWNs. All of the solutions proposed so far have a common ground that they try to get more information about the network situations in order to have better knowledge about what actually happens at lower layers. The exploited information forms the metrics. The metrics should be computed from any layer of the network stacks and can be used directly or jointly with other metrics in the proposed schemes.

Since many metrics were proposed to address the aforementioned challenges so far, they should be collected and classified in a systematic manner in order to provide a general view of their proliferation. Some works such as [72], [73] and [74] were published which concentrated only on the classification of routing metrics. However, to the best of the author's knowledge, there is no publication working on collecting and classifying metrics from four lower layers of the TCP/IP protocol stack.

This chapter provides a survey and comprehensive definition of common metrics from Physical, MAC, Network and Transport layers and thus provides a multi-criteria and hierarchical classification. In this classification, the metrics are first classified according to the protocol layer where the related events reflected by the metrics occur. Within each layer, the metrics are then grouped by their usage which relates to a function of the layer. We also classify the metrics by their method of obtaining, namely availability as intrinsic information, estimation via statistical models, measurement by means of techniques, and combination of other metrics.

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

3.1 Metrics of PHY layer

The function of physical layer is to transmit raw bits over a medium. When the medium is wireless, the transmitter chooses a given frequency carrier and a suitable power level. Due to the propagation environment, the signal can suffer from noise interferences and fading. So the metrics of PHY layer can provide information about channel quality or signal strength.

Received Signal Strength Indication (*RSSI*)

In IEEE 802.11 [28] and 802.16 [30] standards, *RSSI* is the measurement of the signal quality at the receiver side and is reported for each individual message.

RSSI indicates only the strength of the signal at the receiver compared to a threshold. It does not provide much information about the channel and the quality of the received signal because the measurement of *RSSI* is performed on the raw signal which includes noise, interference and other channel impairments. *RSSI* should be used to know whether the signal of the examined channel is strong enough or not [30].

In [28], *RSSI* measurements are unitless and in the range $[0, \text{RSSIMax}]$ and the *RSSIMax* is vendor-dependent. However, in [30], the unit of *RSSI* is dBm and ranges from -40 dBm to -123 dBm.

Signal to Noise Ratio (*SNR*)

SNR is defined as the ratio of signal power to the noise power and is in unit of dB. It is used to indicate the difference between the level of the desired signal and its corresponding background noise. When the value of *SNR* in dB is greater than 0, it is more signal than noise at the receiver. However, a node can receive several signals from its neighbors which can influence over the decoding of the desired signal. *SNR*, unfortunately, does not reflect this interference.

Carrier to Interference Plus Noise Ratio (*CINR*)

The usage of *CINR* (or *SINR*) is the same with *SNR* except the comparison is between the desired signal and its background noise plus interferences from other signals corrupting the desired signal. *CINR* is not defined in IEEE 802.11 standard [28] but in IEEE 802.16 standard [30]. In IEEE 802.16 standard [30], the unit of *CINR* is dB and ranges from -10 dB to 53 dB. The standard also suggests a method to measure *CINR* but the implementation of *CINR* is vendor-dependent. Like *RSSI*, the *CINR* value is normally available from the driver of 802.16 wireless card.

Using *CINR* will provide more accurate and reliable information about the channel signal compared to *RSSI* but with the cost of higher computation complexity and delay as it requires receiver demodulation lock [30]. IEEE 802.16 standard uses both *RSSI* and *CINR* to determine the burst profile (modulation type, Forward Error Correction (FEC) type,...) exchanged between base station and subscribe stations.

Bit Error Rate (BER)

During transmission through wireless channel, the information bits can be changed due to noise, interference, fading and distortion. To indicate the level of this change, the Bit Error Rate BER of a channel is defined as the ratio of received changed bits to the total number of transferred bits during a time interval; in other words, BER is the average number of bits in error. This metric has no unit and is often expressed in percentage.

In fact, BER is not available at PHY layer. However, the BER induced by the candidate modulation can be estimated using some “ BER vs SNR ” curves such as in [75]. Using BER may help to choose an appropriate Forward Error Correction (FEC) type in transmission between nodes.

Interference Ratio (IR)

IR is defined in [76] as the metric to catch the interference level that affects the transmission between two considered nodes. This definition is based on the physical interference model of [49]. The $IR_i(u)$ for a node u in a link $i = (u, v)$ where $(0 < IR_i(u) < 1)$ as

$$IR_i(u) = \frac{SINR_i(u)}{SNR_i(u)} \quad (3.1)$$

where $SINR_i(u)$ and $SNR_i(u)$ are respectively the Signal to Interference plus Noise Ratio and the Signal to Noise Ratio at the node u . The formulas to compute SNR and SINR of each node u, v of a link i are provided in detail in [76].

In bidirectional communication link $i = (u, v)$

$$IR_i = \min(IR_i(u), IR_i(v)) \quad (3.2)$$

IR_i is used to indicate the effect of interferences from neighbors’ transmissions of the link and $IR \leq 1$. When the link i has no interference nodes or no traffic generated by the interference nodes, IR_i is 1. The larger the IR is, the better the link is. However, this metric does not consider the interference in term of contention between nodes such that if two nodes are in their carrier sensing range, they can not perform their transmission at the same time.

It can be seen that the metrics of PHY layer just provide “raw information” of signal strength level. The measurements of these metrics are performed locally at the wireless device. Some of them are available from the wireless card driver, but the others need intervening in the driver in order to be computed.

Using metrics of PHY layer directly for Network and Transport layers’ protocols does not seem to attract much attention. These metrics, however, are most used to enhance the operation of the MAC layer such as in the work [77]. In [77], SNR is used to improve the operation of 802.11 WLANs by changing dynamically the value of

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

a MAC parameter *RetryLimit*. The idea is based on the operation of the Auto Rate Fallback (ARF) procedure implemented by all the 802.11a, b or g card manufacturers. The ARF procedure automatically reduces the MAC data rate when it senses a drop in the SNR. Thus, by observing the current data rate, the MAC layer entity can determine whether the frame loss is caused by signal failure. The value of *RetryLimit* parameter is then adapted to the change of the MAC data rate in order to resolve the frame losses caused by signal failure.

3.2 Metrics of MAC layer

The main functions of wireless MAC layer is to provide link transmission reliability and medium access mechanism over a shared radio channel with minimum overhead and collision. Other functionalities have been added to MAC layer for QoS services to support multimedia applications.

This layer provides channel related information such as current modulation and coding scheme, statistical information of frame transmission and medium access time. In the following, we classify the MAC metrics according to the MAC layer functionalities or services.

3.2.1 The 802.11 MIB

The IEEE 802.11 standard [28] defines some variables within the Management Information Base (MIB) which can be used to improve the operation of MAC layer's error recovery and to provide more information of MAC layer to upper layers.

ShortRetryLimit and *LongRetryLimit* indicate the maximum number of times a MAC transmitter will try to transmit successfully a frame. After transmitting a frame, the MAC transmitter waits for a 802.11 acknowledgement (MACK). If it does not receive the expected MACK within a specific delay, the MAC transmitter assumes that the frame is lost and retransmits the frame. This operation only terminates either if the transmitter receives MACK for the frame or if the number of retransmission attempts reaches a threshold indicated by the parameter (*Short*)(*Long*)*RetryLimit*. *ShortRetryLimit* is used for the frame whose length is less than or equal to a predefined value *RTSThreshold* and its default value is 7. While *LongRetryLimit* is used for the frame whose length is greater than *RTSThreshold* and has the default value of 4.

The *FailedCount* counter gives the number of unsuccessfully transmitted frame. Each time the number of transmission attempts for a frame exceeds the threshold, either the *ShortRetryLimit* or *LongRetryLimit*, the MAC transmitter discards this frame and add one to this counter.

The *RetryCount* counter indicates the number of successfully transmitted frames which were retransmitted one or more times; while the *MultipleRetryCount* counter interests in frames which were retransmitted successfully after more than one attempt.

The *ACKFailureCount* counter provides the number of times that the MAC transmitter does not receive its expected ACK.

The *TransmittedFrameCount* counter provides the number of successfully transmitted frames.

These metrics are available in read-only mode at 802.11 MAC layer [28] and may be used as statistic information of MAC transmission operation to help protocols of MAC and higher layers.

In [77], Lohier et al. proposed a cross-layer Loss Differentiation Algorithm (LDA) in order to determine the loss caused by channel error and then to react consequently. The authors suggested adjusting *RetryLimit* according to the change of the transmission rate in order to avoid congesting the channel unnecessarily. *ACKFailureCount* is also used to help the transport protocol to discriminate losses due to channel error from that of network congestion. Cheng et al. in [78] used *RetryLimit* together with their new variable *RetransmissionLimit* R_F (at MAC layer) to extend the operation of MAC retransmission. In the case when the number of retransmission attempts exceeds *RetryLimit* value, the MAC entity can still retransmit the corrupted packet and records the number of retransmission attempts to R_F . The packet is only dropped when R_F reaches its predefined threshold. This mechanism will reduce the probability that the MAC layer wrongly infer a link failure when the link experiences a high contention level.

3.2.2 Channel access related metrics

Packet Medium Access Time (T_q)

T_q is defined in [79] as a metric which denotes the time that the packet spends to get access to the medium. Zhao et al. [79] derives the estimation for this metric by modelling all nodes which share the same channel and have a packet to send as in a M/M/1 queue, therefore the expected delay is estimated as

$$T_q = T_s \frac{\rho}{1 - \rho} \tag{3.3}$$

where ρ represents the channel busyness, which is the ratio of busy periods to the total time, and T_s is the service time of a packet. For simplicity, T_s is replaced by an average time cost for one channel event in [79]. Nevertheless, this queueing model simplifies a lot the behavior of MAC layer.

T_q is proved in [79] that it is proportional to the traffic load over the channel around the node. When the traffic load of the channel increases, ρ increases accordingly, and as the consequence, the node has to defer longer to have a chance to send a packet. But when the network enters into congested state, T_q does not increase but stays at a steady level. Since congestion event is at IP level, this metric does not include the queuing delay and is usually smaller than the actual value since it can not monitor some extra delays such as SIFS or DIFS.

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

Packet Transmission Time ($T_{transmit}$)

$T_{transmit}$ is defined in [79] as a metric which denotes the packet transmission time in the link and can be calculated as follows

$$T_{transmit} = N_{transmit} \times \frac{L_{pkt}}{R_s} \quad (3.4)$$

where R_s is the link rate, L_{pkt} is the packet size and $N_{transmit}$ is the expected transmission attempts needed for the packet to be transmitted successfully.

In [79], Zhao et al. argued that up to 90% of packets are sent successfully at the first attempt by the help of adaptive multirate PHY. Therefore, Zhao et al. set $N_{transmit} = 1$ in their implementation. Although this assumption is not really correct, it gets rid of the extra overhead of measuring N . If a routing scheme uses only $T_{transmit}$, it may route flows to a few high rate links that may lead to severe contention and congestion. Thus, in [79], $T_{transmit}$ is used in conjunction with T_q for path selection scheme which favors the path with small delay.

Contention Delay (CD)

Contention Delay CD is defined in [68] as the time interval from the time instant a packet arriving at MAC entity starts to contend for transmission to the time instant the transmitter receives correctly the MACK for that packet or drops it after several failed retransmissions as illustrated by Fig. 3.1. If the packet is dropped, the measured value is added to the contention delay of the next packet.

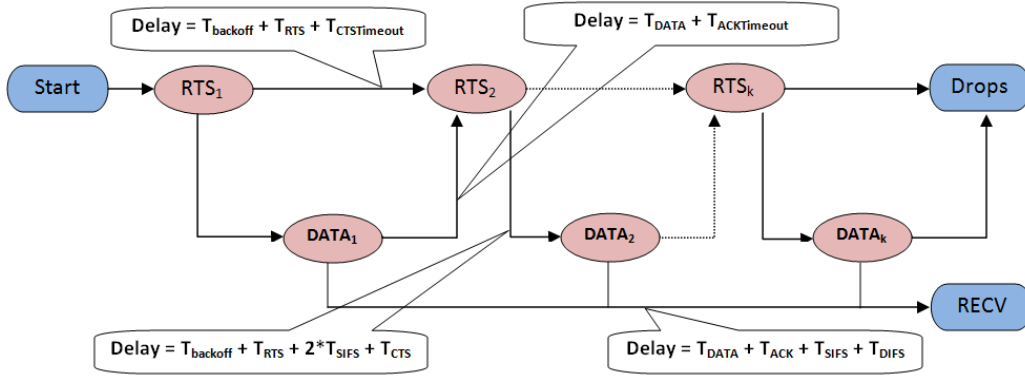


Figure 3.1: Simple model for IEEE 802.11 service time [1]

By this definition, the CD metric comprises the backoff delay, transmission delay and the time to exchange RTS/CTS if this mechanism is enabled. Therefore, CD can be used to indicate the contention level around a node. If the number of neighboring nodes having traffic to transfer over the channel increases, a node has to defer longer in backoff stage to access to the medium and may have a higher probability of packet collision which in turn lengthens the value of CD .

In [68], the cumulative contention delay CCD value of every node along the path is used at the TCP receiver. The receiver calculates the average CDD per hop and the

average throughput during each probe interval and then uses them to determine the optimal congestion window size.

Airtime Cost (C_a) and Frame Error (e_{fr})

Airtime Cost is defined in the IEEE 802.11s standard [3] as a measurement of how much channel resource it takes to transmit a frame over a link. To simplify the implementation, this metric is estimated as follows

$$c_a = \left[O_{ca} + O_p + \frac{B_t}{r} \right] \cdot \frac{1}{1 - e_{fr}} \quad (3.5)$$

where O_{ca} , O_p and B_t are constants listed in the table below, and the input parameters r and e_{fr} are the bit rate in Mbit/s and the frame error rate for the test frame size B_t respectively. The parameters r and e_{fr} are implementation-dependent.

Parameter	802.11a	802.11b
Channel access overhead: O_{ca}	$75 \mu s$	$335 \mu s$
Protocol overhead: O_p	$110 \mu s$	$364 \mu s$
Number of bits in test frame: B_t	8224	8224

Table 3.1: Constants in Airtime [3]

In [3], Airtime Cost is available at MAC layer and is the default radio-aware metric used for path selection protocol in IEEE 802.11s networks. When used for routing, c_a has the advantage of considering both transmission rate and transmission error rate. However, c_a may route traffic to congested areas of the network because links with a higher data rate will always be given higher priority.

3.2.3 Channel load related metrics

The Channel Busyness Ratio (R_b)

The Channel Busyness Ratio R_b for one hop ad hoc networks [70] is derived from DCF model (Fig. 2.1).

Firstly, two parameters, T_{suc} and T_{col} , which respectively represent the average time period associated with one successful transmission and the average time period associated with collisions [70] are defined as:

$$\begin{aligned} T_{suc} &= T_{rts} + T_{cts} + T_{data} + T_{ack} + 3 * T_{sifs} + T_{difs} \\ T_{col} &= T_{rts} + T_{sifs} + T_{cts} + T_{difs} \end{aligned} \quad (3.6)$$

or if RTS/CTS mechanism is not used:

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

$$\begin{aligned} T_{suc} &= T_{data} + T_{ack} + T_{sifs} + T_{difs} \\ T_{col} &= T_{data} + T_{ack_timeout} + T_{difs} \end{aligned} \quad (3.7)$$

Thus, the Channel Busyness Ratio R_b is defined as the ratio of total busy periods of successful transmission or collision to the total time.

$$R_b = \frac{p_s T_{suc} + p_c T_{col}}{p_i \sigma + p_s T_{suc} + p_c T_{col}} \quad (3.8)$$

where p_i , p_s and p_c are respectively the probabilities that the observed backoff time slot is idle, has a successful transmission or has a collision. For implementation, the R_b can be simply calculated as the fraction of the total channel busy period to the interval duration.

If R_b is high, it means that the shared channel is used more frequently by the nodes around with the increase of the offered load. Zhai et al. [70] claim that if the collision probability is smaller than 0.1, there is an optimal point of R_b for the network operation where the throughput is maximized and, delay and delay variation are small. At that point, R_b is around 0.90 ~ 0.95. Therefore, R_b can be used to estimate the available bandwidth of the network. The transport protocol thus can use this information as the measurement of how much data it can pump into but without overloading the network [80] [55].

Permissible Throughput (P)

In [54], Navaratnam et al. used both channel busyness ratio R_b and current throughput to estimate the available channel capacity around a node with regard to the hidden node problem. Thus, a measurement of the current throughput is carried out over a time period including the time wasted due to collisions. The current throughput is estimated using an Exponentially Weighted Moving Average (EWMA) filter for the T_{sample} of each transmitted packet in order to eliminate high frequency components, in which T_{sample} is measured as follow

$$T_{sample} = X / (t_a - t_d) \quad (3.9)$$

where t_d is the time when the packet is ready for transmission and t_a is the time when its MAC acknowledgement (MACK) is received.

Thus, Navaratnam et al. introduced a metric called the Permissible Throughput P which is the combination of the channel busyness ratio R_b and the current throughput.

$$P = \begin{cases} \frac{R_{th} - R_b}{r_b} T & \text{if } R_b > 0 \\ R_{th} \cdot T & \text{otherwise} \end{cases} \quad (3.10)$$

where R_{th} is the threshold for R_b and its value is set to 95% [54]. The Permissible Throughput P is the maximum additional amount of bandwidth that the traffic source

can still pump into the network without overloading it. By keeping the network's operation under saturation, which means small losses and retransmissions at MAC layer, packets will be delivered with smaller delay, jitter and packet loss ratio [54].

Effective MAC Throughput (EMT)

The Effective MAC Throughput, EMT , is the fraction of the total number of successfully transmitted packets to the total MAC service time of packets arrival at MAC in an interval.

$$EMT = \frac{\sum_{N_{sp}} S}{\sum_{N_{ap}} T_{srv}} \quad (3.11)$$

where T_{srv} is the service time which is the time interval from the time instant a frame starts to contend for transmission to the time instant the transmitter receives correctly the MACK of that frame or drops it after several failed retransmissions [70] as illustrated by Fig. 3.1. S is the packet size with assumption that all packets have the same size and N_{ap} and N_{sp} are respectively the number of arrival packets and the number of successfully transmitted packets.

EMT is the average actual bandwidth which is used by the link to transmit a packet. If R_s is the rate supported by the wireless card, then we have $EMT < R_s$.

Note that two components of EMT are inversely proportional to each other. Indeed, in the same observed time with assumption that the node always has packet to send, if the number of successfully transmitted packets increases, the service time spent for a packet (in average) at MAC decreases and vice versa. This makes EMT sensitive to MAC losses which are largely caused by collision between sending nodes which share the same channel.

Summary

The aforementioned MAC metrics provide channel related information, i.e., transmission statistic, channel busyness or contention level. Therefore, they can be used as the indicators of network states. The upper layers' protocols thus can adapt their operation appropriately by observing these indicators.

Table 3.2 summarizes the MAC metrics in this section.

3.3 Metrics of Network layer

The main functions of Network layer are host addressing, routing packets through networks, relaying between interfaces and QoS provision.

The metrics of this layer should take into account not only the information at current layer such as the path length, the interface currently in use, number of hops to

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

Table 3.2: MAC metric table

Categories	Metrics	Channel Error	Contention level	Channel busyness
Reliability	IEEE 802.11 MIB	x		
Channel Access	T_q		x	x
	$T_{transmit}$		x	
	CD		x	
	C_a	x	x	
Channel Load	R_b			x
	P		x	x
	EMT	x	x	

the destination or number of packets in the buffer, but also the information of lower layers such as contention level or available transmission rate in order to estimate the network condition.

It's worth noting here some aspects of wireless networks that routing metrics should reflect. They are packet loss rate, transmission rate of each link and inter/intra-flow interferences [72].

Packet loss rate is one of the most important aspects of the wireless network since the error-prone channel causes several problems for the performance of higher layers. In MHWNs, each link may have a different packet loss rate and the MAC entity may have to transmit successfully a frame by more than one attempt, thus increases the delay and decreases the throughput.

Transmission rate should be reflected since it may vary from link to link or even in one link with adaptive rate selection feature of PHY layer. If two paths have the same number of hops, the one with higher transmission rate may lead to smaller delay and higher throughput.

Inter-flow interference refers to the interference between neighboring nodes which share the same channel. In an area where many flows are routed through, a node may face severe contention and collision in packet transmission. A routing protocol aware of this interference may prevent the flow from routing into dense area where the probability of congestion is high.

Intra-flow interference refers to the interference between intermediate nodes along a same flow path. Since the nodes belonging to the same path have to compete with each other to transmit packets, this problem may lead to low throughput and high delay for the flow on the path. The path selection scheme should take into consider this effect when routes flows in MHWNs.

The routing metric should be also “isotonic” which guarantees that there exists some efficient algorithms like Dijkstra or Bellman-Ford that can use the metric to find a path with minimum weight and loop-free [72].

Some surveys of routing metrics have been published so far such as [72], [73] and [74]. The thesis considers only typical routing metrics and provides additional criteria to classify them, i.e., medium transmission, inter/intra-flow interference and multi-purpose.

3.3.1 Medium transmission related metrics

The metrics in this group provide the information about transmission operation at MAC level of all the nodes along the path. The routing protocols may use this information to assess the reliability of the paths.

Expected Transmission Count (*ETX*)

The *ETX* of a link, defined in [81], is the expected number of (re)transmission attempts required to send a packet over that link. When used in routing protocol, a path is weighted by the sum of *ETX* of all links on that path. The *ETX* of a link is calculated as follows

$$ETX = \frac{1}{d_f \times d_r} \quad (3.12)$$

where d_f and d_r are respectively the forward and reverse delivery ratios which indicate the probabilities that a packet is successfully arrived at the receiver and its ACK is also received correctly on that link. The authors use a probing technique to measure d_f and d_r . Each node broadcasts probing packets with fixed size periodically. After a predefined interval of time, each node calculates the actual and expected number of received probing packets and then derive the delivery ratios.

The advantage of *ETX* is that it takes into account the path length and the packet loss ratios of both forward and reverse directions of a link. Since *ETX* satisfies the constrains in [72], it is an isotonic routing metric. The drawback of *ETX* is that it does not provide transmission rate information, thus *ETX* does not exploit the multirate capacity of links and it may route flows to a link with low packet loss rate but sometimes high traffic load. It also does not reflect the effect of inter- and intra-flow interferences.

Expected Transmission Time (*ETT*)

Draves et al. [82] defined *ETT* of a link as the time for a successful transmission of a packet at that link and can be calculated as follows

$$ETT = ETX \times \frac{S}{R} \quad (3.13)$$

S denotes the packet size and R denotes the data rate of the link. The weight of a path is simply the summation of the *ETT* of all links on the path.

There are several manners to calculate the raw bandwidth of a link. First, it can fix the rate of each 802.11 radio to a given value as in [81] to simplify the measurement. Another possibility is to exploit the multirate capability of today 802.11 wireless cards as it may choose automatically the transmission rate for each packet according to the

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

current propagation condition. Some probing techniques such as packet pairs [82] can also be used to measure the available bandwidth. The value of R is set to the total link capacity instead of available bandwidth in the implementation of [82].

ETT provides more information than ETX as it takes into account the data rate of the link. ETT is also isotonic [72]. However, the drawback of ETT is that it does not fully capture the intra-flow and inter-flow interferences in the network.

The ETT formula has some points of similarity to Airtime Cost (section 3.2.2), where the first part of the formula is used to predict the number of required retransmissions, and the second part reflects the transmission time. Nevertheless, ETT gets rid of the disadvantage of Airtime Cost which may route traffic to congested areas of the network. The reason is that, instead of raw data rate, ETT uses the available bandwidth of the links along the path which takes into account the effect of traffic load.

3.3.2 Inter-flow interference related metrics

Interference-aware Resource Usage (IRU)

IRU was proposed by Yang et al. [83] as a metric which can capture the effect of inter-flow interference and the differences in the transmission rates and loss ratios of wireless links and is calculated as follows

$$IRU(i) = ETT(i) \times N_i \quad (3.14)$$

N_i is the set of neighbors of the link that may interfere the transmission on channel i of that link and $ETT(i)$ the expected transmission time for channel i of that link. The lower the IRU is, the better the link is in term of making use of network capability.

In addition to the advantages of ETT , IRU also takes into account the inter-flow interference. However, the assumption that the interference of all neighboring nodes to the link is the same by using N is not fully correct. The reason is that the signal interference depends on the distance between nodes, and there is no interference at all if all nodes have no data to transmit [76].

Interference Traffic Load (Q) and Link Load (LL)

Le et al. [84] propose a metric called the Interference Traffic Load Q of a link to indicate the effect of traffic load on neighboring nodes since they contribute to the contention around the link when they compete for channel resource. The $Q(l^i)$ of link l^i using channel i is calculated as

$$Q(l^i) = \sum_{k \in N_{nb}^i} Q_k^i \quad (3.15)$$

where N_{nb}^i is the set of interfering neighbors of link l^i on channel i , and Q_k^i is the average backlog at the interface assigned with channel i at node k .

Then the metric Link Load of a link l^i is defined as follows

$$LL(l^i) = ETT(l^i) \times Q(l^i) \quad (3.16)$$

To obtain the backlog information, a mechanism is implemented by which the routing agent Ad hoc On-Demand Distance Vector (AODV) exchanges HELLO messages containing the the average number of packets buffered at its interface. Every node updates the neighbors' load information and then compute the Link Load metric accordingly.

This metric has the advantages of *ETT*, and also inter-flow interference and traffic load by using $Q(l^i)$. Compared to *IRU*, $LL(l^i)$ contains more information than *IRU* as it is aware of traffic load around the link. However, $LL(l^i)$ is relatively more complex to compute than *IRU* since nodes have to exchange the load information with all of their neighbors.

3.3.3 Intra-flow interference related metrics

Channel Switching Cost (*CSC*)

Yang et al. [83] also introduced another metric call *CSC* to work in conjunction with *IRU* (section 3.3.2). *CSC* can capture the intra-flow interference which *IRU* cannot take into account. It is clear that nodes with multi-radio/multi-channel capacity using different channels to transmit packets to their next hops will reduce the intra-flow interference along the path.

The metric *CSC* of node X is defined as follows

$$CSC_X = \begin{cases} \omega_1 & \text{if } CH(prev(X)) \neq CH(X) \\ \omega_2 & \text{if } CH(prev(X)) = CH(X) \end{cases} \quad (3.17)$$

$$0 \leq \omega_1 < \omega_2$$

where $CH(X)$ denotes the channel that the node X uses to transmit the packet, w_1 and w_2 indicate the difference in intra-flow interference level assigned to node X based on the channel it used to transmit the packet to the next hop.

IRU and *CSC* are used together in [83] to provide both inter- and intra-flow interference to aid the path selection algorithms to operate more accurately.

Channel Load (*CL*)

Le et al. [84] also defined $CL(i)$ as the channel load of channel i on the path p and this metric is used in order to exploit the channel diversity to find the path with less intra-flow interference. $CL(i)$ is the summation all link loads $LL(l^i)$ of link l (section 3.3.2) using channel i along the path p

$$CL(i) = \sum_{\text{Link } l \in p} LL(l^i)$$

$$CL_p = \max_{1 \leq i \leq k} CL(i) \quad \text{k the number of channel on path p} \quad (3.18)$$

The value of CL_p indicates the intra-flow interference level of the path p . This metric has the advantages of $LL(l^i)$ plus intra-flow interference. However, beside its complex computation, this metric has another drawback such that it is not isotonic.

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

Compared to CSC , CL_p is more accurate with the cost of computational complexity since it measures the actual load at each node while CSC uses empirical value ω .

3.3.4 Multi-Purpose metrics

Each metric in this group reflects to some extent two or more important aspects for routing, i.e., packet error rate, transmission rate and inter/intra-flow interferences. The selected path constrained by these metrics is the trade-off between these aspects.

Weighted Cumulative ETT ($WCETT$)

Draves et al. [82] proposed $WCETT$ as the metric capturing the transmission rate, packet loss ratio and intra-flow interference characteristics of all links along the path and is calculated as follows

$$X_j = \sum_{\text{Hop } i \text{ is on channel } j} ETT_i \quad 1 \leq j \leq k \text{ (number of channels)}$$

$$WCETT = (1 - \beta) * \sum_{i=1}^n ETT_i + \beta * \max_{1 \leq j \leq k} X_j \quad (3.19)$$

where β is a value $\in (0, 1)$. X_j is the number of times the channel j is used along path p and captures the intra-flow interference. The first part of the $WCETT$ equation is the aggregated delay for a packet to travel through the path while the second part represents the effect of exploiting the multichannel diversity of that path. Therefore, $WCETT$ can capture both intra-flow interference, throughput and end-to-end delay of the network.

The $WCETT$ has two limitations. First, it does not capture the effect of inter-flow interference which may route the flows to dense areas where the probability of congestion occurring is high. Second, $WCETT$ is not isotonic. Therefore, $WCETT$ can not be applied to link-state routing protocols [72].

Metric of Interference and Channel-switching Cost (MIC)

MIC is proposed by Yang et al. [83] as a metric which can capture packet loss ratios, path length, link capacity and inter- and intra-flow interference. MIC is composed of two other metrics: Interference-aware Resource Usage (IRU) (section 3.3.2) and Channel Switching Cost (CSC) (section 3.3.3) as follows

$$MIC(p) = \frac{1}{N \times \min(ETT)} \sum_{\text{link } l \in p} IRU_l + \sum_{\text{node } i \in p} CSC_i \quad (3.20)$$

where N and $\min(ETT)$ are respectively the total number of nodes and the smallest ETT all over the network.

The first component of MIC indicates the aggregated channel resources that the path consumed in the network. This part is used to capture the transmission rate, loss

rate and inter-flow interference of all links along the path. The *CSC* part of *MIC* exploits the channel diversity of the path and thus captures the intra-flow interference on that path. This part helps *MIC* to favour also the paths which have more diversified channel assignments.

The first disadvantage of *MIC* derives from *IRU* as mentioned in the section 3.3.2. The second, *MIC* is not isotonic [72]. Yang et al. [83] proposed a special scheme which introduces virtual nodes to the network to find minimum weight and loop-free path using *MIC*. Despite that, this scheme is still very complex and hard to implement in practice.

PHY/MAC Aware Routing Metric for Ad-hoc Network (*PARMA*)

Zhao et al. [79] introduced *PARMA*, which aims at optimizing the average packet end-to-end delay. The *PARMA* value of a path p is calculated as follows

$$Delay_p = \sum_{\forall link\ s \in p} (T_{transmit} + T_{access} + T_{queuing}) \quad (3.21)$$

where $T_{transmit}$ denotes the packet transmission time in the link (section 3.3.1), T_{access} is derived from the medium access time T_q (section 3.2.2), and $T_{queuing}$ the queuing delay of the packet. Both $T_{transmit}$ and T_{access} are taken from MAC layer in cross-layer manner. When the system is below saturation, the queuing delay $T_{queuing}$ can be omitted [79]. Then we have

$$Delay_{p_i} = \sum_{\forall link\ s \in p_i} \left(\frac{L_{pkt}}{R_s} + T_{access} \right) \quad (3.22)$$

PARMA captures both link data rate and medium access time so that the path selection algorithm using this metric can route packet to high rate links while also avoiding congested areas in the network. Moreover, since T_{access} reflects to some extent of contention level around the node, *PARMA* does indeed capture some form of inter- and intra-flow interference as well.

Interference Aware Routing Metric (*iAWARE*)

Subramanian et al. [76] defined *iAWARE* of a link as

$$iAWARE = \frac{ETT}{IR} \quad (3.23)$$

where *ETT* is the Expected Transmission Time of the link (section 3.3.1) and *IR* is the Interference Ratio of the link (section 3.1). *iAWARE* captures the link loss ratio and packet transmission time of the link from *ETT* and signal interference of the link's neighbors from *IR*.

To exploit the channel diversity, the intra-flow interference on channel j , X_j , is defined as follows

$$X_j = \sum_{\text{conflicting links } i \text{ on channel } j} iAWARE_i, 1 \leq j \leq k \quad (3.24)$$

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

where k is the number of channels available.

The weighted cumulative path metric $iAWARE(p)$ of a path p is defined as follows (α is set to 0.5 in [76])

$$iAWARE(p) = (1 - \alpha) \times \sum_{i=1}^n iAWARE_i + \alpha \times \max_{1 \leq j \leq k} X_j \quad (3.25)$$

This metric has the advantages of taking into account transmission rate, packet loss ratio and inter-/intra-flow interference. However, $iAWARE$ is not isotonic, and another disadvantage of $iAWARE$ is that since the metric guides the protocol to choose the path with smaller weight, the flow may be routed to the path with low ETT but very high interference.

Load Aware Routing Metric ($LARM$)

Le et al. [84] defined $LARM$ as follows

$$LARM = (1 - \alpha) \times \sum_{j=1}^m CL(j) + \alpha \times \max_{1 \leq j \leq m} \{CL(j)\} \quad (3.26)$$

where α is the tunable value in $[0,1]$, m is the number of channel used on the routing path; $CL(j)$ is the channel load of channel (section 3.3.3).

It is obvious that the $LARM$ metric is a trade-off between delay and throughput of the routing path since the first path of $LARM$ is the accumulated load of occupied channels along the path which effects its total delay, while the second path exploits the channel diversity which reflects its total throughput.

The main disadvantage of $LARM$ is that it is relatively complex in computation since it requires information of queue length of all nodes along the path. In addition, this metric is also not isotonic.

Summary

The metrics presented in this section are specifically designed for Multi-hop Wireless Networks. They improve the routing in MHWNs in different ways but with the same idea of involving the MAC and Physical layers' information in addition to those of Network layer.

Since many routing metrics take into account the lower layers' information, they can also be used to aid the operation of transport protocols. For example, ETX and ETT can be use to assess the quality of paths in Stream Control Transmission Protocol (SCTP) [85] [86]. SCTP operation is based on multi-homing feature which allows two endpoints represented by multiple IP addresses to have more than one communication paths. One path is chosen as the primary path for data communication and the others are used for backup in case the primary path experiences the network failure. If the routing protocol uses ETX or ETT to weight the paths, these path assessments can

3.4 Metrics of Transport layer

be also submitted to transport layer. The SCTP agents can use this information to list the available paths in a quality order specified by *ETX* or *ETT*. The primary path and the potential backup paths thus can be chosen accordingly.

Another possibility is to use the metrics Q and LL to report the current load along the path. Since these metrics' value are updated periodically, the transport protocol can also use this load information to prevent overloading the network by adjust its sending rate properly.

Although this idea needs more investigating, the thesis's author believes that it is a potential research issue.

Table 3.3 summarizes the routing metrics presented in this section.

Table 3.3: Routing metric table

Categories	Metrics	Isotonic	Packet loss rate	Transmission rate	Inter-flow interference	Intra-flow interference
Medium Transmission	<i>ETX</i>	x	x			
	<i>ETT</i>	x	x	x		
Inter-flow interference	<i>IRU</i>	x	x	x	x	
	Q	x			x	
	LL	x	x	x	x	
Intra-flow interference	<i>CSC</i>	x				x
	<i>CL</i>					x
Multi-purpose	<i>WCETT</i>		x	x		x
	<i>MIC</i>		x	x	x	x
	<i>PARMA</i>	x		x	x	x
	<i>iAWARE</i>		x	x	x	x
	<i>LARM</i>		x	x	x	x

3.4 Metrics of Transport layer

In general, the Transport layer provides end-to-end communication services for applications over the network. The main services are Connection-oriented Communications, Reliability, Flow Control and Congestion Avoidance.

Since TCP is the most widely used Transport layer protocol in the Internet, it is evident that end-to-end measurements used in TCP have received much consideration of researchers. In MHWNs, as mentioned in Chapter 2, not only network congestion influences the delay and throughput, but also problems induced from wireless characteristics. These characteristics can cause random packet losses, routing path oscillations, MAC layer contention... which lead to false network state detection and notification for such protocols. Therefore, the metrics of the Transport layer, which are end-to-end measurements, should take into account all of the above factors in order to help transport protocols gain better performance in MHWNs.

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

However, since transport metrics are end-to-end information which is affected by measurement noise in MHWNs, they should be used in a combination manner to provide better estimation of network condition.

In the following, the transport metrics will be grouped into three categories which are Throughput related, Reliability related and Packet Delay related.

3.4.1 Throughput Related Metrics

Bandwidth Delay Product (*BDP*)

Bandwidth Delay Product is a concept in measuring the capacity of a data link and is calculated as the product of a data link's capacity (in bits per second) and its end-to-end delay (in seconds). According to [87], in the context of TCP in wire-line network, the maximum number of outstanding data packets is limited by an upper bound calculated as

$$BDP - UB(bits) = Total_Bandwidth(bits/sec) \times round_trip_time(sec) \quad (3.27)$$

However, it is different in MANETs since nodes communicate with each other by wireless links. In IEEE 802.11 standard [28], a node has to take a channel contention phase for a chance of transmission, and after receiving the acknowledgement for that transmission, it has to contend again for the next transmission. It means that the channel can not hold multiple packets "back-to-back" in one transmission. Chen et al. [87] claim that, in MANETs with an assumption that the bottleneck bandwidth is the same for the forward and return paths

$$BDP - UB \leq N \times S \quad (3.28)$$

where N is the number of round-trip hops and S is the TCP packet size.

The more precise formulas of $BDP - UB$ taking into account the effect of signal interference in MANETs based on IEEE 802.11 MAC [28] is

$$BDP - UB \leq kN \times S \quad (3.29)$$

where k in $(1/8, 1/4)$ is a reduction factor due to transmission interference at the MAC layer, or

$$BDP - UB \leq \frac{\sum_{i=0}^n d_i + \sum_{i=0}^m d'_i}{4d_{max}} \times S \quad (3.30)$$

where d_i and d'_i are the per-hop packet transmission delays along the forward and return paths, d_{max} is the maximum per-hop delay of the forward path.

In [87], the authors use the $BDP - UB$ to adjust properly the TCP's Congestion Window Limit, thus better performance of TCP over MANETs is gained considerably. However, $BDP - UB$ provides only the long term upper bound of the available bandwidth over the network. It can not be used as the indicator of network congestion or channel losses.

Short-term Throughput (STT)

STT was defined by Fu et al. [61] as the throughput observed over a time interval T . In [61], T is set to $RTT/2$ as the trade-off between metric accuracy and responsiveness. The main advantage of STT is that STT is slightly affected by transitory route changes induced by mobility in MANETs. The network congestion is identified by comparing STT value to a threshold calculated from all samples.

However, because throughput is an absolute value which depends largely on the sending rates, network disconnections and bursty channel errors, STT may not provide good enough information for the sender or receiver to distinguish whether the network is in congestion or not.

Short-term Goodput (STG)

To overcome the limitation of STT , K. Caihong et al. [88] introduced STG , the ratio of the number of packets successfully delivered to the total number of packets transmitted during an interval of T . Since STG is calculated during an interval, it will not be affected by the source rates and also is not sensitive to transient route changes. Thus, STG can reflect the network congestion level more precisely [88]. Namely, when the value of STG decreases dramatically which means a higher weight on lost packets compared to sent packets, it is possible that the network enters into congestion state.

The three throughput related metrics have their own disadvantages. $BDP - UB$ can not be used for short term detection of network congestion, while STT and STG are not accurate enough to deal with channel losses. Therefore, it is better to combine these metrics with other metrics to jointly identify network congestion as proposed in [61] or [88].

3.4.2 Reliability Related Metrics

Packet Out-of-order delivery Ratio (POR)

POR is defined as the ratio of the number of out-of-order packets to the number of all the packets received in a time interval T [61] [88]. The out-of-order packet is identified by comparing the sending time T_s of the arrived packet with that of the latest received in-order packet T_{max} . If $T_s > T_{max}$, which means this packet arrives after a packet that was sent later than it by the same sender, it will be marked as an out-of-order packet.

Each time a route switching event occurs, it may exist multiple delivery paths. The packets may arrive at the receiver from different paths and lose their ordering. In fact,

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

this phenomenon is coupled essentially with route change events. Hence, POR can be used to indicate this kind of network state, i.e., if the value of POR increases suddenly and largely, it is mostly that a route change event happens.

Packet Loss Ratio (PLR)

The metric PLR [61] is computed during each time interval T as the number of missing packets in the current receiving window. PLR can reflect to some extent the intensity of channel error, e.g., PLR is high when a burst of channel losses occur.

Packet Loss Event Rate (p)

In [47], a loss event is defined as one or more lost or marked packets in a Round Trip Time, where a marked packet refers to a congestion indication from Explicit Congestion Notification (ECN). The first lost packet of the loss event also starts a loss interval. A loss interval is defined in [47] as the number of packets transmitted by the sender starting with the first packet transmitted in that loss interval and ending with but not including the first packet transmitted in the next loss interval.

The TFRC receiver estimates the Loss Event Rate p by first calculating the average loss interval I_{mean} and then we have $p = 1/I_{mean}$. The detail of this calculation can be found in [47].

The Packet Loss Event Rate p is an important information for the TFRC sender to work properly. A receiver wrongly reporting p can easily deceive the sender into transmitting at a sub-optimal rate. This is a big problem for TFRC in MHWNs with error-prone channel since the protocol can not distinguish wireless losses from congestion losses. Thus, an accurate scheme for computing p can help the protocol gain much better performance in such network.

Although the metrics in this group can deal to some extent with the route change or channel error events, there exists some situations which can not be identified correctly by using only one of them. For example, PLR is also high when a number of packets is dropped due to the buffer overflow. Thus, beside these metrics, the transport protocols should observe also other metrics in order to identify the network events more accurately.

3.4.3 Packet Delay Related Metrics

Relative One-way Trip Time ($ROTT$)

In [89], $ROTT$ is defined as travelling time of a packet from the sender to the receiver and is used to identify the state of the current connection. In [89], two schemes based on $ROTT$ can be used to distinguish wireless losses from congestion losses as follows.

In the Spike scheme, two thresholds called $B_{spikestart}$ and $B_{spikeend}$ are defined in this scheme. If with the $ROTT_i$ of a packet i such that $ROTT_i > B_{spikestart}$ and the

connection is currently not in the spike state, the algorithm enters the spike state and the losses in this period are interpreted as congestion. Otherwise, if $ROTT_i < B_{spikeend}$ and the connection is currently in the spike state, the algorithm leaves the spike state and the losses in this period are interpreted as wireless errors.

In the ZigZag scheme, $ROTT$ and its mean, $ROTT_{mean}$ and deviation, $ROTT_{dev}$ are used together with the number of losses, n , to differentiate the loss reasons. A loss is determined as wireless induced loss if

$$\begin{aligned}
 & (n = 1 \text{ AND } rott_i < rott_{mean} - rott_{dev}) \\
 \text{OR} & \quad (n = 2 \text{ AND } rott_i < rott_{mean} - rott_{dev}/2) \\
 \text{OR} & \quad (n = 3 \text{ AND } rott_i < rott_{mean}) \\
 \text{OR} & \quad (n > 3 \text{ AND } rott_i < rott_{mean} - rott_{dev}/2)
 \end{aligned} \tag{3.31}$$

Otherwise, the loss is determined as congestion induced loss.

Inter-packet Arrival Delay (IAD)

IAD [89] is the metric measuring the delay difference between the arrival time of consecutive packets. Denote A_i and A_{i+1} the arrival time of two consecutive packets at the receiver, IAD is measured as follows

$$IAD = A_{i+1} - A_i \tag{3.32}$$

IAD is sensitive to network burst losses on the path as this event will increase the value of IAD . In [89], IAD is used in Biaz scheme to distinguish between loss reasons. Let IAD_{min} denotes the minimum packet inter-arrival delay so far, IAD_i denotes the time between the last in-order received packet and the first packet received after the burst loss size n , then the losses are wireless induced if

$$(n + 1)T_{min} \leq T_i \leq (n + 2)T_{min} \tag{3.33}$$

However, if the loss size is small, i.e one packet, it's hard to distinguish that the increment of IAD was caused by congestion or random channel errors.

Inter-Packet Delay Difference (IDD)

Fu et al. [61] defined IDD as the difference between the travel time (from the time the packet was sent to the time it is received) of consecutive packets. If A_i denotes the arrival time and S_i denotes the sending time of packet i , we have the equation as follows

$$IDD = A_{i+1} - S_{i+1} - (A_i - S_i) \tag{3.34}$$

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

Unlike IAD , IDD is unaffected by random channel errors and packet sending behaviors thanks to subtracting the sending time. IDD also reflects efficiently the growth of the packet queue length. If the value of IDD increases apparently, it is a high probability that the network enters congestion state because since the packet $i + 1$ is affected by congestion, the time $A_{i+1} - S_{i+1}$ is much greater than that of its predecessor packet i which is not affected by congestion.

The metric IDD is less sensitive to short term out-of-order packet delivery which is caused by the mobility in MANETs [61]. Thus, IDD should be used jointly with other metrics to better reflect the network events.

In [61], Fu et al. proposed to use concurrently STT , PLR , POR and IDD to catch more accurately the network events. The same idea was also explained in [88]. Two thresholds are defined for each metric which indicate whether the metric value is “high” or “low”. Hence, each network event is determined according to the metrics’ value as showed in Table 3.4

Table 3.4: Metric patterns for network events

	IDD and STT	POR	PLR
Congestion	(High, Low)	*	*
Route change	NOT (High, Low)	High	*
Channel error	NOT (High, Low)	*	High
Disconnection	(*, ≈ 0)	*	*
Normal	default		

Summary

All the aforementioned metrics are measured at Transport layer. In MHWNs, these measurements are affected by noise which in turn raise doubts about their reliability. It is suggested that the transport metrics should be used together to better detect network events.

Table 3.5 summarizes the metrics presented in this section.

Table 3.5: Transport metric table

Categories	Metrics	Congestion	Route change	Channel error	Disconnection
Throughput	BDP				
	STT	x		x	x
	STG	x		x	x
Reliability	POR		x		
	PLR	x		x	
	p	x		x	
Delay	$ROTT$	x	x		
	IAD	x		x	
	IDD	x	x	x	

3.5 Classification table

The summary of this study is showed in the classification table (Table 3.6). Beside the criteria presented in the above sections, the metrics are also classified by their obtaining methods, i.e availability, measurement, estimation or composition. Note that some intrinsic metrics of widely used protocols in each layer are also added to the table. Since these metrics are very common, they are classified into “Availability” category.

3.6 Summary

In this chapter, a comprehensive classification is proposed for the metrics used to improve the performance of common protocols in wireless networks. The metrics are first classified by protocol layers and then grouped by the functional objectives. Each metric is also belongs to one or more categories of obtaining methods which are Availability, Estimation, Measurement and Combination.

From this classification, a conclusion has been made such that all of the complex metrics which reflect more than one characteristic of the wireless network are composed of simpler metrics, many of them come from lower layers. In addition, each characteristic of the network can be captured in some different ways. These comments come to a suggestion that we can create new multi-purpose metrics which may capture many characteristics of the wireless network by combining the aforementioned simple metrics interchangeably in different methods. The combination should also take into consideration the trade-off between effectiveness and computation complexity of the novel metric.

In recent years, among the research directions for performance improvement of transport protocols in MHWNs, the one which exploits the MAC information has been received major attention. Although several MAC metrics have been introduced so far, their effectiveness in reflecting network states has not been investigated. The next chapter provides a comparative study on the effectiveness of the MAC metrics cited in this chapter and some other novel MAC metrics.

3. METRIC CLASSIFICATION IN WIRELESS NETWORKS

Table 3.6: Metric classification table

Layers	Categories	Availability	Measurement	Estimation	Composition
TRANSPORT	Reliability		Packet Out-of-order Ratio POR , Packet Loss Ratio PLR , Packet Loss Event Rate p		
	Throughput	Received Windows $rwin$, Congestion Window $cwnd$	Bandwidth Delay Product BDP , Short Term Throughput STT , Short Term Goodput STG		
	Delay	Round Trip Time RTT	Relative One-way Trip Time $ROTT$, Inter-packet Arrival Delay IAD , Inter-packet Delay Difference IDD		
NETWORK	Medium Transmission		Expected Transmission Count ETX , Expected Transmission Time ETT		
	Inter-flow Interference	Queue length q	Interference-aware Resource Usage IRU , Interference Traffic Load Q , Link Load LL		
	Intra-flow Interference		Channel Load CL	Channel Switching Cost CSC	
	Multi-purpose				$WCETT$, MIC , $PARMA$, $iAWARE$, $LARM$
MAC	Reliability	802.11 MIB	Frame Error Rate e_{fr}		
	Channel Access	Airtime Cost C_a , Number of channel N_c	Contention Delay CD	Packet Medium Access Time T_q , Packet Transmission Time $T_{transmit}$	
	Channel Load	Link Rate R	Channel Busyness Ratio R_b , Permissible Throughput P , Effective Throughput EMT		
PHYSICAL		$RSSI$, SNR , $CINR$, BER	Interference Ratio IR		

Chapter 4

Effectiveness of MAC metrics to reflect network condition

As described in Chapter 2, Internet predominant transport protocols face challenges to perform properly in Multi-hop Wireless Networks. Since end-to-end information is not enough to solve these challenges, there have been several proposed schemes which have a common ground that they try to take advantage of the MAC layer information, called MAC metrics, to have better knowledge about what happens at lower layers. They are then sent upward to transport layer in a cross-layer manner and are used in various ways to keep the network operating at a reasonable level.

Since MAC metrics allow to provide MAC information to the upper layer protocols, the answer for the question of “how is the effectiveness in reflecting network information of MAC metrics?” should be found out. In our opinion, a good MAC metric for congestion control should be coupled with the network contention level and the medium related losses. Hence, in this study, we propose some new MAC metrics which are expected to reflect accurately MAC states, i.e contention state, collision and loss events. We then investigate the effectiveness in reflecting network states of these metrics in a systematic way by simulating various network situations in order to answer the above question.

4.1 New MAC metrics

In this section, three new MAC metrics will be defined which are the Average Transmission Attempt, the Average Transmission Time and the Medium Access Delay. They provide different measurements taken from the DCF operation at MAC layer. The aim of these metrics is to reflect as much as possible the information about the current network situation such as contention level, collision occurrence or channel busyness.

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

4.1.1 The Average Transmission Attempt

The Average Transmission Attempt, ATA , is defined as the fraction of total transmission and retransmission attempts that the MAC layer carries out to the total number of successfully transmitted packets in an interval. In other words, ATA is the average attempts that MAC takes to transmit successfully a packet in an interval.

$$ATA = \frac{\sum^{N_{ap}} N_{at}^i}{N_{sp}} \quad (4.1)$$

where N_{at}^i is the number of attempts that the MAC layer takes to transmit the packet i until it receives the corresponding MACK or drops the packet, N_{ap} and N_{sp} are respectively the number of arrival packets and the number of successfully transmitted packets. Thus, ATA is relatively sensitive to collision level around a node.

Since MAC specification [28] defines several parameters related to transmission attempt such as *RetryCount* or *TransmittedFrameCount* (Section 3.2 in Chapter 3), this metric is also easy to implement at MAC layer.

4.1.2 The Average Transmission Time

The definition of the Average Transmission Time, ATT , is derived from the MAC Service Time T_{srv} which is the time interval from the time instant a frame starts to contend for transmission to the time instant the transmitter receives correctly the corresponding MACK or drops it after several failed retransmissions [70] as illustrated in Fig. 3.1.

The Average Transmission Time ATT is then the average MAC service time of a successfully transmitted packet in an interval. To calculate ATT , the sum of service times of every packet arrived at MAC during an interval is made and then divided by the total number of transmitted packets whose MACKs are received successfully in that interval.

$$ATT = \frac{\sum^{N_{ap}} T_{srv}}{N_{sp}} \quad (4.2)$$

where N_{ap} and N_{sp} are the same terms as in the equation A.1. ATT , by this definition, comprises the contention delay and transmission delay and therefore can be used to indicate the contention level around a node. If the number of neighboring nodes which have traffic to transfer over the channel increases, a node has to defer longer in backoff stage to access the medium and may have higher probability of packet collision which in turn introduces longer transmission delay. ATT is sensitive to offered load at MAC and collision level in node's neighborhood.

This metric reflects the global network state which includes both contention and successful transmission periods. However, since the congestion is closely coupled with the contention as demonstrated in [90], we claim that the network contention level is

the situation which should be settled rapidly and accurately in order to indicate the congestion at the IP buffers. Therefore, we also define the following new metric which can reflect directly the network contention level.

4.1.3 The Medium Access Delay

The Medium Access Delay, MAD , is derived from $T_{contention}$ (Fig. 2.1), which is the time a packet has to wait at MAC level before it is actually transmitted over the medium. By this definition we have:

$$T_{contention} = \sum^{n_{NAV}} T_{NAV} + \sum^{n_{busy}} T_{busy} + T_{backoff} \quad (4.3)$$

or if RTS/CTS mechanism is not used:

$$T_{contention} = \sum^{n_{busy}} T_{busy} + T_{backoff} \quad (4.4)$$

where $\sum^{n_{NAV}} T_{NAV} + \sum^{n_{busy}} T_{busy}$ represents the total channel busyness time due to the transmission of neighbor nodes that the packet has to defer during a backoff stage. Each T_{NAV} is the reserved channel time taken from a received RTS or CTS packet (if used) and each T_{busy} is a channel busyness duration indicated by physical Carrier Sensing (CS) mechanism. Note that the MAC may freeze the backoff procedure as often as it receives RTS/CTS packets and is indicated by physical Carrier Sensing (CS) mechanism that the channel is busy. Thus, the n_{NAV} and n_{busy} experienced by the node during a backoff stage depends on the number of RTS/CTS packets received and on the number of channel busyness indications from CS mechanism during that duration.

Fig. 4.1 demonstrates the calculation of $T_{contention}$ in the DCF scheme of the IEEE 802.11 standard.

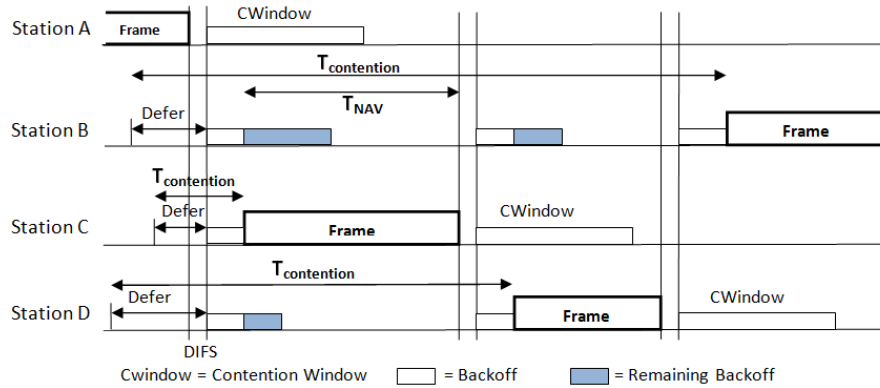


Figure 4.1: $T_{contention}$ in IEEE 802.11 DCF

$T_{backoff}$ is the backoff time calculated as follows:

$$T_{backoff} = N * aSlotTime \quad (4.5)$$

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

where N is a random integer between $[0, CW]$ and CW and $aSlotTime$ are respectively the Congestion Window used in the DCF mechanism and the time unit defined in IEEE 802.11 PHY [28].

The Medium Access Delay, MAD , is simply defined as the average total $T_{contention}$ for a packet at MAC layer before it is successfully transmitted or dropped after several failed retransmissions in an interval. By this definition, MAD includes the first backoff duration after it enters into the MAC layer and all other backoff durations it has to defer after each failed (re)transmission and NAV delay in each backoff stage.

$$MAD = \frac{\sum_{N_{ap}} \sum T_{contention}^i}{N_{ap}} \quad (4.6)$$

where N_{ap} is the number of arrival packets in the interval and $T_{contention}^i$ is the contention time at the i^{th} transmission attempt. Note that the maximum retransmission number is limited by the parameter `RetryLimit` defined in the standard.

The metric MAD is simple to implement with available functions provided by IEEE 802.11 [28]. The node's MAC layer can take T_{NAV} from the header of RTS/CTS packets, $T_{backoff}$ from its intrinsic variables, and physical and virtual carrier sensing mechanisms provide function to determine whether the channel is busy or not.

If the value of MAD increases, either or both possibilities may rise. First, the channel is mostly used by other nodes' transmission so that the node has to defer longer to have a transmission opportunity which in turn increases the $T_{contention}$ value in the equation 4.6. Second, the number of retransmissions increases due to the hidden node problem as the number of interfering nodes which have packets to send increases. Note that the node returns to backoff stage after each failed transmission which in turn increases the number of $T_{contention}$ in the equation 4.6. Thus, MAD takes into account the medium busyness, hidden node problem and can be used to describe the network situation. Refer to Section 3.3 in Chapter 3, we can also claim that MAD metric meets the constrain of the inter/intra-flow interferences.

Note that the work of Hwang [91] also defines a MAC metric called Medium Access Delay. However, this metric provides a different measurement which is the time needed for a packet to be successfully transmitted after it is positioned in the transmission buffer of the MAC entity for the first time.

From the definitions of ATT and MAD , it is the fact that MAD is a part of ATT . This comes from the relation between $T_{contention}$ and T_{srv} . Refer to Fig. 2.1, we have the following equation for the observed packet p

$$MAD_p = \sum^k T_{contention} = T_{srv} - \left(\sum^{n_{suc}} T_{suc} + \sum^{n_{col}} T_{col} \right) \quad (4.7)$$

where k is the total number of transmission attempts for packet p , T_{suc} and T_{col} are defined in Section 3.2.3 of Chapter 3; n_{suc} and n_{col} are respectively the number of successful transmission attempts and the number of transmission attempts which suffer from collision such that $n_{suc} + n_{col} = k$. Also note that n_{suc} has only two possible values, i.e. 0 and 1, since the packet transmission operation also terminates when there is at least one successful transmission attempt.

After providing the definitions of the new metrics, the next sections will provide an evaluation of the effectiveness of these new metrics and some typical ones introduced in Chapter 3. The term effectiveness will be clarified first. Then, the evaluation study will be described in detail.

4.2 Metric effectiveness

MAC metrics are created in order to provide MAC information to the upper layer protocols. Thus, it is very important to study the effectiveness of the MAC metrics, i.e., their ability to reflect the problems of lower layer network operation, especially the indication of network congestion. However, since the congestion is closely coupled with the contention as demonstrated in [90], we claim that the network contention level is the situation which should be settled rapidly and accurately in order to early indicate the congestion at the IP buffers.

In our opinion, an effective MAC metric for congestion control should have representative behavior with the network contention/collision level and the medium related losses. In other words, it should be sensitive to the change of the network state caused by the considered network event and its behavior reacting to that change should also be clear enough to recognize.

In the following study, five MAC metrics are chosen: *ATA*, *ATT*, *MAD* and two metrics *EMT* and R_b which have been introduced in Chapter 3. The question that we try to answer in this study is that comparing with each other, which metric is better in reflecting network events in terms of the aforementioned effectiveness.

4.3 Effectiveness evaluation

As described in Chapter 2, the performance degradation problem of higher layers' protocols is mainly caused by the wireless medium characteristics and multi-hop nature of the Multi-hop Wireless Network. Indeed, the packet loss is caused by not only congestion, but also wireless-induced BER. The nodes have to contend with each other to get access to the medium. The contention level thus depends largely on the number of transmission activities of the interference nodes which in turn depends on the traffic load. Moreover, the increase of the transmission activity number can also exacerbate the hidden node problem which is one of the packet loss source.

In this effectiveness evaluation, the considered MAC metrics are thoroughly investigated through various network situations which affect the performance of higher layers' protocols. To do that, with regard to the above remarks, several scenarios will be built based on the variation of traffic load and channel BER. The simulation will thus show how effectively the considered metrics react to the change of network state due to the variation of the chosen factors.

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

4.4 Confidence Interval

The measurement of metrics by simulation, using a probabilistic model or experimentation, provides different results due to different initial conditions or the changing environment of experimentation. To get a convincing result, we need to repeat the measurement several times. Suppose that the repeated measurements of the quantity X generate a sample of n results x_1, x_2, \dots, x_n , in which x_i is the i^{th} measurement of the sample. An average of all the measurement results in the sample (\bar{x}) is an estimate of the X 's expectation. However, the value of \bar{x} can be different from sample to sample. We need to know how reliable the measurement results are. The **confidence interval** is used to indicate the reliability of an estimate.

The equation 4.8 calculates the 95% confidence interval with $n = 16$ repeated measurements based on Student's t-distribution.

$$\frac{2.131 \times s}{\sqrt{n}} \quad (4.8)$$

where s is calculated as

$$\begin{aligned} \bar{x} &= \frac{x_1 + \dots + x_n}{n} \\ s^2 &= \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2 \end{aligned} \quad (4.9)$$

This confidence interval of 95% means that, in 95% of the measurement cases, the average value of the sample will lie in the range of $[\bar{x} - \frac{2.131 \times s}{\sqrt{n}}, \bar{x} + \frac{2.131 \times s}{\sqrt{n}}]$.

4.5 Simulation and Results

4.5.1 Simulation scenarios

4.5.1.1 General configuration

In order to perform the effectiveness evaluation, extensive simulations were performed using the network simulator ns-2, version 2.34 [92] as ns-2 is one of the most common used and accurate simulator tool for research on networking [93] [94] [95]. The new implementation of MAC (Mac802_11Ext and WirelessPhyExt) has been chosen. This model is integrated in the current version of the simulator as the complete replacement for the legacy model due to its accuracy and new features such as structure design of MAC functionality modules, cumulative SINR computation or multiple modulation scheme support. For more detail about this implementation, please refer to [96]. The table 4.1 displays the general configuration for the simulations.

In order to perform the evaluation, two scenarios will be built. The first scenario will be used to provide the effect of traffic load. The variation of the traffic load is made

Table 4.1: General configuration for simulation

Parameters	Value
Propagation Model	TwoRayGround
MAC protocol	802.11a
Channel Capacity	6Mbps
Interface queue size	50
Carrier Sensing Range	$\simeq 500\text{m}$
Transmission Range	$\simeq 250\text{m}$
Routing protocol	AODV

by changing the traffic source rate of a flow or increasing the number of concurrent flows in the network. The second scenario will be used to investigate the effect of the channel random error by configuring the channel BER of the network to obtain several values.

If not otherwise indicated, the configuration parameters provided in the Table 4.2 will be applied for all the scenarios.

Table 4.2: General scenario setting

Parameters	Value
Topology	9 hop chain
Channel BER	0 (perfect channel)
Connection	UDP with CBR traffic
CBR packet size	1000 bytes
Metric calculation interval	1 second
Simulation time	100 seconds
Simulation run	16

4.5.1.2 Scenario 1: Effect of traffic load

In this scenario, several traffic patterns will be made. The effect of traffic load will be evaluated by changing the traffic source rate of a flow or using a number of concurrent running flows. Three specified sub-scenarios are described in detail as follows.

Scenario 1.1: One traffic source with different rates

In this scenario, only one connection flow is established in the network. In each experiment, the flow runs with a specified rate and maintains the rate during the simulation time. This scenario thus can evaluate the performance of the considered metrics with regard to the intra-flow interference.

- Traffic: CBR with rate = $\{0.5, 1, 1.18, 1.25, 1.5, 2\}$ Mbps
- Traffic pattern: 1 flow connection from node 0 (traffic source) \Rightarrow node 9

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

Scenario 1.2: One traffic source with sudden change in traffic rate

This scenario uses one connection flow with a specified CBR traffic rate. During the simulation, the source rate sometimes increases to a certain value in a short period before turning back to the old value. The metric behavior with regard to short term heavy traffic load thus can be investigated.

- Traffic source: CBR with rate = 0.5 Mbps
- Traffic pattern: 1 flow connection from node 0 (traffic source) \Rightarrow node 9. The rate changes from 0.5 to 1.25 Mbps and sustains at this rate for 0.2s before turning back to 0.5 Mbps. The time instants for the rate change are at the 10th, 20th and 35th second.
- Simulation time: 50 seconds

Scenario 1.3: Different number of concurrent flows

In this scenario, the variation of traffic load is performed by changing the number of concurrently running flows in the network. This scenario uses the topology as showed in the Fig. 4.2. In this topology, the distance between lines of nodes is 300m (greater than the transmission range). The objective of this scenario is to study the metric behavior with regard to the inter-flow interference in the network by creating a heavy traffic region in the network.

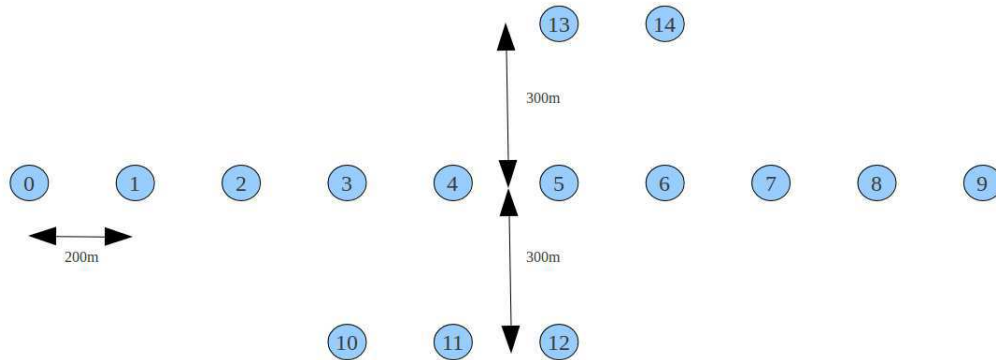


Figure 4.2: Topology for scenario 1.3

3 connection flows are set up as follows

- Flow 1: CBR traffic with rate {1, 1.25} Mbps, node 0 \Rightarrow node 9
- Flow 2: CBR traffic with rate 0.5 Mbps, node 10 \Rightarrow node 12
- Flow 3: CBR traffic with rate 0.5 Mbps, node 14 \Rightarrow node 13

Three experiments are built for this scenario, each one is performed with a specified number of connections. The first one is with connection 1, the second one is with

connection 1 and 2, and the last one is with connection 1, 2 and 3. Note that the term “ cx ” represents the number of connections in each experiment.

4.5.1.3 Scenario 2: Effect of channel random error

In this scenario, the effect of channel BER is taken into consideration. Only one connection flow is established during the simulation and the network is configured with different BER values. Each BER value is also examined with different traffic rates. The detail of the scenario is as follows:

- CBR rate: {0.5, 1, 1.25} Mbps
- Channel BER: {0, 10e-6, 10e-4, 10e-3}
- Traffic pattern: 1 flow from node 0 (traffic source) \Rightarrow node 9

4.5.2 Results and discussion

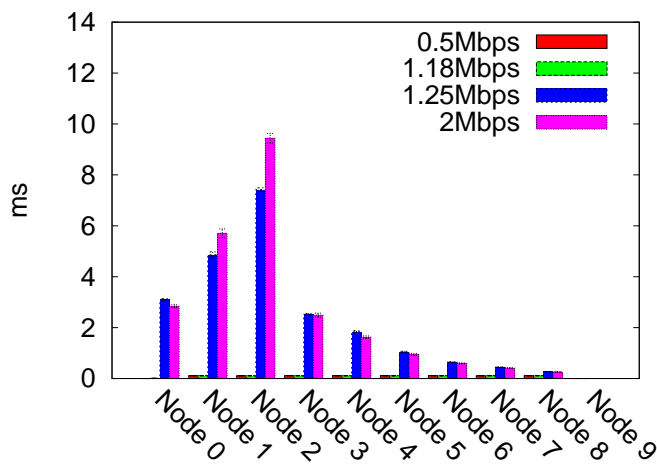
Observing all of the simulation results, we observed that the network had two possible states: non-saturated and saturated. The non-saturated state takes place when the CBR bit rate is less than or equal 1.185 Mbps with packet size of 1000 bytes. In non-saturated state, the collision probability is very small, there is no loss during the simulation and the length of interface queue is $\simeq 0$. When the rate exceeds 1.185 Mbps, the network enters into the saturated state where the collisions become more frequent and packet losses occur.

4.5.2.1 Results for scenario 1

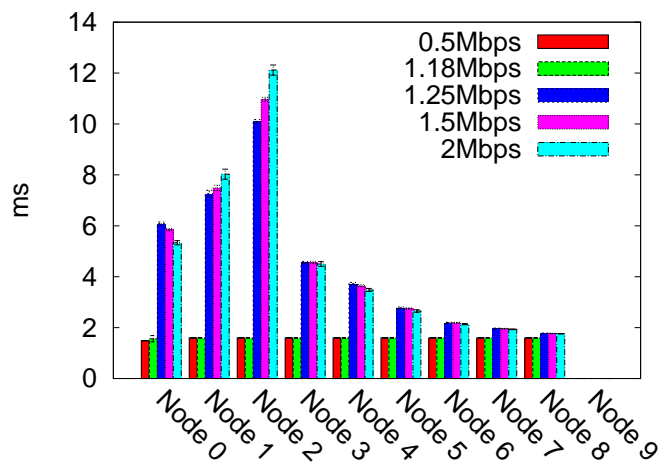
The effect of traffic load is evaluated by changing the traffic source rate of a flow or using a number of concurrently running flows. In scenario 1.1 and 1.2, the intra-flow interference is investigated by using one connection flow. Different traffic rates are assigned to the connection, once and unchanged during simulation in scenario 1.1. While in scenario 1.2, the flow source sudden increases its sending rate and then turns back to its initial rate after a time period. The number of concurrent flows is increased for each simulation in scenario 3 to examine the inter-flow interference.

Fig. 4.3, 4.4, 4.5 and 4.6 show the simulation results for these scenarios. The statement for the behavior of each metric in each scenario, except 1.2, is explained in the following. In the simulation results of scenario 1.2, the sudden increment of the source rate causes the network to enter temporarily into the saturated state during a small period of time. The metric behavior during that time is representative to the overloaded state of the network. Thus, the explanation for the saturated state of scenario 1.1 and 1.3 can be applied to scenario 1.2 (Fig. 4.4).

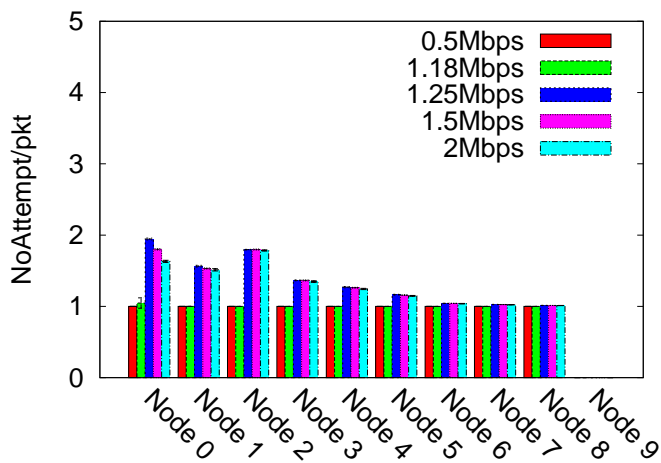
4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION



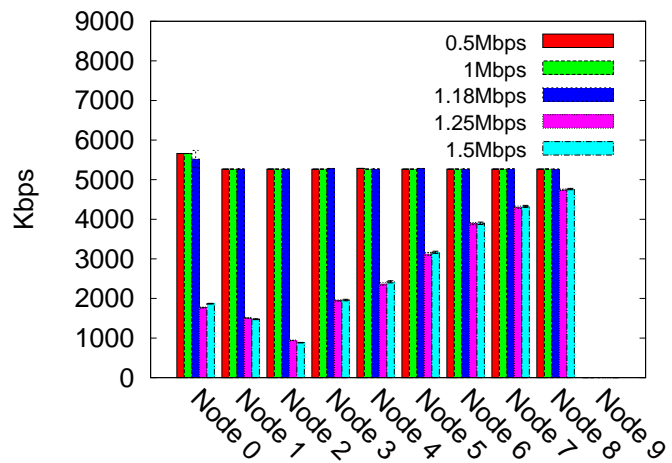
(a) Medium Access Delay



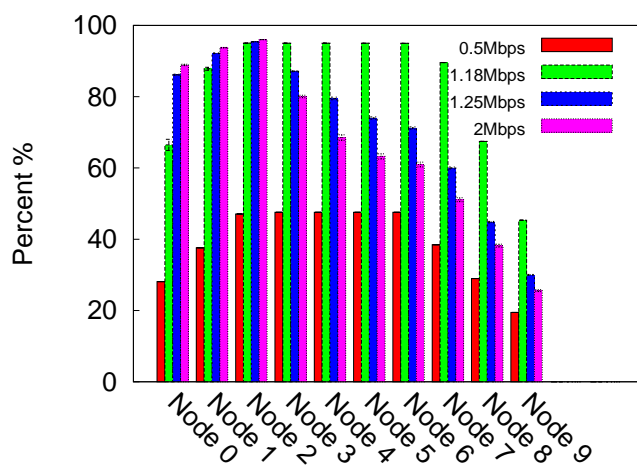
(b) Average Transmission Time



(c) Average Transmission Attempt



(d) Effective MAC Throughput



(e) Channel Busyness Ratio

Figure 4.3: Scenario 1.1: one flow with different source rates

4.5 Simulation and Results

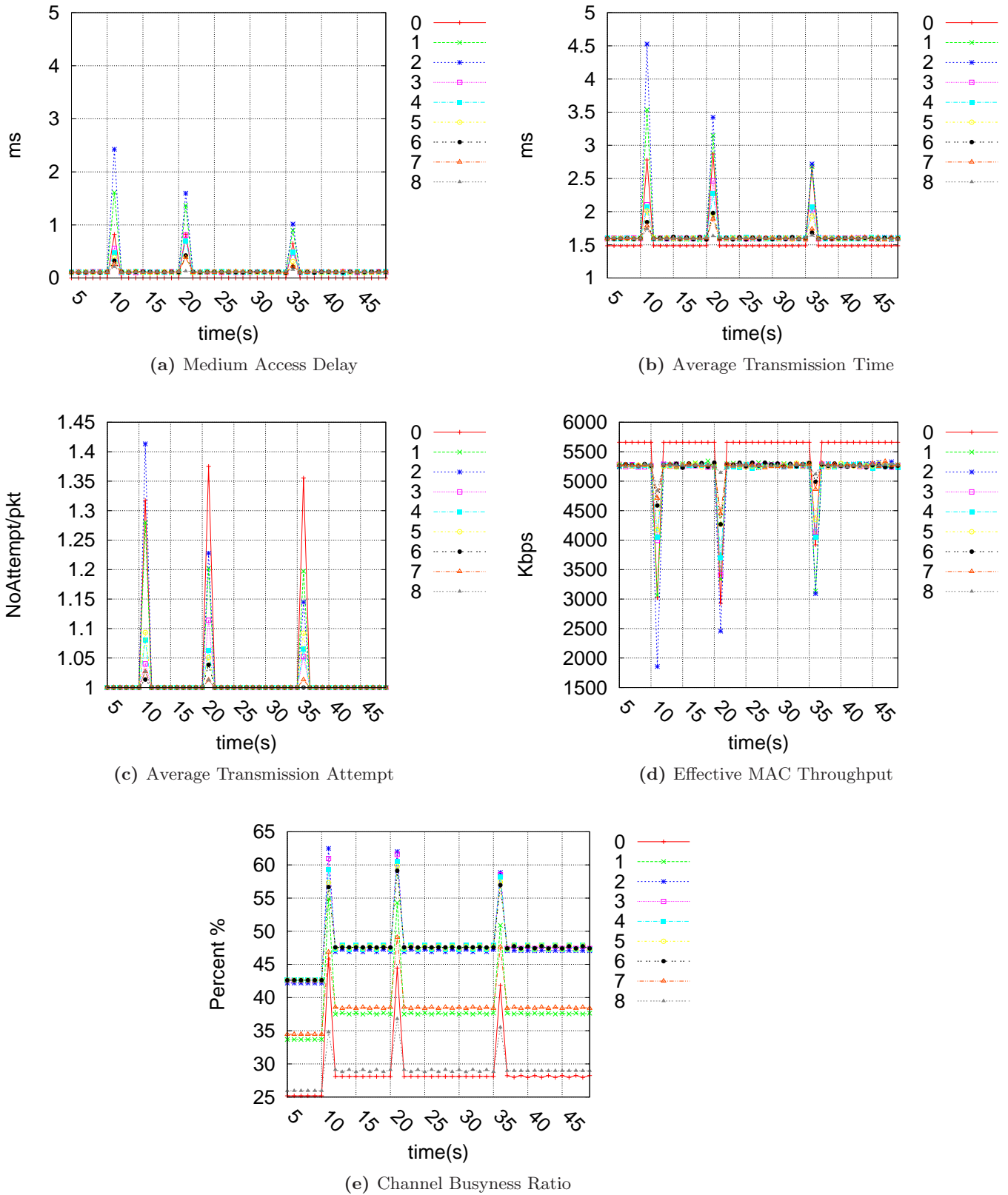
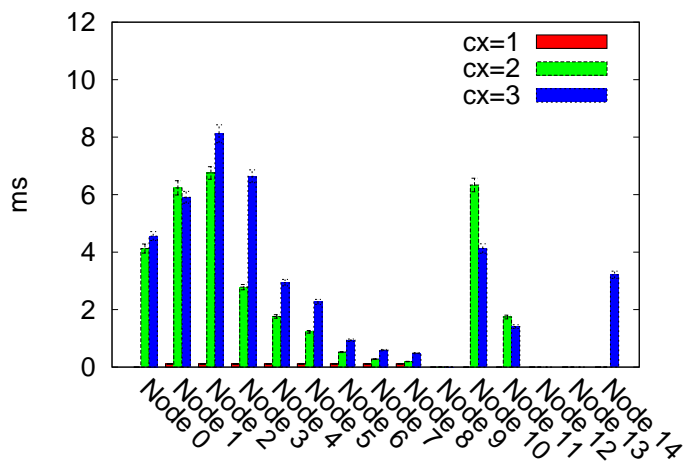
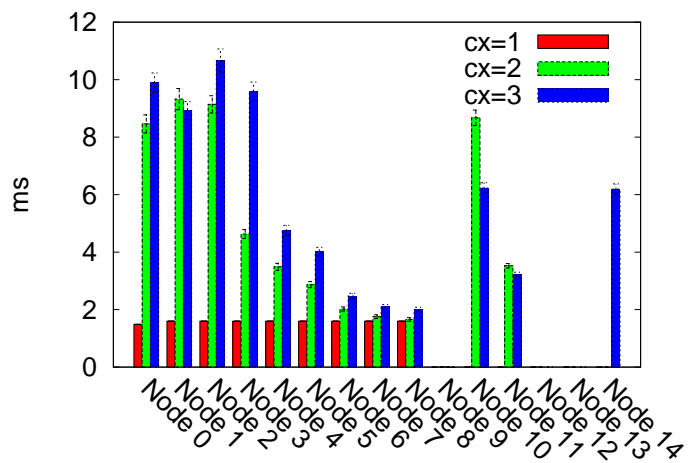


Figure 4.4: Scenario 1.2: one flow with sudden change in traffic rate

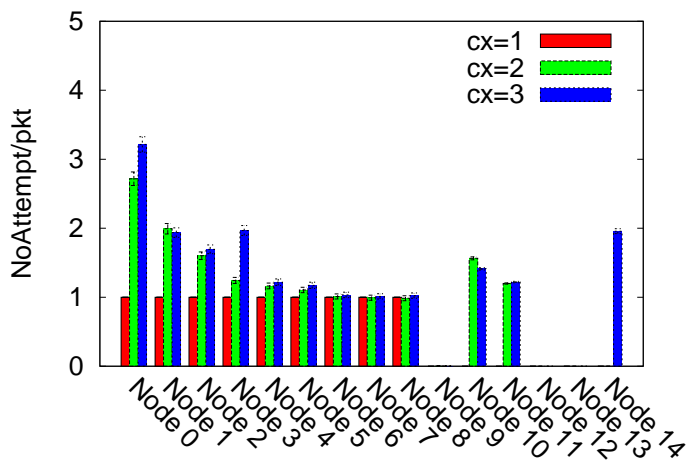
4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION



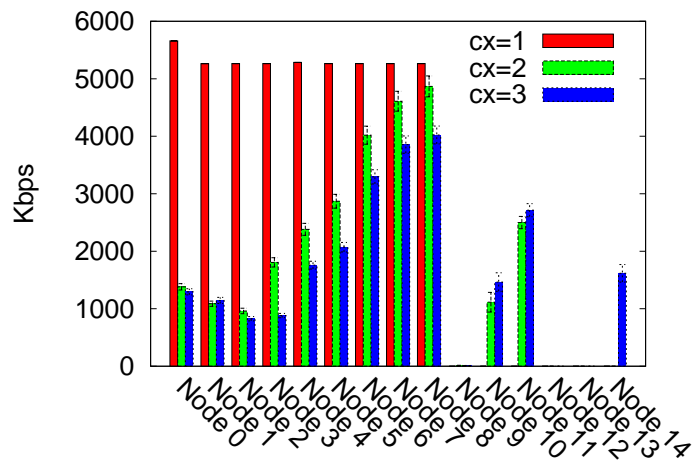
(a) Medium Access Delay



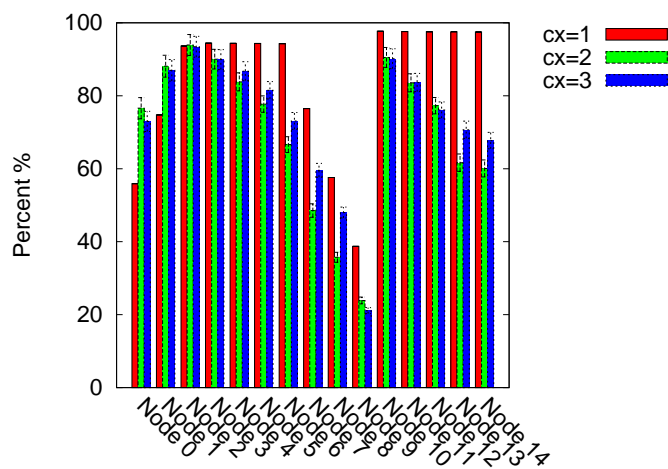
(b) Average Transmission Time



(c) Average Transmission Attempt



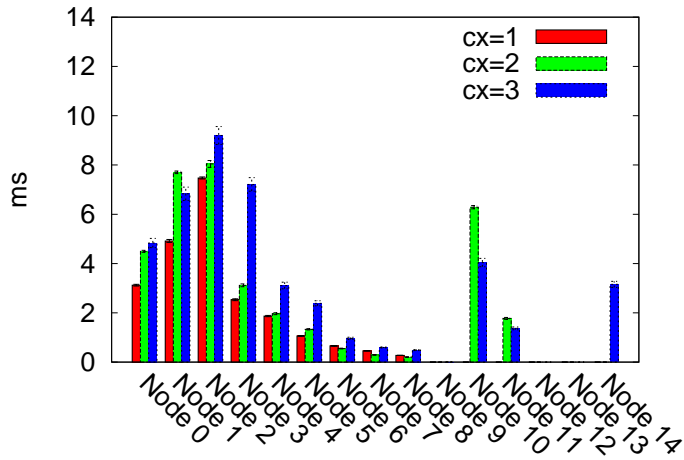
(d) Effective MAC Throughput



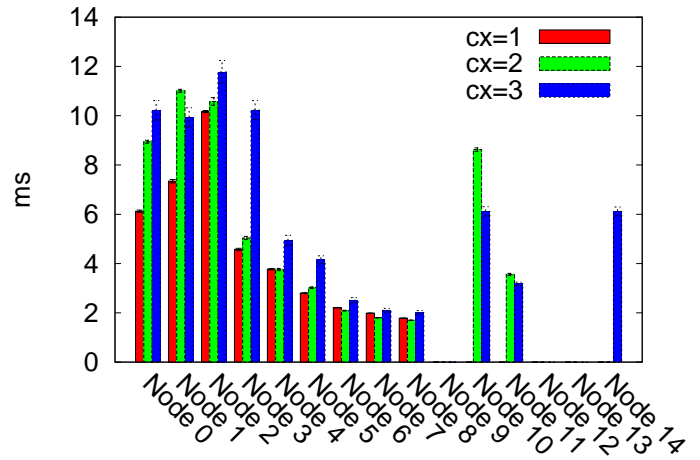
(e) Channel Busyness Ratio

Figure 4.5: Scenario 1.3: flow 1's rate is 1Mbps

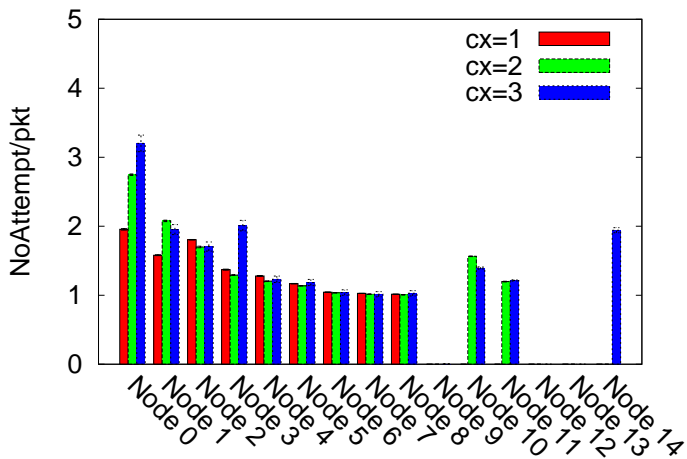
4.5 Simulation and Results



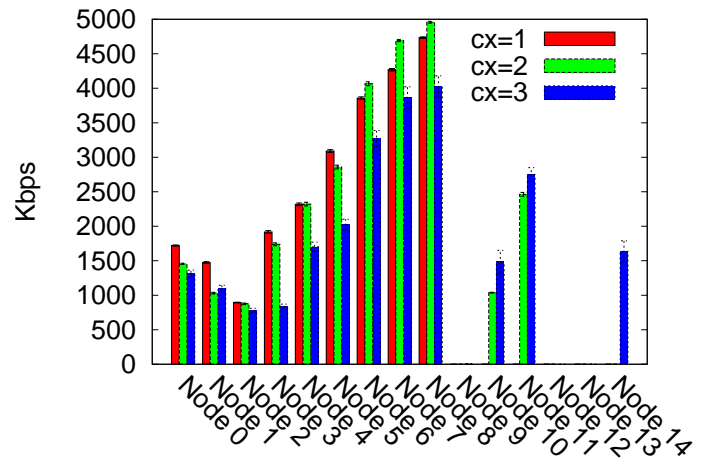
(a) Medium Access Delay



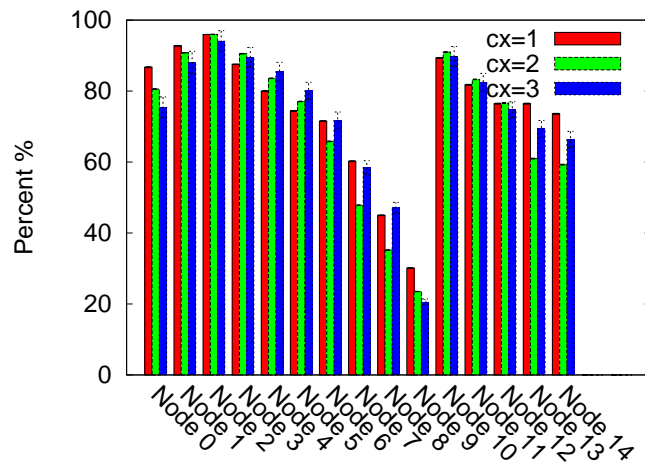
(b) Average Transmission Time



(c) Average Transmission Attempt



(d) Effective MAC Throughput



(e) Channel Busy Ratio

Figure 4.6: Scenario 1.3: flow 1's rate is 1.25Mbps

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

The *ATA* metric

The *ATA* is equal to its intrinsic value, i.e. 1, in non-saturated state for all nodes and regardless of traffic rate, packet size and node's position (Fig. 4.3.c). This comes from the fact that the MAC layer performs only one attempt to successfully transmit a packet. In saturated state, *ATA* value depends on the node's position and on the traffic load. It exceeds 1 in the first nodes where the contention is high while at the ending nodes, *ATA* is close to 1 (Fig. 4.5.c and 4.6.c). However these variations are almost unremarkable compared to those of other metrics.

The *MAD* metric

The *MAD* metric's value is quite constant around a special value ($\simeq 111\mu\text{s}$) in non-saturated state as showed in Fig. 4.3.a. Because the MAC layer invokes only one backoff stage, the *MAD*'s special value is the backoff time with the minimum contention window of the first successful transmission attempt. In this case, *MAD* is independent of packet size, node's position and traffic rate as long as the rate is smaller than a threshold.

When the channel is overloaded by increasing traffic load (in terms of either the data rate (Fig. 4.3.a) or the number of concurrent connections (Fig. 4.5.a and 4.6.a), packet losses occur. Thus, the number of attempts to transmit a packet increases with the number of backoff stages, thanks to ARQ mechanism. After each failed transmission, the backoff time is longer due to the increment of MAC Contention Window [28]. The contention time is longer as well because, at this time, every node in the neighbourhood has packets to send which may make the node's MAC freeze its backoff procedure more frequently. The *MAD* as the total number of all contention times calculated in the interval increases as well. *MAD* value also grows with the increase of traffic rate which is the reason exacerbating the contention level in the network. Thus, *MAD* reflects well both medium busyness and contention level in the neighborhood of a node.

The *ATT* metric

In the non-saturated network, *ATT* behaves like *MAD* as shown in Fig. 4.3.b, 4.5.b and 4.6.b. The MAC layer needs only one attempt to transmit successfully a packet, so *ATT* includes one backoff time and one transmission time and it is relatively constant ($\simeq 1.6$ ms).

In saturated state, *ATT* metric varies largely and increases far from the value in non-saturated state. At this time, its value depends also on the node's position, traffic rate and packet size. Like *MAD*, *ATT* increases with the traffic load but it depends on the packet size. Moreover, they differ in their order of magnitude between the values in non-saturated and saturated states. As *ATT* includes the transmission time, its value in non-saturated state is of 1.6 ms and that in saturated state is of 8.1 ms, whereas *MAD* consists only in contention time with the respective values of 0.111 ms and 6 ms. However, in saturated state, the *MAD* slope is also steeper than that of *ATT*. Thus, *MAD* allows to detect contention faster and clearer than *ATT*.

There are also some comparative observations for MAD and ATT from Fig. 4.3.a and Fig. 4.3.b that should be explained as in the following.

In non-saturated state, the values of MAD and ATT are relatively constant regardless of the traffic rate. The reason is that the total contention duration increases proportionally to the number of successfully transmitted packets when the source rate increases. For example, at a rate of 0.5 Mbps, the number of arrival packets is $\simeq 62$ with a total $T_{contention}$ of 6.7 ms, whereas at the rate of 1.18 Mbps, both values become 147 and 15 ms respectively. Hence, the ATT and MAD values change very slightly.

At node 0, the value of ATT and MAD decreases when the traffic rate increases from 1.25 Mbps to 2.0 Mbps. The reason comes from the analysis of simulation traces that the increasing amount of total channel time used to transmit packets and the corresponding total $T_{contention}$ between the two different traffic rates are small ($\simeq 0.08$ s and $\simeq 0.07$ s) while that of the number of successfully transmitted packets is considerable ($\simeq 50$ packets). Indeed, when the network becomes saturated, the average number of transmission attempts used for a packet does not increase much. It is the same for contention time. Node 0, in comparison to nodes 1 and 2, has a smaller number of interference nodes. In addition, the node experiencing a successful transmission is more likely to take the channel again than the node having a collision [97] [98]. Thus, node 0, the traffic source, can transmit more packets at the rate of 2 Mbps.

At nodes 1 and 2 in saturated state, the time spent for packet transmission and contention is high because they have to contend for the channel with the node 0 (traffic source). But it does not also increase much due to the increase of the source rate. As noted above, nodes 1 and 2 are likely to utilize less channel resource than the node 0. Therefore, most of the packets they received are dropped at the buffer. Also note that the node 0 can transmit more packets when its rate increases. Hence, the number of successfully transmitted packets at node 1 and 2 decreases when the source rate increases. Therefore, ATT and MAD values increase.

Finally, the traffic flow is in only one direction and node 3 is out of the interference range of node 0, all nodes from 3 to 9 do not suffer from severe interference with the traffic source. The contention time at this region is then not too large. The contention time increases less than the increase of successfully transmitted packets which makes the MAD value decrease when the source rate increases.

The R_b metric

Fig. 4.3.e displays the average value of R_b of nodes with several traffic rates. In non-saturated state, R_b at each node is relatively constant and depends on the node's position, i.e. R_b at the end nodes of the path is smaller than that around the middle nodes. The reason is that the channel around the middle nodes experiences more transmission activity than that around the end nodes. The channel time is spent for successful transmission attempts and backoff stage, the collision time is almost zero and the transmission time is almost steady. At some nodes, R_b is around 96% when the traffic rate approaches the threshold. The reason for this high busyness is that the channel is used efficiently to transmit a large amount of packets. The idle time, therefore, is small and decreases when the traffic rate increases. In this state, the higher the rate is, the higher the values of R_b are.

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

However, when the rate exceeds the threshold (Fig. 4.3.e, 4.5.e and 4.6.e), R_b measured at each node oscillates largely and its average value decreases sharply at some nodes but is still as high as 96% at some other critical nodes near the traffic source. Note that nodes 1 and 2 lie in the interference range of node 0. Since the node 0 can still send more packets when the rate increases, the channel in the region of nodes 0, 1 and 2 experiences a higher busyness. Also note that the traffic flow is in one direction from node 0 to node 9, and the interference range is set to double of the transmission range, a lot of packets are dropped at nodes 1 and 2, node 3 lies out of the interference range of node 0, thus the number of arrival packets at node 3 is much smaller than that at node 2. This number is also smaller than that in non-saturated state when the rate is close to the threshold, i.e. 1.18 Mbps. Hence, the channel busyness from node 3 to 9 decreases when the rate increases. These results for R_b also match the work of Zhai et al. [70] [55].

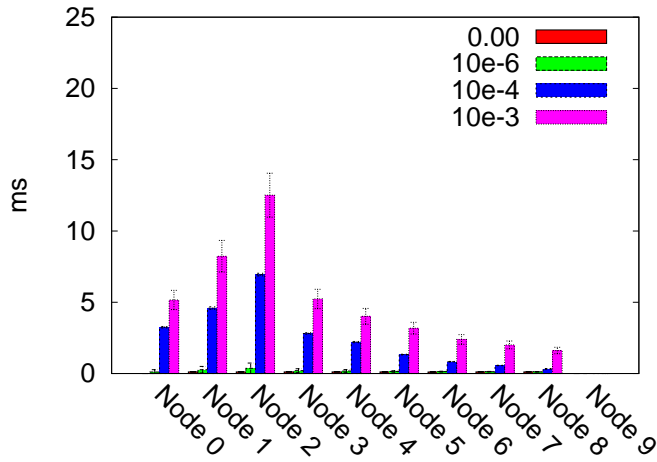
The *EMT* metric

The effective throughput *EMT* of each node reaches its maximum value under non-saturated state, regardless of traffic source rate and node's position (Fig. 4.3.d). When the network is overloaded (Fig. 4.3.d, 4.5.d and 4.6.d), *EMT* decreases and its value depends also on node's position. The obtained results are expected since the throughput relates to the number of successful transmitted packets and to their service time. Indeed, in non-saturated state, the service time for each packet is the smallest (same reason of *ATT*) and the total of service time for all arrival packets in an interval is proportional to the number of arrival packets. Also note that, if there is no collision loss, the number of successfully transmitted packets is equal to the number of arrival packets. Therefore, in this case, the *EMT* has the highest value. When the contention level is high and collision losses occur in saturated state, the number of successfully transmitted packets decreases while the service time for each packet increases. The *EMT* decreases as a consequence.

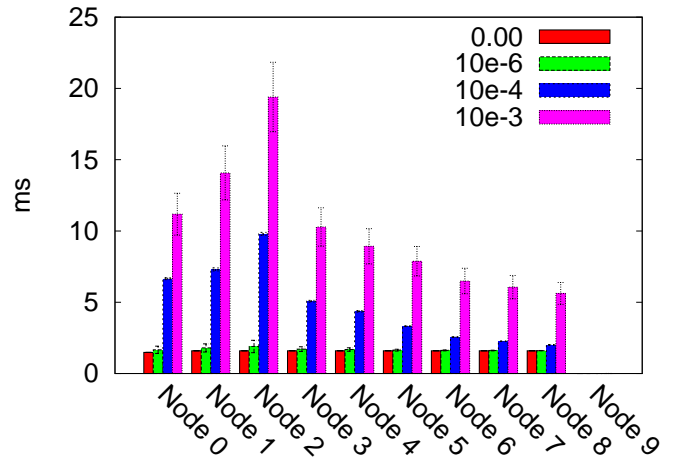
Conclusion

All the metrics that we have evaluated are relatively sensitive to the network load as they all have representative behaviour with the change of traffic rate. *ATA*, *ATT*, *EMT*, R_b and *MAD* can be used to indicate whether the network operation is under non-saturated or saturated state. Among them, *ATA* and *MAD* introduce a better feature that their values in non-saturated state of network operation are independent of node number, position, packet size and traffic rate (as long as it is smaller than a threshold). However, the scale between values of *ATA* corresponding to both network states is not as clear as that of *MAD* and *ATT*. In saturated state, *MAD* and *ATT* reflect faithfully the MAC states compared to R_b as they can point out the nodes where the contention or collision occurs caused by the traffic rate augmentation. Nevertheless, *MAD* reflects better the medium busyness and the contention level in the neighborhood of a node. Furthermore, *ATT* includes also the transmission delay which is relatively large compared to the backoff time. So the change of *MAD* as an early indication of contention or collision is more clearly than that of *ATT*. Thus, *MAD* metric seems to be the most accurate and early indication on network load.

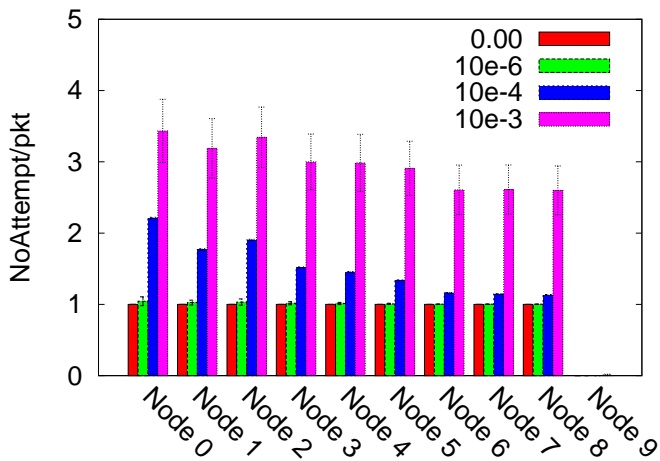
4.5 Simulation and Results



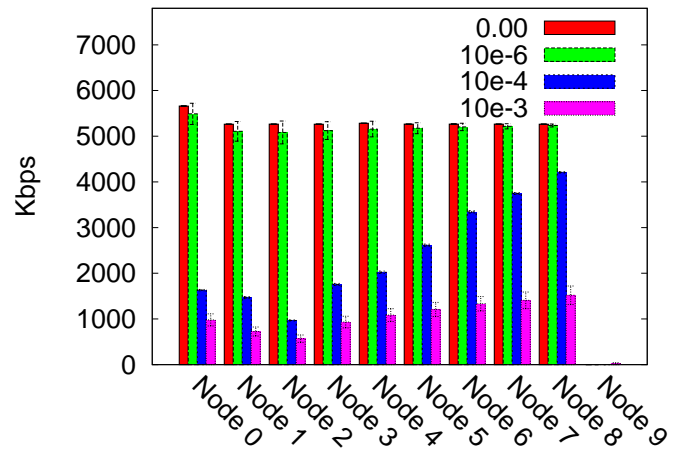
(a) Medium Access Delay



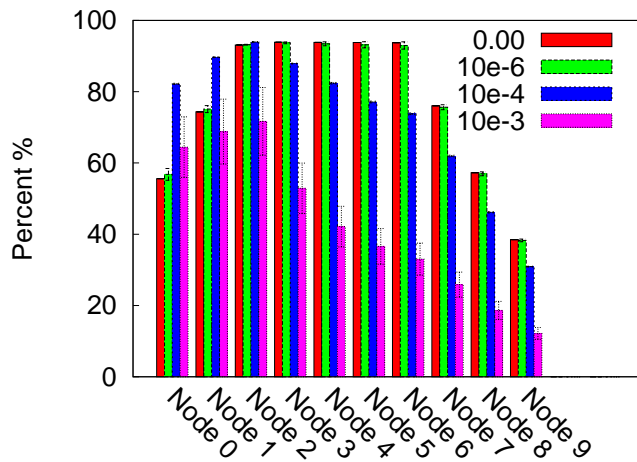
(b) Average Transmission Time



(c) Average Transmission Attempt



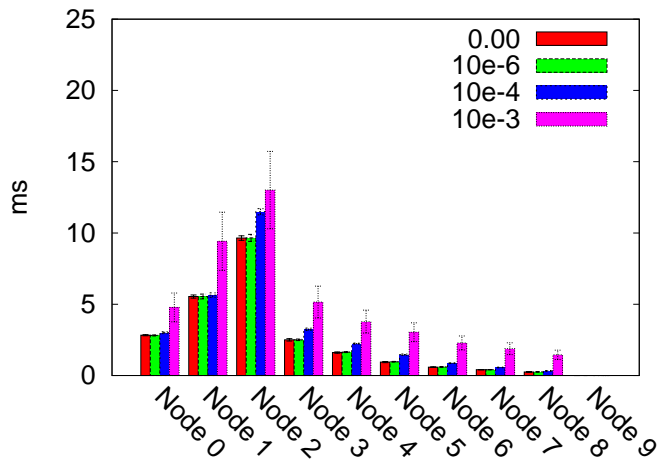
(d) Effective MAC Throughput



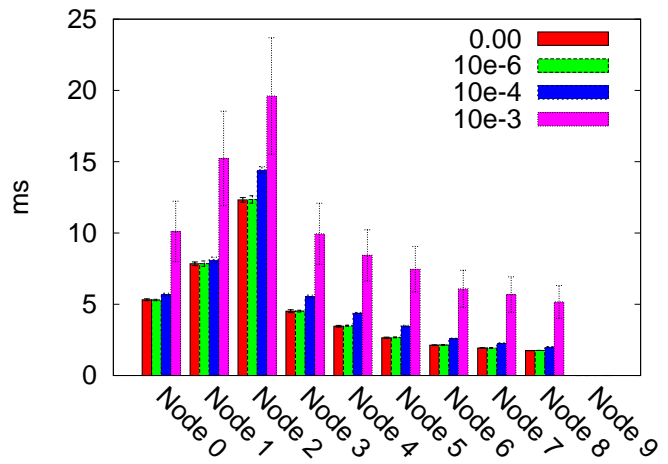
(e) Channel Busyness Ratio

Figure 4.7: Scenario 2.1: traffic rate 1Mbps

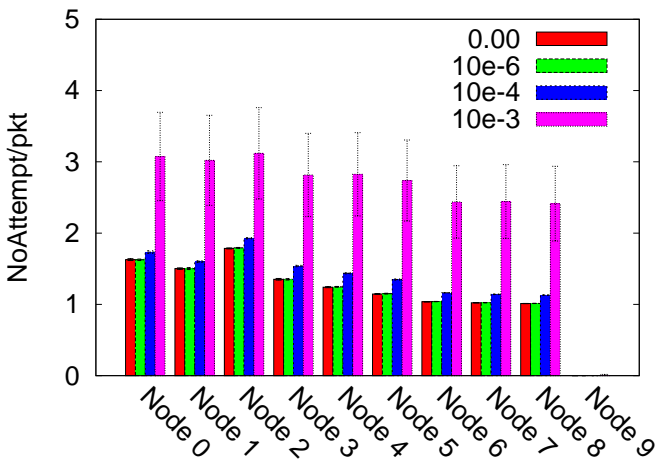
4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION



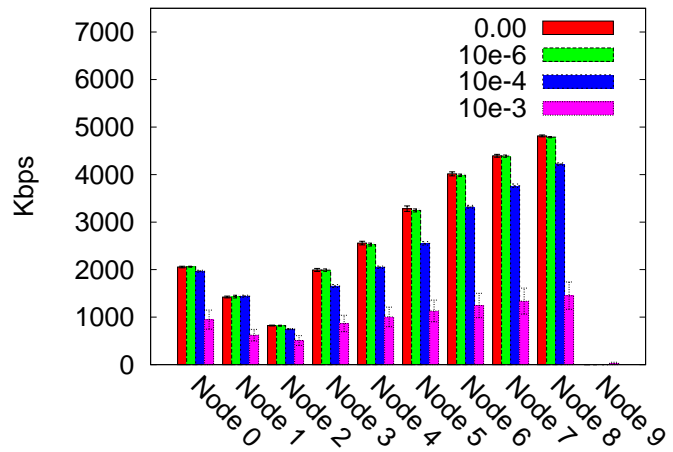
(a) Medium Access Delay



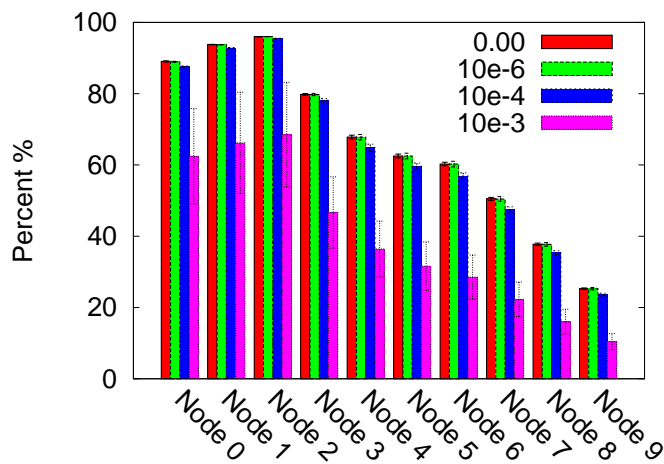
(b) Average Transmission Time



(c) Average Transmission Attempt



(d) Effective MAC Throughput



(e) Channel Busyness Ratio

Figure 4.8: Scenario 2.1: traffic rate 2Mbps

4.5 Simulation and Results

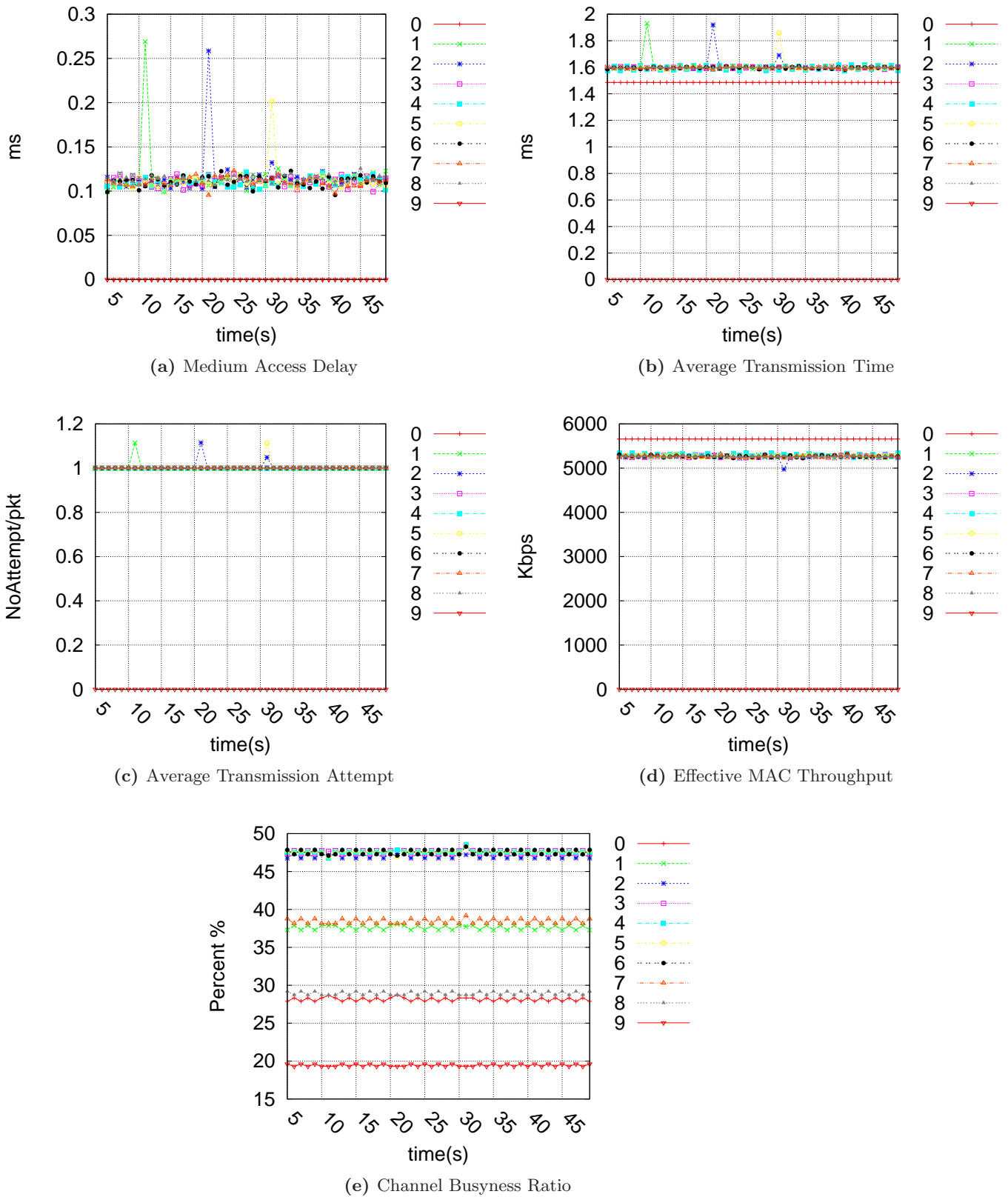


Figure 4.9: Scenario 2.2: 1 connection with rate = 0.5Mbps and BER=10e-6

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

4.5.2.2 Results for scenario 2

In this scenario, the effect of channel BER is taken into consideration. Only one connection flow is established during the simulation and the network is configured with different BER values. Each BER value is also examined with different traffic rates.

Fig. 4.7 shows that, in non-saturated state with small traffic rate, the behavior of the metrics is not affected by small BER ($\leq 10e-6$). But with rather high BER, the metrics lose their best performance since the number of retransmission attempts rises up due to BER and the network may be forced into high contention and collision state. In saturated state (Fig. 4.8), these metrics can not distinguish between BER losses and collision losses since the ARQ mechanism is applied at MAC layer for all kind of loss. Thus, the following presents some remarks for the behaviors of these metrics in non-saturated state with relatively small BER.

In Fig. 4.9.a, 4.9.b, 4.9.c, *MAD*, *ATT* and *ATA* have the same behavior for the channel losses. When channel losses occur, the number of attempts to transmit a packet, *ATA*, increases as well as the number of backoff stages thanks to ARQ mechanism. After each failed transmission, the backoff time is longer due to the increment of MAC Congestion Window [28]. Hence, *MAD*, which includes the total number of all contention durations, and *ATT*, which includes both *MAD* and (re)transmission attempts calculated in the interval, increase accordingly.

After the loss, if the traffic rate is small, *MAD*, *ATT* and *ATA* turn back to the normal behavior. Otherwise, the channel losses may force the network to enter into the high contention and collision state. The reason is that, if the traffic rate is small enough, i.e., the arrival rate is smaller than the frame service rate at MAC, the average queue length is always smaller than 1 and the next frame does not almost have to contend for the medium and needs only one attempt to be successfully transmitted. In contrast, if the traffic rate is high, the average queue length of nodes in the neighbourhood is greater than 1 after the loss, then the sending node has to contend for the medium with its neighbours. Therefore, the contention level grows up and collision may occur which in turn leads to overload the network.

The R_b metric is not really sensitive to channel losses with small BER (Fig. 4.9.e). Before the MAC layer drops the packet after several failed transmissions, the increased amount of the channel idle time around the link is relatively small because this loss is not caused by collision resulting from high contention level. The node performs retransmission attempts with small backoff time and, therefore, the channel is still busy by collision and transmission events. Hence, R_b during the BER loss duration does not significantly change.

In non-saturated state, *EMT* changes significantly with burst losses due to channel error (Fig. 4.9.d). Indeed, the ARQ mechanism will lengthen the packet service time while the total number of successful transmitted packets decreases. This results in decreasing *EMT* computed in the interval at the nodes where the losses occur.

Conclusion

In non-saturated state, the observation of the change of ATA , ATT and MAD can help to determine the losses caused by channel error since there is no collision loss in this state. Nevertheless, the non-saturated state is hard to achieve in common network operation due to rather complex traffic patterns. In saturated state where MAC losses occur frequently due to collision, the BER losses can not be distinguished by these MAC metrics. However, it is also feasible to use ATT , ATA and MAD to indicate the general losses at MAC due to either BER or collision.

4.6 Summary

The approach of improving the transport protocol performance in MHWNs by using MAC metrics has been exploited in several proposals. Since MAC metrics are created in order to provide MAC information to the upper layer protocols, it is very important to study the effectiveness of the MAC metrics, i.e., their ability to reflect the problems of lower layer network operation, especially the indication of network congestion.

In this chapter, we first provided criteria for the term “metric effectiveness” whereby a MAC metric claimed to be effective should have representative behavior with the network contention level and the medium related losses. We then provided a study which investigates the behavior of common MAC metrics through various scenarios to show their effectiveness to reflect the network condition. Through this study, we found out some effective MAC metrics that can be used to improve the transport protocol performance in MHWNs.

All of the considered metrics can be used to indicate whether the network operation is under non-saturated or saturated state. Among them, MAD and ATT appear as potential metrics which provide the accurate information about network congestion/collision level.

In non-saturated state, MAD , ATA and ATT are independent of node number, node position and traffic rate. MAD and ATA does not also depend on the packet size. Although the value of ATA in non-saturated state is also independent of node number, position, packet size and traffic rate, the scale between values of ATA corresponding to both network states is not as clear as those scales of MAD and ATT . Moreover, in non-saturated state, the observation of the change of ATT and MAD can help to determine the losses caused by channel error since there is no collision loss in this state.

In saturated state, MAD and ATT reflect faithfully the MAC states compared to R_b and EMT as they can point out the node region which is experienced high traffic load. Since ATT includes also the transmission delay which is relatively long compared to the backoff time, the change of MAD as an early indication of contention/collision is more clearly than that of ATT . It is also feasible to use both metrics to indicate the general losses at MAC due to either BER or collision.

With those remarkable advantages, in the next chapters, two effective metrics MAD and ATT are exploited in our proposed schemes to improve the rate control of transport protocols in MHWNs.

4. EFFECTIVENESS OF MAC METRICS TO REFLECT NETWORK CONDITION

Chapter 5

Medium Access Delay aware Rate Control for Transport Protocol

In Chapter 2, the performance degradation of common transport protocols in MHWNs and the improvement proposals have been investigated. Most of the proposals concentrate on window-based protocol like TCP. Our approach does not interest in the window-based congestion control but in the rate-based congestion control which is used for VoIP or streaming applications. TCP-Friendly Rate Control (TFRC) [47] is one of the most common candidate as it does not cause network instability, thus avoiding congestion collapse. It is also fair to TCP flows, which is the dominant source of traffic on the Internet. The TFRC's rate fluctuation is lower than TCP, making it more appropriate for streaming applications which require constant video quality. However, as other Internet dominant protocols, TFRC was first designed to work in wired networks which provide high bandwidth and very low loss rate. Therefore, TFRC suffers from performance degradation in MHWNs since its rate control mechanism tends to send more traffic than the capacity of the network. As a consequence, the packet loss rate and latency rise up and shoot out the requirements of VoIP or media streaming applications. Chen et al. [99] claim that the TFRC's loss rate estimation used in the throughput equation is highly inaccurate in MHWNs. In addition, delay measurement is unreliable in MHWNs and does not reflect the growth of the end-to-end hop distance [90]. Hence, the equation is not guaranteed to use in this kind of environment [90]. It creates the need of a new rate control mechanism based on MAC information which operates efficiently in MHWNs.

The aim of this chapter is to propose a new rate regulation method which adapts the source bit rate depending on the MAC layer contention level. Indeed, with regard to these improvement proposals and the fact that the congestion is closely coupled with the contention as demonstrated in [90], it is feasible to improve the performance of transport protocols by considering only the contention state of the network. The contention growth event should be detected as early and accurately as possible, and there should be a mechanism which can react efficiently to this event in order to reduce the effect of high contention level in the network.

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

Moreover, as mentioned in Chapter 2, the unfairness is a severe problem suffered by TCP flows in Multi-hop Wireless Networks [53] [55]. The improvement mechanism should treat carefully this problem, thus ensures that there is a relatively fair share channel bandwidth for competing flows. In other words, the flows which suffer from heavy contention for a long time should be assigned a reasonable portion of channel bandwidth to prevent themselves from starvation. However, this fair share will reduce the channel reuse and the aggregated throughput accordingly. Therefore, the unfairness problem can be solved only with an expense of the aggregate throughput [55].

In this chapter, we explain a new rate-based transport protocol which can early detect the contention growth event in MHWNs and control efficiently the traffic rate transmitted throughout the network. Our proposal employs the *MAD* metric (Section 4.1.3 in Chapter 4) to early determine whether the network enters into high contention/collision level, then applies an effective rate control to prevent the flow from severe performance degradation. The simulation is then performed to evaluate the performance of our proposal in MHWNs. The results show that the proposal not only reduces the unfairness problem, but also introduce a high performance in terms of end-to-end delay and packet loss ratio which are the two critical requirements for real-time streaming applications.

5.1 The design of Medium Access Delay aware Rate Control

5.1.1 General idea

The proposed scheme, called MAD-TP, is aimed at providing an efficient rate control mechanism at transport layer which can reduce the contention effect of MHWNs. The idea behind MAD-TP comes from the observation of *MAD* in Chapter 4. The *MAD* value of all nodes in the interference range of the bottleneck link increases sharply when the contention level around the link becomes severe. For example, the *MAD* value of nodes, when the network (chain topology) is non-saturated, is around $111 \mu\text{s}$ and rather stable while that in saturated state ranges from $1000 \mu\text{s}$ to 10ms and even higher sometimes (Chapter 4). The rate control mechanism then can use the *MAD* metric as an early indication of contention growth event of the network in order to adjust appropriately the pace of sending packet over the network. To do that, every node on the network measures the *MAD* value periodically. For every packet passing the node, it adds its *MAD* value to the existing value stored in an option field in the IP header, called Cumulative *MAD* (*CMAD*). With this rule, when the packet reaches the destination, the *CMAD* field will contain the cumulative contention delay along the path it has travelled. After processing the cumulative contention delay from the arrival packet, the MAD-TP receiver feeds the network contention information back to the sender together with the receiving rate by using appropriate acknowledgement mechanism. The MAD-TP sender then uses this information to control the sending rate. The proposal is explained in detail for each type of nodes involved in the path.

5.1.2 Intermediate nodes

The role of intermediate nodes is to provide estimation of contention level experienced by each node along the connection path. Each node maintains the measurement of MAD in every interval. In the implementation, the interval duration is set to 0.1 second as the trade off between the smoothness and effectiveness. If the interval duration is short, the value of MAD may vary largely due to the change of contention level then the sending rate which is based on MAD may fluctuate as well. In contrast, if the interval is too long, the value of MAD can not react quickly enough to the change of the network status, thus reduce the effectiveness of MAD-TP.

For the i^{th} transmission of every arrived packet in the interval, the node's MAC records the time instant the packet starts to contend for medium access t_s^i and the time instant the packet starts to be actually transmitted over the medium t_t^i . Then the contention time of the i^{th} transmission of the observed packet $T_{contention}^i$ is simply calculated as $t_t^i - t_s^i$. Note that the number of transmission attempts i is limited by parameters $RetryLimit$ defined in IEEE 802.11 standard [28]. If k is the number of transmission attempts that the node takes to successfully transmit the observed packet or drops it after $RetryLimit$ attempts, thus $1 \leq k \leq RetryLimit$ and the contention time of that packet is calculated as

$$MAD_{pkt} = \sum_{i=1}^k (t_t^i - t_s^i) \quad (5.1)$$

During the observed interval, the contention time is aggregated over all arrived packets at MAC layer and the final value is divided by the number of arrival packets in that interval to form the metric MAD .

For all outgoing packets, the node updates the aggregated contention access delay in the IP header field $CMAD$ by adding its MAD value to the existing value in that field. When the packet reaches its destination, the receiver will obtain the cumulative value MAD_{cum} from all nodes along the path. Therefore, the MAD_{cum} value will reflect the current contention level along the connection path.

5.1.3 MAD-TP receiver

The function of MAD-TP receiver is to collect information about network condition, i.e. medium access delay, and to feed it back to the sender together with other helpful information. Every time receiving a packet, MAD-TP receiver takes the MAD_{cum} value from the IP header field $CMAD$, and the number of hops (N_h) from the TTL field or from the routing table of source routing protocols. The MAD-TP receiver takes also the sender estimated Round Trip Time r_{tt} attached to the field RTT of the MAD-TP data packet as in TFRC [47]. First, MAD-TP receiver computes the most recent contention level of the network MAD_{sample} collected by that packet as

$$MAD_{sample} = MAD_{cum}/N_h \quad (5.2)$$

The MAD-TP receiver then derives the average medium access delay by using the

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

Exponentially Weighted Moving Average (EWMA) function as follows:

$$MAD = \alpha MAD + (1 - \alpha)MAD_{sample} \quad (5.3)$$

α is set to 0.5 in the implementation. This average value is calculated as in equation 5.3 for every received packets.

Second, beside the average medium access delay, the receiver also estimates the average receiving rate R_{rcv} as

$$R_{rcv} = \frac{N_{rp}}{T_f} \text{ packet/s} \quad (5.4)$$

where T_f is the time duration from the last report until the time when the current report is generated and N_{rp} is the number of packets received by the receiver during T_f .

Whenever the receiver detects a loss, it computes R_{rcv} by the equation 5.4 and immediately sends a feedback packet which contains the current estimated MAD and R_{rcv} values to the sender. The MAD-TP sender will use these two values in the rate control mechanism in order to update the sending rate according to the change of contention level along the network path.

In addition, the receiver should send at least a feedback every round trip time r_{tt} if there is no loss detected. In this case, the T_f in the equation 5.4 is equal to r_{tt} . This will help the sender to keep in mind the updated knowledge about the connection's condition.

5.1.4 MAD-TP sender

The main function of MAD-TP sender is to adjust properly the traffic rate pumped into the network according to the information fed back from the MAD-TP receiver.

When the sender starts a new connection, the slow-start is invoked in order to probe the network capacity. The initial sending rate is set to 1 packet per second (pkt/s) when the sender has no sample of round trip time RTT . Each time receiving a feedback packet, the sending rate R is updated by the rule

$$R = \max(2 * R_{rcv}, S/RTT) \quad (5.5)$$

where S is the packet size and R_{rcv} is the average receiving rate obtained from the feedback packet. This rule guarantees that the sender sends at least one packet per RTT . The slow-start is terminated whenever the feedback MAD is greater than its threshold MAD_{TH} or the sender does not receive any feedback packet after a Retransmission Timeout RTO . In our implementation, the RTO is set to $4 * RTT$ as recommended in TFRC specification [47].

Depending on the received MAD , the sender controls its sending rate appropriately in order to keep the network operation under a stable state with reasonable contention level.

5.1 The design of Medium Access Delay aware Rate Control

If $MAD > MAD_{TH}$, the MAD-TP sender assumes that the connection experiences a severe contention along the path and decreases the sending rate. The decrease rule proposed by LAMP [54] is used, by which the sending rate is reduced by 1/8 after each RTT but never smaller than one packet per RTT . This reduction is small enough to avoid large rate fluctuation and is “large” enough to properly react to losses because with this reduction rule, the rate will be halved if the sender receives all feedback packets with $MAD > MAD_{TH}$ in 4 consecutive RTT s. The sender also halves the sending rate when the “NoFeedbackTimer” expires as in TFRC.

If $MAD \leq MAD_{TH}$, it means that a conservative amount of traffic ΔR may still be pumped into the network. The additional amount is chosen such that the new expected sending rate is proportional to MAD_{TH}

$$\begin{aligned} \frac{\Delta R + R}{MAD_{TH}} &= \frac{R}{MAD} \\ \Rightarrow \Delta R &= \left(\frac{MAD_{TH}}{MAD} - 1 \right) * R \end{aligned} \quad (5.6)$$

The new expected sending rate is then $R + \Delta R$. However, to avoid a sudden change in the sending rate, a smoothness rule is employed by which the new sending rate is chosen as follows:

$$R = \min(R + \Delta R, R + N * S/RTT, \max(2 * R_{rcv}, S/RTT)) \quad (5.7)$$

where N is the number of RTT s from the last rate change. Note that even being decreased by the rule of LAMP as mentioned above, the sending rate is always greater than 1 packet per RTT . Therefore, the equation 5.7 controls the update of sending rate such that it ensures the MAD-TP sender sends at least one packet per RTT and should not increase more than one packet per RTT .

5.1.5 MAD-TP packet formats

The packet formats of MAD-TP are showed in Fig. 5.1. As described in the previous sections, the MAD-TP sender uses data packets to send the payload and estimated RTT to the receiver, while the MAD-TP receiver uses feedback packets to send estimated receiving rate and the average MAD . MAD-TP sender and receiver also use data packets to control the connection establishment and termination phases.

The MAD-TP data packet has a 12 bytes header which consist of the following fields.

- Source port and destination port (16 bits each): used to uniquely identify the transport connection at both ends.
- Resrv (3 bits): future reservation field
- UG (1 bit): this urgent field is used to request the receiver to send immediately a feedback packet.
- Type (4 bits): used to distinguish between packet types, i.e., control packets or payload packet.

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

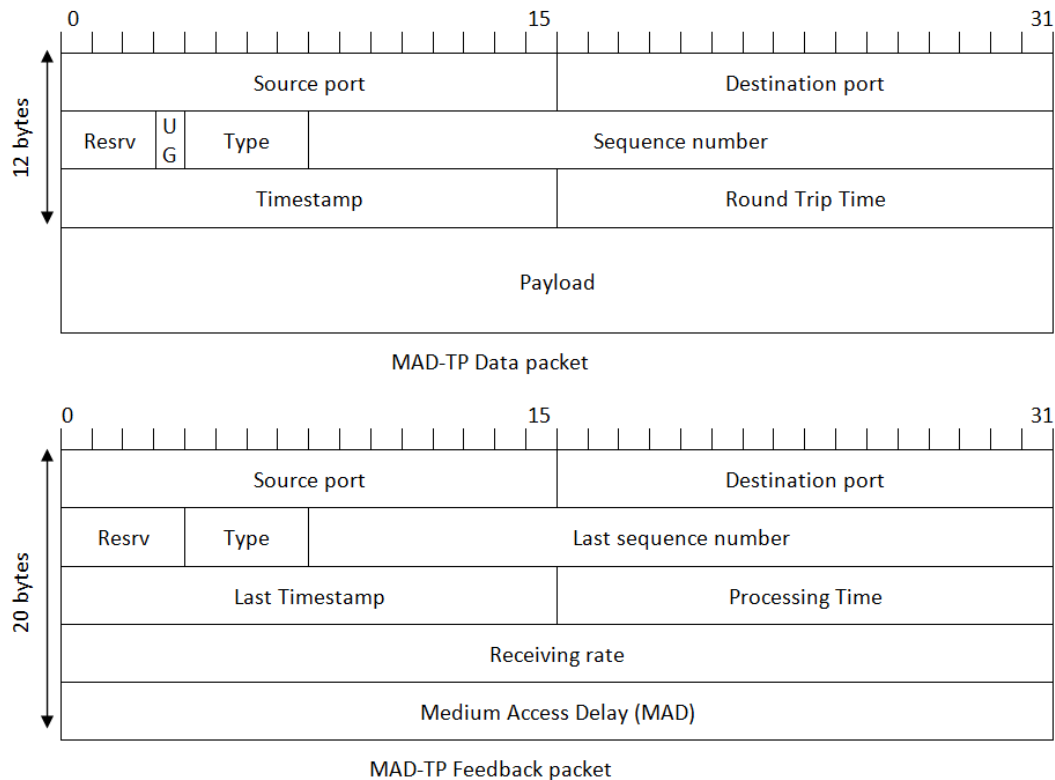


Figure 5.1: MAD-TP packet formats

- Sequence number (24 bits): used as the identifier for each data packet and must be incremented by one for each data packet transmitted.
- Timestamp (16 bits): used to the time instant this data packet is sent. The resolution is measured in millisecond.
- Round Trip Time (16 bits): used to carry the sender currently estimated round trip time. This value is used to estimate the receiving rate at MAD-TP receiver. The resolution is measured in millisecond.

The MAD-TP feedback packet has a 20 bytes header and contains no payload. It consists of the following additional fields.

- Last sequence number (24 bits): the last sequence number of the received data packet.
- Last timestamp (16 bits): the copy of the timestamp in the header of the last received data packet.
- Processing time (16 bits): the time duration from the instant the receiver receives the data packet to the time instant it generates this feedback packet. These three fields will be used to update the RTT at the MAD-TP sender as in TFRC.
- Receiving rate (32 bits): the receiver estimated receiving rate (packet per second) during the time period from the last feedback to this feedback.

- Medium Access Delay (32 bits): the current average MAD estimated at receiver, in millisecond.

Note that the cumulative MAD value along the path is attached to the option field CMAD in the IP header as mentioned in the Section 5.1.2.

In the next section, several simulation scenarios are built in order to evaluate the performance of MAD-TP in MHWNs.

5.2 Performance evaluation

In order to evaluate the performance of our rate control proposal MAD-TP, extensive simulations were performed using the network simulator ns-2, version 2.34 as in Chapter 4. The performance evaluation of MAD-TP is presented in comparison with that of TFRC and LATP [54]. In all topologies, the nodes in the MHWNs are static to reduce the effect of mobility and the channel is set to be perfect to eliminate the effect of channel error loss. There are 16 simulation runs in each scenario, each run is performed in 400s. In the simulation, MAD-TP, TFRC and LATP operate as they always have packets to send for the scheduled sending time instants, thus their operation does not depend on the application rate.

The performance factors are Throughput, End-to-End (E2E) Delay and Packet Loss Ratio (PLR).

The fairness assessment is performed as follows. In each simulation run, the maximum throughput among considered flows is selected. After 16 runs, 16 selected maximum values will be averaged to derive the averaged maximum flow throughput. The same method is used to find the averaged minimum flow throughput. The scale between the averaged maximum and minimum flow throughputs is also used. The minimum flow throughput shows how large a certain amount of bandwidth is at least granted to a flow. The closer to zero the minimum flow throughput is, the more severe the flow starvation level will be. The smaller the scale between the maximum and minimum flow throughputs is, the better bandwidth sharing among flows will be. The Jain's fairness index [100] is also be used.

The detail of simulations and results for each topology are explained in the following sections.

5.2.1 The threshold MAD_{TH}

MAD_{TH} is an important parameter in the operation of MAD-TP. From the Chapter 4, an observation was made such that the network may work in two states: saturated and not saturated. In non-saturated state, the measured value of MAD is about 0.111 ms while in saturated state, that value is more than 1 ms. However, if the first value is used as the threshold for MAD-TP, it is too small to allow a reasonable throughput of MAD-TP. Thus, MAD_{TH} is set to 0.7 ms as the trade-off between Throughput, E2E Delay and PLR.

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

5.2.2 Simulation scenarios

The simulations take place in three types of topology chain, grid and random because of the variety of interference schemes they represent. The general configuration for the simulation is the same as in Chapter 4 (Table 4.1). In all topologies, the nodes in the MHWNs are static to reduce the effect of mobility and the channel is set to be perfect to eliminate the effect of channel error loss.

5.2.2.1 Scenario 1

In this scenario, MAD-TP is investigated with the increase in contention level of the network. A simple chain topology is used and the variation of contention level is made by the increment of the number of hops.

In the chain topology, a pair of nodes is 200 m apart, thus the two adjacent nodes are in the transmission range of each other and two nodes 2 hops away from each other are in their interference range. In this experiment, the number of hops ranging from 4 to 13 will be used in order to observe more clearly the difference between the three protocols' operation.

- Topology: chain
- Number of hops: $\{4, \dots, 13\}$
- Traffic:
 - Type: $\{MAD - TP, TFRC, LATP\}$
 - Pattern: one connection flow from the first node \Rightarrow the last node of the chain, starts randomly at the first 3 seconds
- Transport packet size = 1000 bytes
- Routing scheme: $\{Precomputed, AODV\}$

5.2.2.2 Scenario 2

In this scenario, the operation of the protocols is investigated with the increase of load in a fixed hop chain network.

- Topology: chain
- Number of hops: 9
- Traffic:
 - Type: $\{MAD - TP, TFRC, LATP\}$
 - Pattern: 4 flows with the same sender (node 0) and receiver (node 8), starts randomly at the first 3 seconds

- Transport packet size = 1000 bytes
- Routing scheme: $\{Precomputed, AODV\}$

5.2.2.3 Scenario 3

This scenario tries to evaluate the operation of MAD-TP in a more complex grid topology as showed in Fig. 5.2. This topology provides more intricate and adjustable node contention patterns. 4 connection patterns are set up such that they provide different contention levels in the network. Therefore, the performance of the MAD-TP can be evaluated thoroughly.

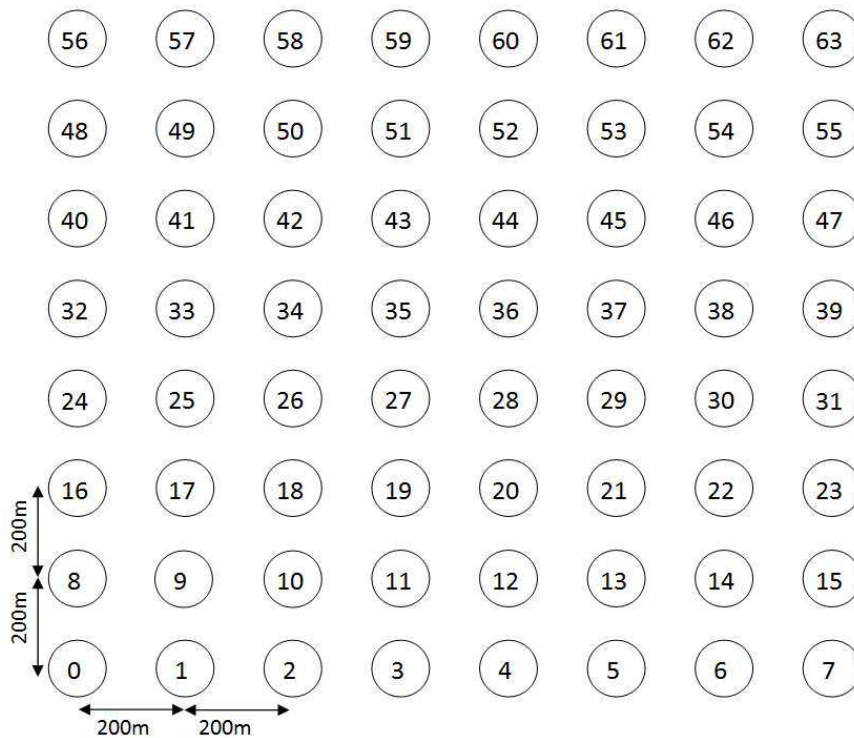


Figure 5.2: Grid 8x8 topology

- Topology: grid 8x8 nodes
- Traffic:
 - Type: $\{MAD - TP, TFRC, LAMP\}$
 - Pattern: 4 connections from node 0 \Rightarrow node 8, starts at 0.001s
 - * Pattern 1: two parallel flows from node 16 to node 23 and from node 39 to node 32. These two flows are 400m apart so that each pair of nodes of the two connection lying on the same column of the grid are out of transmission range but on the carrier sensing range of each other.

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

- * Pattern 2: 4 parallel flows are established from nodes 8, 31, 40, 63 to nodes 15, 24, 47 and 56 respectively. Each pair of flow is also 400m apart.
 - * Pattern 3: 8 parallel flows are initialized from nodes 0, 8, 23, 31, 32, 40, 55, 63 to nodes 7, 15, 16, 24, 39, 47, 48 and 56 respectively
 - * Pattern 4: 5 cross flows established from nodes 2, 8, 31, 40, 61 to nodes 58, 15, 24, 47 and 5 respectively where two parallel flows (2-58 and 61-5) cross three parallel flows (8-15, 31-24 and 40-47).
 - Connection establishment: each connection flow starts randomly in the first 3 seconds of the simulation
- Transport packet size = 1000 bytes
 - Routing scheme: $\{Precomputed, AODV\}$

5.2.2.4 Scenario 4

The operation of MAD-TP is also investigated in a more realistic random topology. Different contention levels are made by increasing the number of connection flows in the network. Each pair of source and destination of a connection is chosen randomly with its hop distance being at least 3 hops.

- Topology: random
- Number of nodes: 60 in 1500mx1500m area
- Traffic:
 - Type: $\{MAD - TP, TFRC, LATP\}$
 - Pattern: 4 patterns $\{4.1, 4.2, 4.3, 4.4\}$ correspond with $\{5, 10, 15, 20\}$ connection flows, each flow starts randomly in the first 3 seconds of the simulation
- Transport packet size = 1000 bytes
- Routing scheme: AODV

5.2.3 Results and discussion

5.2.3.1 Chain topology

Because both scenarios 1 and 2 use chain topology, their results will be presented and discussed in this section. The objective of two scenarios 1 and 2 is to investigate the considered protocols with the increase in contention level of the network. In scenario 1, the contention level of the network is changed by increasing the number of nodes in the chain network. In scenario 2, the network topology is fixed to a chain of 9 hops and 4 connection flows are established in order to increase the contention level.

The results for scenario 1 are showed in Fig. 5.3 and Fig. 5.4. It can be observed that MAD-TP outperforms TFRC in terms of Packet Loss Ratio and End-to-End delay.

5.2 Performance evaluation

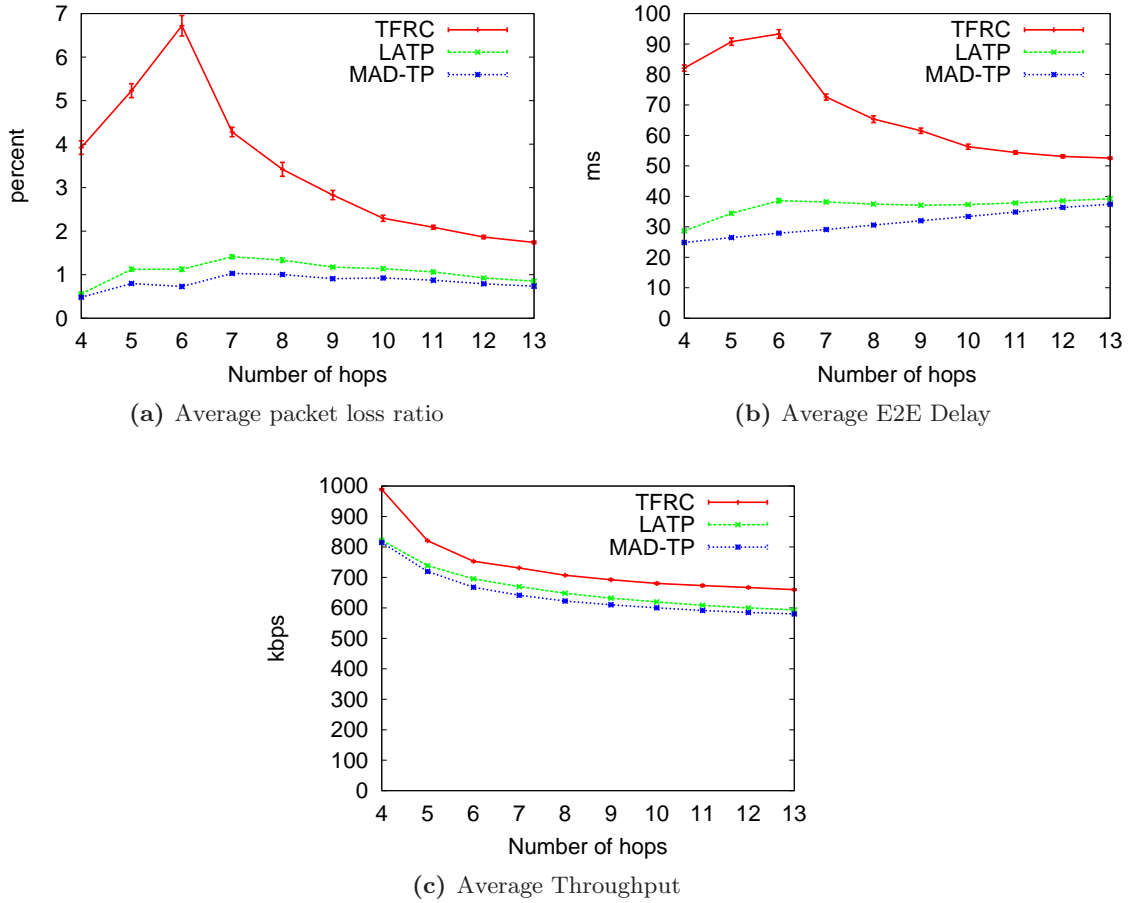


Figure 5.3: Chain topology with 1 connection and precomputed path

The PLR of TFRC is higher than that of MAD-TP from 0.8% (in case of 13 hops) to 6% (for network with 6 hops) and the time scale is from 10 ms (for network with 13 hops) to 60 ms (for network with 6 hops) for E2E delay. Particularly in the common MHWNs whose size is smaller than 10 hops, the difference is at least 1% for PLR and 20 ms for E2E delay. The reason is that TFRC’s rate control wrongly estimates the network capacity and tends to overload the MHWN which has small resource. This problem is caused by TCP throughput equation used in TFRC which depends on inaccurate packet loss ratio measurement in MHWNs [99], where losses are mostly due to channel contention. Thus, TFRC increases the rate inappropriately when the network contention is rather high and does not decrease the rate efficiently enough when the network contention becomes severe. As a consequence, the packets travelling along the path will suffer from high loss rate and delay caused by collision among contending nodes, multiple retransmission attempts at MAC level as well as high level of channel busyness.

In contrast, MAD-TP introduces small loss ratio and delay for all the number of hops. In addition, the E2E delay of MAD-TP flow is getting longer with the increase of the hop number but is always smaller than the delay introduced by TFRC. This increase seems to be more “reasonable” than that of TFRC. This improved result comes from

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

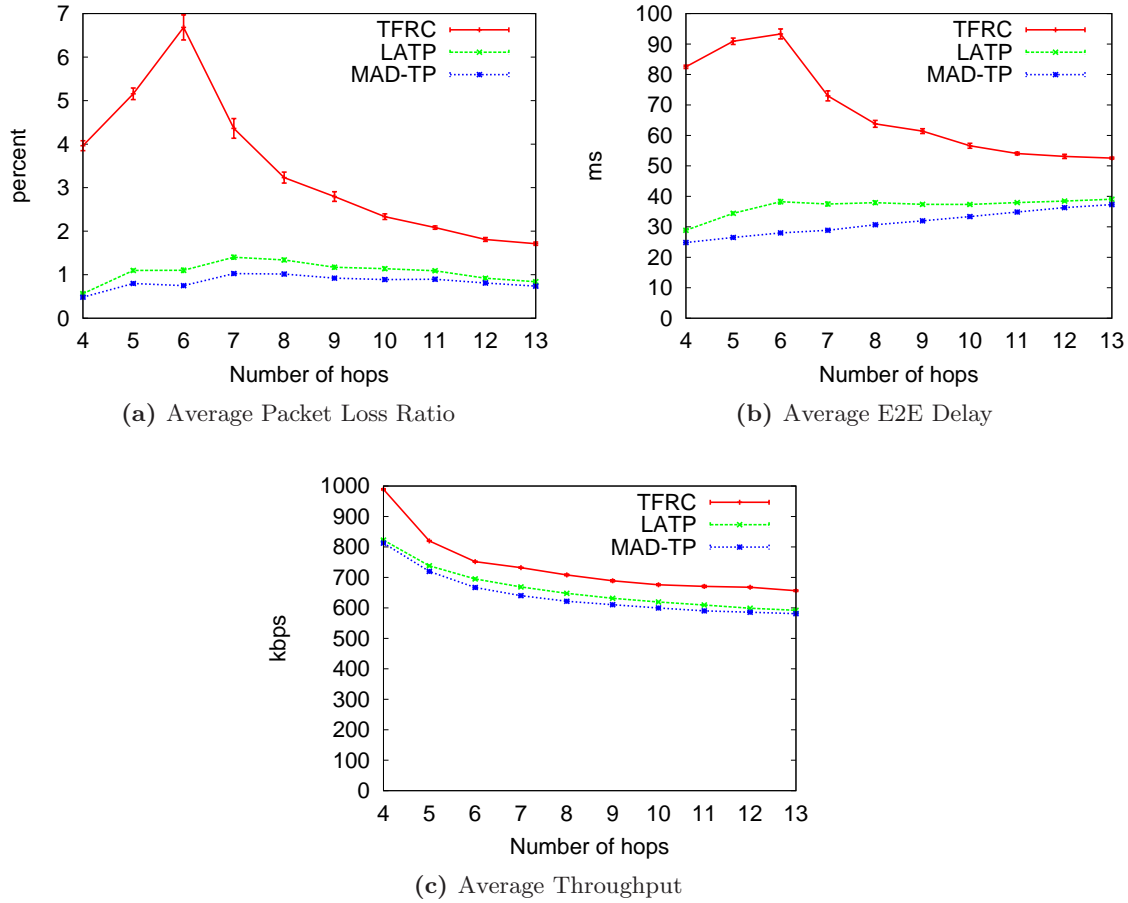


Figure 5.4: Chain topology with 1 connection and routing protocol AODV

the appropriate rate control of MAD-TP since it depends on the contention level in the network. Thus, MAD-TP always tries to keep the network operating in a low contention level status which in turn reduces the transmission attempts to successfully transmit a packet as well as the delay a packet experiences.

Fig. 5.3 and Fig. 5.4 also show that the average throughput of MAD-TP connection is smaller than that of TFRC but the difference is quite small. This is the price MAD-TP has to pay to achieve much better loss ratio and E2E delay. However, for applications which have strict packet loss ratio and latency, this trade-off is acceptable.

MAD-TP's performance is also better than that of LATP in terms of PLR and E2E Delay in a chain network while it achieves almost the same throughput. The reason is that *MAD* detects heavy contention better than the metric Permissible Throughput used by LATP [54], which then makes MAD-TP control its sending rate more efficiently than LATP.

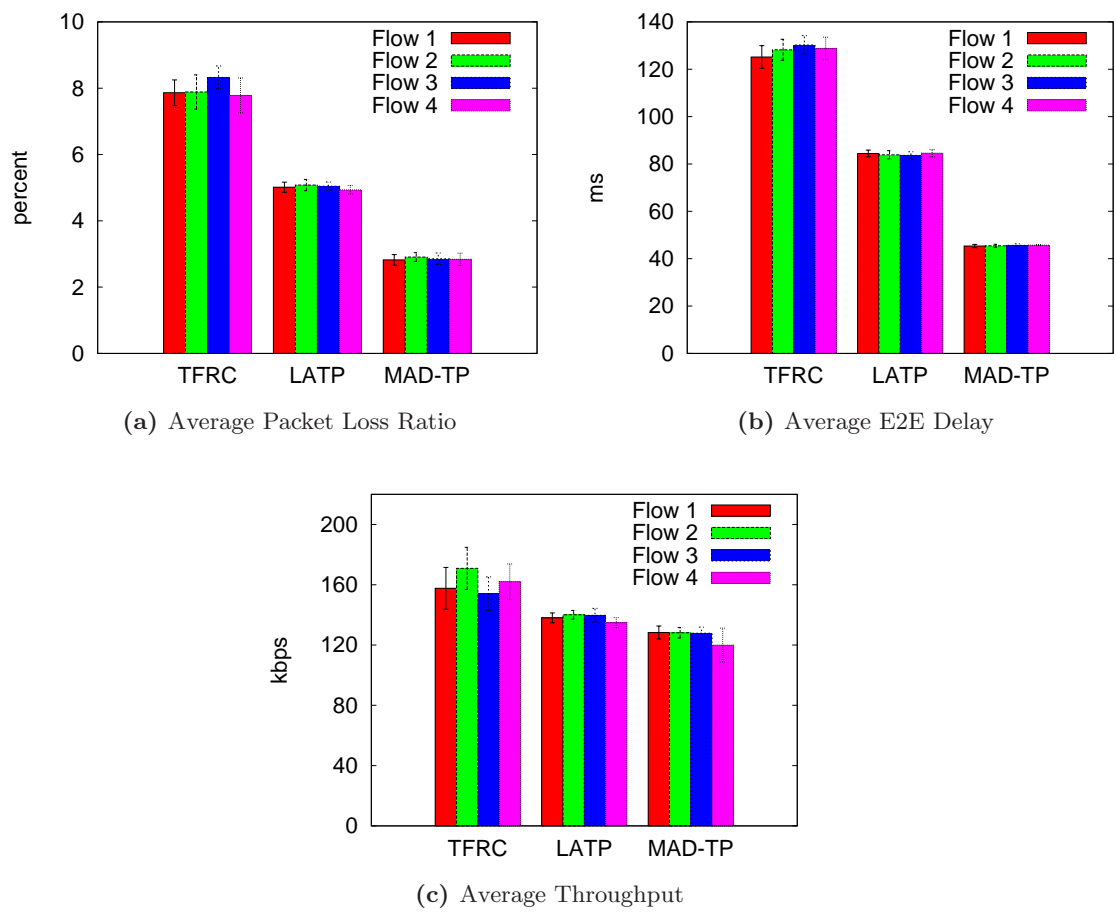


Figure 5.5: Chain topology with 8 hops and 4 connections with precomputed path

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

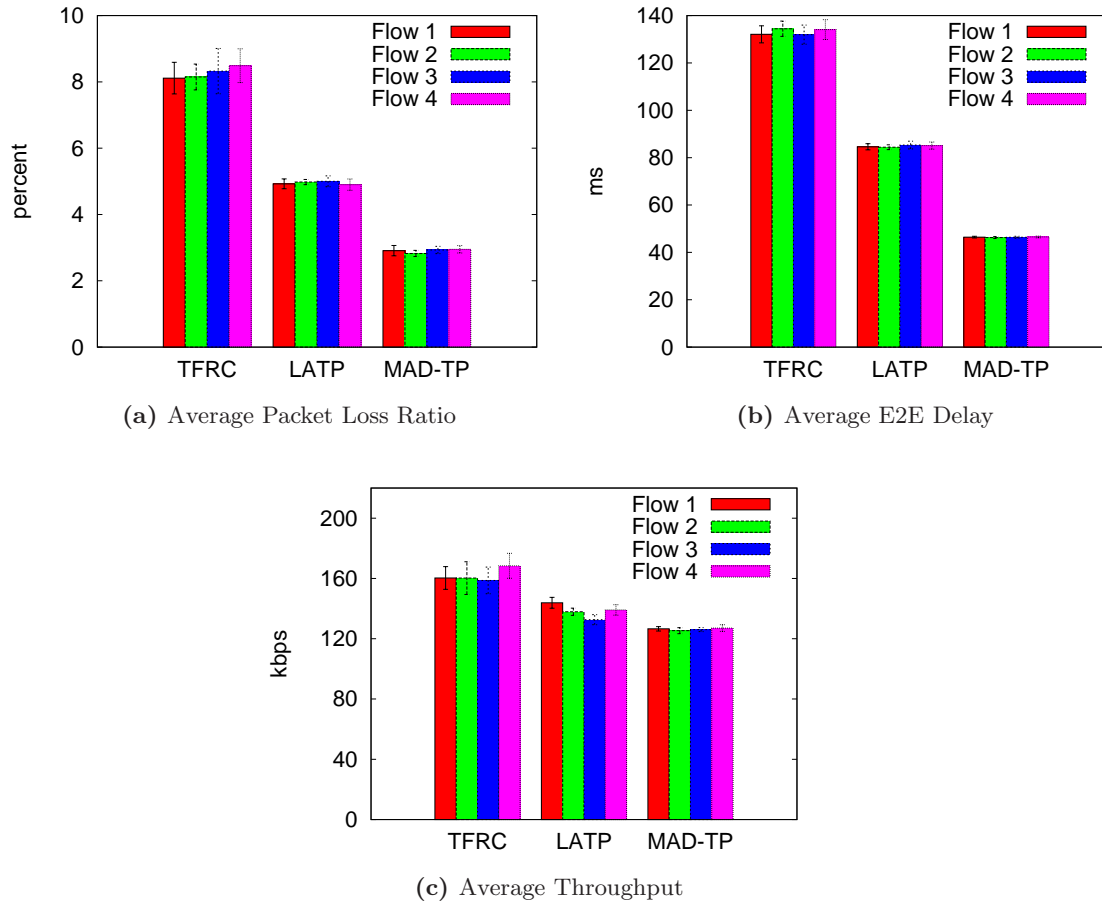


Figure 5.6: Chain topology with 8 hops and 4 connections with routing protocol AODV

Fig. 5.5 and Fig. 5.6 show the results for scenario 2 with 4 connections. As same, MAD-TP outperforms TFRC in terms of PLR and E2E delay with a price of a small degradation of throughput. MAD-TP also presents much smaller PLR and E2E delay than LAMP with almost the same throughput. The improvement is about 2% for PLR and 38 ms for E2E delay. Note that this scenario has four connections which send more packets into the network than the previous scenario. Since the network capacity is unchanged, the network contention level becomes higher. The *MAD* metric signals the growth of network contention level sooner and more accurately than the metric used in LAMP. MAD-TP, therefore, controls the sending rate more efficiently than LAMP and TFRC.

5.2.3.2 Grid topology

This scenario tries to evaluate the operation of MAD-TP in a more complex grid topology. This topology provides more intricate and adjustable node contention patterns. 4 connection patterns are set up such that they provide different contention levels in the network.

Fig. 5.7 and 5.8 show the simulation results for grid topology using precomputed path. It is obviously that MAD-TP outperforms TFRC in terms of E2E Delay, PLR and Fairness for all the scenarios. MAD-TP also provides better performance compared to LATP in terms of E2E delay and PLR while the average throughput is almost the same for both protocols.

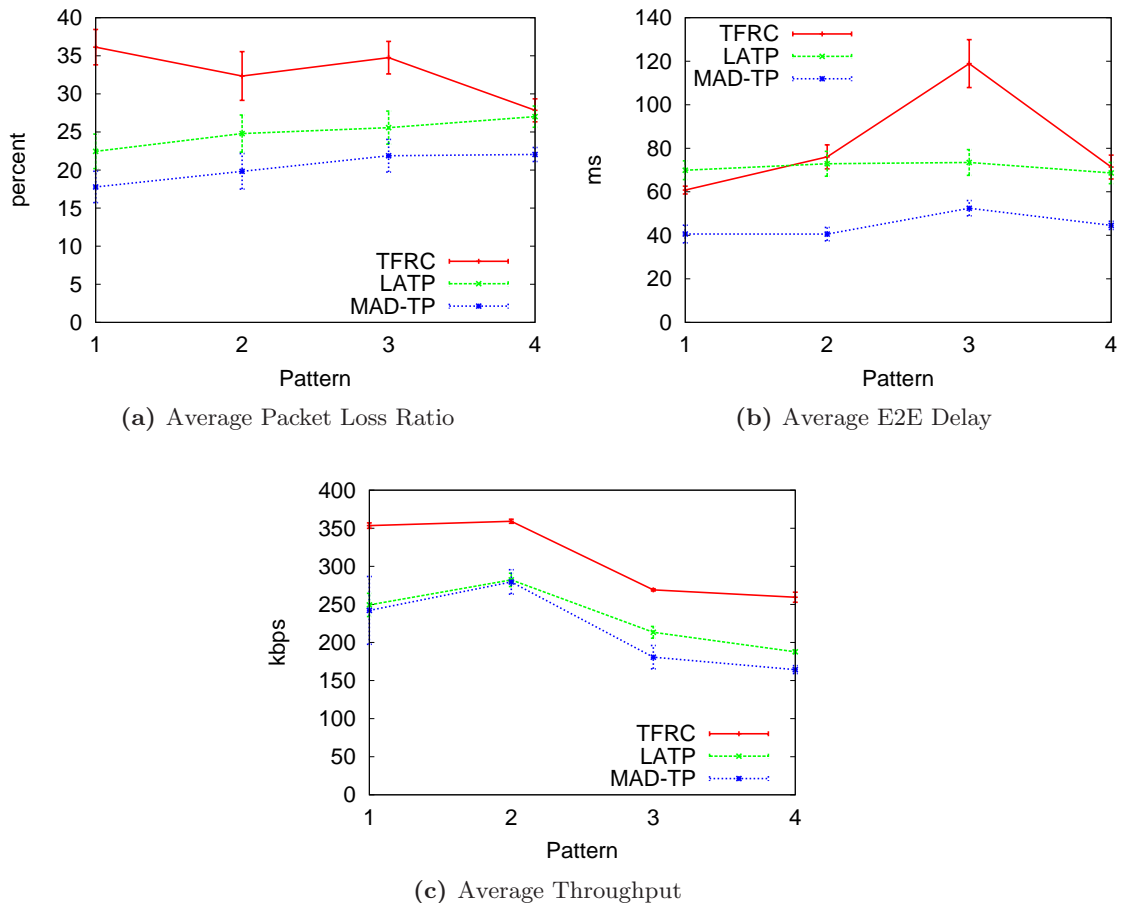


Figure 5.7: Grid topology with precomputed path: the performance

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

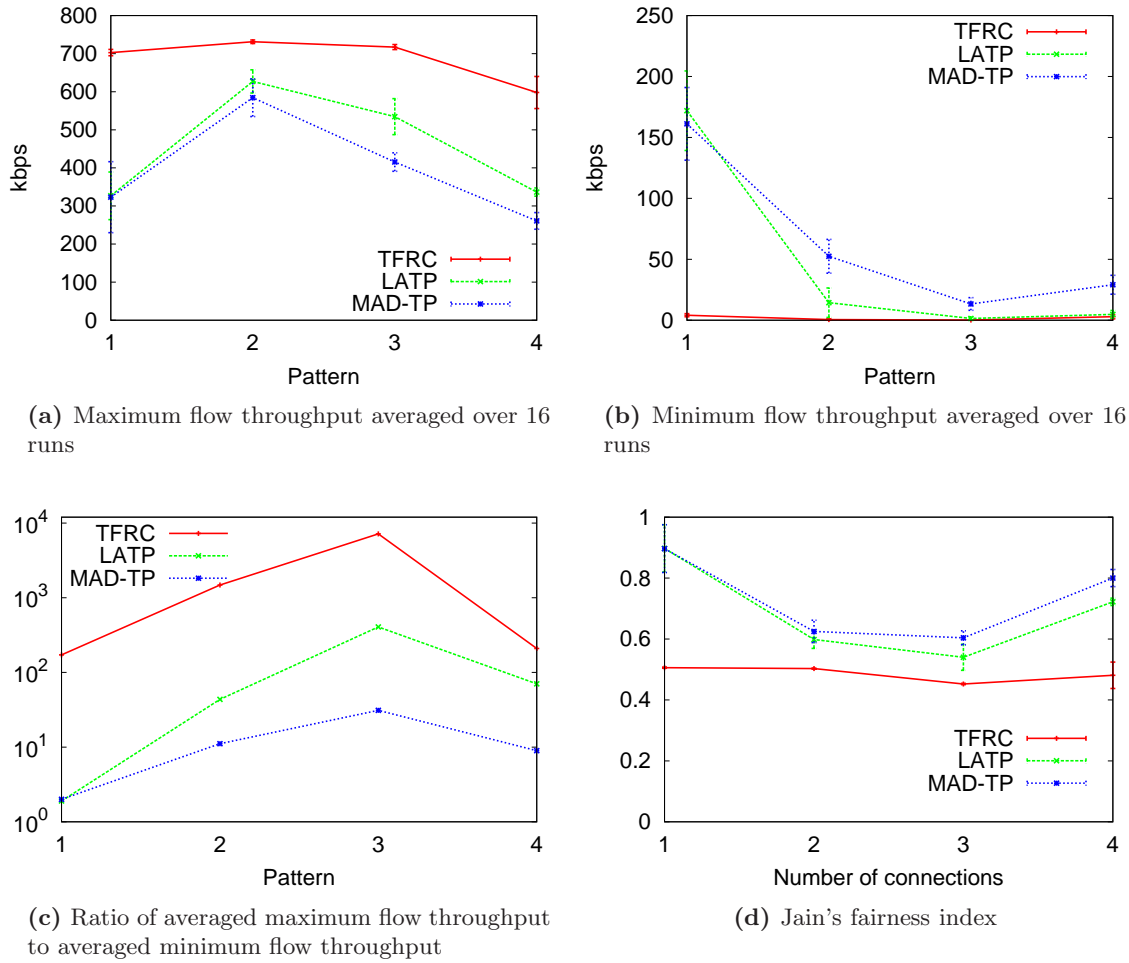


Figure 5.8: Grid topology with precomputed path: the fairness

From the Fig. 5.8.a and 5.8.b we can see that TFRC suffers from severe unfairness problem. Some flows achieve a very high throughput, i.e. 717 kbps for pattern 3 in Fig. 5.8.a, while that of some other ones is very low, i.e. 0.1 kbps for pattern 2 in Fig. 5.8.b. The scale between two values is thus 7170 times (Fig. 5.8.c). Although LAMP exhibits a better result than TFRC, it does not totally eliminate the unfairness problem, i.e. the averaged maximum flow throughput, the averaged minimum flow throughput and the scale between them of LAMP for pattern 3 are respectively 534 kbps, 1.46 kbps and 406. MAD-TP outperforms both TFRC and LAMP in terms of fairness since the average minimum flow throughput is higher and the considered scale is much smaller than those of TFRC and LAMP (13.3 kbps and 31 for pattern 3). Fig. 5.7.c and 5.8.d also show that MAD-TP improves the Jain's fairness index by about 0.1 ~ 0.4 at a price of 22% ~ 33% drop in aggregate throughput compared to TFRC.

5.2 Performance evaluation

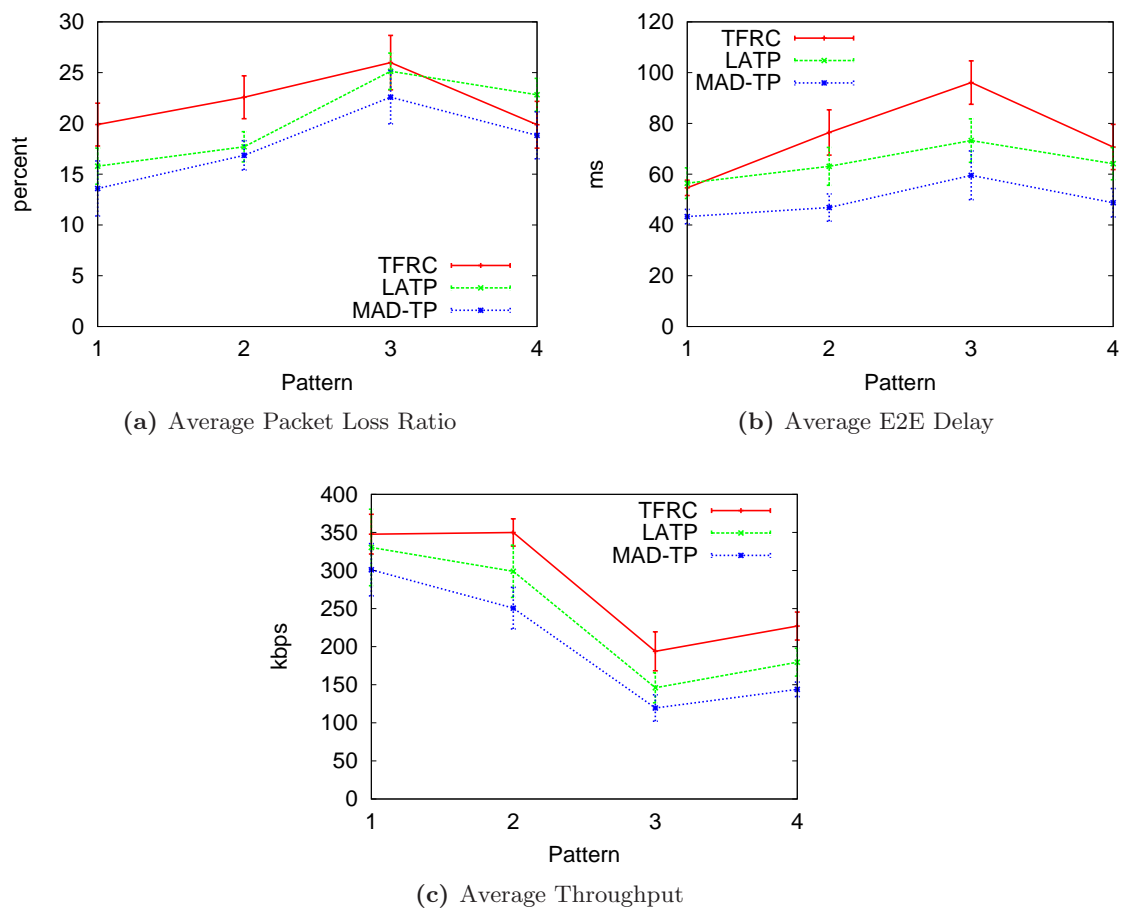


Figure 5.9: Grid topology with routing protocol AODV: the performance

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

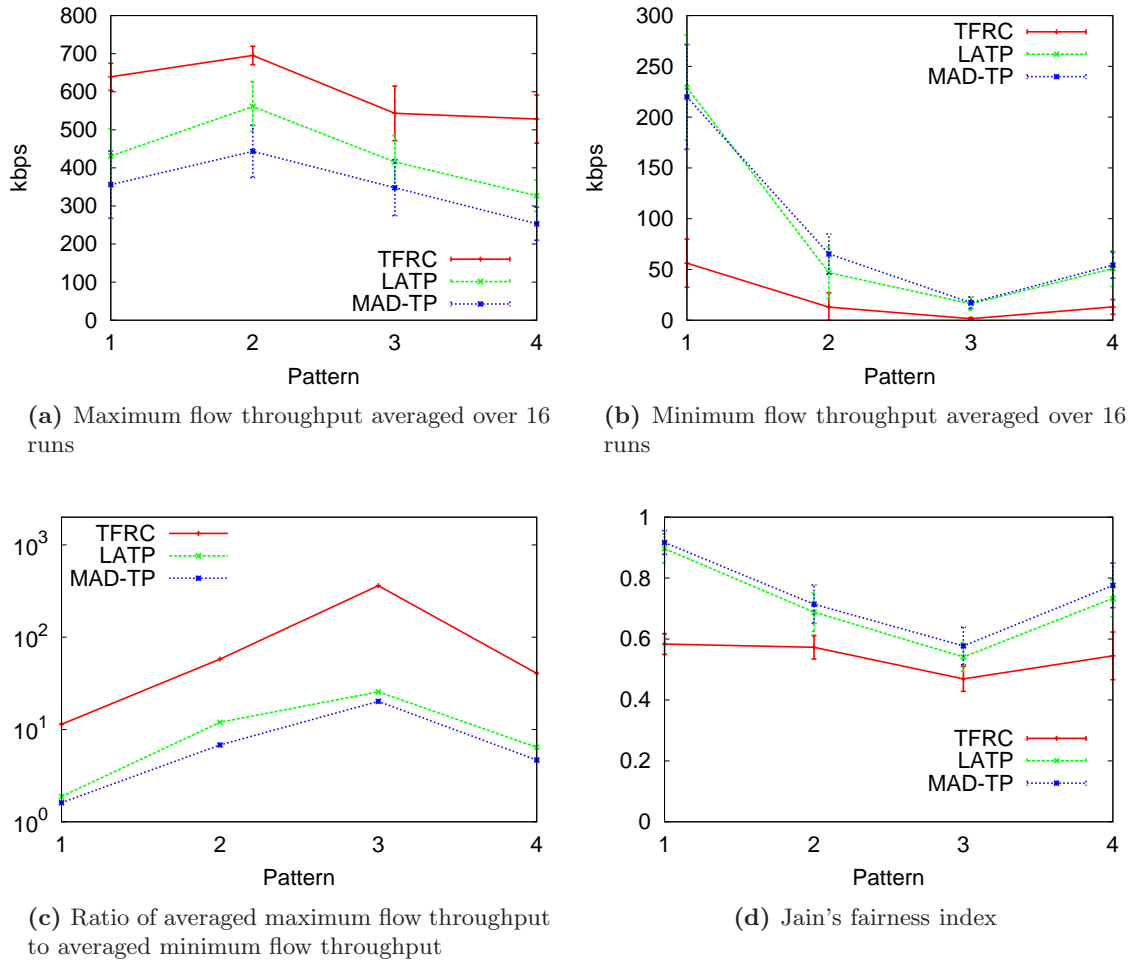


Figure 5.10: Grid topology with routing protocol AODV: the fairness

In grid topology using AODV (Fig. 5.9 and 5.10), the same conclusion can be made for MAD-TP and TFRC. In this case, MAD-TP provides a better result for PLR and E2E delay but has a slightly smaller throughput than LATP. Both protocols have also the same level of fairness.

This prominence in fairness comes from the early detection of high network contention level and a reasonable rate control of MAD-TP. The MAD-TP flows can soon realize that the network is becoming overloaded and thus reduce appropriately the sending rate to release more channel bandwidth for other flows. The increase of MAD-TP flows is also not aggressive, hence the channel is better shared among flows.

5.2.3.3 Random topology

The operation of MAD-TP is also investigated in a more realistic random topology. Different contention levels are made by increasing the number of connection flows in the network. Each pair of source and destination of a connection is chosen randomly with its hop distance is at least 3 hops. Fig. 5.11 and 5.12 exhibit the simulation results for the scenario 4.

The results show that, in such a complex simulation scenario, MAD-TP still outperforms TFRC in terms of PLR, E2E delay and Fairness. MAD-TP also provides better performance than LATP in terms of PLR and E2E delay with almost the same throughput. Both MAD-TP and LATP exhibit the same fairness level which is much better than that of TFRC.

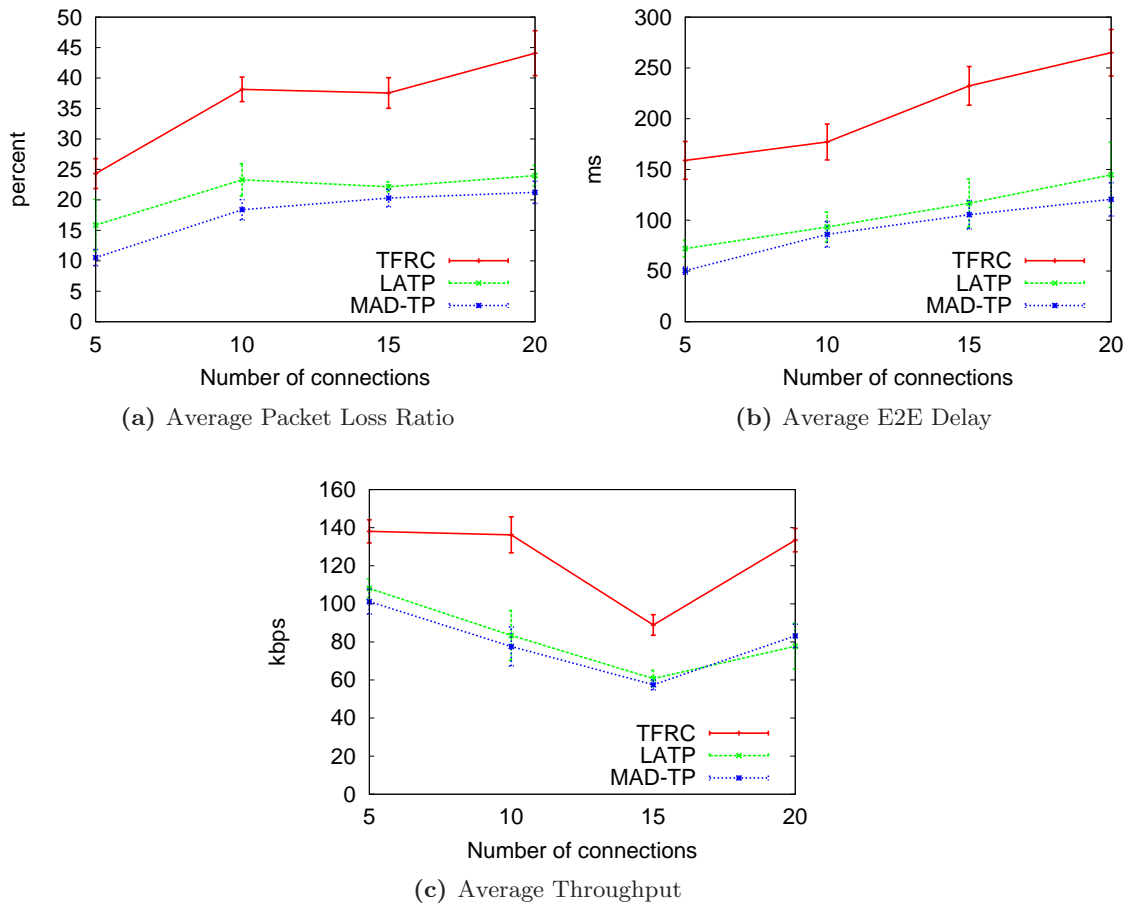


Figure 5.11: Random topology with routing protocol AODV: the performance

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

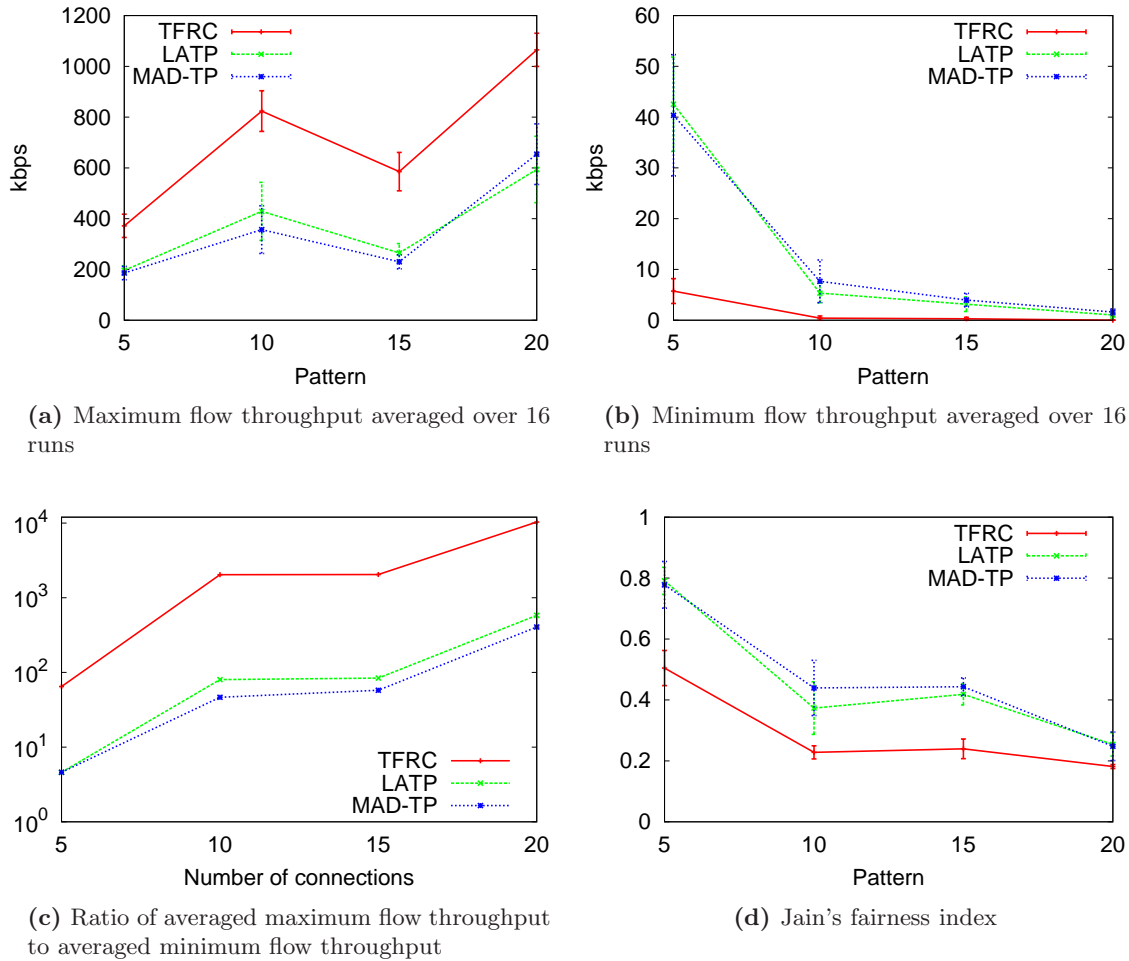


Figure 5.12: Random topology with routing protocol AODV: the fairness

5.3 Summary

The conventional rate control mechanism employed in TFRC is relatively aggressive when working on top of the MAC 802.11 protocol in MHWNs. The problem comes from the utilization of inappropriate TCP throughput equation in MHWNs which depends on the inaccurate loss estimation, fluctuating round trip time measurement and unawareness of lower layer network situation.

In this chapter, the *MAD* metric is proposed to use at transport layer because it can detect accurately and early the network contention growth event. Using the metric *MAD*, a new rate control mechanism is proposed, called MAD-TP, for transport protocol that alleviates the main drawback of TFRC caused by the unreliable estimation of delay and loss rate. The metric *MAD* is accumulated from all the contention time that a packet experiences along the path from the source to the destination. MAD-TP then uses the cumulative *MAD* to adjust the source's sending rate by comparing it with a specified threshold. If the received *MAD* value is smaller than the threshold, MAD-TP increases the rate with an amount proportional to its current rate. Otherwise, i.e.

the received MAD exceeds the threshold, MAD-TP assumes that the network entered into high contention condition so that it reduces the sending rate accordingly. The simulation results also show that MAD-TP outperforms TFRC not only in terms of fairness, but also in terms of end-to-end delay and packet loss ratio which are the two critical criteria for real-time streaming applications. MAD-TP also exhibits a better result in almost all scenarios compared to that of LATP, a recent proposal for real-time streaming applications in MHWNs.

However, MAD-TP has a drawback of choosing an absolute value for MAD threshold and as a consequence, the mechanism to estimate the amount of addition data which can be pumped into the network. To overcome this problem, another MAC metric should be used in conjunction with MAD in the operation of MAD-TP. The next chapter will provide the details of the improvement.

5. MEDIUM ACCESS DELAY AWARE RATE CONTROL FOR TRANSPORT PROTOCOL

Chapter 6

Metric-based Rate Control for Transport Protocol

In Chapter 5, we have proposed a new scheme, called MAD-TP, which is suitable for real-time streaming applications since it provides better performance than TFRC in terms of fairness, end-to-end delay and packet loss ratio. However, there are still some shortcomings in the design of MAD-TP. The first one is the choice of the threshold MAD_{TH} which may depend on the network configuration. The second one is the equation to estimate the additional amount of traffic ΔR since there is no explicit relation between MAD and data rate. These drawbacks will be eliminated in this new proposed scheme.

In this chapter, the design of the proposed scheme, called IMAD-TP, is based on two MAC metrics which are MAD and ATT (Chapter 4). In IMAD-TP, the gradient of MAD is used instead of the absolute value of MAD . The growth of network contention level is detected by observing the behavior of MAD gradient. Depending on the comparison between the value of MAD gradient and two predefined thresholds, the sender will determine the appropriate behavior. Moreover, ATT is used to estimate the effective bandwidth which in turn is used as the upper bound for the source's sending rate. This is the effective rate at which IMAD-TP can make the network to work in its optimal performance point. This technique will provide a more reasonable rate control mechanism than our previously proposed scheme which is based on MAD_{TH} . The simulation results show that IMAD-TP outperforms TFRC, LATP and provides better performance than our previously proposed scheme MAD-TP in terms of fairness, end-to-end delay and packet loss ratio. The design of IMAD-TP will be described in detail in the next sections.

6.1 Network Contention Detection with MAD Gradient

The objective of a rate control scheme is to keep the network in an optimal network load point at which the network is non-saturated and the end-to-end delay and packet loss ratio are small. If the network load surpasses the optimal point, the network contention becomes severe which in turn makes the end-to-end-delay and packet loss

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

ratio sharply increase. The results of Chapter 4 show that the value and variation of the metric MAD in non-saturated state are small. As soon as the network is overloaded, the MAD value increases sharply in a short time and its variation becomes large. Therefore, it is feasible to observe the variation of MAD value along with the time axis (MAD gradient) to determine whether the network enters into severe contention level. The definition of MAD gradient is as follows.

Denote A_i and A_{i+1} respectively the arrival time of the feedback packets i^{th} and $(i+1)^{th}$, MAD_i and MAD_{i+1} the corresponding attached MAD values, then the MAD gradient α is:

$$\alpha = \frac{MAD_{i+1} - MAD_i}{A_{i+1} - A_i} \quad (6.1)$$

A simulation evaluation scenario is built to determine the distribution of α values in both non-saturated and saturated states of the network depending on the offered load. In this scenario, one connection is established between two end nodes of a 8 hop chain topology. The traffic source uses a modified version of MAD-TP such that its sending rate is fixed during each simulation, and the MAD-TP receiver sends periodically a feedback packet every round trip time. The feedback packet contains the MAD value calculated as described in Section 5.1.3 of Chapter 5. In each simulation, the MAD-TP sending rate takes a value from $\{10, 20, 30, 40, 50, 60, 70, 80\}$ packet per second (pkt/s). Every time receiving a feedback, the MAD-TP sender computes α as in the equation A.7. The network configuration is shown in Table 4.1, each simulation is performed 16 runs of 100 seconds. Note that each bar corresponding to the value i of MAD gradient in the Fig. 6.1 represents the number of α occurrences whose values lie in $(i - 1, i]$, and the value range of α from -10 to 10 in this figure takes more than 95% the total number of α samples during each simulation run.

Fig. 6.1 displays the simulation results. The results shows a clear difference for the distribution of α when the rate is smaller and greater than 60 pkt/s. The analysis of trace file exhibits that the network operates in a optimal point, i.e. non-saturated state, when the offered load is around 50 pkt/s. At this point, the packet loss rate is low, the end-to-end delay is small and the effective throughput is high. Almost all values of α fall into the range of $[-5, 5]$. This can be interpreted that, in the optimal network load point, the MAD gradient should not exceed the value of 5. When the offered load surpasses 50 pkt/s, the network leaves the optimal operation point. The values of α then distribute over a larger range.

From those results, we then may define two thresholds $0 < TH_1 < TH_2$ which are used as the indicators of network contention level. If $\alpha < TH_1$, it means that the MAD decreases (in case $\alpha < 0$) or it increases relatively small ($0 < \alpha < TH_1$), the traffic source thus can properly increase its sending rate. From Fig. 6.1, we can set $TH_1 = 5$. If $\alpha > TH_2$, it is a high possibility that the network enters into severe contention state. The traffic source should not increase the sending rate in this case. We set $TH_2 = 7$ in order to react quickly to the sudden increase of the network contention level. Otherwise, i.e. $TH_1 < \alpha < TH_2$, the network may operate in a reasonable point and the traffic source keeps its current sending rate unchanged.

6.1 Network Contention Detection with *MAD* Gradient

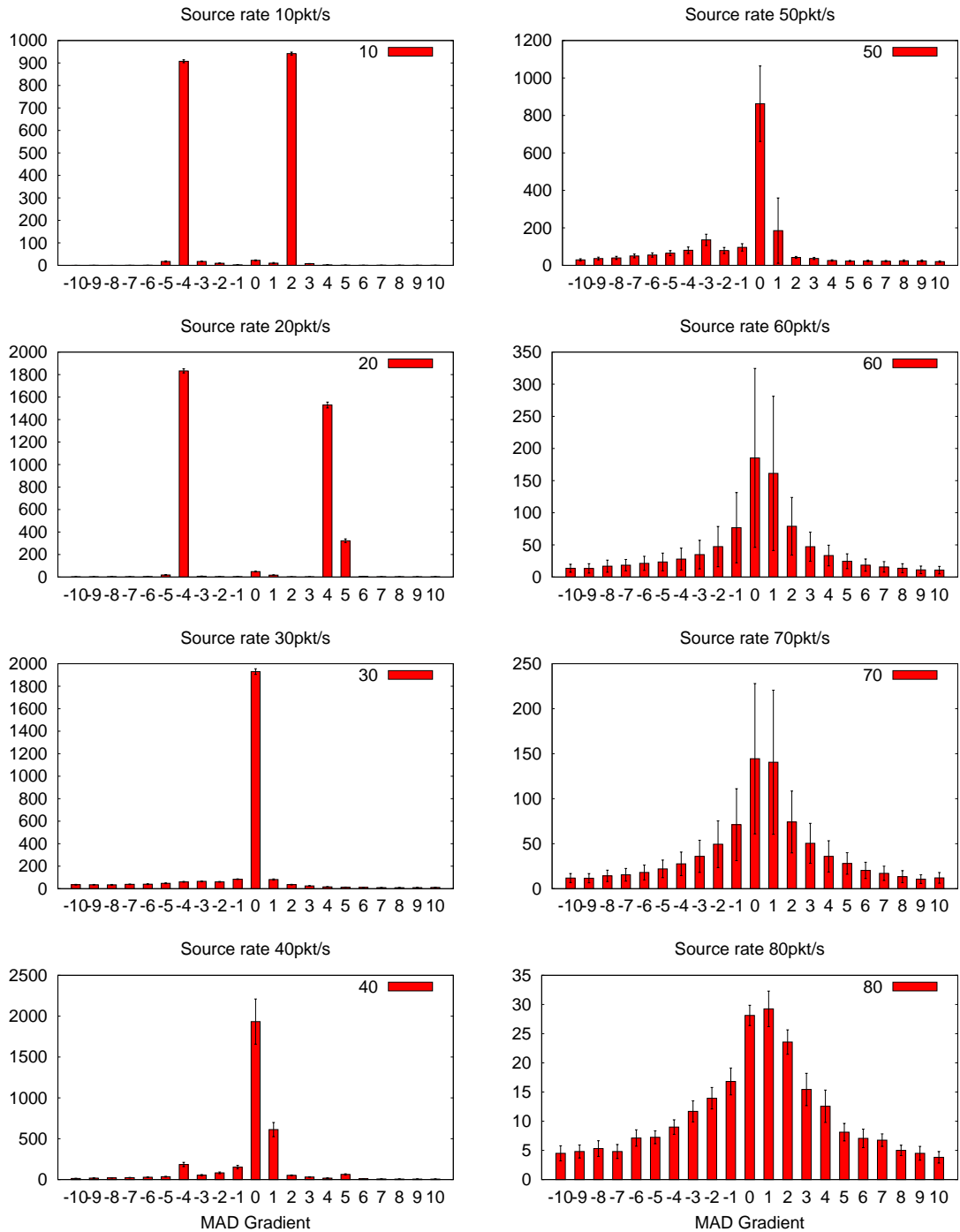


Figure 6.1: MAD gradient with different offered load

6.2 Effective Bandwidth Estimation with ATT

The idea of using ATT metric to estimate the effective bandwidth comes from the work of Chen et al. [87]. The corollary 2 of this work claimed that, in a IEEE 802.11-based MANET where the interference range is set to double of the transmission range, the bandwidth-delay product of a chain of nodes is constrained by an upper bound BDP_{UB} such that

$$BDP_{UB} \simeq S \times \frac{\sum_{i=0}^n d_i + \sum_{i=0}^m d'_i}{4 \times d_{max}} \quad (6.2)$$

where S is the packet size, d_i and d'_i are respectively the per-hop packet transmission delays along the forward (n hops) and return (m hops) paths, and d_{max} is the maximum per-hop delay of the forward path. The per-hop packet transmission delay d_i of a packet with size S over a link i is computed as follows

$$d_i = \frac{S}{B} \quad (6.3)$$

where B is the effective bandwidth at link i which includes contention overhead. With this definition, and referring to the definition of ATT metric in Section A.3 of Chapter 4, if d_i is averaged in an interval, then we have $d_i \simeq ATT$.

In [87], BDP_{UB} is computed for each pair of TCP data and ACK packets. However, in the case of rate-based transport protocol, the feedback packet is not generated for each arrived data packet but for every interval of time, i.e. a round trip time, or for every new detected loss event (for TFRC). Therefore, we can reasonably deduce that

$$\begin{aligned} BDP_{UB} &\simeq S \times \frac{\sum_{i=0}^n ATT_i + \sum_{i=0}^m ATT'_i}{4 \times ATT_{max}} \\ &\simeq S \times \frac{2 \times \sum_{i=0}^n ATT_i}{4 \times ATT_{max}} \\ &\simeq S \times \frac{\sum_{i=0}^n ATT_i}{2 \times ATT_{max}} \end{aligned} \quad (6.4)$$

The upper bound for the sending rate R_{UB} can be computed from BDP_{UB} and current Round-trip Time RTT as follows

$$\begin{aligned} R_{UB} &= \frac{BDP_{UB}}{RTT} \\ &= \frac{\sum_{i=0}^n ATT_i}{2 \times ATT_{max}} \times \frac{S}{RTT} \end{aligned} \quad (6.5)$$

R_{UB} is thus the maximum sending rate by which the network is not overloaded. The thresholds TH_1 , TH_2 of MAD and R_{UB} will be used together in the design of IMAD-TP in order to adapt properly the traffic rate of the IMAD-TP sender. The design of IMAD-TP will be explained in detail in the next section.

6.3 IMAD-TP: Improvement for MAD-TP

The design of IMAD-TP follows the same scheme as MAD-TP. Therefore, in the following, only the design related to ATT metric is explained.

6.3.1 Intermediate nodes

Beside MAD , each node maintains also the periodical measurement of ATT according to the equation A.2 in Chapter 4. For all outgoing packets, the node updates the cumulative packet transmission delay in an option field in IP header, called $CATT$, by adding its ATT value to the existing value in that field. In addition, another option field in IP header, called $MATT$, is also updated such that, if value contained in $MATT$ is smaller than the node's ATT , it will be replaced by the node's ATT . With this rule, $MATT$ will contain the maximum value of packet transmission delay of all links along the path.

With this design, the IP packet needs 3 option fields in its header which are $CMAD$ for the cumulative MAD , $CATT$ for the cumulative ATT and $MATT$ for the maximum value of packet transmission delay of all links along the path.

6.3.2 IMAD-TP receiver

Every time receiving a packet, IMAD-TP receiver takes the ATT_{cum} value from the IP header field $CATT$, and the ATT_{max} from the IP header field $MATT$. Then, IMAD-TP receiver computes the most recent upper bound of bandwidth-delay product BDP_{sample} for the path collected by that packet as

$$BDP_{sample} = \frac{ATT_{cum}}{2 \times ATT_{max}} \quad (6.6)$$

The IMAD-TP receiver then derives the average upper bound bandwidth-delay product by using the EWMA function as follows:

$$BDP_{UB} = \alpha BDP + (1 - \alpha) BDP_{sample} \quad (6.7)$$

α is set to 0.8 in the implementation in order to avoid the large oscillation of BDP_{UB} . This average value is calculated as in equation 6.7 for every received packets.

The current estimated BDP_{UB} , MAD and R_{rcv} are fed back together to the sender. To contain the BDP_{UB} value, the ACK packet of MAD-TP is redesigned such that a new field, called BDP , is inserted into the ACK header.

The structure of IMAD-TP ACK packet is then as in Fig. 6.2.

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

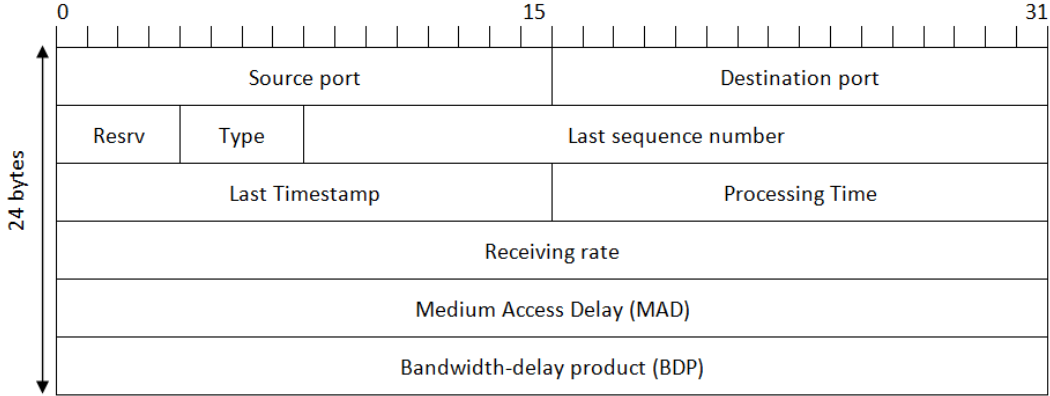


Figure 6.2: ACK packet structure of IMAD-TP

6.3.3 IMAD-TP sender

The slow start phase of IMAD-TP is exactly the same with that of MAD-TP. When the IMAD-TP connection enters into congestion avoidance phase, the rate control scheme is designed as follows.

Upon receiving MAD and BDP values from the feedback packet, the sender computes the maximum sending rate R_{UB} by the equation 6.5. Afterwards, the sending rate is updated by the following rule:

```

if ( $R_{UB} > R$  &&  $\alpha < TH_1$ )
    increase rate
elseif ( $R_{UB} < R$  &&  $\alpha > TH_2$ )
    decrease rate

```

where R is the current sending rate.

IMAD-TP sender decreases the sending rate using the same rule in MAD-TP, by which the sending rate is reduced by 1/8 its current sending rate after each RTT but never smaller than one packet per RTT .

To increase the rate, IMAD-TP sender applies the following equation

$$R = \min(R_{UB}, R + N * S / RTT) \quad (6.8)$$

Equation 6.8 ensures that the new rate does not exceed the upper bound rate and increases at most one packet per RTT . Note that the sending rate is always greater than one packet per RTT with these increase and decrease rules.

The simulation evaluation for IMAD-TP will be mentioned in the next section.

6.4 Performance evaluation

6.4.1 Simulation scenarios

To evaluate the performance of IMAD-TP, we use the same set of scenarios and configuration which were provided in Section 5.2 of Chapter 5. The performance of IMAD-TP is compared to that of TFRC, LAMP and MAD-TP in terms of three performance metrics Throughput, End-to-End (E2E) Delay and Packet Loss Ratio (PLR). For the assessment of fairness, Jain's fairness index, the maximum and minimum flow throughputs averaged over a certain number of simulation runs and the scale between two values will be used.

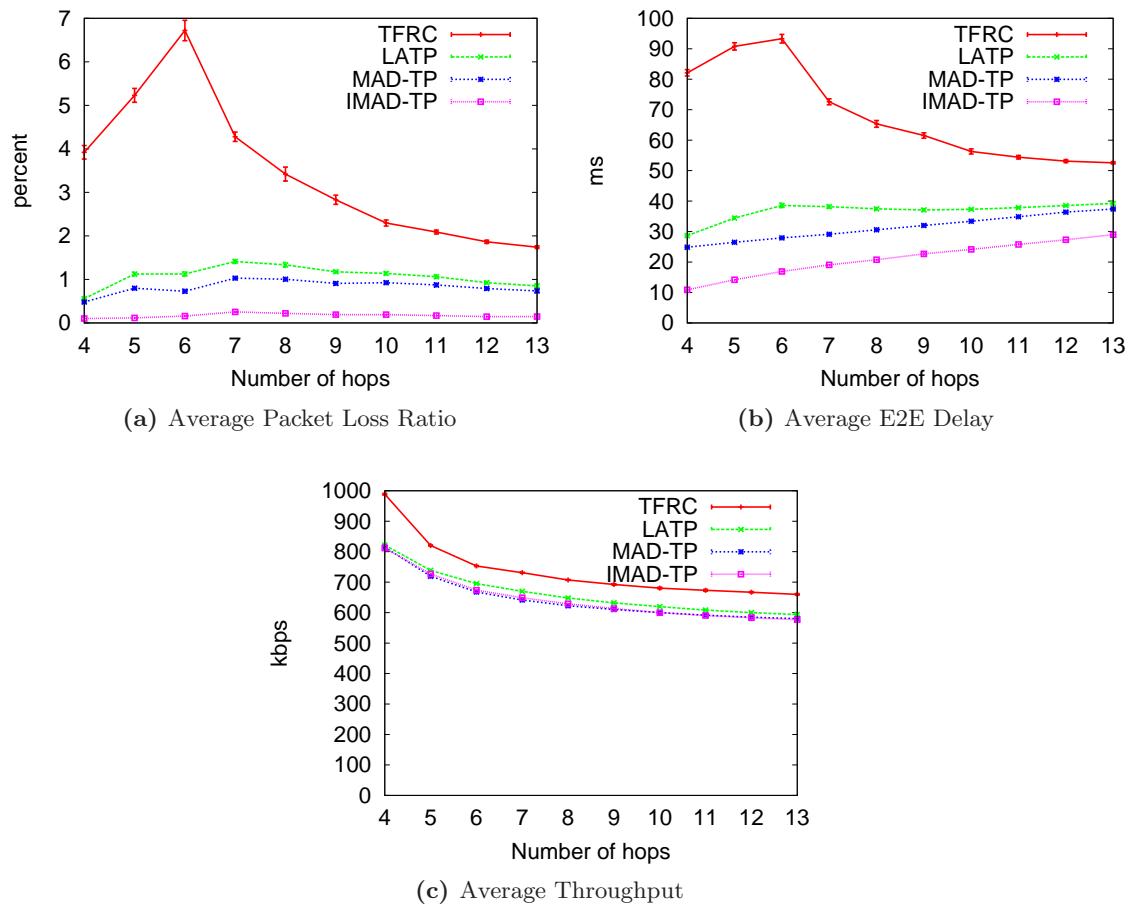


Figure 6.3: Chain topology with 1 connection and precomputed path

6.4.2 Results and discussion

6.4.2.1 Chain topology

The objective of both scenarios 1 and 2 is to investigate the considered protocols with the increase in contention level of the network. In scenario 1, the contention level of

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

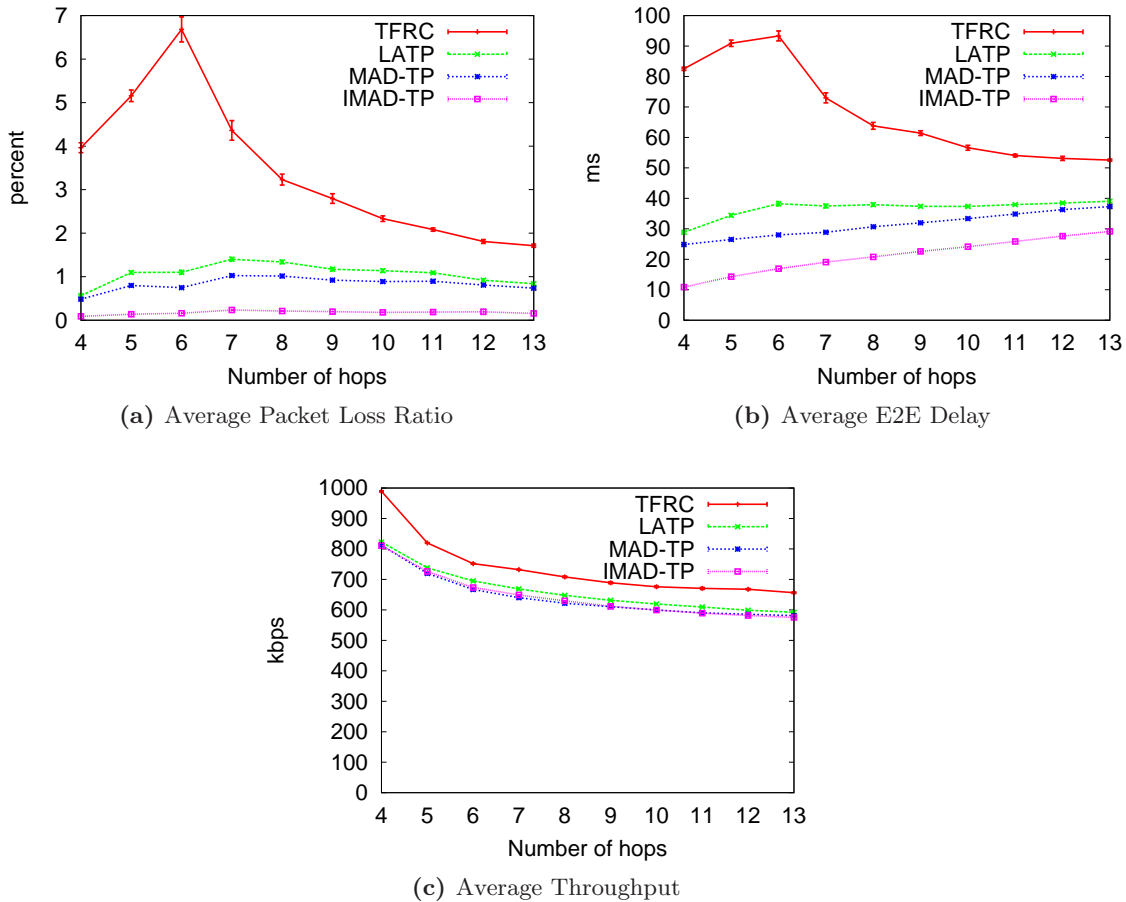


Figure 6.4: Chain topology with 1 connection and routing protocol AODV

the network is changed by increasing the number of nodes in the chain network. In scenario 2, the network topology is fixed to a chain of 9 hops and 4 connection flows are established in order to increase the contention level.

The performance of IMAD-TP in scenario 1 are showed in Fig. 6.3 and Fig. 6.4. The results show that IMAD-TP exhibits a better performance in terms of PLR and E2E delay in comparison with the other protocols, i.e. TFRC, LATP and MAD-TP. The PLR of IMAD-TP ranges from 0.1% (for 4 hop chain) to 0.25% (for 7 hop chain), while those of MAD-TP, LATP and TFRC are respectively [0.5%, 1%], [0.6%, 1.4%] (all for 4 and 7 hop chain) and [1.7%, 6.7%] (for 13 and 6 hop chain). These values mean that the average PLR of IMAD-TP is approximately equal to 1/4, 1/5 and 1/20 that of MAD-TP, LATP and TFRC respectively. IMAD-TP also introduces much smaller E2E delay for all number of hops than other considered protocols and the increase of E2E delay reflects adequately the increase of the number of hops. Although MAD-TP has the same behavior with IMAD-TP, the E2E delay introduced by MAD-TP is larger than that of IMAD-TP. There is always a difference of about 10 ms between the E2E delay of MAD-TP and IMAD-TP for all number of hops. Another remarkable point is that, although IMAD-TP exhibits much smaller PLR and E2E delay, it keeps an almost the same Throughput with those of MAD-TP and LATP.

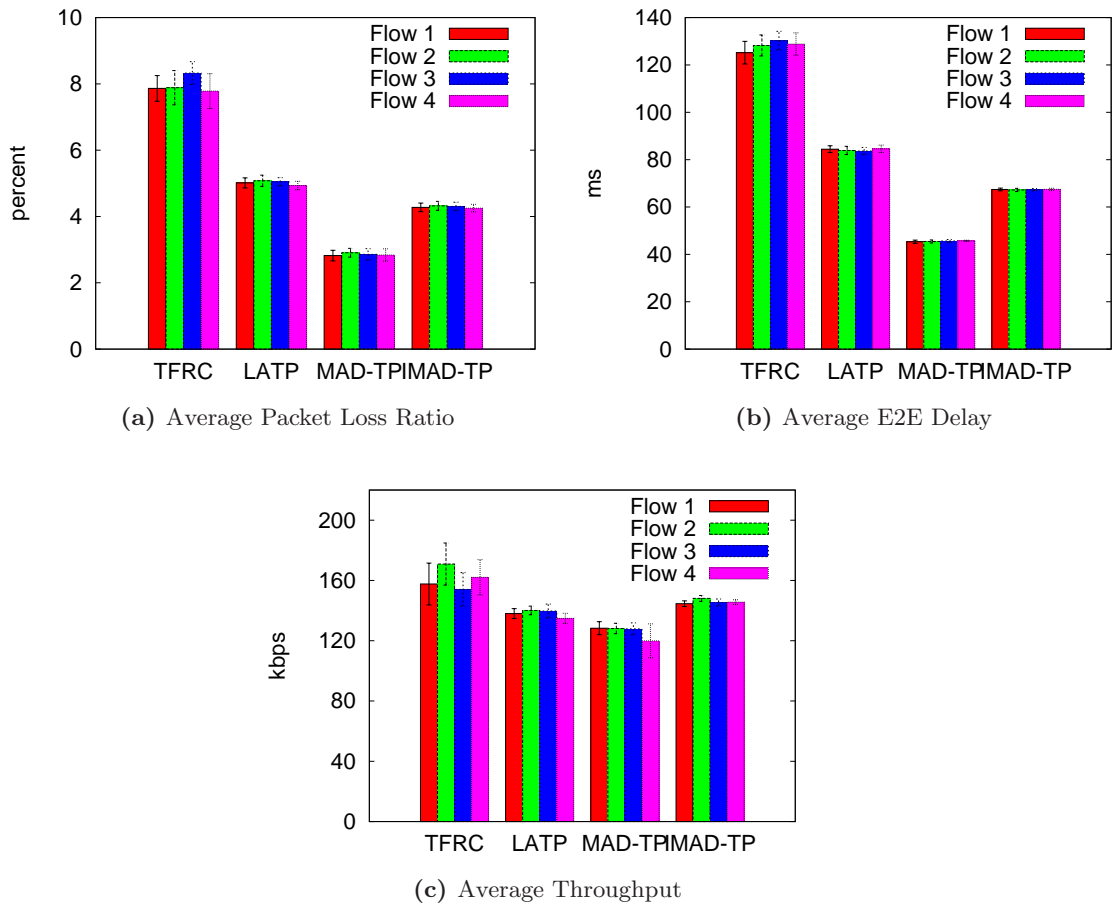


Figure 6.5: Chain topology with 8 hops and 4 connections with precomputed path

This prominence is made by the accurate bandwidth estimation and the efficient rate control scheme of IMAD-TP. The bandwidth estimation reflects accurately the current capability of the network, thus prevents the IMAD-TP sender from overloading the network. The proposed rate control scheme also maintains a relatively smooth sending rate which in turn keeps the network steady. Therefore, IMAD-TP achieves this high performance.

Fig. 6.5 and Fig. 6.6 show the results of the scenario 2 with 4 connections. In this scenario, IMAD-TP outperforms TFRC in terms of packet loss ratio (PLR) and end-to-end (E2E) delay with a price of an insignificant degradation of throughput. Moreover, the performance of IMAD-TP is better than that of LAMP in all three factors. Indeed, the PLR and E2E delay of IMAD-TP are smaller than those of LAMP by an amount of 0.8% and 8 ms, while the higher amount of Throughput is 7 kbps. These results again prove that the rate control mechanism of our proposed scheme is essentially effective. The results also show that IMAD-TP's performance is worse than that of MAD-TP in terms of PLR and E2E delay but with better Throughput. The reason is that MAD-TP uses MAD_{TH} to restrict the behavior of the sender and the rate will be decreased as soon as the received MAD surpasses this threshold. Therefore, the network with MAD-TP flows works at a point close but lower than the optimal point. In contrast,

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

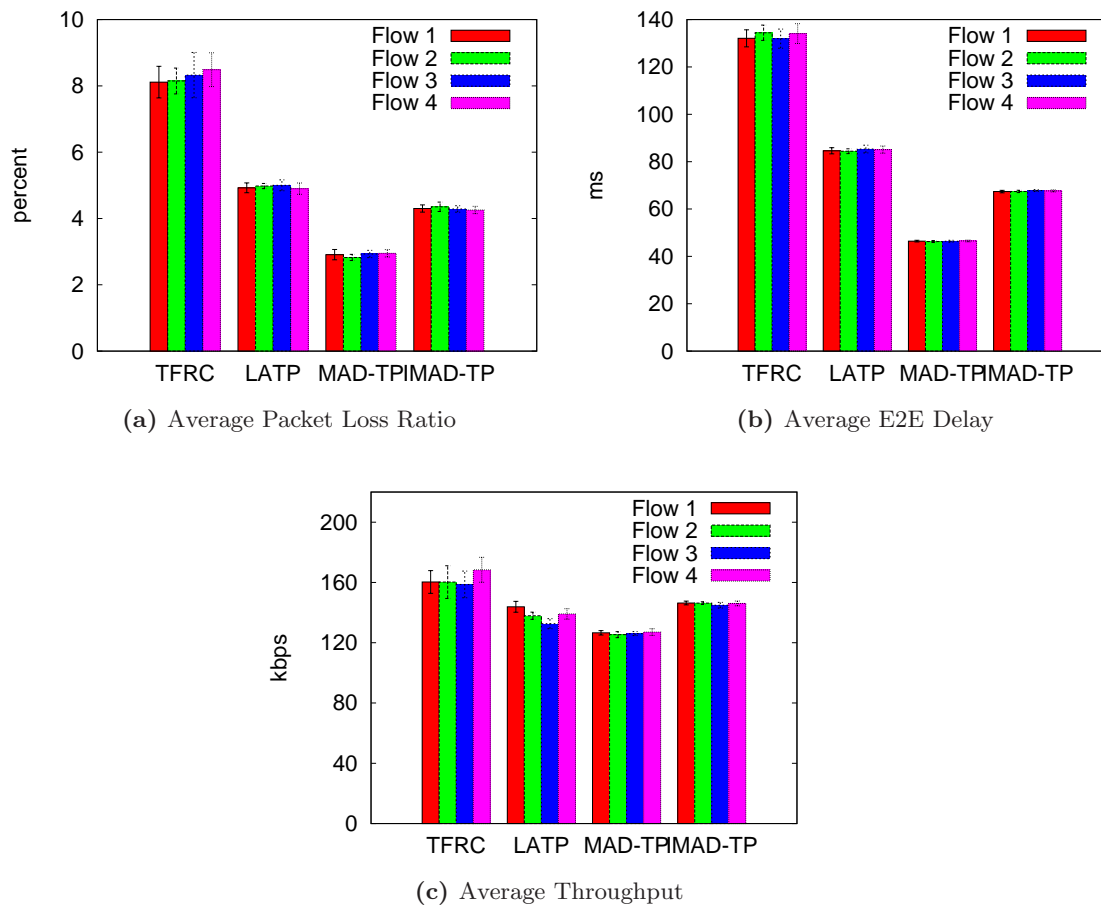


Figure 6.6: Chain topology with 8 hops and 4 connections with routing protocol AODV

IMAD-TP with its accurate and effective rate control makes the network work around the optimal point. This fact makes MAD-TP introduces smaller PLR, E2E delay and Throughput than IMAD-TP.

6.4.2.2 Grid topology

This scenario tries to evaluate the operation of the considered protocols in a more complex grid topology. This topology provides more intricate and adjustable node contention patterns. 4 connection patterns are set up such that they provide different contention levels in the network.

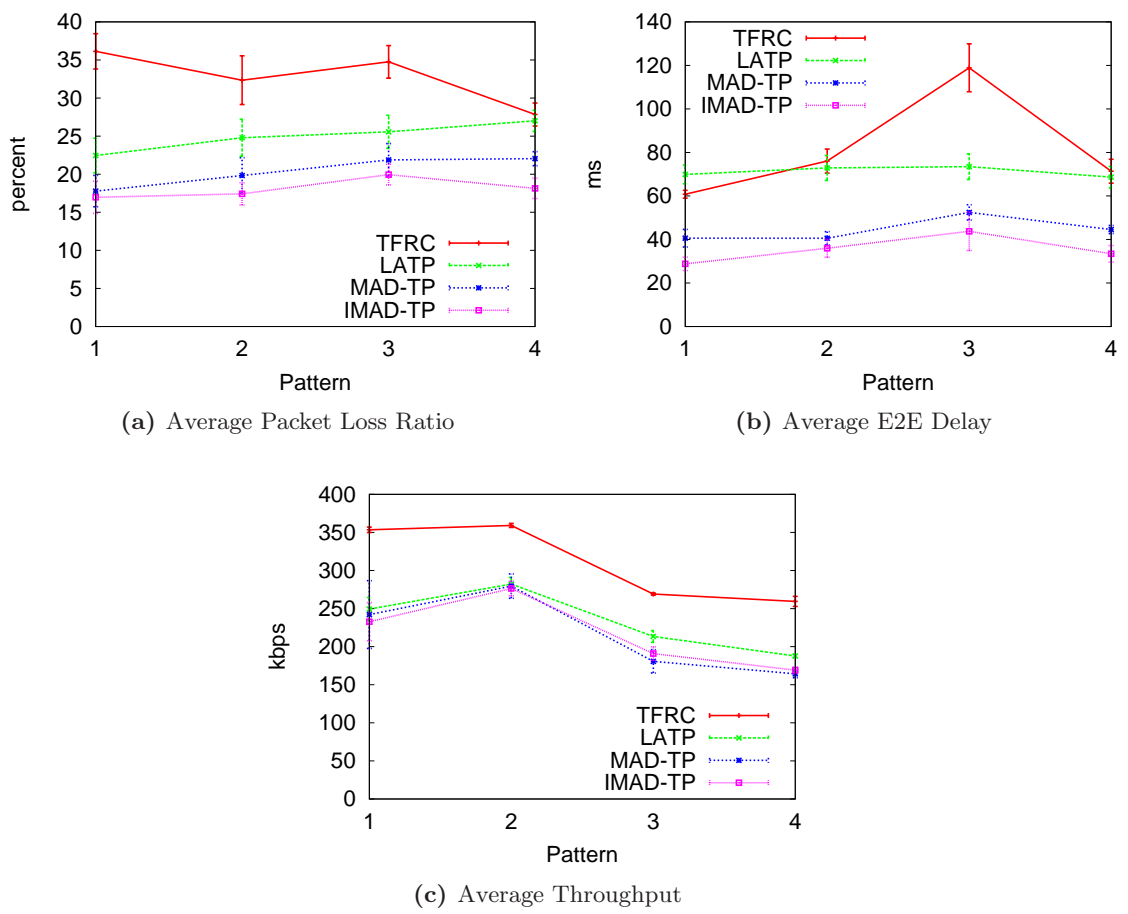


Figure 6.7: Grid topology with precomputed path: the performance

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

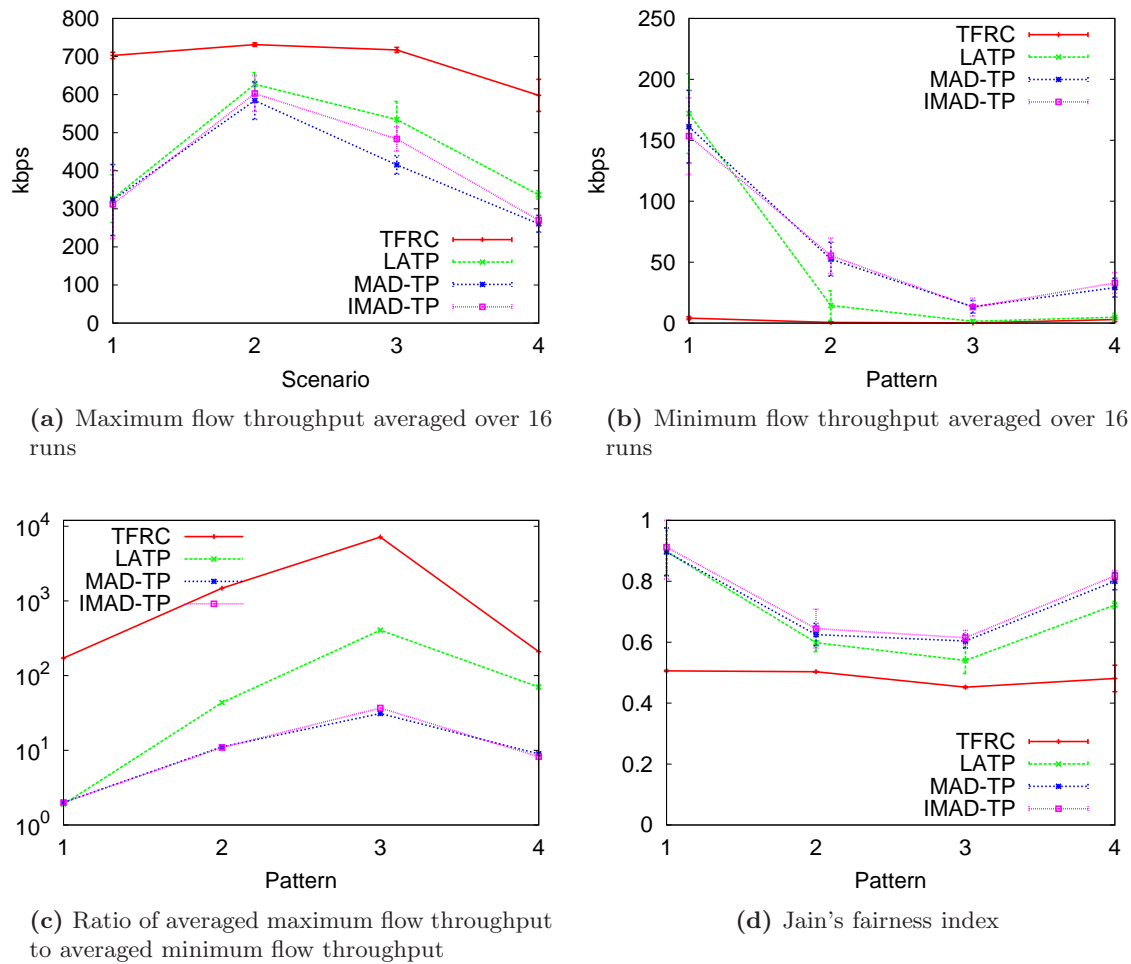


Figure 6.8: Grid topology with precomputed path: the fairness

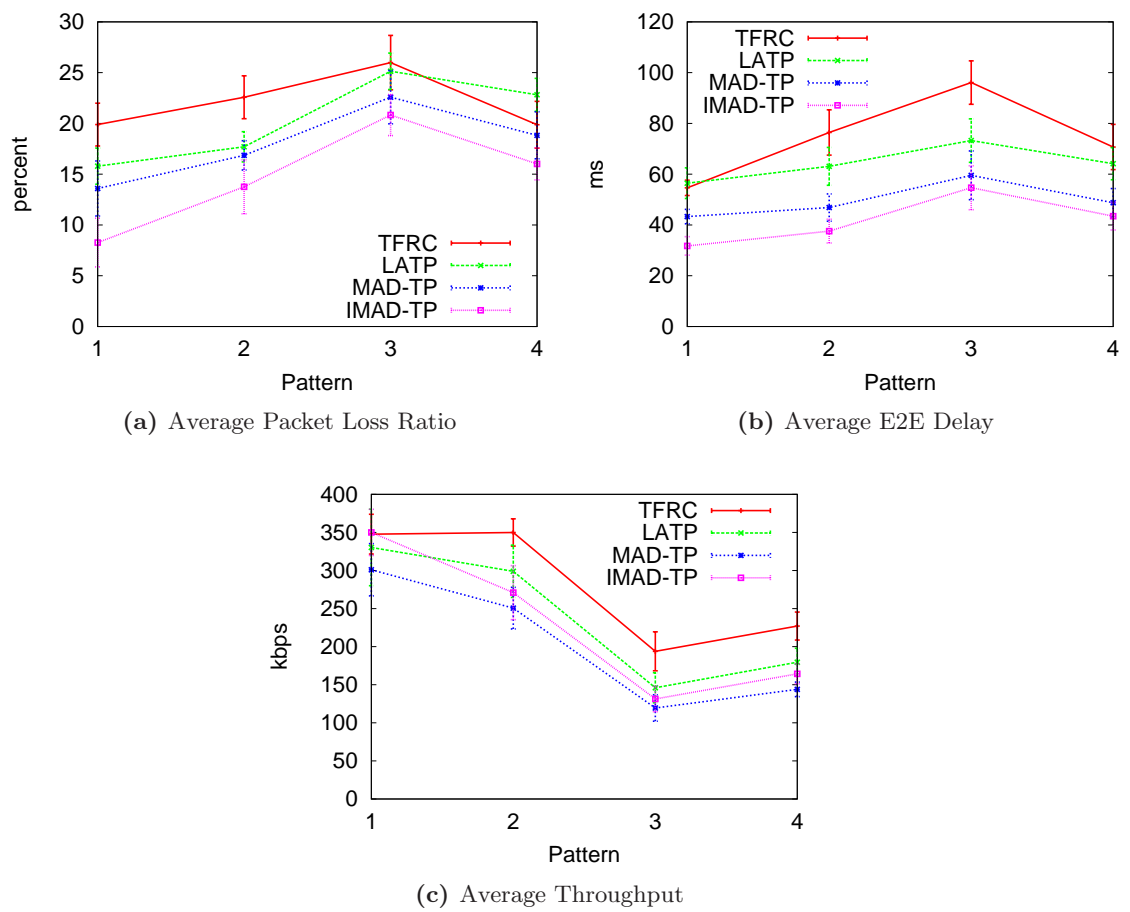


Figure 6.9: Grid topology with routing protocol AODV: the performance

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

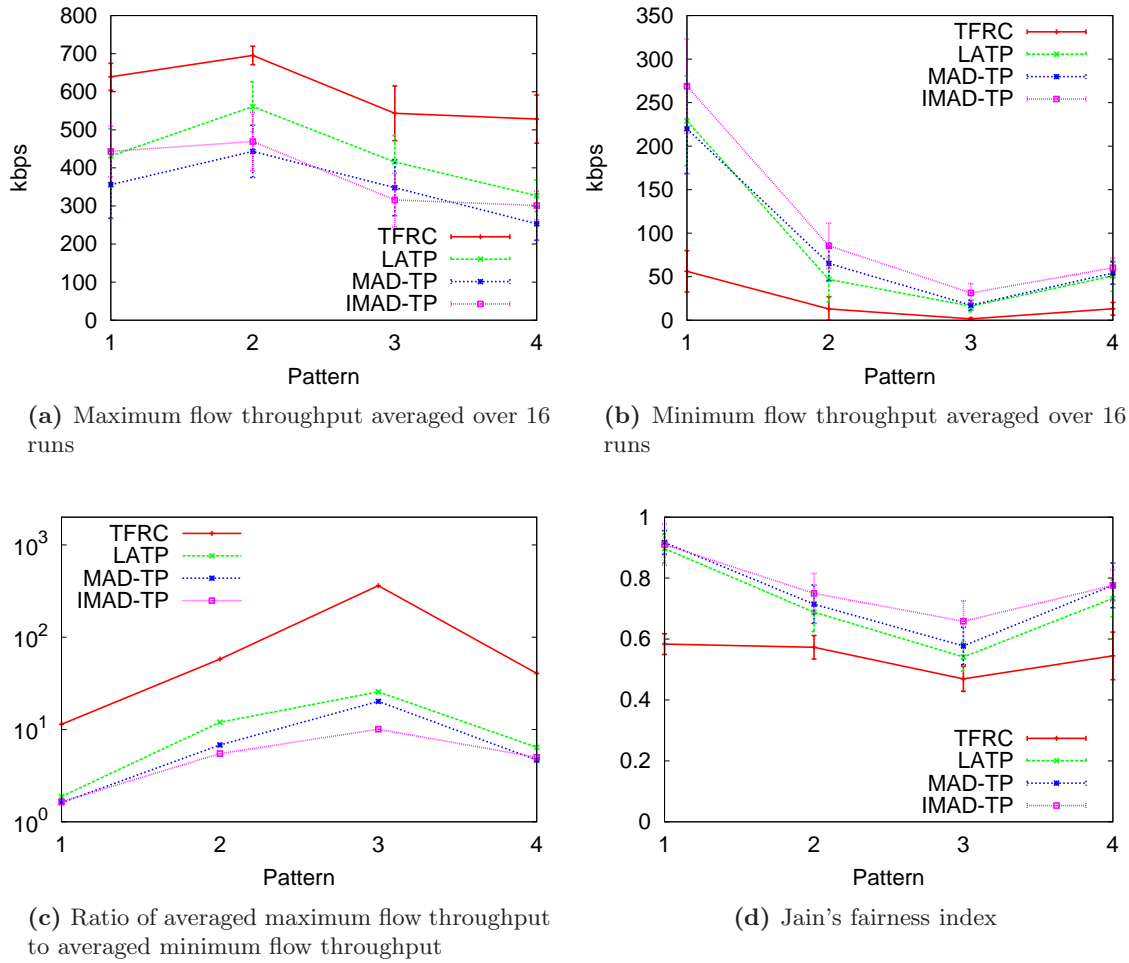


Figure 6.10: Grid topology with routing protocol AODV: the fairness

In this scenario, IMAD-TP introduces the best performance in comparison with those of TFRC, LAMP and MAD-TP. The simulation results in Fig. 6.7, 6.9, 6.8 and 6.10 show that IMAD-TP outperforms TFRC and LAMP in terms of fairness, E2E Delay and PLR for all the connection patterns and routing schemes while maintains a reasonable throughput. The average throughput of IMAD-TP and LAMP is slightly different for both routing schemes. IMAD-TP provides even better performance than that of MAD-TP. The results for PLR and E2E delay of IMAD-TP are always smaller than those of MAD-TP, while IMAD-TP exhibits the same throughput for the scenario with precomputed routing paths and higher throughput than MAD-TP for the scenario with AODV routing scheme. Fig. 6.8 and 6.10 also shows that IMAD-TP provides the same fairness level with MAD-TP for precomputed path scheme being used or even better for AODV being used. It is observed from Fig. 6.10.b and 6.10.c that IMAD-TP ensures a higher minimum flow throughput than that of MAD-TP, and a smaller scale between the maximum flow throughput and minimum flow throughput, i.e. the scale of of IMAD-TP is only a half that of MAD-TP at pattern 3.

These results can be explained that IMAD-TP better detects the optimal perfor-

mance point of the network and provides an efficient rate regulation scheme. The performance of IMAD-TP is thus more optimal than the others.

6.4.2.3 Random topology

The operation of the considered protocols is also investigated in a more realistic random topology. Different contention levels are made by increasing the number of connection flows in the network. Each pair of source and destination of a connection is chosen randomly with its hop distance is at least 3 hops. Fig. 6.11 and 6.12 exhibit the simulation results for the scenario 4.

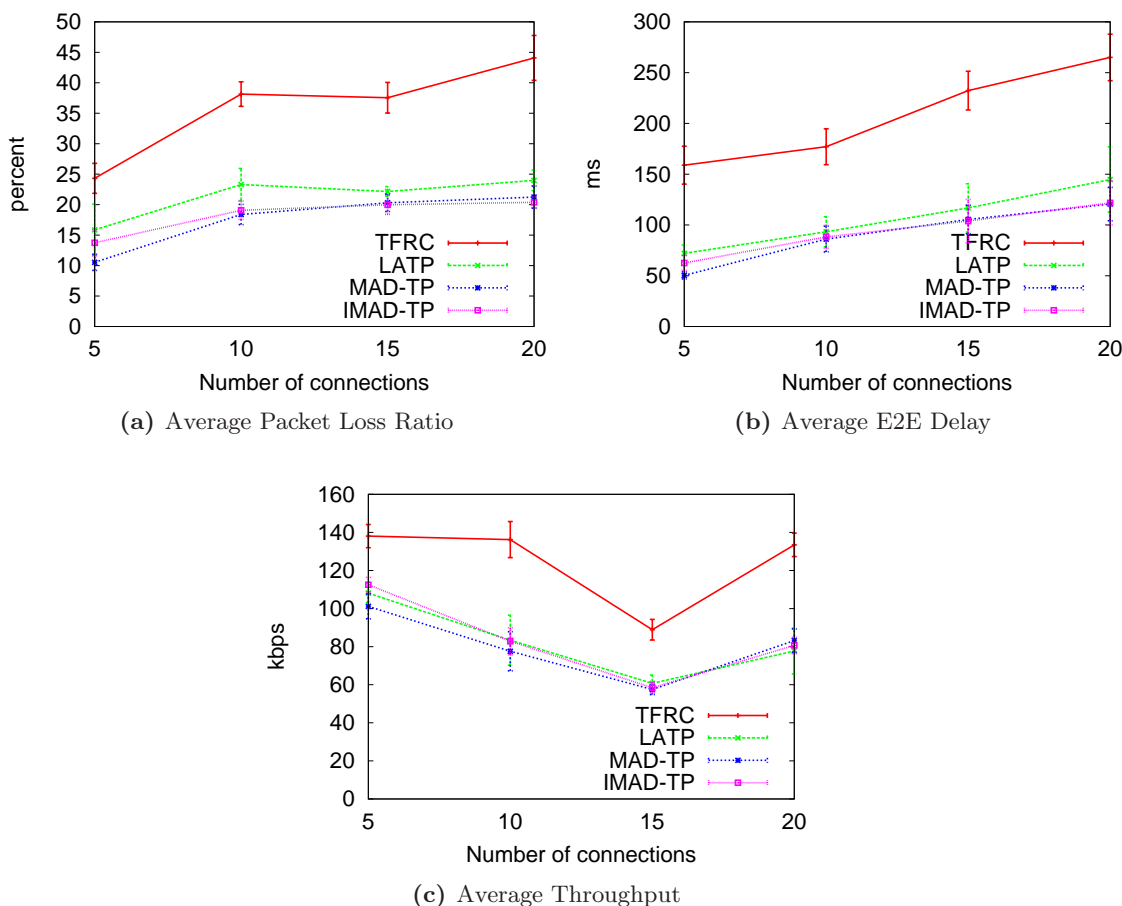


Figure 6.11: Random topology with routing protocol AODV: the performance

The results show that, in such a complex simulation scenario, IMAD-TP still outperforms TFRC in terms of fairness, PLR and E2E delay. IMAD-TP also provides better performance than LATP in terms of fairness, PLR and E2E delay with the same throughput. In this scenario, IMAD-TP and MAD-TP perform the same behavior.

Moreover, IMAD-TP exhibits a much better fairness level than three other schemes. Fig. 6.12.b and 6.12.c show that IMAD-TP guarantees a higher minimum flow throughput and a smaller scale between the maximum flow throughput and minimum flow

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

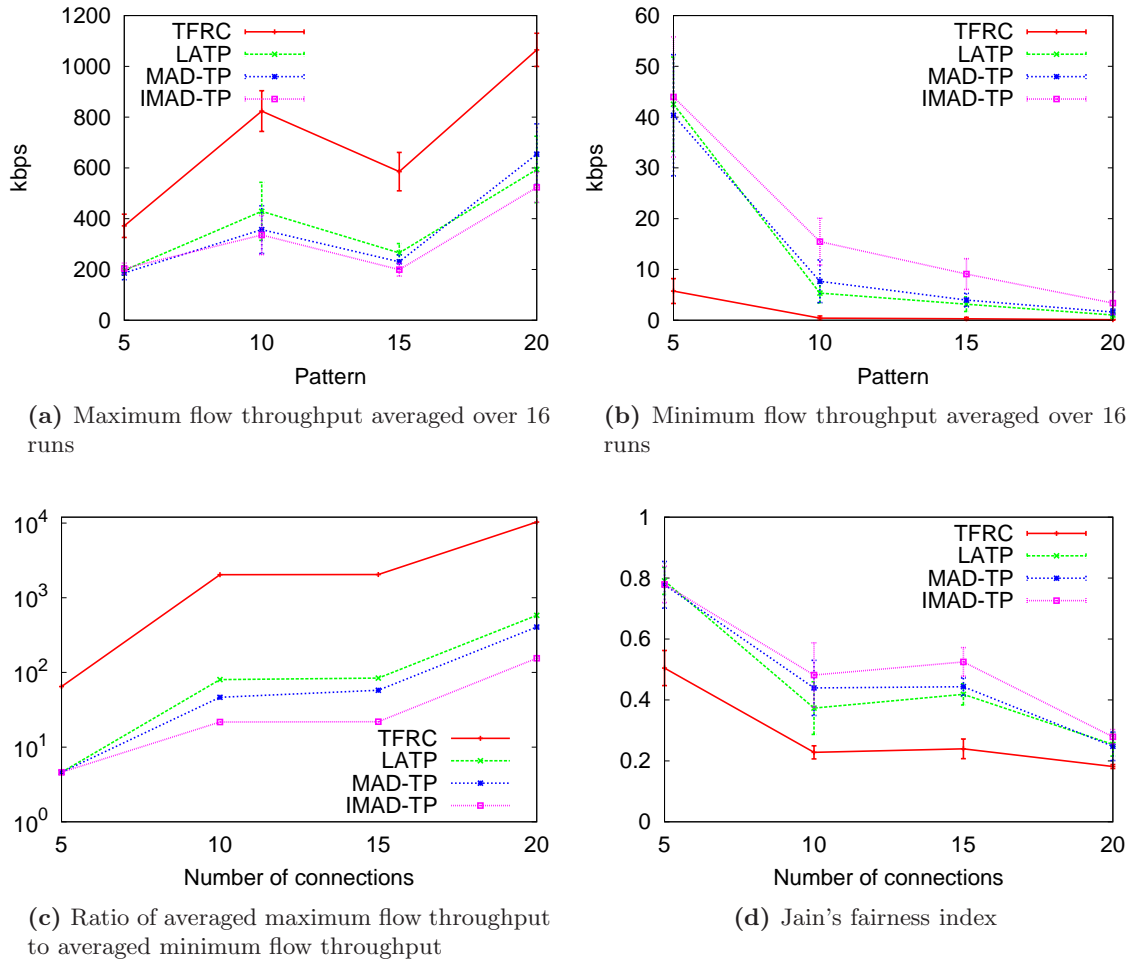


Figure 6.12: Random topology with routing protocol AODV: the fairness

throughput than the others. For example, with 15 concurrent connections, the minimum flow throughput of IMAD-TP, MAD-TP, LATP and TFRC are respectively 9, 4, 3 and 0.3 kbps, and the considered throughput scale of IMAD-TP is respectively 1/3, 1/4 and 1/100 that of MAD-TP, LATP and TFRC.

This can be explained that, in this scenario, the MAD_{TH} used by MAD-TP and MAD gradient used by IMAD-TP reflect the network contention level identically. Therefore, both IMAD-TP and MAD-TP can make the network to work in an optimal point which introduces the same performance. Nevertheless, the rate control based on the effective bandwidth estimation of IMAD-TP is more reasonable than that of MAD-TP, thus IMAD-TP introduces better fairness level than MAD-TP.

6.5 Summary

In this chapter, a new rate control scheme, IMAD-TP, is proposed which improves the shortcomings of the previously scheme MAD-TP. In IMAD-TP, two metrics MAD and ATT are used together to provide a more quickly and accurate network contention/collision detection and a more reasonable rate regulation. Instead of using the absolute threshold MAD_{TH} , IMAD-TP utilizes the gradient of MAD in order to detect the growth of network contention level. Two corresponding thresholds for MAD gradient are defined to direct the rate regulation mechanism. In addition to the contention detection task, IMAD-TP also uses ATT metric to accurately estimate the effective bandwidth for the connection flow, and thus derives the upper bound of the sending rate. This upper bound is the maximum rate that the IMAD-TP sender can use to pumps packets into the network without overloading it. With these techniques, IMAD-TP gets rid of the MAD_{TH} related shortcomings and thus provides an accurate and efficient rate control scheme over Multi-hop Wireless Networks. The simulation results show that IMAD-TP provides better fairness level between flows in MHWNs than that of MAD-TP, LAMP and TFRC. IMAD-TP also outperforms three other schemes in terms of end-to-end delay and packet loss ratio which are the two critical criteria for real-time streaming applications.

However, IMAD-TP still has its shortcomings. The first one is the choice of the exact values for TH_1 and TH_2 . Although the values found out by simulation work well in all the experiments, they need to be proved more precisely, i.e. by analytical model. The second one is the assumption in the estimation of BDP that the forward path is the same with the return path. This assumption is not always correct. Thus, this estimation should also be improved.

6. METRIC-BASED RATE CONTROL FOR TRANSPORT PROTOCOL

Chapter 7

Conclusions and Future Research

7.1 Concluding Remarks

This thesis addressed the performance degradation problem of rate-based transport protocols in Multi-hop Wireless Networks. Our objective was to develop effective rate control schemes which enable rate-based transport protocols to obtain low packet loss rate and small end-to-end delay over MHWNs as these criteria are critical for real-time streaming applications. Our approach was based on cross layer design between Transport and MAC layers by which, the information about the network state from MAC layer, called metrics, can be provided up to Transport layer.

In order to clarify the important role of metrics, the thesis first provides a survey of the main metrics from Physical, MAC, Network and Transport layers and thus provides a multi-criteria and hierarchical classification. In this classification, the metrics are first classified according to the protocol layer and then are grouped by their usage, or a function of the layer. Each metric belongs also to one or more categories of obtaining methods which are Availability, Estimation, Measurement and Combination. The classification shows that all of the complex metrics which reflect more than one characteristic of the wireless network are composed of simpler metrics, many of them coming from lower layers. This observation comes to a suggestion that we can create new multi-purpose metrics which may capture many characteristics of the wireless network by combining the aforementioned simple metrics interchangeably in different methods.

After the survey on metrics, the thesis also introduced novel MAC metrics and performed a comparative study on the effectiveness of these novel metrics and some typical ones taken from the survey. The evaluation method is based on simulation with various scenarios representing several factors that may affect the operation of a MHWN. The evaluation results show that the Medium Access Delay *MAD* and Average Transmission Time *ATT* metrics appear as potential metrics which provide the accurate information about network congestion/collision level. In non-saturated state, *MAD* and *ATT* are independent of node number, node position and traffic rate. *MAD* also does not depend on the packet size. In saturated state, *MAD* and *ATT* reflect faithfully the MAC states as they can point out the node region where experiences high traffic load.

7. CONCLUSIONS AND FUTURE RESEARCH

Finally in the two last chapters, two rate control schemes based on MAD and ATT have been proposed. In the first scheme, called MAD-TP, the metric MAD is accumulated from all the contention time that a packet experiences along the path from the source to the destination. MAD-TP then compares the cumulative MAD with a specified threshold to predict the network condition and then to adjust the sending rate. The simulation evaluation showed that MAD-TP outperforms TFRC in terms of end-to-end delay and packet loss rate. The second scheme, called IMAD-TP, eliminates the MAD threshold drawbacks of the first one by using the gradient of MAD . The steep of MAD gradient determines whether the network enters into severe contention state. This scheme also uses ATT to estimate the effective bandwidth along the connection path. Thus, the sending rate is regulated more effectively and accurately by the combination of two metrics. The simulation evaluation also showed the even better results for the operation of the second scheme.

7.2 Future Research

The research reported in this thesis suggests several interesting open problems. Firstly, an analytical model for the MAD metric should be developed. MAD metric has been proved by simulation that it is effective and accurate in reflecting the network contention level. An analytical model with a mathematical proof will better affirm the advantages of MAD . In addition, the designs of the proposed schemes require to choose carefully the thresholds of MAD , i.e. MAD_{TH} , TH_1 and TH_2 . In the current design, the choice of these thresholds was relatively empirical as the trade-off between achievable throughput, and packet loss rate and end-to-end delay. The MAD analytical model will provide accurate thresholds by which, the proposed schemes can detect efficiently the network condition, thus perform appropriate responses.

The second interesting open research issue is the cross layer design between Transport and Network layers which is discussed in Section 3.3 of Chapter 3. As the hop metric is not efficient enough to find paths in MHWNs, the ad hoc routing protocols need other metrics which can provide more information about the network condition. Most of them, as presented in Chapter 3, come from MAC and Physical layers. Instead of deploying the MAC/Physical metrics themselves, transport protocols can make use of the routing results, i.e. path assessments, in order to enhance their operation over MHWNs. The combination between an efficient routing protocol with a transport protocol with an adaptive rate control, therefore, can improve the quality of service (QoS) in MHWNs. As routing metrics have been integrated into ad hoc routing schemes, e.g. *ETX* and Optimized Link State Routing protocol (OLSR) [101], we believe that this is a potential research issue.

Another open research problem is the cross layer design for transport protocols over heterogeneous MHWNs based on different wireless technologies, i.e. IEEE 802.11, WiMAX and LTE. Although 4G wireless technologies are expected to bring a high bandwidth wireless communication with a QoS oriented MAC scheduling system, it can not get rid completely of the challenges induced by wireless medium characteristics. The design of transport protocols working effectively over a heterogeneous multi-hop wireless network faces different challenges. However, we believe that the cross layer metric approach is still a potential research issue.

Appendix A

Version française

A.1 Introduction

Dans la dernière décennie, nous avons été témoins de la prolifération des dispositifs sans fil ainsi que la demande des utilisateurs pour l'informatique ubiquitaire. Les communications sans fil sont de plus en plus populaires parmi les utilisateurs à domicile et dans les entreprises et, elles vont jouer un rôle clé dans les systèmes de communication à venir. Les principaux avantages des réseaux sans fil en comparaison avec leurs homologues câblés incluent la gestion de la mobilité flexible, un déploiement plus rapide et moins cher, et finalement, une maintenance plus facile. Le réseau sans fil multi-sauts (Multi-hop Wireless Networks - MHWN) est un réseau maillés de noeuds (des ordinateurs par exemple) reliés par des liens de communication sans fil. Dans ce réseau, il existe un ou plusieurs noeuds intermédiaires, et donc plusieurs liaisons sans fil, sur le chemin entre la source et la destination. Par conséquent, comme un sous-ensemble des réseaux sans fil, les réseaux sans fil multi-sauts héritent également de ces avantages. Le nombre de réseaux multi-sauts sans fil a cru de façon spectaculaire au cours des dernières années.

L'émergence des réseaux sans fil multi-hop a suscité un intérêt important dans le domaine de la recherche en réseaux sans fil. Une des principales questions est la performance dans ce contexte des protocoles très répandus de l'Internet comme le protocole de transport, c'est à dire Transmission Control Protocol (TCP). En général, ces protocoles de transport ont d'abord été conçus pour fonctionner dans les réseaux câblés sous l'hypothèse que le réseau présente une bande passante élevée et un très faible taux d'erreur bit. Cependant, les caractéristiques du médium sans fil et du multi-saut sont une faible bande passante partagée et un ensemble plus riche de pertes de paquets dues à la contention d'accès, aux interférences sur le canal et les ruptures de liaison sans fil. Aussi, les protocoles de transport classiques souffrent de la dégradation de leurs performances quand ils opèrent sur des réseaux sans fil multi-hop. Plusieurs solutions avec des approches différentes ont été proposées afin d'améliorer la performance des protocoles de transport dans les réseaux sans fil multi-hop.

Cette thèse traite de l'amélioration inter-couches ou "cross-layer" des protocoles de transport dits "rate-based" comme TFRC (TCP-friendly Rate Control) dans les

A. VERSION FRANÇAISE

réseaux sans fil multi-hop. Les protocoles de transport dits “rate-based” sont dédiés aux applications streaming temps réel qui sont contraintes par le taux de perte de paquets et à faible délai de bout-en-bout. Néanmoins, ces critères sont difficilement respectés dans les réseaux sans fil multi-hop. Prenant en considération tous les facteurs ci-dessus, le but de notre travail est de proposer des systèmes de contrôle du débit basés sur des informations cross-layer qui introduit un taux de perte de paquets raisonnable et un délai de bout en bout pour les application de streaming temps réel dans les réseaux sans fil multi-hop. La performance des systèmes proposés est étudiée de manière approfondie et comparée avec celle de contrôle du protocole TCP-friendly. L'évaluation de métriques telles que le débit, le taux de perte de paquets, le délai de bout en bout et l'équité sont utilisés pour présenter l'efficacité des algorithmes proposés dans les réseaux sans fil multi-hop.

Les contributions de cette thèse sont résumées comme suit:

- Une classification des métriques cross-layer par couche Cette classification multi-critères par couche liste et donne une définition complète des principales métriques des niveaux physique, MAC, réseau et transport. Comme les mesures fournissent des informations sur l'état du réseau, leur rôle est très important dans l'approche cross-layer. Cette classification donne aussi un aperçu de l'utilisation de paramètres et puis, nous suggérons des pistes d'utilisation.
- Une étude comparative de l'efficacité des métriques MAC dans les réseaux sans fil multi-hop. La fonction d'une métrique MAC est de refléter de manière efficace les problèmes au niveau MAC comme le niveau de contention ou la perte suite à une collision. Cette étude présente de nouvelles métriques MAC et évalue leur efficacité à refléter les événements réseau grâce à des simulations. Les résultats montrent que nos nouvelles métriques peuvent être utilisées comme des indicateurs précis et efficaces des événements de la couche MAC.
- Deux nouveaux protocoles de transport basés sur le débit pour les réseaux sans fil multi-hop. La conception de ces protocoles est basée sur des informations de l'état du réseau fournies par des métriques MAC de manière cross-layer. Le premier schéma utilise l'une de nos nouvelles métriques MAC pour prédire le niveau de contention sur le chemin entre une source et une destination, puis ajuste le débit d'émission en conséquence. Le second schéma utilise deux métriques MAC pour obtenir à la fois le niveau de contention du réseau et la bande passante optimale efficace du chemin de connexion. Ces schémas empêche le protocole de transport de surcharger le réseau, et maintient ainsi le fonctionnement du réseau à un niveau optimal avec un faible taux de perte de paquets et un faible délai de bout-en-bout.

A.2 Une classification des métriques cross-layer par couche

Les protocoles génériques ou encore indépendants des technologie sous-jacentes, c'est à dire ceux des niveaux réseau et transport, voient leurs performances se dégrader dans l'environnement sans fil. En effet, le fonctionnement de ces protocoles est basé sur les informations intrinsèques de la couche à laquelle ils appartiennent, sous l'hypothèse que la bande passante réseau disponible est grande et le taux d'erreur binaire (BER) très faible. Toutefois, ce n'est pas le cas dans les MHWNs où la ressource réseau est limitée et le BER est relativement élevé. Par conséquent, ces protocoles génériques doivent être améliorés ou re-conçus de façon à fonctionner correctement dans les MHWNs. De nombreux schémas ont été proposés dans la littérature sur l'amélioration de la performance des protocoles de routage et aussi sur l'amélioration du fonctionnement de TCP dans les MHWNs. Toutes les solutions proposées ont en commun qu'elles essaient d'avoir plus d'informations sur le comportement du réseau dans les couches inférieures. On parle alors de protocoles cross-layer. Les informations exploitées forment des métriques qui peuvent provenir de n'importe quelle couche des piles réseau et peuvent être utilisées directement ou conjointement avec d'autres indicateurs.

Comme de nombreuses métriques ont été proposées pour relever les défis mentionnés ci-dessus, nous proposons de les lister et de les classer d'une manière systématique afin de fournir une vue d'ensemble de leur prolifération. Certains ouvrages ont été publiés qui se concentrent uniquement sur la classification des métriques de routage. Toutefois, à la connaissance de l'auteur, il n'existe aucune publication sur la collecte et la classification des mesures de quatre couches inférieures de la pile TCP / IP. Ce chapitre donne un aperçu et une définition complète des principaux paramètres des couches physique, MAC, réseau et transport et fournit ainsi une classification hiérarchique multi-critères des métriques. Dans cette classification, les paramètres sont d'abord classés en fonction de la couche de protocole où les événements qui reflètent ces indicateurs se produisent liés. Dans chaque couche, les métriques sont ensuite regroupées par leur utilisation qui se rapporte à une fonction de la couche. Nous avons également classé les métriques selon la manière de les obtenir, à savoir la disponibilité intrinsèque (métrique appartenant au protocole, par exemple, le nombre de retransmissions après collision), l'estimation par des modèles statistiques, la mesure au moyen de techniques de sonde, et la combinaison d'autres mesures.

Metrics of Physical layer

La fonction de couche physique est de transmettre les bits sur un support. Avec un support sans fil, l'émetteur choisit une fréquence porteuse donnée, et un niveau de puissance approprié puis transmet un signal modulé dans le temps. En raison de l'environnement de propagation, le signal peut souffrir d'interférences de bruit et d'atténuation. Ainsi, les métriques de la couche PHY peuvent fournir des informations sur la qualité du canal ou de la force du signal. Les paramètres physiques pris en considération sont : Received Signal Strength Indication (*RSSI*), Signal to Noise Ratio (*SNR*), Carrier to Interference Plus Noise Ratio (*CINR*), Bit Error Rate (*BER*), Interference Ratio (*IR*).

A. VERSION FRANÇAISE

On considère souvent que les paramètres de la couche PHY fournissent seulement une information “brute” du niveau de puissance du signal. Les mesures de ces paramètres sont effectuées localement au niveau du dispositif sans fil. Certains d’entre eux sont disponibles à partir du pilote de la carte sans fil, mais le calcul d’autres métriques impliquent la modification du pilote de la carte sans fil.

Métriques de la couche MAC

Les principales fonctions de la couche MAC sans fil sont la fiabilité de la transmission et le mécanisme d’accès au support sur un canal radio partagé avec un overhead minimum et des collisions. D’autres fonctionnalités ont été ajoutées à la couche MAC pour les services de qualité de service nécessaires aux applications multimédias. Cette couche fournit des informations sur le canal telles que la modulation et le schéma de codage, de l’information statistique sur les transmissions des trames et le temps d’accès au support.

Nous classons les paramètres MAC selon les fonctionnalités de la couche MAC ou des services : IEEE 802.11 MIB, accès support et charge. Le standard IEEE 802.11 définit des variables dans la base “Management Information Base (MIB)” qui peuvent être utilisées pour améliorer la reprise sur erreurs au niveau MAC ou fournies aux couches supérieures. Les métriques relatives à l’accès au support sont : Packet Medium Access Time (T_q), Packet Transmission Time ($T_{transmit}$), Contention Delay (CD) and Airtime Cost (C_a). Les métriques relatives à la charge sur le réseau sont : Channel Busyness Ratio (R_b), Permissible Throughput (P), Effective MAC Throughput (EMT).

Métriques de la couche réseau

Les principales fonctions de la couche réseau est l’adressage des hôtes, le routage des paquets à travers les réseaux, le relayage des paquets entre les interfaces et la fourniture de la QoS. Les paramètres de cette couche doivent tenir compte non seulement des informations à la couche en cours, comme la longueur du chemin, l’interface en cours d’utilisation, le nombre de sauts jusqu’à la destination ou le nombre de paquets dans le buffer, mais aussi les informations des couches inférieures telles que le niveau de contention ou le taux de transmission disponible pour estimer l’état du réseau. Certains aspects des réseaux sans fil dont les métriques de routage doivent prendre en compte: taux de perte de paquets, le taux transmission de paquets sur chaque lien et les interférences inter/intra-flux. La métrique de routage doit être “isotonique” ce qui garantit qu’il existe des algorithmes efficaces comme Dijkstra ou Bellman-Ford qui peuvent utiliser la métrique pour trouver un chemin de coût minimum et sans boucle. Nous classons les paramètres réseau par critères suivants: transmission sur le support, interférences inter/intra-flux et multi-usages.

Les métriques relatives au support réseau sont : Expected Transmission Count (ETX), Expected Transmission Time (ETT). Les métriques inter-flux sont : Interference-aware Resource Usage (IRU), Interference Traffic Load (Q) and Link Load (LL). Les métriques intra-flux sont : The intra-flow interference related metrics are Channel Switching Cost (CSC) and Channel Load (CL). Les métriques multi-usages sont :

A.2 Une classification des métriques cross-layer par couche

Weighted Cumulative ETT (*WCETT*), Metric of Interference and Channel-switching Cost (*MIC*), PHY/MAC Aware Routing Metric for Ad-hoc Network (*PARMA*), Interference Aware Routing Metric (*iAWARE*) and Load Aware Routing Metric (*LARM*). Les mesures considérées sont spécifiquement conçus pour les réseaux sans fil multi-hop. Ils améliorent la routage des MHWNs de différentes manières, mais avec la même idée d'utiliser les informations des couches MAC et physique en plus de celles de la couche réseau. Comme de nombreuses métriques de routage tiennent compte des informations des couches inférieures, ces métriques peuvent aussi être utilisées pour améliorer le fonctionnement des protocoles de transport. Bien que cette idée ait besoin d'être creusée, l'auteur de la thèse est d'avis que c'est un sujet intéressant d'investigation.

Métriques de la couche Transport

De manière générale, la couche Transport fournit des services de communication de bout en bout pour les applications sur le réseau. Les principaux services sont axés sur la connexion des communications, la fiabilité, les contrôles de flux et de congestion. Comme TCP est le protocole de transport le plus utilisé dans l'Internet, il est évident que les métriques de bout en bout utilisées dans le protocole TCP ont reçu beaucoup de considération des chercheurs. Dans les MHWNs, tel que mentionné dans le chapitre 2, non seulement la congestion du réseau influe sur le délai et le débit, mais aussi les problèmes induits par l'environnement sans fil. Ces caractéristiques peuvent entraîner des pertes aléatoires de paquets, des oscillations des chemins de routage, de la contention au niveau MAC ce qui conduit à la détection d'un état erroné (situation de congestion) du réseau et à sa notification. Par conséquent, les métriques de la couche transport, qui sont de bout en bout, devraient prendre en compte tous les facteurs ci-dessus afin d'aider les protocoles de transport à obtenir de meilleures performances dans les MHWNs. Cependant, comme les métriques de transport sont les informations de bout en bout qui sont affectées par le contexte particulier des MHWNs, elles doivent être utilisées de manière combinée afin de mieux appréhender l'état du réseau. Nous classons les mesures de transport en trois catégories qui sont liées au débit, à la fiabilité et au délai des paquets. Les métriques liées au débit sont : Bandwidth Delay Product (BDP), Short-term Throughput (STT) and Short-term Goodput (STG). Les métriques liées à la fiabilité sont : Packet Out-of-order delivery Ratio (POR), Packet Loss Ratio (PLR) and Packet Loss Event Rate (p). Les métriques liées au délai sont : Relative One-way Trip Time (ROTT), Inter-packet Arrival Delay (IAD) et Inter-Packet Delay Difference (IDD).

Toutes les métriques mentionnées ci-dessus sont évaluées dans la couche transport par le protocole. Dans les MHWNs, ces métriques sont grandement affectées par l'environnement de propagation ce qui pose des questions sur leur fiabilité. Il est suggéré que les métriques de transport doivent être combinées afin de mieux détecter les événements du réseau.

Classification

Le résumé de cette étude est montré dans le tableau de classement (tableau 3.6). Outre les critères présentés dans les sections ci-dessus, les métriques sont également classées

A. VERSION FRANÇAISE

selon leurs méthodes obtention, c'est-à-dire disponible, mesurée, estimée ou composée. Notons que certains paramètres intrinsèques des protocoles couramment utilisés dans chaque couche sont également ajoutés à la table. Étant donné que ces mesures sont très fréquents, elles sont classées dans la catégorie "disponible".

A partir de cette classification, nous concluons que les métriques complexes qui reflètent plus d'une caractéristique du réseau sans fil sont composés de métriques plus simples, provenant la plupart des couches inférieures. En outre, chaque caractéristique du réseau peut être capturée de différentes manières. Aussi, nous pouvons créer de nouvelles métriques multi-usages afin de capturer de nombreuses caractéristiques du réseau sans fil en combinant les métriques simples mentionnées ci-dessus. La combinaison de métriques doit également prendre en considération le compromis entre l'efficacité et la complexité de calcul de la nouvelle métrique.

Ces dernières années, les travaux de recherche visant à améliorer les performances des protocoles de transport dans les MHWNs, ont porté sur l'exploitation des informations MAC par une approche dite "cross-layer". Bien que plusieurs métriques MAC aient été introduites, leur efficacité à refléter les états du réseau n'a pas été étudiée. Le chapitre suivant présente une étude comparative sur l'efficacité (effectiveness) des métriques MAC citées dans ce chapitre ainsi que celle de nouvelles métriques MAC que nous avons proposées.

A.3 Fidélité de différentes métriques MAC à refléter les conditions réseau

Comme décrit précédemment, les principaux protocoles de transport de l'Internet doivent faire face à des difficultés pour fonctionner correctement dans les réseaux multi-sauts sans fil. Comme l'information de bout-en-bout ne suffit pas à résoudre ces difficultés, plusieurs schémas ont été proposés qui ont en commun la propriété de tirer profit des informations de la couche MAC, appelées métriques MAC, afin de mieux connaître ce qui se passe au niveau bas du réseau. Ces informations sont ensuite transmises vers le protocole de transport d'une manière cross-layer et sont utilisées de diverses manières pour faire fonctionner le réseau correctement.

Comme ces métriques donnent des informations de niveau MAC aux protocoles des couches supérieures, on peut se poser la question suivante : quelle est l'efficacité ou la fidélité des métriques MAC à refléter le comportement de réseau ? Par exemple, nous souhaitons étudier si une métrique reflète bien les situations de contention ou les erreurs de transmission. En effet, une bonne métrique MAC que l'on va utiliser dans le contrôle de congestion Transport doit être couplé avec le niveau de contention du réseau et les pertes moyennes de transmission. Par conséquent, dans cette étude, nous proposons quelques nouvelles métriques MAC qui sont censées refléter fidèlement les différents états de la couche MAC, comme les contentions, les collisions ou les pertes. Nous étudierons ensuite l'efficacité de ces métriques à refléter les états du réseau d'une manière systématique, en simulant diverses situations de réseau, afin de répondre à la question ci-dessus.

A.3 Fidélité de différentes métriques MAC à refléter les conditions réseau

Table A.1: Metric classification table

Layers	Categories	Availability	Measurement	Estimation	Composition
TRANSPORT	Reliability		Packet Out-of-order Ratio POR , Packet Loss Ratio PLR , Packet Loss Event Rate p		
	Throughput	Received Windows $rwin$, Congestion Window $cwnd$	Bandwidth Delay Product BDP , Short Term Throughput STT , Short Term Goodput STG		
	Delay	Round Trip Time RTT	Relative One-way Trip Time $ROTT$, Inter-packet Arrival Delay IAD , Inter-packet Delay Difference IDD		
NETWORK	Medium Transmission		Expected Transmission Count ETX , Expected Transmission Time ETT		
	Inter-flow Interference	Queue length q	Interference-aware Resource Usage IRU , Interference Traffic Load Q , Link Load LL		
	Intra-flow Interference		Channel Load CL	Channel Switching Cost CSC	
	Multi-purpose				$WCETT$, MIC , $PARMA$, $iAWARE$, $LARM$
MAC	Reliability	802.11 MIB	Frame Error Rate e_{fr}		
	Channel Access	Airtime Cost C_a , Number of channel N_c	Contention Delay CD	Packet Medium Access Time T_q , Packet Transmission Time $T_{transmit}$	
	Channel Load	Link Rate R	Channel Busyness Ratio R_b , Permissible Throughput P , Effective Throughput EMT		
PHYSICAL		$RSSI$, SNR , $CINR$, BER	Interference Ratio IR		

A. VERSION FRANÇAISE

Nouvelles métriques MAC

Dans cette section, nous définissons trois nouvelles métriques MAC qui sont : le nombre moyen de transmissions d'une trame (ATA), le délai moyen de transmission d'une trame (ATT) et le délai d'accès moyen (MAD). Ils fournissent des différentes mesures prises à partir de l'opération DCF à la couche MAC. L'objectif de ces mesures est de refléter autant que possible les informations sur la situation actuelle du réseau tels que le niveau de contention, de collision ou les erreurs de transmission.

Nombre moyen de transmissions d'une trame

Le nombre moyen de transmissions d'une trame ou *ATA* (Average Transmission Attempt) est défini comme le nombre total de tentatives de transmission et retransmission réalisées par le protocole MAC pour transmettre une trame sur le nombre total de trames transmises avec succès dans un intervalle :

$$ATA = \frac{\sum_{N_{ap}} N_{at}^i}{N_{sp}} \quad (A.1)$$

où N_{at}^i est le nombre de tentatives de transmission de la trame i jusqu'à réception de l'acquittement MACK correspondant ou abandon de la transmission, N_{ap} et N_{sp} sont respectivement transmises avec succès. Thus, *ATA* est relativement sensible au niveau de collision autour d'un noeud.

Délai moyen de transmission d'une trame

Le délai moyen de transmission d'une trame (Average Transmission Time, *ATT* est dérivé du temps de service MAC T_{srv} qui est la durée écoulée entre le début où une trame entre en compétition pour être transmise jusqu'au moment où l'émetteur reçoit l'acquittement MACK correspondant ou abandonne la transmission après plusieurs tentatives infructueuses (voir Fig. A.1).

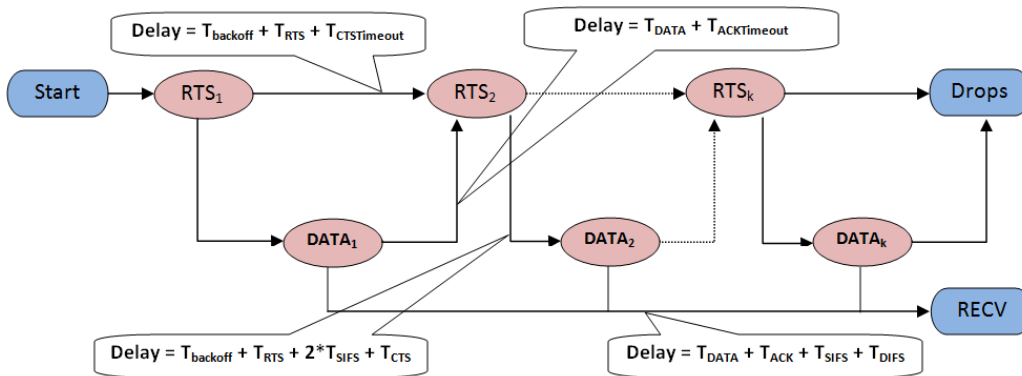


Figure A.1: Modèle du temps de service IEEE 802.11 [1]

Contrairement à T_{srv} , *ATT* ne prend en compte que les transmissions réussies et est donc le temps de service moyen d'une trame transmise avec succès dans un intervalle

A.3 Fidélité de différentes métriques MAC à refléter les conditions réseau

de temps. On calcule ATT , comme la somme des temps de service de toutes les trames recues par la couche MAC divisée par le nombre total de trames transmises avec succès.

$$ATT = \frac{\sum^{N_{ap}} T_{srv}}{N_{sp}} \quad (\text{A.2})$$

où N_{ap} et N_{sp} sont identiques à l'équation A.1. ATT , par définition, incluent le délai de contention et le délai de transmission et peut aussi être utilisé pour indiquer le niveau de contention autour d'un noeud. Si le nombre de noeuds voisins qui transfèrent du trafic augmente, un noeud doit attendre plus longtemps lors des périodes de backoff pour accéder au support et peut avoir plus de risques de collision de transmission, ce qui à son tour introduit un retard de transmission plus long. ATT est sensible à la fois à la charge offerte au MAC et au niveau de collision dans le voisinage du noeud.

Le délai d'accès moyen

Le délai d'accès moyen (Medium Access Delay, MAD) est défini comme le délai de contention moyen pour une trame à la couche MAC avant qu'elle ne soit transmise avec succès ou abandonnée après plusieurs échecs de retransmissions sur une période. Par cette définition, MAD comprend la première durée de backoff quand la trame arrive au niveau MAC et toutes les périodes de backoff successives après collision ainsi que la durée NAV à chaque reprise de retransmission.

$$MAD = \frac{\sum^{N_{ap}} \sum T_{contention}^i}{N_{ap}} \quad (\text{A.3})$$

où N_{ap} est le nombre de trames transmises durant la période et $T_{contention}^i$ est la durée de la contention à la i^{th} tentative de transmission (Fig. A.1). Notons que le nombre maximum de retransmission est limité par le paramètre $RetryLimit$ défini dans le standard IEEE 802.11 MAC.

Si la valeur de MAD augmente, il y a deux possibilités. Tout d'abord, le canal est très occupé de telle sorte que le noeud doit différer plus longtemps avant d'avoir une opportunité de transmission. Deuxièmement, le nombre de retransmissions augmente en raison du nombre plus élevé de collisions et chaque échec renvoie le noeud dans l'état backoff. Par conséquent, MAD peut être utilisé pour indiquer à la fois l'occupation du canal et le niveau de collision autour d'un noeud.

Evaluation de la représentativité des métriques

Les métriques MAC ont été définies afin de fournir des informations de niveau MAC aux protocoles des couches supérieures. Ainsi, il est très important d'étudier la représentativité de ces métriques, c'est à dire, leur capacité à refléter les problèmes de fonctionnement des couches inférieures du réseau, en particulier ceux reliés à la congestion du réseau. Toutefois, étant donné que la congestion est étroitement couplée avec la contention, nous prétendons que le niveau de saturation réseau est la situation qui doit être réglée

A. VERSION FRANÇAISE

rapidement et avec précision afin d'indiquer le début de la congestion dans les tampons IP.

À notre avis, une métrique MAC efficace pour le contrôle de congestion devrait avoir un comportement représentant à la fois la contention et les collisions ainsi que les pertes dues aux erreurs. En d'autres termes, elle doit être sensible aux changements d'état du réseau causés par un des événements et sa réaction à ces changements doit également être facilement identifiable. Dans l'étude de l'efficacité ou de la représentativité, cinq métriques MAC sont étudiées : *ATA*, *ATT*, *MAD*, *EMT* et R_b . La question à laquelle nous tenterons de répondre dans cette étude est : quelle est la meilleure métrique capable de refléter efficacement et clairement les événements du réseau? Dans cette évaluation de la représentativité, les mesures MAC considérées sont étudiées de manière approfondie à travers des situations réseau diverses qui affectent la performance des protocoles des couches supérieures. La dégradation des performances de ces protocoles est principalement causée par les caractéristiques du support sans fil et la nature multi-sauts du réseau. En effet, la perte de paquets est causée non seulement par la congestion, mais aussi par les erreurs de transmission. Les noeuds doivent entrer en compétition les uns avec les autres pour obtenir l'accès au support. Le niveau de contention dépend donc en grande partie des transmissions des noeuds, donc de la charge et des interférences inter-flux qui en découlent. En outre, l'augmentation du nombre des transmissions peut également exacerber le problème du noeud caché qui est l'une des sources de perte de paquets. Par conséquent, plusieurs scénarios seront construits sur la base de la variation de charge de trafic et le BER canal. La simulation va donc montrer comment effectivement les métriques considérées réagissent aux changements de l'état du réseau.

Simulation et résultats

Les simulations ont été réalisées avec le simulateur NS-2.34. La configuration étudiée est une chaîne de 9 noeuds qui supporte une connexion UDP entre les 2 noeuds terminaux écoulant un trafic CBR. Le calcul des métriques se fait toutes les secondes.

Le premier scénario vise à évaluer l'effet de la charge de trafic sur les métriques. Ceci est réalisé d'une part en augmentant le débit de la source du trafic d'un flux et d'autre part, en ouvrant plusieurs connexions en parallèle. Un second scénario simule l'effet des erreurs de transmission sur une seule connexion par augmentation du BER et plusieurs valeurs de débit. Les résultats des simulations montrent que toutes les métriques que nous avons évaluées sont relativement sensibles à la charge du réseau car toutes ont un comportement représentant avec le changement de débit. *ATA*, *ATT*, *EMT*, R_b et *MAD* peuvent être utilisés pour indiquer si le réseau est dans un état non-saturé ou saturé. Parmi elles, *ATA* et *MAD* présente la propriété que leurs valeurs à l'état non saturé sont indépendantes l'un numéro de noeud, de sa position, de la taille des paquets et de débit (pour autant qu'il soit inférieur à un seuil). Cependant, l'échelle entre les valeurs de *ATA* correspondant aux deux états du réseau n'est pas aussi claire que pour celles de *MAD* et *ATT*. Dans l'état saturé, *ATT* et *MAD* reflètent fidèlement les Etats MAC par rapport à R_b , car ils peuvent signaler les zones saturées suite à une collision causée par l'augmentation du débit. Néanmoins, *MAD* reflète mieux l'occupation moyenne et le niveau de contention dans le voisinage d'un noeud.

A.4 Un nouveau protocole de transport “rate-based” utilisant la métrique MAD

En outre, par rapport à *MAD*, *ATT* comprend également le délai de transmission qui est relativement long par rapport à la durée de contention. Donc, le changement de valeur de *MAD* indique précocement une situation de contention ou une collision et plus clairement que celle de *ATT*. Ainsi, la métrique *MAD* semble être l’indication la plus précise et la plus précoce.

Pour le scénario 2, dans l’état non saturé, l’observation du changement de *ATA*, *ATT* et *MAD* peut aider à déterminer les pertes causées par une erreur de transmission car il n’y a pas de perte due aux collisions dans cet état. Néanmoins, l’état non-saturé est difficile à réaliser dans le fonctionnement habituel du réseau en raison des modèles de trafic assez complexes. Dans l’état saturé où les pertes se produisent fréquemment suite à une collision, les pertes dues aux erreurs de transmission peuvent ne pas être distingués par ces métriques MAC. Cependant, il est également possible d’utiliser *ATT*, *ATA* et *MAD* pour indiquer les pertes générales au niveau MAC suite aux erreurs ou aux collisions. Avec ces avantages remarquables, dans les chapitres suivants, les deux métriques efficaces *MAD* et *ATT* seront exploitées dans les nouveaux schémas que nous proposons pour améliorer la régulation du débit des protocoles de transport dans les réseaux sans fil multi-sauts.

A.4 Un nouveau protocole de transport “rate-based” utilisant la métrique MAD

Principes

Le but de ce chapitre est de proposer un nouveau protocole de transport “rate-based” dit “cross-layer” car il utilise la métrique *MAD* qui est issue du niveau MAC. En effet, en considérant le fait que la congestion est étroitement couplée avec la contention, il est possible d’améliorer les performances des protocoles de transport en ne considérant que l’état de contention du réseau. La croissance de la contention doit être détectée au plus tôt et le plus précisément possible, et un mécanisme adéquat doit réagir efficacement à cet événement afin de réduire l’effet du niveau de contention élevée dans le réseau c’est-à-dire en réduisant le débit d’émission au plus vite.

Notre proposition utilise la métrique *MAD* pour déterminer au plus tôt si le réseau entre dans un état de haute contention, puis applique un contrôle de débit effectif pour empêcher au flux de subir une dégradation des performances. L’idée derrière *MAD-TP* vient de l’observation de *MAD* au chapitre 4. La valeur de *MAD* de tous les noeuds dans la zone de contention augmente fortement lorsque le niveau de contention autour du lien congestionné est grave. Par exemple la valeur de *MAD*, lorsque le réseau (chaîne topologie) est non-saturée, est d’environ 111μ s et plutôt stable, tandis que dans l’état saturé, elle est dans un intervalle de 1000μ s à 10 ms et même plus parfois. Le mécanisme de contrôle de débit peut alors utiliser la métrique *MAD* comme une indication précoce de l’augmentation de niveau de contention sur la connexion afin d’ajuster correctement le débit d’envoi de paquets sur le réseau.

La conception du contrôle du débit, appelé *MAD-TP*, se présente comme suit. Chaque noeud intermédiaire sur le chemin de la connexion fournit une estimation du

A. VERSION FRANÇAISE

niveau de contention ressenti et maintenant la métrique MAD dans chaque intervalle. Dans la mise en oeuvre, la durée de l'intervalle est réglée sur 0,1 secondes qui est un compromis entre le lissage et l'efficacité. Pour tous les paquets sortants, chaque noeud cumule la valeur de MAD dans la variable $CMAD$ de l'en-tête IP $CMAD$ en ajoutant sa valeur de MAD à la valeur existante. Lorsque le paquet atteint sa destination, le récepteur obtient la valeur cumulée MAD_{cum} de tous les noeuds le long du chemin. Par conséquent, la valeur MAD_{cum} sera fonction du niveau de contention courant le long du chemin de connexion.

La fonction du récepteur MAD-TP est de recueillir une information sur l'état du réseau, à savoir le délai d'accès au support, et de le renvoyer à l'émetteur ainsi que d'autres renseignements utiles. A chaque réception d'un paquet, le récepteur MAD-TP prend la valeur de MAD_{cum} dans le champ $CMAD$ de l'en-tête IP, et le nombre de sauts (N_H) à partir du champ TTL ou de la table de routage de la source et calcule $MAD_{sample} = MAD_{cum}/N_H$. Le récepteur MAD-TP utilise également le délai Round Trip Time r_{tt} attachée au champ RTT du paquet MAD-TP comme dans TFRC [47]. Le récepteur MAD-TP estime alors la valeur moyenne de MAD en utilisant la moyenne pondérée exponentielle (EWMA) comme suit:

$$MAD = \alpha MAD + (1 - \alpha) MAD_{sample} \quad (A.4)$$

où α est égal à 0.5. Cette valeur moyenne est calculée comme dans l'équation A.4 pour tous les paquets reçus. Chaque fois que le récepteur détecte une perte, il calcule le taux moyen de réception R_{rcv} et envoie immédiatement un paquet qui contient la valeur courante estimée de MAD et R_{rcv} à l'émetteur.

L'émetteur MAD-TP utilise ces deux valeurs dans le mécanisme de contrôle de débit afin de mettre à jour le débit en fonction du changement de niveau de contention le long du chemin de réseau. En outre, le récepteur doit envoyer au moins une mise à jour à chaque aller-retour r_{tt} s'il n'y a pas de perte détectée. Cela permettra à l'émetteur de garder à l'esprit la bonne connaissance de l'état de la connexion.

La fonction principale de l'émetteur MAD-TP est de réguler correctement le débit injecté dans le réseau en fonction de la valeur de MAD renvoyée par le récepteur MAD-TP. Si $MAD > MAD_{TH}$, l'émetteur MAD-TP suppose que la connexion subit une contention grave le long du chemin et diminue le débit d'émission. La règle est que la diminution du débit d'émission est réduit de 1/8 après chaque RTT , et au minimum à un paquet par RTT . L'émetteur réduit de moitié également le débit lorsque le temporisateur "NoFeedbackTimer" expire comme dans TFRC. Si $MAD \leq MAD_{TH}$, cela signifie qu'une partie conservatrice du trafic ΔR peut encore être injectée dans le réseau. Cette partie additionnelle est choisie de telle façon que le nouveau débit d'émission soit proportionnel à MAD_{TH}

$$\begin{aligned} \frac{\Delta R + R}{MAD_{TH}} &= \frac{R}{MAD} \\ \Rightarrow \Delta R &= \left(\frac{MAD_{TH}}{MAD} - 1 \right) * R \end{aligned} \quad (A.5)$$

Le nouveau débit d'émission est alors $R + \Delta R$. Toutefois, pour éviter un changement

A.4 Un nouveau protocole de transport “rate-based” utilisant la métrique MAD

brusque débitnvoi, une règle de lissage définit le nouveau taux d’émission comme suit:

$$R = \min(R + \Delta R, R + N * S / RTT, \max(2 * R_{rcv}, S / RTT)) \quad (\text{A.6})$$

où N est le nombre de RTT s depuis le dernier changement de débit. Notons que même avec la diminution suivant la règle de LATP, le débit d’émission est toujours supérieur à 1 paquet par RTT . Par conséquent, l’équation A.6 contrôle la mise à jour du débit de telle sorte qu’il assure à l’émetteur MAD-TP au moins un paquet émis par RTT et une augmentation de débit de seulement un paquet par RTT .

Résultats de simulation

Pour évaluer la performance de MAD-TP, nous avons construit trois scénarios de simulation avec trois topologies différentes en raison de la variété des régimes de perturbations qu’ils représentent : la chaîne, la grille et topologies aléatoires. Dans le scénario 1 avec la topologie de la chaîne, le niveau de contention du réseau varie en augmentant soit le nombre de sauts ou le nombre de flux simultanés. Dans le scénario 2 avec une grille de 8x8 noeuds, 4 schémas de connexion sont mis en place de telle sorte qu’ils offrent des niveaux de contention différents dans le réseau. Dans chaque schéma, les flux de connexion sont établis le long de plusieurs lignes et colonnes de la grille. Dans le scénario 3, le fonctionnement de MAD-TP est étudié dans une topologie plus réaliste, aléatoire avec 60 noeuds dans une zone de 1500mx1500m. Différents niveaux de contention sont joués en augmentant le nombre de flux dans le réseau. Chaque paire de source et destination d’une connexion est choisie au hasard avec une distance d’au moins 3 sauts. Les facteurs de performance évalués sont le débit, le délai de bout-en-bout (E2E), le taux de perte de paquets (PLR) et l’équité. Dans notre implémentation, MAD_{TH} est fixé à 0,7 ms comme un compromis entre débit, le délai E2E et PLR.

Dans ce résumé, nous ne considérons que la topologie de la chaîne en faisant varier nombre de sauts. Pour les résultats complets, voir le chapitre 5. Dans un résumé, on ne met que les conclusions des résultats.

La figure A.2 donnent les résultats pour le scénario 1. On voit que MAD-TP surpasse TFRC en termes de PLR et de délai. Le PLR de TFRC est supérieur à celui de MAD-TP de 0,8% (pour 13 noeuds) jusqu’à 6% (pour 6 noeuds) et l’échelle de temps est de 10 ms (pour 13 noeuds) à 60 ms (pour 6 noeuds) pour le délai. Particulièrement dans les MHWNs communs, dont la taille est inférieure à 10 sauts, la différence est d’au moins 1% pour le PLR et de 20 ms pour le délai. Cela vient du contrôle de débit de TFRC qui estime à tort la capacité du réseau et a tendance à surcharger le MHWN qui a peu de ressources. Ce problème est causé par l’équation de débit TCP utilisé dans TFRC qui dépend d’une mesure de PLR erronées dans les MHWNs, où les pertes sont principalement dues à la contention de canal ou aux erreurs de transmission.

Ainsi, TFRC augmente le débit de façon inappropriée lorsque la contention du réseau est assez élevée et ne diminue pas le débit de manière suffisamment efficace quand la contention du réseau devient grave. Par conséquent, les paquets qui transitent le long du chemin vont souffrir de pertes et d’un retard causés par les collisions entre les noeuds en compétition. En revanche, MAD-TP Cependant, le délai de MAD-TP s’allonge avec l’augmentation du nombre de sauts mais il est toujours plus petit que

A. VERSION FRANÇAISE

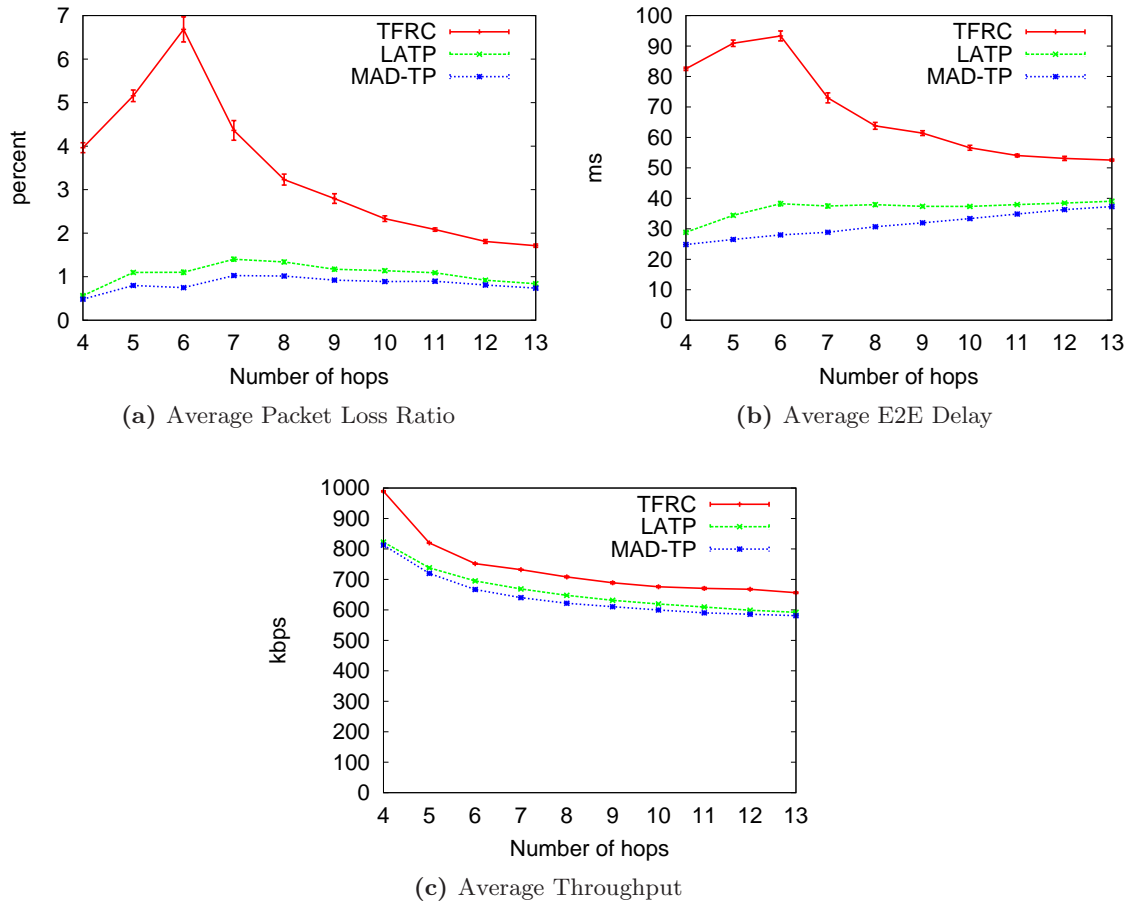


Figure A.2: Chain topology with 1 connection and routing protocol AODV

celui introduit par TFRC. Cette augmentation semble être plus “raisonnable” que celle de TFRC. Ce résultat provient de l’amélioration du contrôle de débit de MAD-TP, car il dépend du niveau de contention dans le réseau. Ainsi, MAD-TP tente toujours de maintenir le fonctionnement du réseau à un niveau bas de contention.

La figure A.2 montre également que le débit moyen d’une connexion MAD-TP est inférieure à celui de TFRC, mais la différence est assez faible. C’est le prix que MAD-TP doit payer pour atteindre de meilleurs taux de perte et délai. Toutefois, pour les applications qui demandent une garantie en termes de taux de perte de paquets et de latence, ce compromis est acceptable. Les performances de MAD-TP sont également meilleures que celle de LAMP en termes de PLR et de délai dans une chaîne de noeuds alors qu’il atteint presque le même débit. La raison en est que *MAD* détecte les contentions sévères mieux que la métrique “permissible throughput” utilisée par LAMP, ce qui permet alors à MAD-TP de contrôler son débit plus efficacement que LAMP. Toutefois, MAD-TP a un inconvénient celui de choisir une valeur absolue de seuil pour *MAD* ce qui nuit au paramétrage du mécanisme d’estimation de la quantité de données à ajouter qui peut être injectée dans le réseau. Pour surmonter ce problème, une autre métrique MAC doit être utilisée en conjonction avec *MAD*. Le chapitre V suivant que nous ne détaillons pas ici donne les détails de l’amélioration.

A.5 Contrôle de débit basé sur métrique pour protocole de transport

Dans cette partie, la conception du schéma proposé, appelé IMAD-TP, est basée sur des mesures qui sont deux MAC MAD et ATT . En IMAD-TP, le gradient de MAD est utilisée à la place de la valeur absolue de MAD comme dans MAD-TP. La croissance du niveau de contention réseau est détecté par l'observation du comportement du gradient de MAD . Selon la comparaison entre la valeur de MAD gradient et deux seuils prédéfinis, l'expéditeur sera de déterminer le comportement approprié. En outre, ATT est utilisé pour estimer la bande passante effective qui à son tour est utilisé comme la limite supérieure pour la vitesse d'envoi de la source. C'est le taux effectif au cours de laquelle IMAD-TP peut rendre le réseau de travailler dans son point de rendement optimal. Cette technique constitue un mécanisme de taux de plus raisonnable que notre régime de contrôle précédemment proposé, qui est basé sur MAD_{TH} .

Détection de contention du réseau avec un gradient de MAD

La définition de MAD gradient est la suivante. Notons A_i et A_{i+1} , respectivement, l'heure d'arrivée des paquets de rétroaction i^{th} et $(i + 1)^{th}$, MAD_i et MAD_{i+1} les annexes correspondantes valeurs MAD , alors le MAD gradient α est la suivante:

$$\alpha = \frac{MAD_{i+1} - MAD_i}{A_{i+1} - A_i} \quad (A.7)$$

Nous avons construit un scénario d'évaluation de simulation afin de déterminer la distribution de α valeurs dans les deux Etats non-saturés et saturés du réseau en fonction de la charge offerte. Dans ce résumé, nous expliquons que des résultats remarquables de l'évaluation. Les résultats ont montré que lorsque le réseau n'est pas surchargé, c'est à dire non-saturée Etat, le taux de perte de paquets est faible, le délai de bout en bout est petit. Près de toutes les valeurs de α l'automne dans l'intervalle $[-5, 5]$. Cela peut être interprété que, dans le point de charge optimale du réseau, le MAD gradient ne doit pas dépasser la valeur de 5. Lorsque le réseau est surchargé, les valeurs de α , alors répartir sur un plus grand nombre.

De ces résultats, nous avons alors peut définir deux seuils $0 < TH_1 < TH_2$ qui sont utilisés comme des indicateurs de niveau de contention du réseau. Si $\alpha < TH_1$, cela signifie que le montant de MAD de baisses (en cas $\alpha < 0$) ou il augmente relativement faible ($0 < \alpha < TH_1$), la source du trafic peut donc bien augmenter son envoi taux. Nous avons mis en $TH_1 = 5$. Si $\alpha > TH_2$, il ya une possibilité élevée que le réseau entre en état de discord grave. La source de trafic ne devrait pas augmenter le taux d'envoi dans ce cas. Nous avons mis en $TH_2 = 7$ afin de réagir rapidement à l'augmentation soudaine du niveau de contention du réseau. Sinon, c'est à dire $TH_1 < \alpha < TH_2$, le réseau peut fonctionner dans un point raisonnable et la source du trafic maintient son taux d'envoi actuelle inchangée.

A. VERSION FRANÇAISE

Estimation de la bande passante efficace avec ATT

L'idée d'utiliser ATT métrique pour estimer la bande passante effective provient du travail de Chen et al. [87]. Pour résumé, nous utilisons ATT métrique des noeuds le long du chemin de connexion pour estimer la limite supérieure du produit délai-bande passante BDP_{UB} telles que:

$$BDP_{UB} \simeq S \times \frac{\sum_{i=0}^n ATT_i + \sum_{i=0}^m ATT'_i}{4 \times ATT_{max}} \quad (\text{A.8})$$

où S est la taille du paquet, ATT'_i et ATT_i sont respectivement les retards per-hop moyenne de transmission de paquets le long de l'avant (n sauts) et retour (m sauts) chemins, et ATT_{max} est le maximum per-hop délai moyen de la voie à suivre.

Dans [87], BDP_{UB} est calculé pour chaque paire de données TCP et des paquets ACK. Cependant, dans le cas de protocole de transport basé sur la fréquence, le paquet de retour n'est pas généré pour chaque paquet de données arrivé, mais pour chaque intervalle de temps, c'est à dire un temps aller-retour, ou pour chaque événement de perte détecté nouvelle (pour TFRC). Par conséquent, nous pouvons raisonnablement déduire que:

$$\begin{aligned} BDP_{UB} &\simeq S \times \frac{2 \times \sum_{i=0}^n ATT_i}{4 \times ATT_{max}} \\ &\simeq S \times \frac{\sum_{i=0}^n ATT_i}{2 \times ATT_{max}} \end{aligned} \quad (\text{A.9})$$

La limite supérieure pour le taux d'envoi R_{UB} peut être calculée à partir de BDP_{UB} et le courant aller-retour RTT comme suit:

$$\begin{aligned} R_{UB} &= \frac{BDP_{UB}}{RTT} \\ &= \frac{\sum_{i=0}^n ATT_i}{2 \times ATT_{max}} \times \frac{S}{RTT} \end{aligned} \quad (\text{A.10})$$

R_{UB} est donc le taux maximal d'envoi par lequel le réseau n'est pas surchargé. Les seuils TH_1, TH_2 de MAD et R_{UB} seront utilisés ensemble dans la conception de IMAD-TP afin d'adapter correctement le taux de trafic de l'expéditeur IMAD-TP.

La conception de IMAD-TP

La conception de IMAD-TP suit le même schéma que MAD-TP. Par conséquent, dans ce qui suit, que la conception liée à ATT métrique est expliqué.

À côté de MAD , chaque noeud intermédiaire maintient également la mesure périodique de ATT selon l'équation A.2 dans le chapitre 4. Pour tous les paquets sortants, les mises à jour de noeud le délai des paquets cumulatif de transmission dans un champ

A.5 Contrôle de débit basé sur métrique pour protocole de transport

d'option en-tête IP, appelés $CATT$, en ajoutant sa ATT de la valeur à la valeur existante dans ce domaine. En outre, un autre champ de l'option en-tête IP, appelé $MATT$, est également mis à jour tels que, si la valeur contenue dans $MATT$ est plus petit que du noeud ATT , il sera remplacé par du noeud ATT . Avec cette règle, $MATT$ contiendra la valeur maximum du paquet délai de transmission de tous les liens le long du chemin. Avec cette conception, le paquet IP a besoin de 3 champs d'option dans son en-tête qui sont $CMAD$ pour le cumulatif MAD , $CATT$ pour le cumulatif ATT et $MATT$ pour la valeur maximale du retard de transmission de paquets de tous les liens le long du trajet.

Chaque fois que la réception d'un paquet, IMAD-TP récepteur prend le ATT_{cum} la valeur du champ en-tête IP $CATT$, et le ATT_{max} à partir du champ d'en-tête IP $MATT$. Puis, IMAD-TP récepteur calcule la partie supérieure la plus récente de la bande passante liée à retard produit BDP_{sample} pour le chemin recueillies par ce paquet comme suit:

$$BDP_{sample} = \frac{ATT_{cum}}{2 \times ATT_{max}} \quad (A.11)$$

Le récepteur IMAD-TP tire alors la moyenne limite supérieure de la bande passante-retard de produit en utilisant la fonction EWMA comme suit:

$$BDP_{UB} = \alpha BDP + (1 - \alpha) BDP_{sample} \quad (A.12)$$

α est fixé à 0,8 dans la mise en oeuvre afin d'éviter la grande oscillation de BDP_{UB} . Cette valeur moyenne est calculée comme dans l'équation A.12 pour tous les paquets reçus.

Le estimative actuelle BDP_{UB} , MAD et R_{rcv} sont réinjectés ensemble à l'expéditeur. Pour contenir la BDP_{UB} la valeur, le paquet ACK de MAD-TP est redessiné par exemple un nouveau champ, appelé BDP , est inséré dans l'en-tête ACK.

Dès réception de MAD et BDP valeurs à partir du paquet retour, l'expéditeur IMAD-TP calcule le taux maximal d'envoi R_{UB} par l'équation A.10. Ensuite, le taux d'envoi est mis à jour par la règle suivante:

```

if ( $R_{UB} > R$  &&  $\alpha < TH_1$ )
    increase rate
elseif ( $R_{UB} < R$  &&  $\alpha > TH_2$ )
    decrease rate

```

où R est le taux d'envoi en cours.

IMAD-TP expéditeur diminue le taux d'envoi en utilisant la même règle en MAD-TP, par lequel le taux d'envoi est réduit de 1/8 de son taux actuel après chaque envoi RTT , mais jamais inférieur à un paquet par RTT .

Pour augmenter le taux, IMAD-TP expéditeur demande l'équation suivante:

A. VERSION FRANÇAISE

$$R = \min(R_{UB}, R + N * S/RTT) \quad (\text{A.13})$$

L'équation [A.13](#) assure que le nouveau taux ne dépasse pas le taux de la borne supérieure et une augmentation d'au plus un paquet par RTT . Notez que la vitesse d'envoi est toujours supérieure à un paquet par RTT avec celles-ci augmentent et les règles de baisse.

A.5.1 Résultats des simulations

Pour évaluer la performance de IMAD-TP, nous utilisons le même ensemble de scénarios et de configuration qui ont été utilisés pour MAD-TP. La performance de IMAD-TP est comparée à celle de TFRC, LATP et MAD-TP en termes de performances métriques trois Débit, End-to-End (E2E) Delay et Ratio de perte de paquets (PLR). Pour l'évaluation de l'équité, l'indice de l'équité Jain, les débits d'écoulement maximum et minimum en moyenne sur un certain nombre de simulations et de l'échelle entre les deux valeurs seront utilisées.

Dans ce résumé, nous ne considérons que la topologie de la chaîne avec la variation du nombre de sauts. Pour les résultats complets, s'il vous plaît voir le chapitre [6](#).

La performance de IMAD-TP dans le scénario 1 sont montré dans la figure [A.3](#). Les résultats montrent que IMAD-TP présente une meilleure performance en termes de DPP et retard E2E en comparaison avec les autres protocoles, c.-à-TFRC, LATP et MAD-TP. Le PLR de IMAD-TP est comprise entre 0,1% (pour 4 hop chaîne) à 0,25% (pour 7 chaîne hop), tandis que celles de MAD-TP, LATP et TFRC sont respectivement [0,5%, 1%], [0,6%, 1,4%] (tout pour 4 et 7 de la chaîne hop) et [1,7%, 6,7%] (pour 13 et 6 de la chaîne hop). Ces valeurs signifient que le DPP moyenne de IMAD-TP est approximativement égale à 1/4, 1/5 et 1/20 celle de MAD-TP, LATP et TFRC respectivement. IMAD-TP introduit également le retard E2E beaucoup plus faible pour toutes sortes de houblon que les autres protocoles considérés et de l'augmentation de retard E2E reflète adéquatement l'augmentation du nombre de sauts. Bien que MAD-TP a le même comportement avec IMAD-TP, le retard introduit par E2E MAD-TP est plus grande que celle de IMAD-TP. Il ya toujours une différence d'environ 10 ms entre le retard E2E de MAD-TP et IMAD-TP pour toutes sortes de houblon. Un autre point remarquable est que, bien que IMAD-TP présente ??beaucoup plus petit PLR et retard E2E, il garde un peu près le même débit avec celles de MAD-TP et LATP.

Cette prééminence est réalisée par l'estimation de la bande passante exacte et le régime de taux de contrôle efficace de IMAD-TP. L'estimation de largeur de bande correspond exactement la capacité actuelle du réseau, empêche ainsi l'expéditeur IMAD-TP de surcharge du réseau. Le régime de taux proposée pour le contrôle maintient également un taux d'envoi relativement lisse qui tient à son tour le réseau régulier. Par conséquent, IMAD-TP réalise cette performance de haut.

Toutefois, IMAD-TP a toujours ses lacunes. La première le choix des valeurs exactes pour TH_1 et TH_2 . Bien que les valeurs trouvées par le travail de simulation bien dans toutes les expériences, elles ont besoin pour être prouvé, plus précisément, c'est à dire

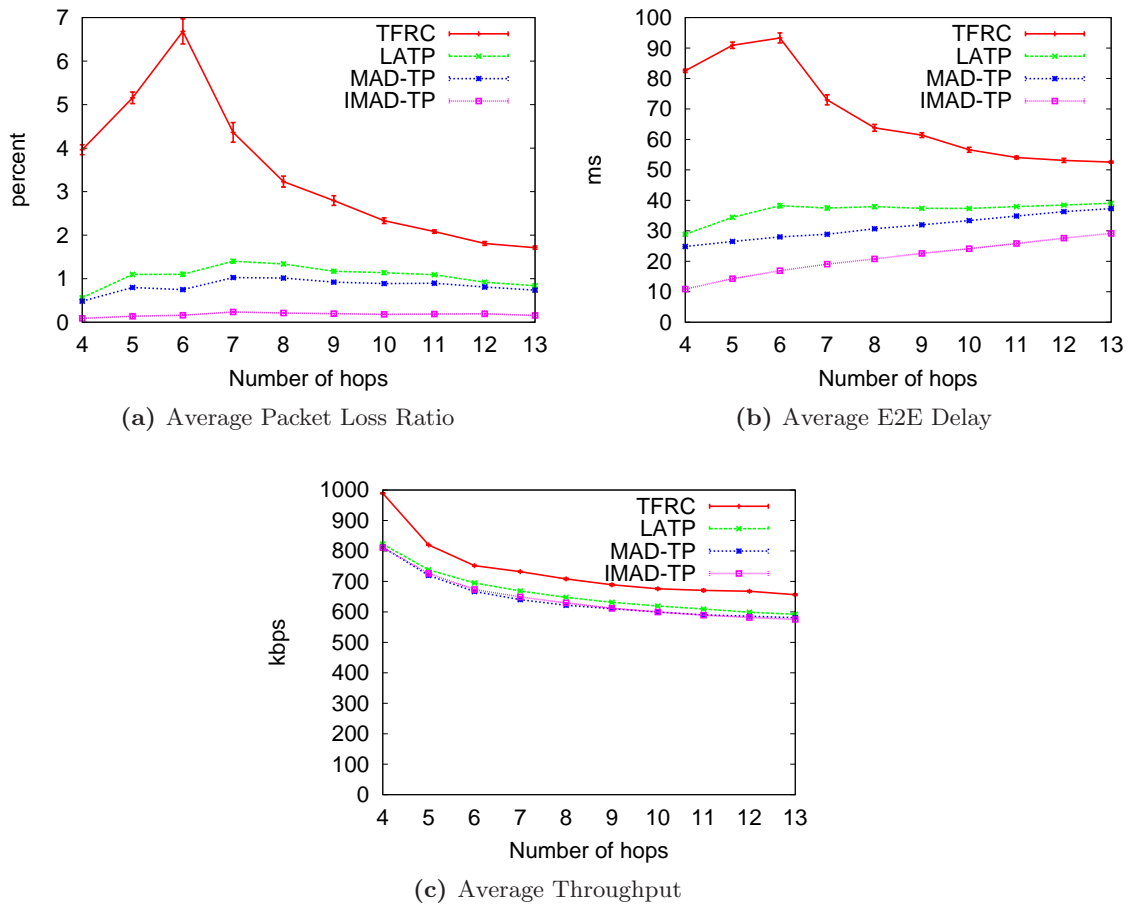


Figure A.3: Chain topology with 1 connection and routing protocol AODV

par le modèle analytique. La seconde est l’hypothèse dans l’estimation de la BDP que la voie à suivre est la même chose avec le chemin de retour. Cette hypothèse n’est pas toujours correcte. Ainsi, cette estimation devrait également être améliorée.

A.6 Conclusion

Cette recherche traite du problème de la dégradation des performances des protocoles de transport dits “rate-based” dans les réseaux sans fil multi-hop. Notre objectif était de développer des systèmes efficaces de contrôle de débit qui permettent aux protocoles de transport dits “rate-based” d’obtenir de faible taux de perte de paquets de faible délai de bout-en-bout sur les MHWNs car ces critères sont essentiels pour les applications streaming temps réel ou non. Notre approche est basée sur la conception cross-layer entre le transport et les couches MAC par lequel, des informations sur l’état du réseau de la couche MAC, appelées métriques, peuvent être fournies à la couche Transport. Afin de clarifier le rôle important des métriques, nous avons présenté d’abord une étude sur les principaux indicateurs des niveaux physique, MAC, réseau et transport et fournit ainsi une classification multi-critères et hiérarchique. Dans cette

A. VERSION FRANÇAISE

classification, les métriques sont d'abord classées en fonction de la couche de protocole à laquelle elles appartiennent puis sont regroupées selon leur utilisation ou par fonction de la couche. Chaque métrique appartient également à une ou plusieurs catégories selon la manière de les obtenir à savoir la disponibilité, l'estimation par mesure et la combinaison. La classification montre que les métriques complexes composées de métriques simples (provenant de couches inférieures) reflètent plus d'une caractéristique du réseau sans fil.

Cette observation entraîne la conclusion que nous pouvons créer de nouvelles métriques multi-usages qui peuvent capturer plusieurs caractéristiques du réseau sans fil en combinant les métriques simples dans différentes méthodes. Après l'étude des métriques existantes, nous avons également introduit de nouvelles métriques MAC et effectué une étude comparative sur leur représentativité. La méthode d'évaluation est basée sur la simulation avec différents scénarios représentant plusieurs facteurs qui peuvent affecter le fonctionnement d'un réseau de type MHWN. Les résultats montrent que le délai moyen d'accès MAD et le temps de transmission moyen ATT sont des métriques intéressantes qui fournissent une information précise sur le niveau de contention et de congestion du réseau. Dans un réseau non-saturé, MAD and ATT son indépendante du numéro de noeud, de sa position et de la charge. De plus, MAD ne dépend de la taille du paquet. Dans un réseau saturé, MAD and ATT fefflètent fidèlement l'état du niveau MAC et révèlent la région c'est à dire les noeuds qui subissent un trafic élevé. Enfin, dans les deux derniers chapitres, deux schémas de contrôle de débit basés sur les métriques MAD et ATT ont été proposés. Dans le premier schéma, appelé MAD-TP, la métrique MAD est calculée à partir de tous les délais de contention accumulés par chaque paquet le long du trajet de la source à la destination. MAD-TP compare ensuite la valeur cumulative de MAD avec un seuil spécifié pour prédire l'état du réseau et ensuite pour réguler le débit d'émission. L'évaluation par simulation montre que MAD-TP surpasse TFRC en termes de délai de bout en bout et de taux de perte de paquets. Le second schéma, appelé IMAD-TP, élimine les inconvénients de la définition d'un seuil pertinent pour MAD en utilisant cette fois le gradient de MAD . La pente abrupte du gradient de MAD détermine si le réseau entre en état de discord grave. Ce schéma utilise aussi ATT pour estimer la bande passante effective le long du chemin de connexion. Ainsi, le débit d'émission est régulé de manière plus efficace et plus précise par la combinaison de ces deux métriques. L'évaluation par simulation a également montré des résultats encore meilleurs pour le fonctionnement du second schéma.

References

- [1] K. WANG, F. YANG, Q. ZHANG, AND Y. XU. **Modeling Path Capacity in Multi-hop IEEE 802.11 Networks for QoS Services**. *IEEE Trans. Wireless Communication*, **6**:738–749, 2007. [vii](#), [viii](#), [26](#), [116](#)
- [2] J. HOEBEKE, I. MOERMAN, B. DHOEDT, AND P. DEMEESTER. **An Overview of Mobile Ad hoc Networks : Applications and Challenges**. *Journal of the Communication Network*, **3**(3):60–66, 2004. [ix](#), [5](#), [6](#)
- [3] **IEEE P802.11sTM/D0.01. Draft amendment to standard IEEE 802.11TM: ESS Mesh Networking**, March 2006. [ix](#), [27](#)
- [4] C. MURTHY AND B. S. MANOJ. *Ad Hoc Wireless Networks: architectures and protocols*, chapter Ad Hoc Wireless Networks. Prentice Hall, 2004. [3](#), [4](#)
- [5] I. F. AKYILDIZ, X. WANG, AND W. WANG. **Wireless mesh networks: a survey**. *Comput. Netw. ISDN Syst.*, **47**:445–487, March 2005. [3](#), [4](#)
- [6] T. BRAUN, A. KASSLER, M. KIHLE, V. RAKOCEVIC, V. SIRIS, AND G. HEIJENK. **Multihop Wireless Networks**. In *Traffic and QoS Management in Wireless Multimedia Networks*, **31** of *Lecture Notes in Electrical Engineering*, pages 201–265. Springer US, 2009. [3](#)
- [7] H. LABIOD. *Wireless Ad hoc and Sensor Networks*, chapter Ad Hoc Networks: Principles and Routing. John Wiley and Sons, 2008. [4](#)
- [8] J. A. FREEBERSYSER AND B. LEINER. **Ad hoc networking**. chapter A DoD perspective on mobile Ad hoc networks, pages 29–51. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001. [4](#)
- [9] C.M. CHLAMTAC AND J.J.-N. LIU. **Mobile ad hoc networking: imperatives and challenges**. *Ad Hoc Networks*, **1**:13–64, 2003. [4](#), [5](#)
- [10] H. HARTENSTEIN. *VANET: Vehicular Applications and Inter-Networking Technologies*, chapter Introduction. John Wiley and Sons, 2010. [4](#)
- [11] I. F. AKYILDIZ, W. SU, Y. SANKARASUBRAMANIAM, AND E. CAYIRCI. **Wireless sensor networks: a survey**. *Computer Networks*, **38**:393–422, 2002. [4](#)
- [12] H. KARL AND A. WILLIG. *Protocols and Architectures for Wireless Sensor Networks*, chapter Introduction. John Wiley and Sons, 2005. [4](#)

REFERENCES

- [13] RADHIKA RANJAN ROY. *Handbook of Mobile Ad Hoc Networks for Mobility Models*, chapter Mobile Ad Hoc Networks. 3, 2011. 5
- [14] L. BAO AND J. J. GARCIA-LUNA-ACEVES. **Topology management in ad hoc networks**. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '03, pages 129–140, 2003. 5
- [15] P. SANTI. **Topology control in wireless ad hoc and sensor networks**. *ACM Comput. Surv.*, **37**(2):164–194, June 2005. 5
- [16] M. GERLA, K. TANG, AND R. BAGRODIA. **TCP Performance in Wireless Multi-hop Networks**. In *WMCSA '99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, Washington, DC, USA, 1999. IEEE Computer Society. 5
- [17] G. HOLLAND AND N. VAIDYA. **Analysis of TCP performance over mobile ad hoc networks**. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '99, pages 219–230, New York, NY, USA, 1999. ACM. 5, 16
- [18] Z. FU, X. MENG, AND S. LU. **How Bad TCP Can Perform In Mobile Ad Hoc Networks**. In *Proceedings of IEEE ISCC 2000*, pages 298–303, 2002. 5
- [19] Z. FU, P. ZERFOS, H. LUO, S. LU, L. ZHANG, AND M. GERLA. **The Impact of Multihop Wireless Channel on TCP Throughput and Loss**. In *INFOCOM 03'*, pages 1744–1753, 2003. 5
- [20] A. HANBALI AND E. ALTMAN. **A Survey of TCP over Ad Hoc Networks**. *IEEE Communications Surveys and Tutorials*, **7**:22–36, 2005. 5
- [21] Z. FU, H. LUO, P. ZERFOS, S. LU, L. ZHANG, AND M. GERLA. **The Impact of Multihop Wireless Channel on TCP Performance**. *IEEE Transactions on Mobile Computing*, **4**:209–221, March 2005. 5
- [22] L. ZHOU AND Z. J. HAAS. **Securing ad hoc networks**. *IEEE Network Magazine*, **13**:24–30, 1999. 5
- [23] H. YANG, H. LUO, F. YE, S. LU, AND L. ZHANG. **Security is mobile ad hoc networks: Challenges and solutions**. *Wireless Communications*, **11**:38–47, 2004. 5
- [24] M. CONTI. *Handbook of Ad Hoc Networks*, chapter Body, personal, and local wireless ad hoc networks. CRC Press, 2003. 5
- [25] M. SCHWARTZ. *Mobile Wireless Communications*, chapter Wireless LANs and Personal-area networks. Cambridge University Press, 2005. 5
- [26] L. NUAYMI. *WiMAX: Technology for Broadband Wireless Access*, chapter Introduction to Broadband Wireless Access. John Wiley and Sons, 2007. 5
- [27] **Bluetooth Special Interest Group (SIG)**. <https://www.bluetooth.org/>. 7

-
- [28] **IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, June 2007. 7, 8, 9, 10, 22, 24, 25, 38, 46, 48, 58, 64, 69
- [29] **Wi-Fi Alliance**. <http://www.wi-fi.org/>. 7
- [30] **IEEE 802.16-2004 IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems**, 2004. 9, 10, 22
- [31] **IEEE 802.16-2009 IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Broadband Wireless Access Systems**, 2009. 9
- [32] J. G. ANDREWS, A. GHOSH, AND R. MUHAMED. *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*, chapter Overview of WiMAX. Prentice Hall, 2007. 9
- [33] **WiMAX Forum**. <http://www.wimaxforum.org/>. 9
- [34] **ITU Radiocommunication Sector (ITU-R)**. <http://www.itu.int/ITU-R/>. 9, 10
- [35] **The 3rd Generation Partnership Project**. <http://www.3gpp.org/>. 10
- [36] S. SESIA, I. TOUFIK, AND M. BAKER. *LTE - The UMTS Long Term Evolution*, chapter Introduction and Background. John Wiley and Sons, 2009. 10
- [37] W. JOHN AND S. TAFVELIN. **Analysis of internet backbone traffic and header anomalies observed**. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, IMC '07, pages 111–116, New York, NY, USA, 2007. ACM. 10
- [38] S. EBRAHIMI-TAGHIZADEH, A. HELMY, AND S. GUPTA. **TCP vs. TCP: a Systematic Study of Adverse Impact of Short-lived TCP Flows on Long-lived TCP Flows**. In *IEEE INFOCOM*, pages 926–937, 2005. 10
- [39] INFORMATION SCIENCES INSTITUTE. **RFC 793 - Transmission Control Protocol**, 1981. 10
- [40] M. ALLMAN, V. PAXSON, AND W. STEVENS. **RFC 2581 - TCP Congestion Control**, 1999. 11
- [41] S. FLOYD AND T. HENDERSON. **RFC 2582 - The NewReno Modification to TCP's Fast Recovery Algorithm**, 1999. 11
- [42] K. RAMAKRISHNAN, S. FLOYD, AND D. BLACK. **RFC 3168 - The addition of explicit congestion notification (ECN) to IP**, 2001. 11, 17
- [43] S. FLOYD, T. HENDERSON, AND A. GURTOV. **RFC 3782 - The NewReno Modification to TCP's Fast Recovery Algorithm**, 2004. 11
- [44] T. HENDERSON, S. FLOYD, AND A. GURTOV. **RFC 6582 - The NewReno Modification to TCP's Fast Recovery Algorithm**, 2012. 11

REFERENCES

- [45] C.-K. TOH. *Ad Hoc Mobile Wireless Networks: Protocols and Systems*, chapter TCP over Ad hoc. Prentice Hall, 2002. 11
- [46] J. POSTEL. **RFC 768 - User Datagram Protocol**, 1980. 11
- [47] S FLOYD, M HANDLEY, J PADHYE, AND J WIDMER. **TCP Friendly Rate Control (TFRC): Protocol Specification**, 2008. RFC 5348. 12, 40, 67, 69, 70, 120
- [48] E. KOHLER, M. HANDLEY, AND S. FLOYD. **RFC 4340 - Datagram Congestion Control Protocol (DCCP)**, 2006. 12, 13
- [49] P. GUPTA AND P. R. KUMAR. **The capacity of wireless networks**. *IEEE Transaction on Information Technology*, 46(2):388–404, 2000. 14, 23
- [50] J. LI, C. BLAKE, DOUGLAS S.J. DE COUTO, H. I. LEE, AND R. MORRIS. **Capacity of Ad Hoc wireless networks**. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, MobiCom '01, pages 61–69, New York, NY, USA, 2001. ACM. 14
- [51] A. KUMAR AND A. KARNIK. *Performance analysis of wireless ad hoc networks*, pages 83–101. CRC Press, Inc., Boca Raton, FL, USA, 2003. 14
- [52] M. GARETTO, P. GIACCONE, AND E. LEONARDI. **On the capacity of ad hoc wireless networks under general node mobility**. In *In Proc. of IEEE INFOCOM*, 2007. 14
- [53] S. XU AND T. N. SAADAWI. **Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks**. *Computer Networks*, 38(4):531–548, 2002. 15, 68
- [54] P NAVARATNAM, H CRUICKSHANK, AND R TAFAZOLLI. **A link adaptive transport protocol for multimedia streaming applications in multi hop wireless networks**. In *MobiMedia '07*, pages 1–6. ICST, 2007. 15, 17, 18, 20, 28, 29, 71, 73, 78
- [55] H. ZHAI, X. CHEN, AND Y. FANG. **Improving Transport Layer Performance in Multihop Ad Hoc Networks by Exploiting MAC Layer Information**. *IEEE Transactions on Wireless Communications*, 6(5):1692–1701, 2007. 15, 17, 18, 20, 28, 60, 68
- [56] H. KHALIFE AND N. MALOUCH. **Interaction Between Hidden Node Collisions and Congestions in Multihop Wireless Ad-hoc Networks**. In *IEEE International Conference on Communications, ICC '06*, 2006. 15
- [57] K. XU, M. GERLA, AND SANG BAE. **How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks**. 1, pages 72–76 vol.1, 2002. 15
- [58] M. GARETTO, J. SHI, AND E. W. KNIGHTLY. **Modeling media access in embedded two-flow topologies of multi-hop wireless networks**. In *In Proceedings of ACM MobiCom '05*, 2005. 15

-
- [59] J. LI, C. BLAKE, DOUGLAS S.J. DE COUTO, H. I. LEE, AND R. MORRIS. **Capacity of Ad Hoc wireless networks.** In *Proceedings of the 7th annual international conference on Mobile computing and networking*, MobiCom '01, pages 61–69, New York, NY, USA, 2001. ACM. 15
- [60] F. WANG AND Y. ZHANG. **Improving TCP performance over mobile ad-hoc networks with out-of-order detection and response.** In *ACM MOBI-HOC 02'*, pages 217–225, 2002. 16
- [61] Z. FU, B. GREENSTEIN, X. MENG, AND S. LU. **Design and Implementation of a TCP-Friendly Transport Protocol for Ad Hoc Wireless Networks.** In *ICNP '02: Proceedings of the 10th IEEE International Conference on Network Protocols*, pages 216–225, Washington, DC, USA, 2002. IEEE Computer Society. 16, 39, 40, 41, 42
- [62] V. T. RAISINGHANI AND S. IYER. **Cross-layer design optimizations in wireless protocol stacks.** *Computer Communications 27 (2004)*, pages 720–724, 2004. 16
- [63] V. SRIVASTAVA AND M. MOTANI. **Cross-layer design: a survey and the road ahead.** *IEEE Communications Magazine*, 43(12):112–119, December 2005. 16
- [64] V. KAWADIA AND P. R. KUMAR. **A cautionary perspective on cross-layer design.** *Wireless Communications, IEEE*, pages 3–11, 2005. 16
- [65] M. CHIANG, S. H. LOW, A. R. CALDERBANK, AND J. C. DOYLE. **Layering as Optimization Decomposition: A Mathematical Theory of Network Architectures.** *Proceedings of the IEEE*, 95(1):255–312, January 2007. 16
- [66] J. LIU AND S. SINGH. **ATCP: TCP for Mobile Ad Hoc Networks.** *IEEE Journal on Selected Areas in Communications*, 19:1300–1315, 2001. 17
- [67] M. LI, C. LEE, E. AGU, M. CLAYPOOL, AND R. KINICKI. **Performance Enhancement of TFRC in Wireless Ad Hoc Networks.** In *In DMS '04: Proceedings of the 10th International Conference on Distributed Multimedia Systems*, 2004. 17, 20
- [68] E. HAMADANI AND V. RAKOCEVIC. **A Cross Layer Solution to Address TCP Intra-flow Performance Degradation in Multihop Ad Hoc Networks.** *Journal of Internet Engineering*, 2:146–156, 2008. 17, 18, 20, 26
- [69] X.M ZHANG, W.B ZHU, AND N LI. **TCP Congestion Window Adaptation Through Contention Detection in Ad Hoc Networks .** *IEEE Transactions on Vehicular Technology*, 59:4578–4588, 2010. 17, 18, 20
- [70] H. ZHAI, X. CHEN, STUDENT MEMBER, Y. FANG, AND SENIOR MEMBER. **How Well Can the IEEE 802.11 Wireless LAN Support Quality of Service?** *IEEE Transaction on Wireless Communications*, 4:3084–3094, 2005. 18, 27, 28, 29, 46, 60

REFERENCES

- [71] L. MA, J. ZHANG, AND K. LIU. **Contention-based Congestion Control in Wireless Ad hoc Networks**. In *Information Networking and Automation (ICINA), 2010 International Conference on*, Oct 2010. [19](#), [20](#)
- [72] Y. YANG, J. WANG, AND R. KRAVETS. **Designing routing metrics for mesh networks**. *Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh)*. IEEE Press, 2005. [21](#), [30](#), [31](#), [32](#), [34](#), [35](#)
- [73] R. BAUMANN, S. HEIMLICHER, STRASSER AND M., AND A. WEIBEL. **A Survey on Routing Metrics**. TIK Report, Computer Engineering and Networks Laboratory ETH-Zentrum, Switzerland, February 2007. [21](#), [31](#)
- [74] G. PARISSIDIS, M. KARALIOPOULOS, R. BAUMANN, AND T. SPYROPOULOS. *Guide to Wireless Mesh Networks*, chapter Routing Metrics for Wireless Mesh Networks. Springer-Verlag London, 2009. [21](#), [31](#)
- [75] D POULIN, P PIGGIN, R YANIV, AND D ANDELMAN. **Correction to Rx SNR, Rx Sensitivity, and Tx Relative Constellation Error for OFDM and OFDMA Systems**, 2005. document number IEEE C802.16maint-05/112r8. [23](#)
- [76] A. P. SUBRAMANIAN, M. M. BUDDHIKOT, AND S. MILLER. **Interference aware routing in multi-radio wireless mesh networks**. In *Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on*, pages 55–63, 2006. [23](#), [32](#), [35](#), [36](#)
- [77] S. LOHIER, Y. GHAMRI-DOUDANE, AND G. PUJOLLE. **Cross-Layer Loss Differentiation Algorithms to Improve TCP Performance in WLANs**. *Telecommunication Systems*, pages 297–309, 2007. [23](#), [25](#)
- [78] R. S. CHENG AND H. T. LIN. **A Cross-layer Design for TCP End-to-end Performance Improvement in Multi-hop Wireless Networks**. *Computer Communications*, **31**(14):3145–3152, 2008. [25](#)
- [79] S. ZHAO, Z. WU, A. ACHARYA, AND D. RAYCHAUDHURI. **PARMA: A PHY/MAC Aware Routing Metric for Ad-Hoc Wireless Networks with Multi-Rate Radios**. *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 286–292, 2005. [25](#), [26](#), [35](#)
- [80] H. ZHAI, X. CHEN, AND Y. FANG. **Rate-Based Transport Control for Mobile Ad Hoc Networks**. In *Proceedings of IEEE WCNC'05*, pages 2264–2269, 2005. [28](#)
- [81] DOUGLAS S. J. DE COUTO, D. AGUAYO, J. BICKET, AND R. MORRIS. **A high-throughput path metric for multi-hop wireless routing**. In *Proceedings of the 9th annual International Conference on Mobile computing and networking*, pages 134–146, 2003. [31](#)
- [82] R. DRAVES, J. PADHYE, AND B. ZILL. **Routing in multi-radio, multi-hop wireless mesh networks**. In *Proceedings of the 10th annual International Conference on Mobile computing and networking*, pages 114–128, 2004. [31](#), [32](#), [34](#)

-
- [83] Y. YANG, J. WANG, AND R. KRAVETS. **Interference-aware Load Balancing for Multihop Wireless Networks**. Technical report, University of Illinois at Urbana-Champaign, 2005. 32, 33, 34, 35
- [84] A. N. LE, D. W. KUM, Y. Z. CHO, AND I. S. LEE. **LARM: A Load-Aware Routing Metric for multi-radio Wireless Mesh Networks**. In *International Conference on Advanced Technologies for Communications, ATC 2008*, pages 166–169, January 2009. 32, 33, 36
- [85] L. ONG AND J. YOAKUM. **RFC 3286 - An Introduction to the Stream Control Transmission Protocol (SCTP)**, 2002. 36
- [86] R. STEWART, I. ARIAS-RODRIGUEZ, K. POON, A. CARO, AND M. TUEXEN. **RFC 4460 - Stream Control Transmission Protocol (SCTP) Specification: Errata and Issues**, 2006. 36
- [87] K CHEN, Y XUE, S SHAH, AND K NAHRSTEDT. **Understanding Bandwidth-Delay Product in Mobile Ad Hoc Networks**. *Computer Communications*, 27:923–934, 2003. 38, 39, 92, 124
- [88] K. CAIHONG, Y. NENGHAI, AND C. YUZHONG. **An enhancement scheme of TCP protocol in mobile Ad hoc networks: MME-TCP**. *Journal of Electronics (China)*, 2007. 39, 42
- [89] S. CEN, P. C. COSMAN, AND G. M. VOELKER. **End-to-end differentiation of congestion and wireless losses**. *IEEE/ACM Trans. Netw.*, 11(5):703–717, 2003. 40, 41
- [90] K. NAHM, A. HELMY, AND J. C. KUO. **On Interaction between MAC and Transport Layers for Multimedia Streaming in 802.11 Ad hoc Networks**. In *in Proc. SPIE ITCOM 2004*, 2004. 46, 49, 67
- [91] G. HWANG. **Analysis of Medium Access Delay and Packet Overflow Probability in IEEE 802.11 Networks**. In *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, 4712, pages 419–430. 2007. 48
- [92] **The Network Simulator - NS-2**. <http://isi.edu/nsnam/ns/>. 50
- [93] E. WEINGÄRTNER, H. VOM LEHN, AND K. WEHRLE. **A performance comparison of recent network simulators**. In *Proceedings of the 2009 IEEE international conference on Communications, ICC'09*, pages 1287–1291, Piscataway, NJ, USA, 2009. IEEE Press. 50
- [94] D. ORFANUS, J. LESSMANN, P. JANACIK, AND L. LACHEV. **Performance of wireless network simulators: a case study**. In *Proceedings of the 3rd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, PM2HW2N '08*, pages 59–66, New York, NY, USA, 2008. ACM. 50
- [95] S. MEHTA, N. ULLAH, M. H. KABIR, M. N. SULTANA, AND K. S. KWAK. **A Case Study of Networks Simulation Tools for Wireless Networks**. In *Proceedings of the 2009 Third Asia International Conference on Modelling*

REFERENCES

- Et Simulation*, pages 661–666, Washington, DC, USA, 2009. IEEE Computer Society. 50
- [96] Q. CHEN, F. SCHMIDT-EISENLOHR, D. JIANG, M. TORRENT-MORENO, L. DELGROSSI, AND H. HARTENSTEIN. **Overhaul of iee 802.11 modeling and simulation in ns-2**. In *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, MSWiM '07, pages 159–168, New York, NY, USA, 2007. ACM. 50
- [97] Z. LI, S. NANDI, AND A. K. GUPTA. **Modeling the short-term unfairness of IEEE 802.11 in presence of hidden terminals**. *Perform. Eval.*, **63**(4):441–462, May 2006. 59
- [98] A. DUDA. **Understanding the Performance of 802.11 Networks**. In *Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008, France*. IEEE, Sept 2008. 59
- [99] K. CHEN AND K. NAHRSTEDT. **Limitations of Equation-Based Congestion Control in Mobile Ad Hoc Networks**. In *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW'04) - Volume 7*, ICDCSW '04, pages 756–761, Washington, DC, USA, 2004. IEEE Computer Society. 67, 77
- [100] R. K. JAIN, D. W. CHIU, AND W. R. HAWE. **A Quantitative Measure Of Fairness And Discrimination For Resource Allocation In Shared Computer Systems**. Technical report, Digital Equipment Corporation, September 1984. 73
- [101] **Optimized Link State Routing protocol**. <http://www.olsr.org/>. 108