A study of IP network mobility in a multihomed context

Pratibha Mitharwal

UNIVERSITE
BRETAGNE
LOIRE

THÈSE / Télécom Bretagne
sous le sceau de l'Université Bretagne Loire
pour obtenir le grade de Docteur de Télécom Bretagne
En accréditation conjointe avec l'Ecole Doctorale Matisse
Mention : Informatique

présentée par
Pratibha MITHARWAL
préparée dans le département Informatique
Laboratoire Irisa

A study of IP Network Mobility in a Multihomed Context

Thèse soutenue le 19 septembre 2016
Devant le jury composé de :

Véronique Veque
Professeure, Université de Paris-Sud (Paris 11) / présidente

Stefano Secci
Maître de conférences (HDR), Université Pierre et Marie Curie / rapporteur

Yacine Ghamri-Doudane
Professeur, Université de La Rochelle / rapporteur

Jean-Louis Rougier,
Professeur, Telecom ParisTech / examinateur

Tijani Chahed
Professeur, Telecom SudParis, / examinateur

Christophe Lohr
Maître de conférences, Télécom Bretagne / examinateur

Annie Gravey
Directrice d'études, Télécom Bretagne /Directrice de thèse

N° d'ordre: 2016telb0407

Sous le sceau de l'Université Bretagne Loire

Télécom Bretagne

Ecole Doctorale - MATISSE

A study of IP network mobility in a multihomed context

Thèse de Doctorat

Mention : Informatique

Présentée par **Pratibha MITHARWAL**

Département : Informatique

Laboratoire : IRISA

Directeur de thèse : Prof. Annie GRAVEY

Soutenance le 19 Septembre 2016

Jury :

Rapporteurs	
M. Stefano SECCI	Professeur, Université Pierre et Marie CURIE
M. Yacine GHAMRI-DOUDANE	Professeur, Université de La Rochelle
Examinateurs	
Mme. Annie GRAVEY	Professeur, Télécom Bretagne (Directeur de thèse)
M. Christophe LOHR	Professeur, Télécom Bretagne (Encadrant de thèse)
Mme. Veronique VEQUE	Professeur, University of Paris Sud (Paris 11), Orsay
M. Jean-Louis ROUGIER	Professeur, Telecom ParisTech

Abstract

This thesis presents a solution for boosting network mobility in the context of vehicular communications and content distribution in fixed network. Existing solutions for vehicular communications (i.e., network mobility), relies on tunneling in order to use multiple available interfaces on a vehicle. Even with tunnels, these solutions are unable to balance the traffic over available network interfaces thus do not reach the goal to provide optimum multi-homing benefits. Moreover, some of the existing solutions for network mobility, hide the mobility from the hosts connected to the mobile router. This in result inhibits the host nodes from participating in multi-homing related decisions such as interface selection which can be helpful in performing least cost routing. In this thesis, we propose to combine network mobility protocol with MPTCP which enables the host nodes to participate in mobility and multi-homing. This novel combination significantly improves routing and tunneling packet overhead. Moreover it increases throughput, fault tolerance, round-trip time and reduces transmission delay.

The second contribution of this work is providing a solution for session continuity in context of content distribution in 5G networks. In 5G network, the IP edges will be closer to the host nodes in order to improve the user experience and reduce traffic load in the core network. The fact that a host can only be connected to a single gateway (SGW/PGW) at a time, would break the ongoing sessions for real time applications like video streaming or gaming during an occurrence of mobility event requiring gateway relocation. The thesis presents the solution for session continuity with the help of multipath TCP by benefiting from the fact that the content servers are stationary.

Acknowledgements

This thesis work has given me an excellent opportunity to have a deeper level understanding of the computer networks. I am grateful to my PhD advisors Prof. Annie Gravey and Prof. Christophe Lohr for all the necessary support and guidance during these years. Their technical knowledge and academic thinking had a profound professional impact on my way of raising right questions and solving problems. I would like to thank my jury members for showing interest in my work.

The experience and the education before beginning my PhD has definitely made this journey a little easier. Therefore, I am thankful to my school teachers, university professors and my mentors at IBM during my professional career. I am also grateful to my colleague Souhier Eido for her support and camaraderie during these years. I also highly appreciate the kindness and friendliness of our departmental secretary Armelle Lannuzel. The stay in France has been more colorful due to my friends, thanks to Jigyasa, Mukesh, Nivedita and Purush.

My parents have always instilled in me the importance of education since childhood. Through, this thesis I want to acknowledge their love and support for all these years. They have always inspired me to endure through the tough times. I am also grateful to my sister and brother whose cheerfulness has always been source of inspiration for me. I cannot express my gratitude in words to my lovable baby son Dhruv whose playtime was unwillingly sacrificed on writing this manuscript. Last but not the least, my husband should be thankful to me for all the support during these years without which even his thesis would have been in jeopardy. On a serious note, his support and willingness to support all my endeavors is highly appreciated.

Contents

List of Figures

List of Tables

Abbreviations

CN	**C**ommunicating **N**ode
CoA	**C**are-of- **A**ddress
EPS	**E**volved **P**acket **S**ystem
EPC	**E**volved **C**ore **N**etwork
HA	**H**ome **A**gent
IP	**I**nternet **P**rotocol
LFN	**L**ocal **F**ixed **N**ode
LGW	**L**ocal **G**ateway
LTE	**L**ong **T**erm **E**volution
MNN	**M**obile **N**etwork **N**ode
MIPv6	**M**obile **IP**v6
MR	**M**obile **R**outer
NS1	**N**etwork **S**cenario 1
NS2	**N**etwork **S**cenario 2
NS0	**N**etwork **S**cenario 0
NS2C	**N**etwork **S**cenario 2 **C**lassical
NS2P	**N**etwork **S**cenario 2 **P**roposed
NS1C	**N**etwork **S**cenario 1 **C**lassical
NS1P	**N**etwork **S**cenario 1 **P**roposed
PGW	**P**acket **D**ata **N**etwork **G**ateway
SGW	**S**erving **G**ateway
UE	**U**ser **E**quipment

To my son Dhruv...

Chapter 1

Introduction

The legacy TCP/IP architecture was designed for the computers that were heavy to move around and had a single network interface. Being stationary made them easy to be identifiable with their one and only IP address. With the evolution of technology, things have drastically changed. Computers (such as laptops, tablets, etc.) can be easily moved around and can be connected to more than one network interface while the Internet architecture is very much the same. This situation is similar when the address becomes identification of a person instead of his name.

Let's consider an example for understanding the challenges faced by a mobile host which are similar to the challenges faced by an individual in the reality when he/she is identified by his/her location. A person/host lives in Street 1 so he/she is known as Mr. Street 1 by the rest of world/Internet. Now, the user moves to a new place, from Street 1 to Street 2. Since the person is identified by the location, he/she will be known as Mr. Street 2. The people such as his/her old neighbors or friends, who used to know him/her as Mr. Street 1 will no more recognize him/her. Therefore, he/she will have to convince people that he/she still is Mr. Street 1 which can be a difficult task. The problem is called the IP address ownership problem. Now, Mr. Street 1 is also known as Mr. Street 5 assuming that his/her house has a back door address also. He/She would like to use this back door whenever there is jam on Street 1. Thus, he/she has to convince other people that he is Mr. Street1. Once again, he/she will have to face the ownership problem.

Mobility and multihoming are closely related to each other regarding IP addressing. Concerning mobility, IP address changes due to changing network attachment point (location) of the host (interface), whereas in multihoming, IP address changes while changing the communication path (the selected network interface)

either for the host or for the network. Since upper layer sockets are bound to IP address, any change in IP address would cause connection disruption.

Mobility and multihoming share one common requirement, i.e., having to carry a given flow over different network interfaces. During mobility, this change in network interface happens due to change in IP address. While in case of multihoming, this change in network interface is caused by path disruption or an attempt to split the connection over all available network interfaces. The simultaneous use of all the available network interfaces can improve throughput, provide load balancing and make the system more resilient. With an increased demand for connectivity, there is an increased demand for bandwidth as well as throughput. Therefore, mobility combined with multihoming can be beneficial in improving mobility, making handover smooth and increasing throughput.

Multihomed mobile hosts (such as smartphones, tablets, etc.) usually use a single link at a given time. The network selection for every data connection on such technologies is based on "the best availability" or "on user choice". These two options do not provide the user with cost effective benefits of multihoming scenario. For example, one link may be free of charge but with a poor connection, while another may provide dedicated services, a managed quality of service and be costly with a specific cost scheme (by volume of data, time of the day, distance, etc.). Similarly, in multihomed mobile networks (e.g., train, ship, airplanes, etc.), there are many users and every user will have different requirements. These user choices (influenced by user & application preferences) and network characteristics (e.g., price, bandwidth, quality, etc.), can be used to select the best available interface. If the interface selection is done appropriately, it can improve the performance of network applications [1].

1.1 Mobility and Multihoming

Mobility refers to a situation where an end-host changes its topological point of attachment to the Internet. Whenever a host moves, its network layer address changes. Thus, in order to continue to communicate, the host must be able to signal the changes in its addresses to its active peers. This signaling must be secure as non-secured signaling can lead to an unauthorized traffic diversion and denial-of-service attacks. If end user hosts are mobile it is considered as "*host mobility*", and if border routers and interconnected edge network hosts are mobile it is considered as "*network mobility*".

Multihoming refers to a situation where an end-point has several parallel paths for communication with rest of the Internet [2]. This situation can be characterized as the host being reachable through several topological paths (with multiple network layer addresses) which are completely independent of each other. When a host is connected to different edge networks it is known as *"host multihoming"*, and when an edge network is interconnected to the core redundantly with multiple connections via multiple borders or via multiple interfaces of a border router it is known as *"site multihoming"*.

Multihoming helps to achieve redundancy and fault tolerance, increase bandwidth, balance the load on the access network and provide traffic engineering by stripping the flows over all existing paths, using user defined rules[3].

1.2 Issues concerning Mobility and Multihoming

The dual role of identifier and locator of IP address becomes the main problem while solving mobility and multihoming. Whenever IP address changes due to the occurrence of a mobility event the location management of the user becomes the first issue. This change in the location would also require the management of handover for an ongoing session. These are explained as follows [4]:

- Location Management: When a mobile node moves from one topological point of attachment to another point of attachment, it needs to have a way to communicate its new address with all the communicating nodes having an active connection. This communication needs to be authentic as this change in address raises the risk of address-spoofing. Therefore, mobility solutions need to have a secure mechanism to manage mobile node's current location.

- Handover Management: When any mobile node (MN) moves in between topological point of attachment two different type of handovers occur. When mobile node changes point of attachment between network technologies for example from UMTS to WLAN, i.e., known as vertical handover. When the mobile node changes point of attachment in the same network, i.e., known as horizontal handover. The occurrence of vertical and horizontal handover requires several authentication and authorization processes. Mobile node needs to get a new IP address at the new location which will break the old connections and create a new connection. There are two ways to perform handover. One way is to break the existing connection first, then

connect with the new interface, i.e., hard handover or break before make. Another way is to connect with the new interface, then disconnect from the previous interface, i.e., soft handover or make before break. Therefore, mobility solutions need to have a mechanism to manage vertical and horizontal handover by performing break before make mechanism to provide seamless transition by minimizing the disconnection time.

- Transparency: The ongoing TCP connection breaks due to the occurrence of a mobility event. Therefore, whenever a mobility event occurs, it should be transparent to the upper layers protocols and applications.

- Applications: During mobility, the connection break would cause the loss of application data. Any solution that supports mobility should support the current applications and services without any need for modification in them.

- Infrastructure Free - A mobility solution that is implemented with requiring minor changes in the network is more desirable than one that requires major or full modification in the network infrastructure. The solution should allow end-users to support mobility either with the help of the end host or with the help of the network.

However, the multihoming would require a different set of issues to deal with legacy Internet architecture such as the management of multiple available data paths and routing, and a mechanism for interface selection, which is explained as follows [4]:

- Multipath Data Transport: Multihoming mechanism needs to deal with the concurrent multipath transfer to provide load balance. As in the current network architecture, connections are established between source and destination IP addresses. If one of these address changes, the netwrok layer connection breaks. Therefore, A multihoming mechanism needs to provide a mechanism to share all the existing interfaces and use any of them to exploit the available bandwidth fully and balancing the load.

- Multihoming and Routing: In classical routing, routers treat all the IP addresses independent from each other, even if the destination is multihomed, routers route packets according to the available destination address. So, the classical routing lacks in exploiting alternate routes existing in a multihomed host.

- Interface Selection: *Interface selection* refers to the selection of source IP address among all existing interfaces for a connection association or indirectly selection of first hop router influenced dynamically by user application preferences. In mobile networks, user's participation can play a major role in interface selection as shown in [5]. Interface selection can be divided into static interface selection and dynamic interface selection. Static interface selection can be managed by putting some filtering rules in the Operating System (OS) whereas the management of dynamic interface selection is a challenge in multihomed mobile networks due to frequent changes of topological location of the interface, changes in application requirement or change in the availability of access. Dynamic network interface selection decisions lie on the various information such as user preferences, application requirements, hardware capacity, available network's characteristics, service provider's constraints, network administrator preferences, etc. [6].

1.3 Context & Requirements

The major work of this thesis related to mobility and multihoming is to propose solutions for specific problems faced by two research projects which are discussed below.

1.3.1 Terminal Marine Stablisé (TMS)

This thesis was done in the framework of TMS project[1], which aims to design a stabilized terminal for marine communication. The ship terminal is based on WiMax 3.5GHz and 2.6GHz LTE (long Term Evolution - 4G) which is adapted to the marine environment (e.g., hardened mechanical, resistance to humidity, salt spray, etc.). This terminal will be associated with an intelligent antenna system for providing the optimized signal by pointing the antenna in the suitable direction. This terminal will facilitate the IP broadband access for the users on various boats in the sea (e.g., fishermen, boaters, coastguard, lifeboat, cruise ships, etc.) and in the port areas. The main objective is to provide Internet access, weather maps, port maps, boats plans (rescue), medical documents, photos/videos, scientific readings, sea observations report, video transmission for crane operators on the port, etc.

[1]The project is supported by the French Government (Direction Générale des Enterprises)

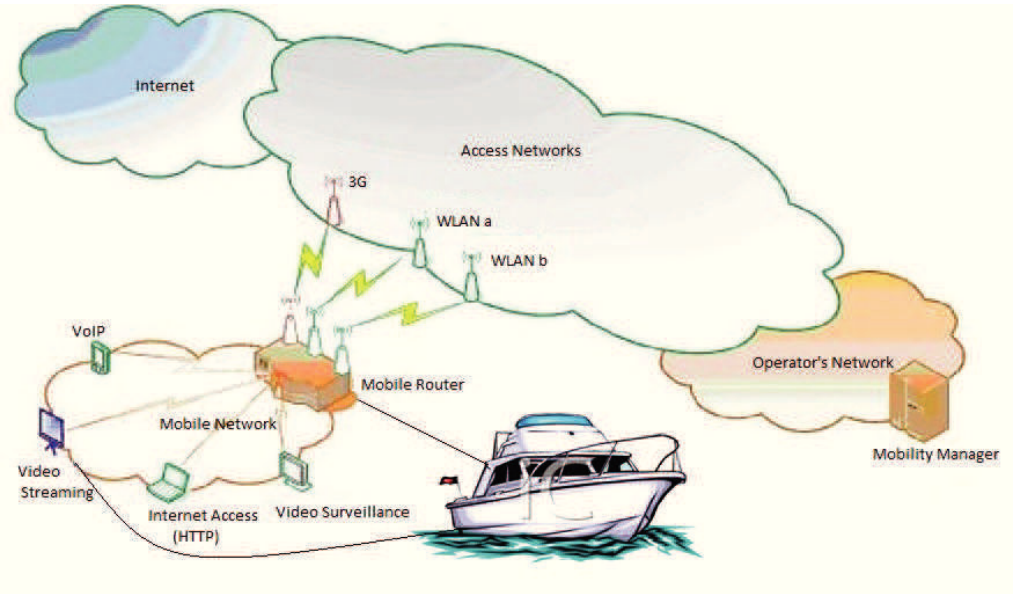

FIGURE 1.1: Network Mobility in context of Ship

All the activities of the TMS project, from study to implementations and validation, are shared among its partners THALES, Alcatel-Lucent (ALU), SATIMO, Déti, Télécom Bretagne and TES electronics. The main tasks of TES Electronic are to realize licenses for WiMax & development costs and validation, certify WiMax marine terminal. Thales Communications deals with the requirement analysis and in the validation of testing. Alcatel-Lucent participates in the implementation and management of an intelligent routing system for multi-ISP providers. SATIMO is responsible for the development of antennas. Déti contributes to the development of low-cost mechanical stabilization system. Télécom Bretagne produces results for measurement & impact analysis of the systems propagation characteristics of the transmission channel and realization of a smart router with Alcatel-Lucent.

The project was completed in January 2015, with the development, implementation and a real-time demonstration of the Stabilized Marine Terminal based on WiMax and LTE frequency bands which would help in providing broadband communications at sea and in port areas at a lower cost with improved technologies.

The main contribution of our work is on the IP routing issues in multihomed mobile networks. On a ship, the entire network infrastructure (networks, subnets, devices, terminals, etc.) is subject to mobility. However, Internet access can be either sporadic or be multi-hosted with multiple connections (satellite, LTE, 3G, WiFi), as shown in Fig. 1.1. An overview of all these requirements is given in Table 1.1.

TABLE 1.1: Requirements of TMS project

$\mathcal{R}1$: Network Mobility	Session Continuity, Security, Handover, Reachability
$\mathcal{R}2$: Network Multihoming	Session Continuity, Security, Handover, Interface Selection

1.3.1.1 Requirement $\mathcal{R}1$: Network Mobility

The first requirement for TMS project is, network mobility management. The network mobility management [7, 8] needs to provide support for handover management to forward the packets towards new location for an ongoing communication imposing minimal disconnection time for reducing unacceptable data loss, reachability to mobile network's new location, support for existing applications and services without any change, transparency to user applications about mobility, minimal infrastructure changes, roaming agreement and authentication process while switching network interfaces between different operators to avoid security concerns, e.g., address stealing, address flooding which causes Denial-of-Service, man-in-middle etc. In TMS project, mobile networks are ship based where network changes do not happen too often, so handover speed is of minor interest.

1.3.1.2 Requirement $\mathcal{R}2$: Multihoming

The second requirement for TMS is multihoming management. The multihoming solutions [9] needs to provide support for interface selection mechanism required when a communication is established (e.g., when a TCP connection is opened for an outgoing & incoming traffic), a secure recovery mechanism for handover management and session continuity to divert ongoing communication from one interface to another in case of failure with minimal delay, a mechanism to handle growth of routing tables in case of aggregated routes, a mechanism to handle change of traffic characteristics, and a mechanism for controlling the load balance (symmetric flow of packets across all existing paths) based on address assignment. In multihoming, the one important issue faced is interface selection which is the key to manage traffic to provide load balancing, or least cost routing, etc.

1.3.2 COnvergence of fixed and Mobile BrOadband access/aggregation networks (COMBO)

The main aim of COMBO project is to investigate and propose new integrated approaches for Fixed Mobile Convergence (FMC) and Fixed–Mobile Network Integration in broadband access and aggregation networks in different scenarios such as urban, dense urban or rural. COMBO targets an optimal and seamless quality of experience for the end user together with an optimized network infrastructure ensuring increased performance, reduced cost and lower energy consumption. The architectures proposed by COMBO are expected to be an integration of optimized fixed and mobile access /aggregation networks, which will be demonstrated experimentally in lab and field test, at the end of the project, to show the feasibility of the proposed architectures.

COMBO project is a European Union project among 17 different partners from various countries which are listed in [10]. The main requirements for realizing the fixed and mobile convergence architecture are identified as follows [11]:

- unified optical access and aggregation network
- Heterogeneous radio networks
- Baseband unit hostelling and mobile fronthaul technologies
- Advanced mobility and offloading

The fixed mobile network integration would provide more efficient control over different network elements, bandwidth gain in the core & metro through mobile data offloading, network resource sharing, etc. FMC has been studied considering different use cases such as simultaneous use of Wi-Fi and mobile networks and seamless switching of traffic in between interfaces (i.e., multihoming), or an integrated caching system for optimizing content distribution, etc. [12]. COMBO introduces the idea of Unified Access Gateway (i.e., a unified gateway for fixed, mobile and Wi-Fi) with Next Generation Point of Presence (NG-POP) for having a better distribution of all essential functions, equipment, and infrastructures of convergent networks.

Our focus of work is related to seamless continuity in the context of content distribution in 5G network. The content servers are distributing the caches closer to the user to accommodate the high traffic. Moreover, in 5G, IP edges will also be put closer to the user. A user can only connect to a single gateway (SGW) at

a time. Therefore, whenever a mobility event occurs, which requires a gateway relocation, the ongoing communication would break. However, some real time application like video streaming or gaming would need the continuity of the session to be preserved.

1.4 Outline of thesis

In this thesis, an evaluation of the existing protocols for mobility and multihoming are presented in Chapter 2 where all possible issues are discussed. Chapter 3 proposes a novel methodology of boosting network mobility with improved multihoming. Chapter 4 presents a quantitative analysis of the proposed methodology compared to the existing approaches. Chapter 5 presents the solution provided for session continuity in the context of content network distribution in 5G network. Chapter 6 presents the conclusion and future perspective.

Chapter 2

An Evaluation of Existing Protocols for Mobility and Multihoming

2.1 Introduction

Evolution in technology has made computers and phones portable anywhere in the world. This portability raises the need to be connected anytime and anywhere which leads to tremendous growth in the numbers of user and data. The growth of users and data result in the evolution of mobile network architecture to support higher bandwidth, speed, and improved QoS. Currently, the devices can be connected to multiple networks at a given point of time, i.e., they are multihomed. With the single devices, networks are also multihomed and mobile. Thus, seamless mobility becomes a new challenge when more and more users and networks (e.g., bus, train, ship, etc.) are mobile and multihomed.

In this chapter, first, we are going to discuss the current mobile network architecture with its mobility management practices in the section 2.2. Section 2.4 presents the existing IP-based solutions for multihomed mobility for host and network in addition to a brief description of the Internet Protocol (IP) address in section 2.3. Section 2.7 presents a qualitative analysis of the existing approaches followed by the conclusion in section 3.4.

2.2 Long-Term Evolution

LTE (Long-Term Evolution, both radio and core network evolution), i.e., 4G is the latest standard for mobile networks that provides high-speed data for mobile phones and data terminals. 3GPP (3rd Generation Partnership Project) has developed and specified this specification in its Release 8 document series. LTE aims to provide reduced latency, higher data rates, scalable bandwidth, all IP network, improved quality of service to the user, reduced costs (CAPEX and OPEX) with an interface that can support a multitude of user types by unifying the fixed wireless and mobility cellular networks [13] [14].

LTE is the latest step in the mobile technology tree from GSM to UMTS to HSPA to LTE (or CDMA to LTE) which may also be referred as Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). It is the access part of the Evolved Packet System (EPS) to fulfill the requirements for the new access network, i.e., high spectral efficiency, high peak data rates, short round-trip time as well as flexibility in frequency and bandwidth[14].

GSM was developed for the real-time services over the circuit switched network with the help of circuit switched modem connection, with a very low data rates. The next phase in the evolution from GSM to GPRS was the first step towards an IP based packet switched solution, using the existing air interface and access methods. GPRS was based on time division multiple access (TDMA) methods, which then evolved into Universal Mobile Terrestrial System (UMTS). UMTS aimed to provide higher data rates by replacing TDMA with the new access technology Wideband Code Division Multiple Access (WCDMA). UMTS allowed packet switch connection for data services in the access network but for real-time services it was still using circuit switched connection.

The latest evolution, i.e., Evolved Packet System (EPS) is purely IP-based and uses IP protocols for both real time and data services. EPS uses the concept of EPS bearers i.e. an IP packet flow with a defined quality of service, to route IP traffic between user equipment (UE) and a gateway in packet data network. The E-UTRAN (access network) and EPC (core network) together set up and release bearers on requirement basis.

Fig. 2.1, shows the overall network architecture, including the network elements and the standardized interfaces. The E-UTRAN or access part of the network is made up of base stations, i.e., evolved NodeB (eNB), which connects to UE. These eNBs are usually interconnected via X2-interface and linked to the core network via S1-interface. There is no centralized intelligence controller in the

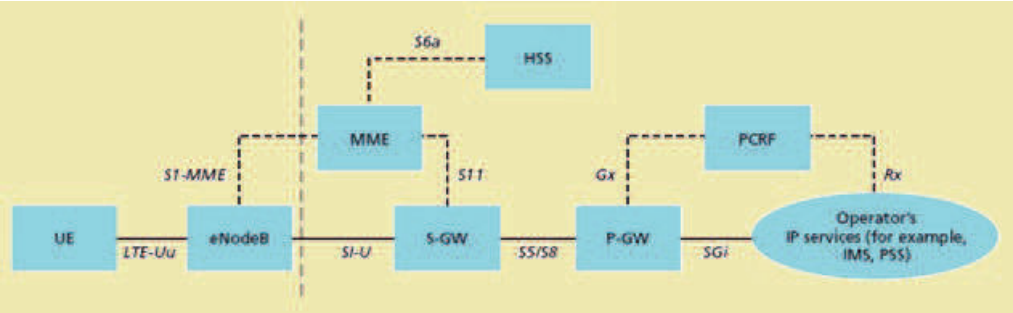

FIGURE 2.1: EPS network elements. (source [15])

LTE access network; eNBs have the knowledge to speed up the connection set up and reduce the time required for handovers. The reason behind it is that an increased handover time may result in dropped calls concerning real-time services. The core network (called EPC) is responsible for overall control of the UE and establishment of bearers. The main logical nodes in the EPC are [15], [16]:

- MME - Mobility Management Entity: MME is the key control node for LTE access network that processes the signaling between the UE and the core. MME is responsible for the tracking, the paging procedure including retransmission, and also for the idle mode of UE. MME is also involved in bearer activation and deactivation procedures. MME also selects the appropriate SGW for the UE during initial attachment or intra-core-network-handover. The protocols running between UE and MME are known as NonAccess Statum (NAS) protocols. Moreover, NAS protocol generates and allocates temporary UE identities (GUTI). "MME is also termination point of ciphering and integrity protection for NAS signaling" [16]. It also provides the control plane function for mobility between LTE and 2G/3G networks by the S3 interface (from SGSN to MME).

- SGW - Serving Gateway: SGW is the gateway which terminates the S1 interface towards access network. UE can be connected to a single SGW in EPS, at given point of time. All user IP packets traverse through the SGW over the user plane, and it is responsible for the handover with neighboring eNB's (S1-based handover). Its tasks also comprise monitoring and maintaining context information related to UE during its idle state and generating paging requests when data arrives for the UE in the downlink direction. (e.g. UE receive a call). SGW is also responsible for interworking with other 3GPP technologies such as general packet radio service and UMTS.

- PDN GW - Packet Data Network Gateway (PGW): The PDN gateway is responsible for IP address allocation to the user, as well as QoS enforcement. It is also responsible for the filtering of downlink user IP packets into the different QoS based bearers. It also provides DHCP and DHCPv6 related functions. PGW also acts as an anchor of mobility between 3GPP and non-3GPP technologies.

In, addition to these nodes, core network also includes other logical nodes such as Home Subscriber Server (HSS) and the Policy Control Charging Rules Function (PCRF). PCRF is responsible for policy control decision-making and ensures the QoS authorization is in agreement with user's subscription profile. HSS holds the information about the PDNs to which the user can connect and the information about the identity of MME to which user is currently attached or registered.

All IP packets for a UE are encapsulated in EPC-specific protocols and tunneled between the PGW and the eNBs. The tunneling protocols are specified over the interfaces. A 3GPP-specific tunneling protocol, i.e., GPRS tunneling protocol (GTP) is used over the user plane in EPC interfaces (S1, S5, and S8). In the access area, UE and eNB communicates over Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC) and Medium Access Control (MAC) sub-layers. During handover due to user's mobility in the access network, data protection is the responsibility of PDCP layer while RLS and MAC start new after the handover. The Radio Resource Control (RRC) protocol is the upper layer of PDCP, which is responsible for the establishment of radio bearers and configuring all the lower layers using RRC signaling between eNB and the UE.

2.2.1 Mobility in LTE

LTE supports mobility in both access and the core network. For providing session continuity support, two types of handovers are defined in LTE, inter-MME and intra-MME. During inter-MME handover, UE moves in between the eNBs. These eNBs are connected with different MMEs. Whereas, in intra-MME handover, UE moves in between two eNBs which are attached to the same MME. These handovers can be executed using the X2 interface or S1 interface [17]. X2 interface based handover can only be performed if the source and target eNBs are directly connected with X2 interface. In the absence of X2 interface or due to the failure of an X2 based handover fails an S1 based handover is initiated. These handover procedures can either be initiated by the UE or the network.

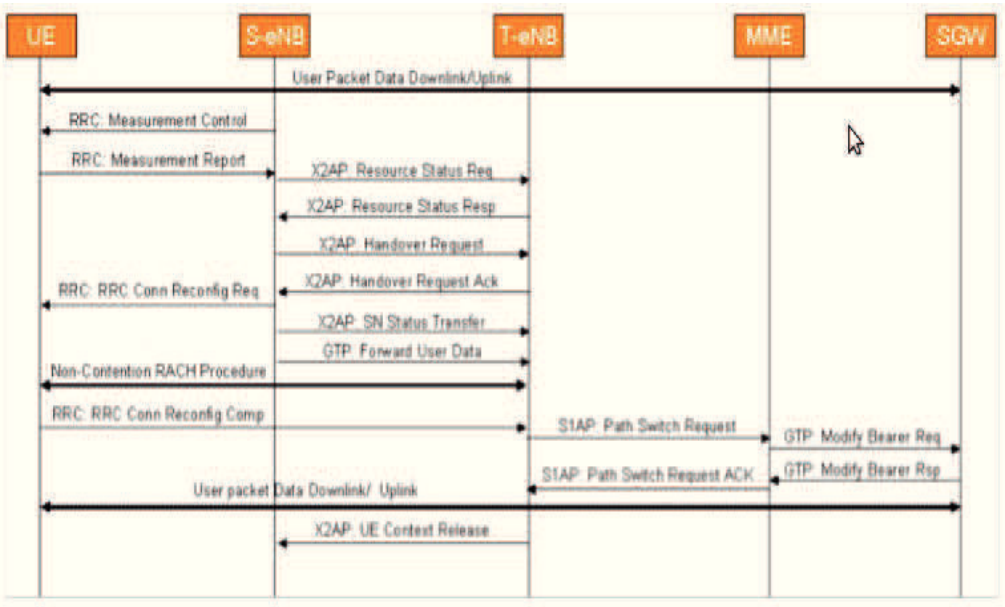

FIGURE 2.2: Intra-LTE (Intra-MME/SGW) Handover Using the X2 Interface (source [17])

Whenever the UE moves in between two cells in the network, it receives a measurement control request from eNB. UE then sends the information to the eNB related to the cell signal quality as a response. Using this reply the eNB decides whether to initiate a handover or not. If the handover needs to be initiated, it issues a resource status request towards the eNB in the target cell and verifies the existence of X2 interface. The source eNB (SeNB) then issues a handover request message to the target eNB (TeNB) with the necessary information such as UE security context etc. On reception of handover request, TeNB reserves the resources for the UE and sends a handover request acknowledgment. A GTP-U tunnel is established between the source and target eNBs. SeNB starts to perform the handover and start forwarding the downlink data towards the TeNB and meanwhile the UE tries to access the TeNB cell. TeNB then sends a path switch request message to MME for informing that UE has changed the cell. On receiving path switch request, MME determines whether SGW can continue to serve UE and sends a modify bearer message to SGW. On reception, SGW establishes the bearer and starts to send the data towards TeNB. Then it also sends an acknowledgment for the modifying bearer to the MME. SGW also sends an end-marker on the old path to the SeNB. On reception of end marker, SeNB can release the resources allocated to the UE. MME then sends the "path switch request acknowledgment message" to the TeNB, to notify the handover completion. These steps have been illustrated in Fig. 2.2.

LTE supports mobility with both 3GPP and non-3GPP access systems, i.e., local

and global mobility respectively. Local mobility can be performed using GPRS tunneling protocol and Mobile IP based protocols [18] [19] (discussed in section 2.5.1.1) however global mobility can only be performed using mobile IP-based solutions.

In LTE, the real-time data traffic for applications such as videos, gaming, etc., is increasing exponentially. For accommodating this growth, network operators are breaking out some part of LTE traffic for offloading the traffic by putting IP edges (SGW&PGWs) closer to the user. This distribution allows a user to offload the IP traffic with the help of Selected IP Traffic Offloading (SIPTO) techniques, as explained in the next subsection.

2.2.2 Traffic Offloading in LTE

In 3GPP Release 9 [20], two traffic offloading concepts are defined for LTE. The first one is Local IP Access (LIPA) and the second one is Selected IP Traffic Offload (SIPTO). LIPA supports traffic offloading by enabling local network access with femtocell deployments. A femtocell is Home eNodeB (HeNB) co-located with the Local gateway (LGW) deployed in user's residential and enterprise area that is directly connected to other IP-capable devices in the local network avoiding the core network.

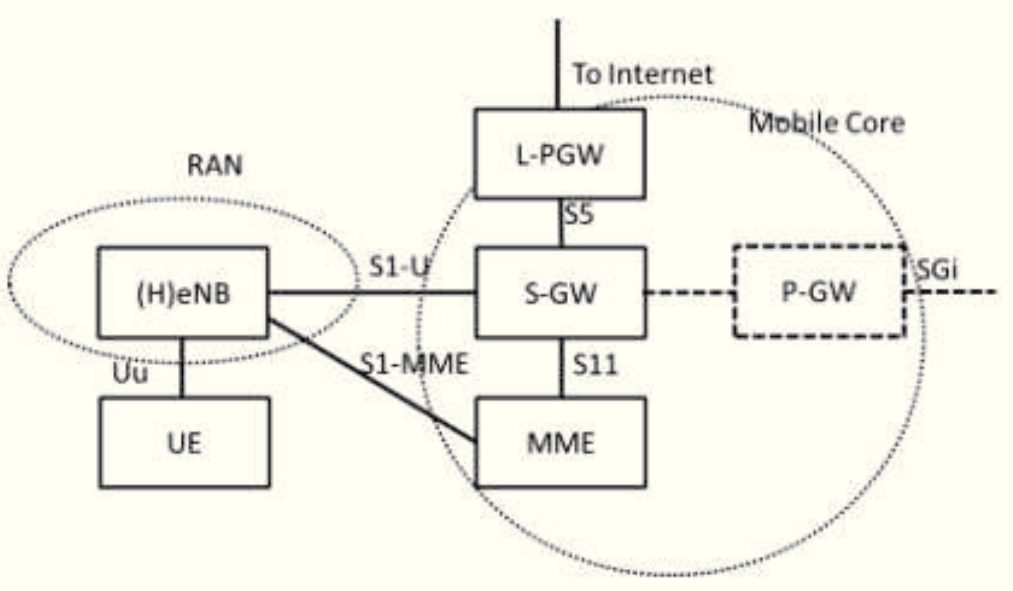

FIGURE 2.3: SIPTO above RAN(source [21])

SIPTO offloads the data by breaking out a part of traffic towards the closer gateways for alleviating the traffic load in the core network. MME is the control

entity that decides whether to offload the traffic or not by looking at the APN's entry in the HSS. In SIPTO above RAN, On the attachment of UE, MME selects a SGW &PGW which is geographically closer to the user. This SGW and PGW can either be co-located or be as a separate entity. The SIPTO above RAN architecture is shown in the Fig. 2.3.

SIPTO has been extended to break out a part of IP traffic in the local network [22]. This proposal enables UE to access the external IP network via LGW. SIPTO offloads the selected IP traffic in the local network contrary to LIPA, which completely avoids the core network. The architecture for LIPA and SIPTO at the local network is similar, as shown in Fig. 2.4.

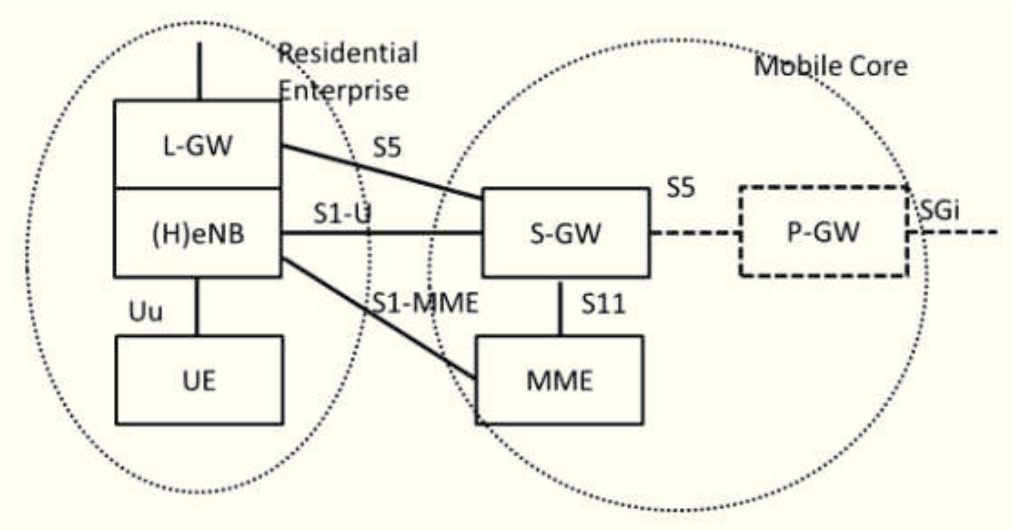

FIGURE 2.4: LIPA, SIPTO@LN with LGW function co-located with the (H)eNB (source [21])

Since 3GPP uses IP address for all communications related to UE, the next section provides a brief overview of Internet Protocol address (IP address).

2.3 Internet Protocol (IP) address

IP address is an attribute assigned to each machine (e.g., computer, mobile, etc.), by which it is identified in the Internet [23]. The IP address serves the role of both network interface identifier and locator for the host in the Internet. Currently, two versions of IP address are in use i.e. IP version 4 and IP version 6, which are discussed in the following subsections.

2.3.1 IPv4

An IP address version 4 is a 32-bit number which uniquely identifies the hosts/equipment in the Internet [24]. These 32 bits has four parts octets, i.e., 8 bits. Each octet ranges from 0 to 255 when converted into decimal. These four octets are separated by dots making a dot-decimal notation for IP address, e.g., 172.25.254.1.

This 32-bit address can further be divided into two parts based on their class. The first part is used to identify the network gateway and the second part is used to identify the hosts which are connected to the given network.

Currently, IPv4 addresses can be assigned using CIDR method, as explained in [25], [26], [27]. In CIDR, IP addresses are organized into subnetworks independent of its values. Using CIDR, each IP address has a network prefix that identifies either one or several network gateways. CIDR notation to represent IP address adds a left most bit value that can be set to one in the mask, into the classful representation, e.g., 172.152.12.0/23. This representation means that the address ranges from 172.152.12.0 to 172.152.13.255. CIDR way of address assignment is a hierarchical way where each domain takes the IP address from its higher level, e.g., ISP.

This new way of address allocation was enough to sustain the growth for a short term but was not a long-term solution.

2.3.2 IPv6

Due to the growth of the Internet and the prediction of depletion of available addresses, the new version of IP, i.e., IPv6, using 128 bit for the address was proposed and standardized in RFC 2460 [28]. Therefore, total no of addresses would be 2^{128}. The IPv6 address also can be divided into network prefix and the host identifier, i.e., MAC address. IPv6 simplifies aspects of address assignment (stateless address autoconfiguration [29]), network renumbering, and router advertisements when changing network connectivity providers [30]. It also provides hierarchical address allocation using CIDR method of address allocation and reduces the size of routing tables. The 128 bits of an IPv6 address consists 8 groups of 16 bits each. Each group is represented as 4 hexadecimal digits and separated by colons (:) e.g., 2001:0db8:0000:0000:0000:ff00:0042:8329.

IPv6 and IPv4 creates a parallel and independent network. The interoperability in the two requires some gateway to translate one into another. This has resulted

into several transition mechanisms like NAT64, or a tunneling protocol like 6to4, 6in4, or Teredo [30].

Compared to IPv4, IPv6 provides a larger address space, facilitates router aggregation by hierarchical address allocation and simplifies the use of multicast addressing.

IPv6 is mainly designed by considering mobility and security aspects. The simplification of address assignment and the separation of the host & the network part makes it beneficial in solving mobility (and/or multihoming) issues that are raised due to the dual role of IP address as identifier and locator. The host part of IPv6 can be used as an identifier, and the network part of IPv6 can be used as a locator. IP-based solutions for mobility and multihoming have been proposed on several layer of the protocol stack which are discussed in the next section.

2.4 IP-based solutions for Mobility and Multihoming

During mobility, the availability of network interfaces and the characteristics of access networks are constantly changing as the system moves. Whenever this happens, one may want to transfer the ongoing communication from one network interface to another interface. Multihoming uses the same scenario to provide the best available connection or to use all available connections.

The need to solve host/network mobility and multi-homing has resulted in many proposals. These proposals for mobility and multi-homing can be classified based on their implementation layers of the network stack. Also, they can be categorized on the solution strategy followed by them, [31] as:

- core/edge separation: These solutions require changes either in the host or the network or both (hybrid).
- locator/identifier separation: These solutions separate the identifier and locator for each user which results into either introducing a new mapping space or using address translation in the existing IP address naming space.

Locator/Identifier Separation (LIS) suggests separating the identity of a node from its location referred as locator such as Host Identity Protocol (HIP), Site Multihoming by IPv6 Intermediation (SHIM6) [32, 33]. The node identity is considered to be unique and independent of the locator. Based on that, the locator is used only for routing purpose, while the unique node identity is used

only for a persistent node identification. This separation requires changes in all end user node's protocol stacks. In the proposed solutions the transport layer sockets are identified with separate node identifiers, not anymore with IP addresses. There is a dynamic relationship or binding between a node identifier and one or more IP addresses or locators. The mapping of this binding can be 1:1 or 1: many. This binding makes it easy to manage mobility and multihoming, and the node identifiers provide secure binding updates due to their cryptographic nature.

Core/edge separation approach enables site multihoming support, simplifies routing and avoids the scalability problem introduced by PI (Provider-Independent) addresses in edge networks [34–36]. Moreover, this approach does not require any change in host stack protocol. However, it requires the usage of an additional mapping system of address spaces of edge networks to locate the border routers of the source & destination edge networks. Moreover, the packets need to be tunneled in between the border routers of the source & destination edge networks. This kind of routing can be supported by specialized border routers that support core/edge separation concept and their deployment at global scale.

There has been some attempts to solve mobility and multihoming with border gateway protocol (BGP) or by using network address translation NAT (network prefix translation in IPv6) [37], [38], [39]. The utilization of provider-aggregatable addresses (globally-unique addresses) with BGP or NAT allows the user to change the upstream ISP due to mobility or multihoming, without readdressing the network nodes in the edge networks. However, it would not consider transport layer survivability and multi-interface selection. Mobile users should be able to choose paths or egress and ingress exits, with the help of service providers, e.g. providing path characteristics. These require a modification of domain name system (DNS).

There are some proposals that extends the DNS towards Dynamis DNS for supporting mobility and multihoming [40], [41], [42], [43]. Dynamic DNS (DDNS) enables a mobile host (and DHCP server etc.) to update its current address in the DNS, in real time, based on some predefined set of rules. There exists three different secure functions in Dynamic DNS, i.e., update (add, delete or modify), notify (notification whenever a zone has changed) and incremental zone transfer (transfer of zone data after a change has occurred in the primary master's zone file) [44], [45]. The mobile host can update the record using "the DNSSEC digital signatures covering requests and data to secure updates and restrict updates to those authorized to perform them as indicated by the updater's possession of

cryptographic keys" [44]. However, the use of Dynamic DNS faces the latency issues during mobility. Moreover, Dynamic DNS offers a break before make solution for mobility which means there is no session continuity.

All the solutions present pros and cons regarding deployment, infrastructure changes, handover delay, throughput, tunneling overhead, transparency to application layers, etc. For mobility and multihoming, whether the mobile host should be modified or the network or both (hybrid) remains an open question. IPv6 addresses make the idea of locator and identifier separation simplifies the mobility and multihoming. Therefore, we will consider the solutions based on IPv6.

In the next section, the functionalities of existing multi-homing mobility protocols are explained followed by an analysis of these solutions according to our project requirements.

2.5 Mobility and Multihoming Approaches

2.5.1 Network Layer Mobility

Network layer mobility solutions can be categorized into two types depending on the area they cover to solve the mobility whether it is inside domain or between different domains. Herein, we are going to discuss the solutions which consider the movement between different domains. Network layers solutions for mobility solution use a level of indirection in routing to support a seamless connection. However, the solution for multihoming mainly use network address translation approach as explained in [37], [38], [39].

2.5.1.1 Mobile IP with Extensions

Mobile IP is a network layer protocol, which enables a mobile host to leave its home network and continue to receive packets at its home address irrespective of its current location. Each mobile host is identified by its home address. A new entity called *home agent* (HA) is introduced, which is a router at a static location in the host's home network for supporting mobility services. HA intercepts the packets destined to mobile host's home address when it is away. The idea was standardized for IPv4 (Mobile IPv4, MIPv4) in RFC 3344 [46] and IPv6 (Mobile IPv6, MIPv6) in RFC 3775 [47].

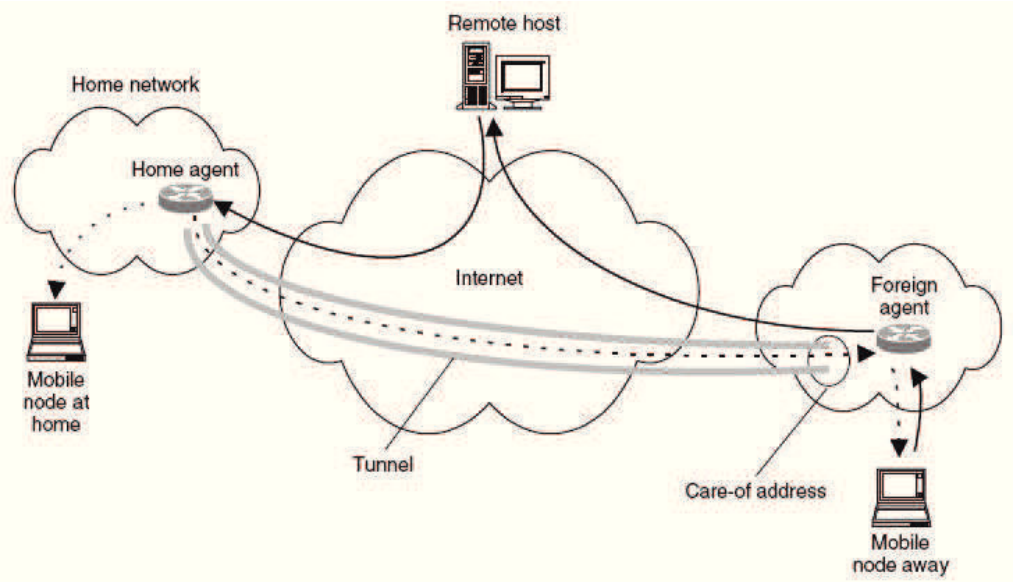

FIGURE 2.5: Mobile IP6. (source [48])

When the host moves from its home network to a visited network, it acquires a new IP address through either stateless or stateful autoconfiguration [29], i.e., care-of address (CoA). The mobile host then informs the home agent of its acquired address. A binding is created between mobile host's home address and the acquired care-of address. Any host communicating with the mobile host is known as a corresponding node (CN). The CN uses the mobile host's permanent home address (belongs to the network associated with HA) as the destination address. Standard IP routing mechanisms forward these packets to the home agent. HA then redirects these packets to care-of-address through the bi-directional tunnel by encapsulating the datagram with a new IP header using the care-of address of the mobile host. Fig. 2.5 tries to illustrate the functionality of Mobile IPv6.

The Mobile IP(v6 & v4) protocol offers transparent movement of a mobile host to transport layer protocols and applications. Moreover, it solves the problem of host mobility and provides a way of hard handover, i.e., break before make. However, the solutions come with some trade-offs such as additional packet tunneling overhead, inefficient routing, less fault tolerant due to the home agent and home network being a single point of failure even the mobile host is attached to some other network. Moreover, to minimize potential issues during handover such as delay, there is a need for communication with upper layers. That is because during mobility a network transition occurs and TCP's round-trip time and the congestion window estimates may be invalid after the transition and need to be reset.

Moreover, to minimize potential issues during handover might need communication with upper layers when mobility is taking place, and a network transition occurs as TCP's round-trip time, and congestion window estimates may be invalid after the transition and need to be reset.

Hierarchical Mobile IPv6 (HMIPv6), an extension of Mobile IPv6, was defined in RFC 5380 [49] as an attempt to improve the performance of Mobile IPv6 mobility management by reducing signaling traffic and by optimizing delays that are introduced by binding updates. HMIPv6 protocol proposes mobility anchor point (MAP) which handles the movement of the mobile node within a defined set of the access router. MAP adds hierarchy in the network by splitting mobility management between home agent which handles inter-domain movements and mobility anchor points which manage local movement. The hierarchy targets to optimize overhead during handover among local domain access routers, reduces signaling control and handover latency as the exchange is between the mobile node and mobility anchor point only.

In HMIPv6, mobile node requires to control both local and global domain signaling and introduces an additional tunnel over the air. Compared to Mobile IPv6, this extension saves some signaling overhead and delay.

There is another extension for fast handover in Mobile IPv6, specified in RFC 5568 [50], to improve handover latency due to Mobile IPv6 procedures which can be beneficial for non-real-time or throughput-sensitive applications. For reducing handover latency, FMIPv6 enables the next access router to generate a care-of-address for the mobile node and to pre-process the return routability procedure as an early binding update, even before the mobile node connects to it. However, this would require a correct prediction about MN's movement. Otherwise, all the prediction-based handover procedures will become useless, and the regular Mobile IPv6 handover will take place after the MN has connected to the new access router. This process involves significant overheads.

Proxy Mobile IPv6 (PMIPv6), specified in RFC 5213 [51], extends MIPv6 signaling and reuses many concepts such as the home agent functionality. It is a network-based mobility management solution which frees the mobile host from participating in any mobility related signaling. The proxy mobile agent in the serving network performs mobility-related signaling on behalf of the mobile host. However, this protocol does not support multihoming.

Mobile IPv6 combined with DDNS (Dynamic DNS) server has been proposed as an attempt to solve these issues [40]. The location updates can be sent with or

without using the home agent. However, this procedure requires lengthy handover processing delays, e.g., the QoS will be degraded for real-time applications. Moreover, all of the extension of Mobile IPv6 inherits all the issues of MobileIPv6 discussed above.

2.5.1.2 Network Mobility Basic Support Protocol (NEMO)

NEMO is also an extension of Mobile IPv6 to support mobility for mobile networks, proposed in RFC 3963 [52], [53]. NEMO provides mobility supports in case of both IPv4 [54] and IPv6. Herein, we discuss the solution for IPv6 only. The mobile network has a router inside which is known as the mobile router (MR) and different kind of nodes such as mobile network nodes (MNNs), visiting mobile node (VMN) and local fixed nodes (LFNs) [55]. Local fixed nodes are unable to change their network point of attachment during an ongoing communication whereas the mobile network nodes have this ability[56]. VFNs are the nodes that do not belong to the mobile network and is also able to change its point of attachment while maintaining the ongoing session.

NEMO enables MR to change its network point of attachment in the Internet and continue to receive packets destined to MNN's home address, keeping the mobility transparent from MNNs. Similar to Mobile IP, this is done with the help of an anchor point inside mobile network's home network, i.e., home agent. Differently from Mobile IP, in NEMO, the home agent is responsible for intercepting packets for all the nodes in the mobile network and MR configures a care-of-address with the prefix of visited network attachment point using the IPv6 address auto-configuration [29], whenever it changes its network attachment point in the Internet. After the address configuration, MR creates a binding between its home address and CoA with HA. When HA receives any packet destined for MNN from a communicating node (CN) in the Internet, it encapsulates the incoming packet with MR's CoA in the destination and HA's address in the source and routes it towards MR over the tunnel. Once MR receives the packet, it decapsulates the packet and routes it inside the mobile network. When MNN receives the packet, it finds its home address in the destination address of the incoming packet. This way the mobility is kept transparent from MNNs. The above explained functionality of NEMO can be shown by Fig. 2.6.

NEMO and Mobile IPv6 has been extended to provide multihoming support by **Multiple care-of addresses registration (MCoA)**. MCoA is an extension for Mobile IPv6 and NEMO that was standardized in RFC 5648 [57]. In Mobile

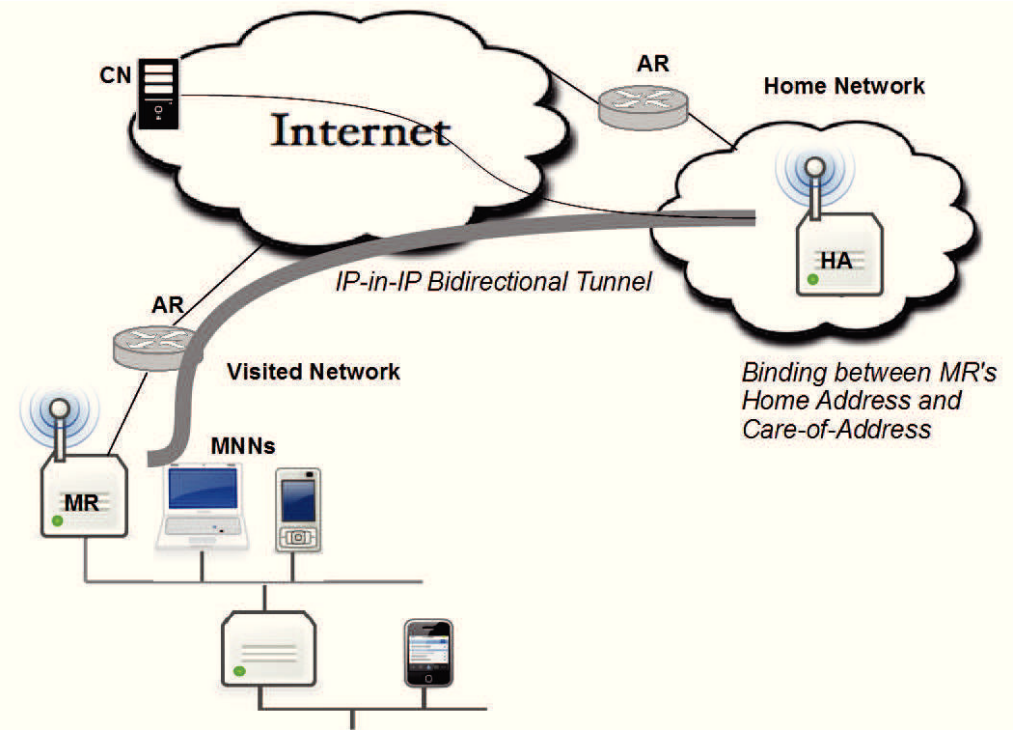

FIGURE 2.6: Network Mobility Basic Support Protocol

IPv6 and NEMO care-of-address is a single point of failure for the whole network, so MCoA mechanism allows multiple care-of-addresses registration with mobile host's or network's home agent. In MCoA, a new binding identification (BID) generated by mobile host/router for each care-of-address, is used as a unique key for distinguishing multiple bindings that are registered by the same mobile host. The home agent caches the received binding identifications in a binding table and is therefore able to distinguish the multiple care-of-addresses of the mobile host/network. The multi-homing support enables the mobile network to have one or more MR, HA, and MNNs thus different combinations which are discussed in [58]. MCoA enables Mobile IPv6 and NEMO to support multihoming, which fulfills requirement $\mathcal{R}2$.

Flow binding is also an extension for Mobile IPv6 and NEMO that was standardized in RFC 6089 [59] which allows hosts to bind one or more flows to a care-of address. These extensions allow multihomed hosts to instruct home agents and other Mobile IPv6 entities to direct inbound flows to specific addresses. In flow binding extension user can define any policies at OS level, but not in real time. It is assumed that the policies are configured on the mobile host's packet filtering tool [60] and the rules specified by the user are according to interface and binding, so the rules are protocol specific [61].

NEMO provides network mobility support and multihoming, which fulfills the requirement $\mathcal{R}1$ and $\mathcal{R}2$ of TMS but it also inherits all the drawbacks of Mobile IPv6. NEMO introduces new entities like the home agent and extends the exit router of the mobile network to work as a mobile router. The location management is easy here without any additional entities but comes with added tunneling packet overhead.

2.5.1.3 Locator Identifier Separation Protocol (LISP)

LISP achieves site-multihoming through core-edge separation and provides end-to-end packet delivery [36, 62, 63]. The idea is standardized in RFC 6830 [36]. It follows three simple principles: address role separation, encapsulation, & mapping. To achieve the first principle, LISP splits the semantics of IP addresses into endpoint identifiers (EID) and routing locators (RLOC). RLOCs are assigned to border routers by ISPs and EIDs are assigned inside edge networks. In LISP, the packets are created with EIDs in source and destination addresses, then these are encapsulated in a UDP segment with LISP header and finally forwarded through tunnels between edge networks. Border routers of the packet source are known as ingress tunnel routers (ITR), which perform encapsulation, and the border routers of the destination site are referred to as egress tunnel routers (ETR), which perform the decapsulation. A mapping system (like DNS) is created for the mappings between EIDs & RLOCs. LISP's tunnel routers can query the mappings for specific EIDs, and the system returns all the related mappings. LISP provides improved traffic engineering capabilities and multihoming (i.e., $\mathcal{R}2$). The functionality of LISP has been illustrated in Fig. 2.7.

LISP mobile host [64] receives an EID from its home network and a different address inside foreign network which can be used as RLOCs. Whenever mobile host moves and its RLOC changes, it registers the new mapping into the map server of its home network. LISP extension for network mobility (i.e., $\mathcal{R}1$) has been proposed in [65]. This locator identifier split can improve Internet scalability, but it has deployment constraints due to its introduction of a new mapping system and different routing methods. Moreover, LISP does not provide any interface selection mechanism considering user preferences. Similar to NEMO, LISP also fulfills both the requirements ($\mathcal{R}1$ and $\mathcal{R}2$) of TMS project but at the cost of making infrastructure changes in the Internet.

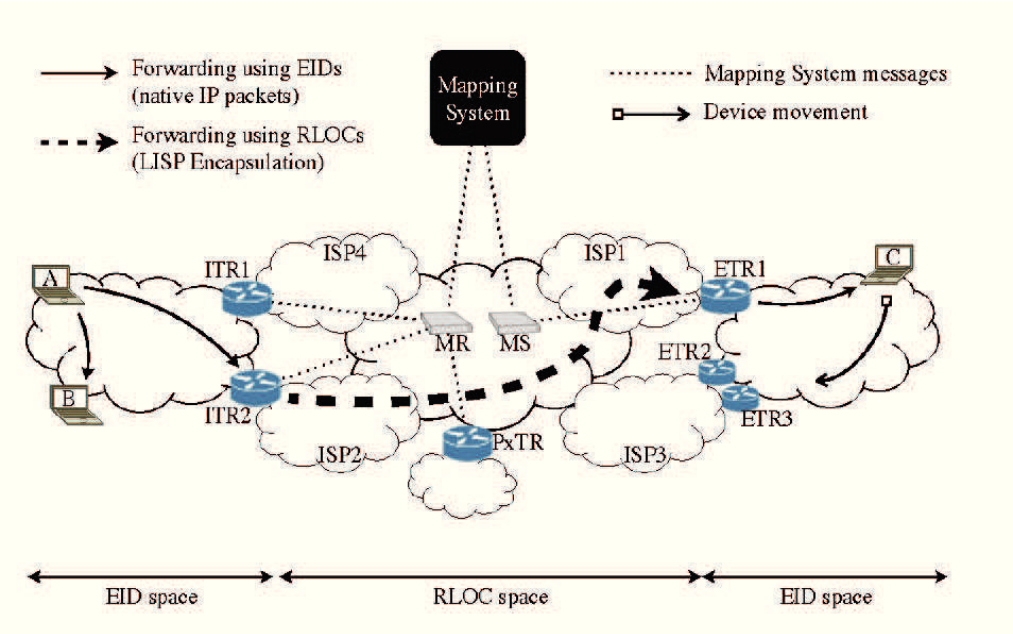

FIGURE 2.7: Locator Identifier Seperation Protocol (source [63])

2.5.2 Transport Layer Approaches

There are some solutions for mobility and multihoming that are introduced in the transport layer. However, most of these solutions are considering multihoming. Host mobility can also be fulfilled in provided with some additions, but network mobility remains unsupported. Some of these solutions, which are standardized by IETF, are discussed in the following subsections.

2.5.2.1 Stream Control Transmission Protocol

Stream Transmission Control Protocol (SCTP) standardized in RFC 4960, is a connection-oriented protocol for the transport layer [66–68], similar to TCP, but it provides message-oriented data transfer, similar to UDP. It provides reliable transmission control, flow and congestion control same as TCP but offers new features such as unordered delivery, multi-streaming and multihoming (fulfills $\mathcal{R}2$). A key difference to TCP is the concept of several streams (sequence of messages) within a connection which are known as associations. An SCTP stream represents a sequence of messages as opposite to a sequence of bytes in TCP. SCTP performs a four-way handshake during connection initiation, unlike TCP's 3-way handshake, as shown in Fig. 2.8 [69]. During association startup (i.e. connection initiation in SCTP), a list of IP address-port pairs is provided between the communicating hosts. These addresses are used as the endpoints of different streams. One of the addresses is selected as the initial primary path, which is

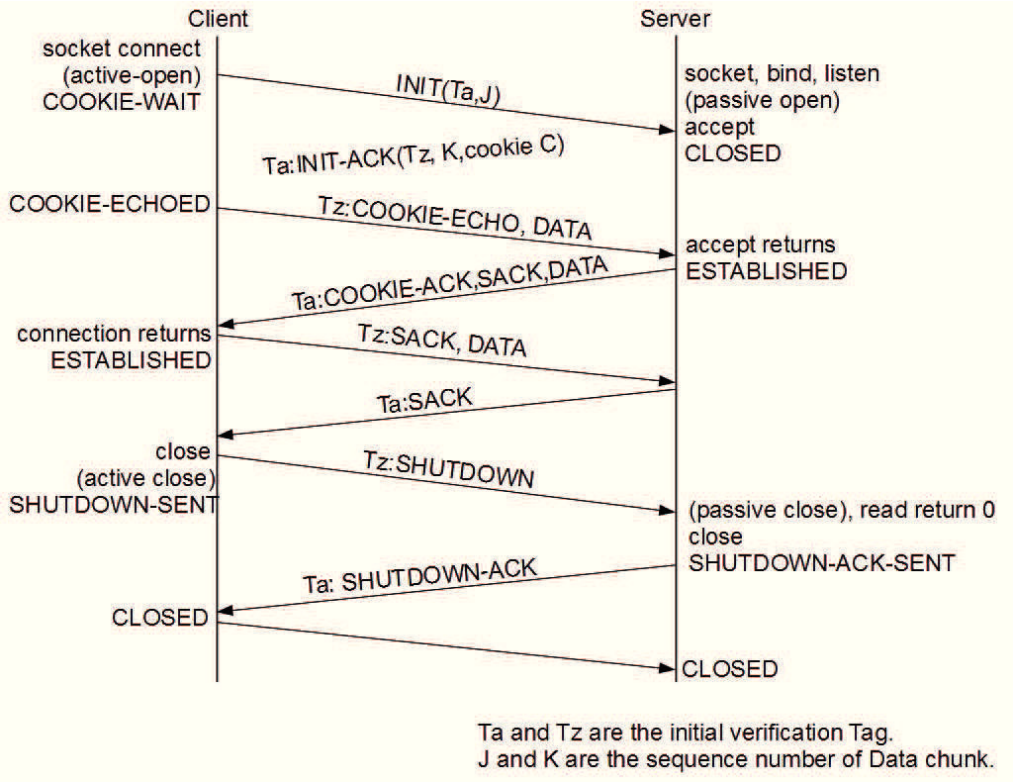

FIGURE 2.8: SCTP Four-way handshake during Association Establishment and Termination (source [70])

used as destination address for all packets and may be changed later if needed. A host has one primary path and zero or more alternative paths. Alternate addresses are used to retransmit packets when any failure occurs on the primary path.

The Dynamic address reconfiguration (ADDIP) [71] extension for SCTP enables this protocol to add, delete, and change the IP addresses during an active connection. The SCTP with the ADDIP extension is called mobile SCTP (mSCTP) and provides a seamless handover for mobile hosts that are roaming between IP networks. The protocol is mainly targeted for client-server services, in which the client initiates the session with a fixed server. For supporting peer-to-peer services, the mSCTP must be used along with an additional location management scheme.

Being a transport layer protocol, SCTP has the advantage of using security services, offered by the network layer but some vulnerabilities still exist to Men-in-the-Middle attacks. Socket API extension for SCTP [72] describes implementing interface selection mechanism but at application level which may not be very efficient. There is another extension of SCTP in order to provide concurrent multipath transfer i.e., CMT-SCTP ([73]).

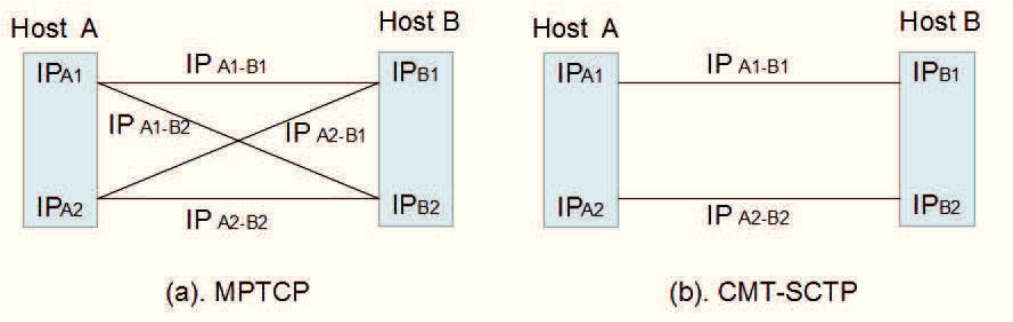

FIGURE 2.9: Path Combination

This solution fulfills only the requirement $\mathcal{R}2$ of TMS project. Moreover, SCTP requires modifications in the application to be compatible and even though it supports concurrent multipath transfer, it lacks to provide full load balancing due to its direct binding in between two IP addresses of communicating hosts. For e.g., if host A has IP_{a1} and IP_{a2} and host B has IP_{b1} and IP_{b2}. Then, in concurrent multipath transfer IP_{a1} can only be bound to either of IP_{b1} and IP_{b2} and similar for IP_{a2}, as shown in Fig. 2.9 [74].

2.5.2.2 Multi-Path Transmission Control Protocol (MPTCP)

MPTCP is an extension of transmission control protocol (TCP) standardized in RFC 6824 [75]. It was originally proposed to provide support for multi-homed hosts. It enables a mobile host to use multiple available interface connections simultaneously as shown in Fig. 2.10, thus allows multi-path streaming. Its target benefit is load balancing. The traffic is distributed over different interfaces of a mobile host, which potentially results in improved throughput. MPTCP is backward compatible to TCP and uses the standard socket API used by most Internet applications, which makes it compatible with existing application and network [76]. The use of multiple paths between source and destination provides reliability, flexibility, fault tolerance and efficiency. In the case of any failure, MPTCP can divert the traffic towards the other active paths. Compared to TCP, MPTCP does not add any overhead to data or tunnels. MPTCP just needs an additional signaling for starting a communication. This signaling is also necessary for adding or removing the subflows due to IP address changes. MPTCP uses "make before break" method which is beneficial in providing seamless mobility and the smooth handover. The Fig. 2.11 shows a mobile host having multiple communication paths with a remote host/server using MPTCP.

MPTCP connection establishment starts as a standard TCP connection with SYN segment included with MPTCP option MP-CAPABLE in the TCP packet

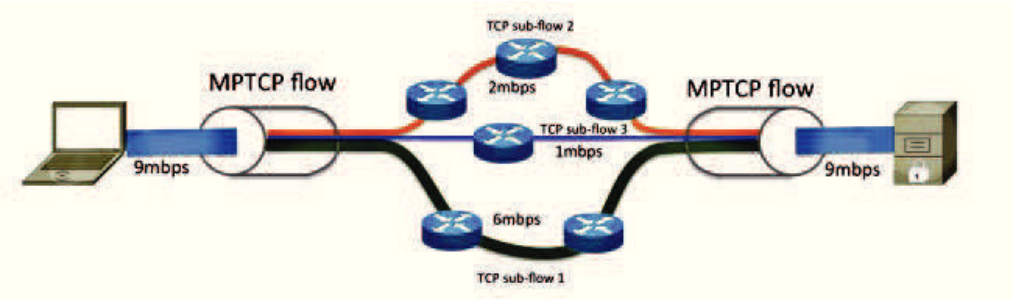

FIGURE 2.10: Multi-Path TCP (source [77])

header as discussed in [75], to know whether the receiving host supports MPTCP or not. If the recipient host or remote host supports MPTCP, it will add the MP-CAPABLE option in SYN-ACK reply. The two hosts also include cryptographic tokens to these packets to identify this connection uniquely. If there are more than one network interfaces available at the start of the connection the additional sub-flows can be added to this MPTCP connection with the final ACK. The subflows in any MPTCP ongoing communication can be added and removed at any point of time with the help of ADD_ADDR option and REMOVE_ADDR option for any interface. These subflows behave as separate regular TCP connections inside the network. These options can be helpful during mobility of a mobile host when it moves from one network to another network, i.e., it receives or configures a new IP address through new network attachment.

Fig. 2.11 demonstrates full mesh created by subflows between two MPTCP enabled nodes each having two active IP addresses. The mobile host (MH) can represent user equipment here, and Remote Host (RH) accounts for any peer node (e.g., content server).

MPTCP provides different handover modes, namely full handover mode, backup mode and single-path mode [76]. In full handover mode, all the subflows are used simultaneously between two communicating hosts. Whereas, in backup mode, MPTCP opens subflows over all the existing interfaces but uses only a subset of subflows for transmission of data packets. MPTCP uses MP-PRIO option to specify any subflow as the backup mode. The subflow which is defined in MP-PRIO option will be utilized only when rest of the other addresses are not working. In the single-path mode, only one TCP subflow is used at any time. If this interface goes down, then another subflow can be created and used for packet forwarding. There is another benefit of MPTCP [78, 79], i.e., its coupled congestion control. Each subflow maintains its congestion window and then performs a slow start. The MPTCP can optimally use the network resources by redirecting the traffic towards the non-congested paths. This feature of MPTCP

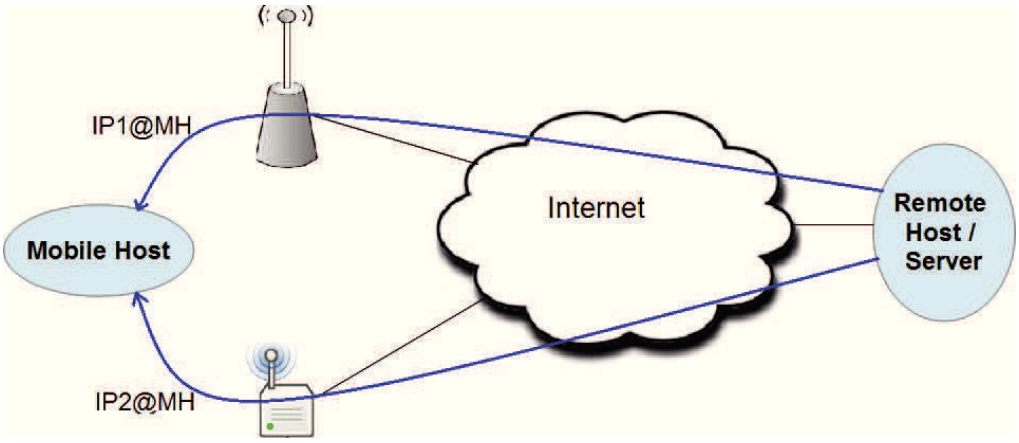

FIGURE 2.11: Multi-Path TCP

can be performed due to its separate congestion windows for each subflow which results in efficient load balancing.

IETF has proposed the use of proxy MPTCP for non-MPTCP compliant clients in [80]. Different deployment scenarios for MPTCP proxy have been discussed in [81] which enables end points to communicate using MPTCP. For a non-MPTCP compliant user, there is a proposal of lightweight proxy MPTCP installation on UE, if the user is comfortable in installing an application that is implemented on packet filter same as IPsec and tunneling. Some filter-based solutions such as IPsec and tunneling are already being used, which makes it easy to deploy MPTCP on the end host. After the installation, UE can be benefited with multi-homing benefits. MPTCP proxies can also be implemented using a global anchor point for non-MPTCP compliant servers in IP edge. When an MPTCP compliant client (e.g., UE) initiates communication with a server using the MPTCP-capable option in SYN packet, the global anchor proxy MPTCP server intercepts the packets and creates a temporary entry consisting of UE IP, Server IP, UE port number and server port number for this connection. Then the proxy forwards this SYN packet to the server. If the server replies with an MP-CAPABLE option in SYN+ACK packet, then the proxy will remove the temporary entry for this connection. Otherwise, the proxy will initiate an MPTCP connection with the UE and sustain the temporary entry to record all the subflows. Proxy MPTCP is transparent to the UE and all the TCP applications on both the hosts. These proxies can also be used for the simultaneous movement of both mobile host and remote host.

MPTCP fulfills only the requirement $\mathcal{R}2$ of TMS project and would require host stack modifications for implementation. Since this solution is backward compatible to TCP, it has got the benefit of exploration further. There has been

developed some work around to install MPTCP on the host stack without the inbuilt support as discussed earlier. Also, this solution provides load balancing to the greater extent and does not require any new name space and compatible to middle-boxes.

2.5.3 New Layer Protocol

There are some approaches which solve mobility and multihoming by introducing a new layer in TCP/IP stack of the host. This new layer will be introduced either in between IP and transport layer or will be added to IP layer. Some of these approaches, which are standardized by IETF, are discussed in the following subsections.

2.5.3.1 Host Identity Protocol

Host identity protocol (HIP) is standardized in RFC 5201 [82–84] has been developed to solve security, mobility, and host multihoming issues in an integrated concept. It separates host identification & location and introduces a new namespace, namely the host identity (HI). The purpose of HI is to support trust between systems, enhance mobility, and significantly reduce the DoS attacks to provide better security than other multihomed mobility solutions. HIP introduces a new host identity layer (layer 3.5) between the IP layer (layer 3) and the upper layers to avoid a dual role of IP address as endpoint and forwarding identifier, as shown in Fig. 2.12. In HIP, upper layer sockets are bound to HI instead of IP addresses. Besides, the binding of these host identities to IP addresses is done dynamically. A significant advantage of this mobility solution is that the hosts can easily have both the IPv4 and the IPv6 addresses. Furthermore, there is no need to change the current routing methods.

Multihoming and avoiding man in the middle (MitM) attacks are the other features offered by HIP. The HIP authenticates the connection and establishes security associations for a secure connection with IPsec ESP. For this purpose, it uses a four-way handshake with the Diffie-Hellman key exchange.

During mobility, HIP protocol is needed to take care of the dynamic binding between the host's IP address and HI as HIs are used to identify the mobile host instead of IP addresses, the location of the host is not bound to the identifier. When one of the communicating peers changes location, it simply sends an HIP readdress (REA) packet through the secured ESP channel. However, if both

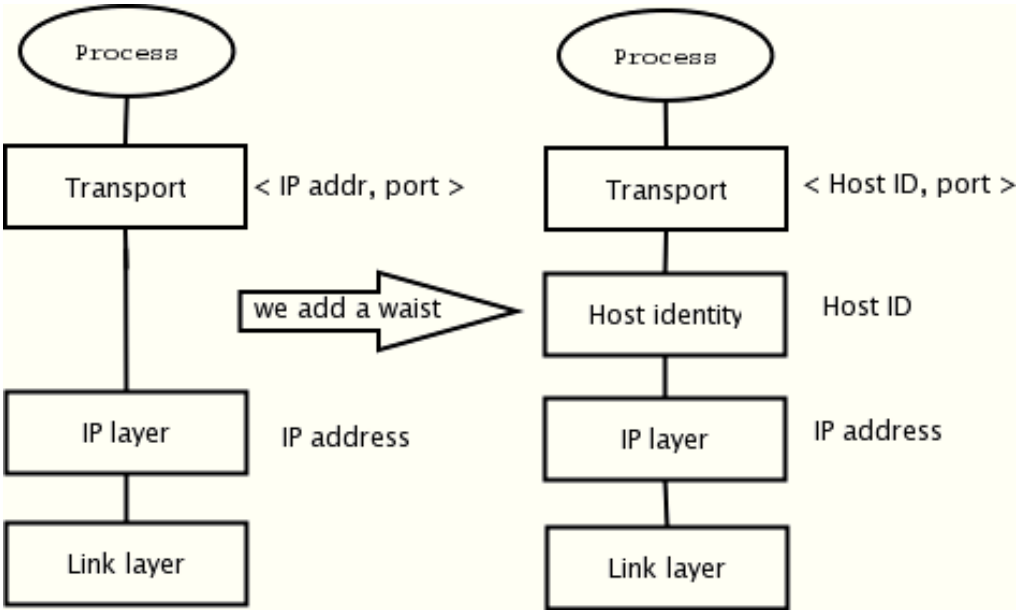

FIGURE 2.12: Host Identity Layer (source [85])

of the peers change the place at the same time (the double jump problem), a rendezvous server (RSV) is needed [86]. RSV is a packet forwarding agent who merely temporarily forwards the initial HIP packet to the responder.

For HIP, an interface selection mechanism is defined in RFC 6136 using application program interface socket [87], which enables participation from applications in interface selection per packet flow basis for both peers. HIP provides a solution for multihoming (fulfills $\mathcal{R}2$), however, implementing this solution would require introducing a new name space for all the hosts and changing host stack. Moreover, there is no way to communicate for an HIP with the legacy host in the Internet which has hampered its popularity in deployment field.

2.5.3.2 Site Multihoming by IPv6 Intermediation (SHIM6)

The SHIM6 protocol is another multihoming host-centric solution, which is standardized in RFC5533 [88–90]. It also introduces a new shim sublayer within the IP layer, as shown in Fig. 2.13. It supposes that each host in the network owns multiple global IPv6 addresses. Each IPv6 address can be used as the *locator* for IP routing and the identifier or ULID (upper layer ID), for upper layer identification. It also maintains a mapping between locators and ULIDs in all active connections between two hosts. In SHIM6 operation, first a standard TCP connection is established between two hosts, then hosts exchange SHIM6 context. At this point, ULIDs and locators have same IPv6 addresses. For failure detection and recovery, SHIM6 uses REAP (REAchability Protocol). In the case of any

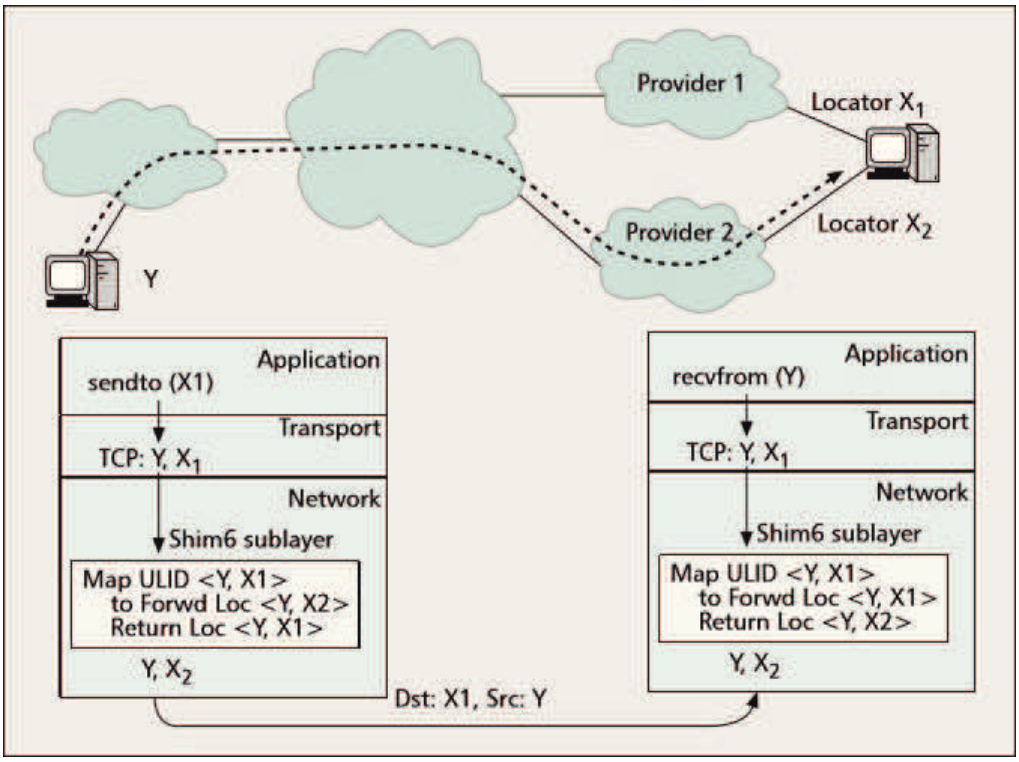

FIGURE 2.13: SHIM6 Operations (source [33])

failure, ULIDs will remain same to the upper layers, but the underlying locators will change, and SHIM6 manages this mapping between locators and ULIDS. Thus, the change of locator is transparent to the upper layers. SHIM6 provides denial-of-service (DoS) attack protection to the responder. However, these security methods are not strong enough to fully avoid the possibility of DoS attacks but to some extent these are useful.

For SHIM6, an interface selection mechanism is defined in RFC 6136 having application program interface socket [87], which provides applications the liberty to choose preferred locators for both source & destination host and allows to perform per-packet flow distribution. Similar to HIP, this solution fulfills only one requirement, i.e., $\mathcal{R}2$, of TMS project and its implementation would require changes in the changes into host stack. The main advantage of SHIM6 over HIP is that it allows the SHIM6 enabled the host to communicate with the legacy host, surely without multihoming benefits.

2.5.4 Application Layer Approaches

There are some solutions for mobility and multihoming that are introduced at the application layer, are discussed in the following subsections.

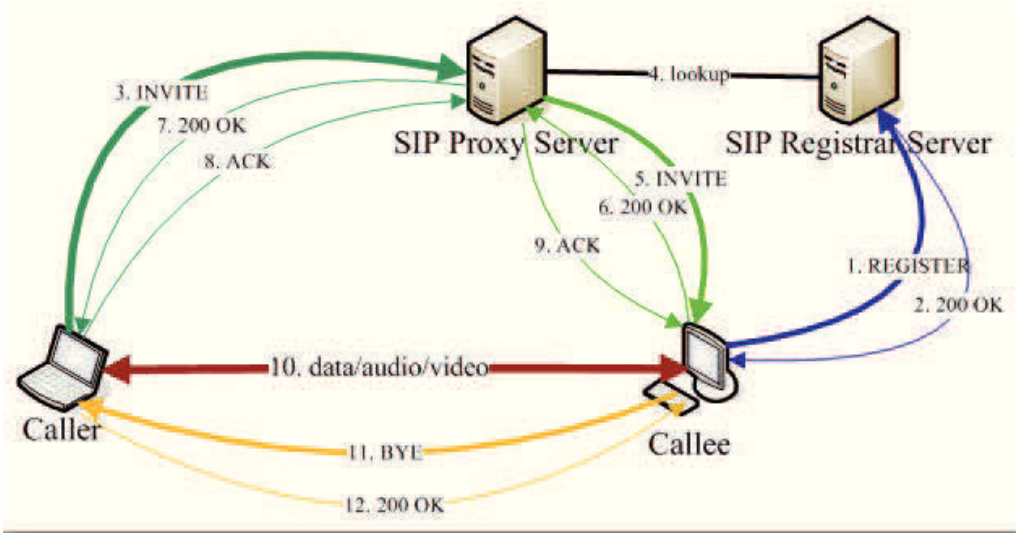

FIGURE 2.14: Session Initiation Protocol (source [69]

2.5.4.1 Session Initiation Protocol (SIP)

Session initiation protocol is standardized by IETF in RFC 3261 [91]. It is an application-layer protocol mainly used for the multimedia applications such as VoIP[92]. In SIP a session is not bound to IP address anymore, it is bound to uniform resource identifier (URI) which does not change during a running session due to mobility. So SIP also follows the idea of decoupling node's identity from IP address at the application layer. SIP architecture is a combination of several entities as user agent clients and servers, which also includes stateless and stateful proxies and registrars. Each SIP capable client device runs user agent and SIP sessions are established and managed by proxy servers. The registrar server is used for URI/IP resolution and cooperates with a location information server. The SIP connection establishment between two peer hosts is illustrated in the Fig. 2.14.

Whenever mobile node moves from one network to another network, it receives a new IP address from the new network. The mobile node then updates this IP address in the registrar, and these updates help to keep a right URI/IP resolution in a session's lifetime. The mapping of URI to IP will be refreshed by binding updates. The SIP user agent sends a Register Request to the registrar server and updates the registered IP address into the location information server wherever the register request will be generated by any new IP address. Whenever mobile node changes its location, its IP address changes but URIs do not so the running session will not be broken.

SIP provide mobility solution which uses IP-address independent identification of end user nodes and enables seamless handoff from the perspective of application layer independent of the network layer.

However, although SIP supports seamless user mobility at the application layer, it does not lead to improving the network behavior on lower layers, especially network layer. Although SIP supports mobility of several multimedia services, it is not compatible with the service mobility for all types of services.

2.6 Comparison Of Mobility-Multihoming Approaches

LTE has inbuilt support for mobility with the help of MME. However, multihoming is still in the research field. LTE uses SCTP protocol to ensure delivery which is mainly a multihoming solution. However, there is no proposal for introducing multihoming in LTE. Mobile IP and its extension can also be used to support mobility in LTE, which makes LTE closer to network layer approaches.

Network layer mobility solutions are based on routing mechanism, so a modification in endpoint and router is required for addressing binding [93]. They need the third device of agents for packet forwarding and location management. The infrastructure changes can be a drawback. While Transport layer mobility solutions are based on the end-to-end model, they require no change in intermediate routers. There is no deployment of the third device, so they need little infrastructure changes. At most, facilities like DHCP and dynamic DNS are required, but since these are already a well-deployed part of the infrastructure, this represents no additional requirement for change.

In Network layer, location management is built in for mobility while seamlessness is only accomplished with a cooperating transport protocol. Transport layer mobility can allow for seamless transitions between networks, by pausing transmissions pro-actively to minimize losses during the handover, and by implementing policies that reset congestion control after reattachment.

Network layer solutions do not yet support multihoming. New layer solution of HIP must define new API for host identity, which requires modification of current applications. Transport layer by itself can not track node, so it is short of location management function. Therefore, this layer approaches are dependent on other layers for location management. After obtaining a new address, the existing binding needs to be updated to the remote host. As routing is handled below transport layer, it must make use of a higher level service. Transport layer needs

to provide a way for dynamic rebinding of connection's IP addresses. The readily available dynamic DNS extension may be employed for this purpose, but it may take quite some time to converge globally to a host's current address, by which time it may be ready to move again. On the other hand, it seems to be easier to include support for concurrent multipath transfer into the session management of transport layer.

Another problem is that if each transport protocol is to implement binding updates, then each one requires an authentication scheme to prevent spoofing. Ensuring the security of each authentication scheme could be tedious and error-prone if they are significantly different between transport protocols. Network layer solutions were thought to be helpful in limiting safety hazard. However, the implemented solutions face security risk as address stealing or address flooding, etc.

Mobility solution at the network layer also involves signaling overhead problem caused by tunneling and extension headers etc. Transport layer solution seems to alleviate the problem because they manage mobility by negotiating and switching connections directly between endpoints.

New layer solutions need modification of endpoint. Also, they employ rendezvous server for location management. Thus, additional entities are required here too. Moreover, the introduction of new protocol layer requires changes in traditional TCP/IP infrastructure, hosts, applications which hamper its acceptability.

There is also an application layer solution for mobility. The advantages of working at the application layer include support of end-to-end mobility, providing means for route optimization and improved performance for real-time services. One drawback of application layer mobility is the delay introduced by the network layer and data-link layer detection of movement, attachment to the new network and obtaining a valid IP address and not all applications can be supported by such solutions.

If the comparison is done based on core/edge separation and locator/identifier separation then, core/edge separation based approaches such as LISP typically improve the scalability of the global routing system through its decoupling of core and edge networks, therefore, the problem of PI (provider-independent) addresses in the edge networks does not affect the global routing system anymore which leads to shorter routing tables and improved routing efficiency. Whereas locator/identifier separation based approaches such as SHIM6 [89] leave scalability mostly unchanged. Every approach that applies locator/identifier separation

TABLE 2.1: Comparison between mobility approaches at various Layers

Layer	Seamless Transitions	Location Management	Infrastructure
Network Layer	Transport layer must deal with losses and path changes	in-built	Deployment of HAs and router support for fast/smooth handovers
Transport Layer	included	requires external manager	little or more
New Layer	included	included	Deployment of rendezvous servers or Dynamic DNS, Changes in Traditional Internet layer
Application Layer	included	requires external manager	Deployment of registrar for path discovery, Home location agent

needs modification at host node network stacks which is the main argument against it.

The main drawback of core/edge separation approach is, new network entities are required and needed to be deployed at global scale to enable full global support. These new network entities will further introduce an additional latency which is another drawback.

Table 2.1 [93] summarizes the comparison of existing solutions based on the implemented layers considering seamless transition, location management and infrastructure changes requirements.

2.7 Qualitative Analysis

For evaluating the capabilities of existing solutions, we consider the two requirements of TMS projects with their sub requirements as follows.

- Mobility Support: We are considering host mobility and network mobility are separate. Network mobility is supported only by NEMO and LISP, but host mobility is supported mostly by all approaches. For some approaches mobility is supported as a special case of multihoming such as SCTP and

TABLE 2.2: Summary of multihomed mobility approaches

	Requirements		Features			
Approaches	Network Mobility $\mathcal{R}1$	Multihoming $\mathcal{R}2$	Modification at Host Network Stack	Transparency to Application Layer	Additional or modified network entities	Tunneling
MIPv6 + Ext	No	Yes	Yes	Yes	HA	Yes
NEMO	Yes	Yes	No	Yes	HA & MR	Yes
LISP	Yes	Yes	No	Yes	Border routers, Mapping System	Yes
HIP	No	Yes	Yes	Yes	PKI, rendez-vous mechanism	No
SHIM6	No	Yes	Yes	Yes	NA	NA
SCTP	No	Yes	Yes	No	NA	NA
MPTCP	No	Yes	Yes	Yes	NA	NA
SIP	No	No	No	No	proxy, registrar server	NA

MPTCP. Simultaneous mobility is not handled by some approaches such as SHIM6 or HIP (without rendezvous server), especially if there is no intermediate entity for managing the location updates for both the peers. LTE also support mobility but only for a UE, i.e., host mobility not for the whole network.

- Multihoming Support: Host multihoming and site multihoming are considered separately. Network layer approaches support site multihoming, and there is an apparent correlation to strategies that apply core/edge separation architecture. A similar correlation can be found when considering locator/identifier separation and host multihoming, network and transport layer approaches both comes under this. Host multihoming approaches at network and transport layer have their advantages and disadvantages. For example, network layer approaches may have the capability to explore the path diversity, where this is not possible for transport layer approaches as available paths are transparent in the transparent layer. On the other hand, it seems to be easier to include support for concurrent multipath transfer into the session management of transport layer. Table 2 shows that none of the investigated network layer approaches are capable of enabling concurrent multipath transfer, whereas SCTP with extension CMC-SCTP and MPTCP are capable of supporting concurrent multipath transfer at the transport layer.

An overview of the features of the discussed mobility and multihoming approaches is provided in Table. 2.2. The feature "Modifications at host network stack" shows if a modification of the network stack at the host is necessary to apply the new approach. If the approach requires some modification then this can introduce

some additional expenditures. Hosts with legacy network stacks will not be able to communicate with the hosts with modified network stacks except for SHIM6 and MPTCP.

The feature "Transparency to application layer" shows whether applications need modifications to enable the interaction with the proposed approaches, e.g. by adjusting sockets or by creating new interfaces. If so, this would require every application to be amended accordingly, which may not be acceptable widely easily. There are only a few approaches which are not transparent to the application layer such as SIP and SCTP. In the case of SCTP, new sockets need to be applied while SIP requires the support from the applications. MPTCP is backward compatible with legacy applications. However, to use the benefits of MPTCP, applications must be MPTCP aware.

The next feature "Additional or modified network entities" shows if other network entities are needed for protocol operation such as modified border routers and mapping systems. The introduction of new network entities would raise a cost of deployment, operational and maintenance expenditures for network operators. This additional expense is one of the main drawbacks of core/edge separation approaches because each core/edge separation approach need new network entities. Another drawback is that these entities would introduce additional latencies in the network while processing the packets.

The feature "Tunneling / Encapsulation" refers to layer three approaches only and provides an overview how mapping functionalities, e.g. between core/edge address spaces, are solved.

2.8 Conclusion

In this chapter, the state of art of the existing mobility and multihoming protocols providing (partial or full) solutions is discussed in the context of a multihomed mobile network. Multihomed mobile networks & host will be connected through different access technologies and access networks, which offer various services regarding bandwidth, cost, QoS, etc. To provide the seamless connectivity with multihoming benefits best available network services, the network interface selection should be influenced dynamically by user preferences, policies, service provider's and network administrator's constraints to adapt the real-time environment.

Table 2.2 summarizes all the multihomed mobility approaches detailed in the previous section. The primary results are summed up as:

- Locator/identifier separation approaches such as LISP, HIP, SHIM6 are promising to solve mobility and multihoming but come at the cost of modifying end user hosts or of deploying new network entities such as mapping systems or specialized borders as in LISP.
- Transport layer approaches as SCTP and MPTCP support concurrent multipath transfer, but do not address mobility and multihoming.
- NEMO, together with the MCoA extension, does support network mobility and multihoming but with inefficient routing which may require some modifications on the multihoming front.

Therefore, the existing protocols would need some modification or may be coupling with a different layer protocol for providing seamless connectivity to multihomed mobile networks with multihoming benefits such as load balancing. As discussed in section 2.6, that network layer, and transport layer approaches are the better candidates to have a collaboration for improving existing solutions for multihomed mobile networks.

Chapter 3

Proposed Solution: Boosting Network Mobility through the Hybridization of NEMO and MPTCP

3.1 Introduction

A solution for network mobility combined with multihoming requires location management, information related to network characteristics, traffic routing, and a smooth handover-mechanism for providing better support regarding routing, transmission delay, throughput, load balancing, etc. Most of the mobility protocols are network layer based where location management is easy to provide. For performing “make before break" mobility, the mobility solution requires the transport layer information regarding RTTs, congestion or path disruption. Moreover, transport layer solutions need a mechanism for location management. This brings up the requirement of collaboration in the network layer and transport layer. In the absence of this collaboration between network and transport layer, the mobility protocols achieve “break before make", which causes extra handover delay for the flow. This leaves room for improvement.

There are several proposals to combine network layer approach with transport layer in an attempt to improve mobility support with multihoming. In [94], there is a novel combination of MIPv6 and MPTCP, which improves host mobility and multihoming. However, it does not support mobility for a whole network. In [95],

there is a combination of LISP and improved MPTCP to improve multihoming benefits to the host. However, LISP requires significant infrastructure changes in current Internet as it requires an adhoc IP addressing plan in order to assign EIDs and RLOCs. This adhoc IP addressing plan would require additional operational overhead. On the other hand, NEMO requires minimal infrastructure changes into standard Internet architecture as compared to LISP [96]. Moreover, in NEMO there is no signaling overhead in order to support network mobility compared to LISP. However, NEMO needs an improvement in multihoming support. There is also a proposal for network mobility in space [97] combining modified NEMO where its location management is replaced by dynamic DNS with SCTP. However, in this proposal mobile nodes do not participate in mobility and multihoming. In the combination of LISP and MPTCP, the nodes need to gather traffic-related information from the mapping system.

In this chapter, we propose a novel combination of network layer approach NEMO and transport layer approach MPTCP to achieve better mobility support with better multihoming support concerning reduced cost, improved throughput and load balancing for multi-homed mobile networks. This proposal provides location management with the help of NEMO and multihoming using MPTCP by enabling the mobile nodes to participate in multihoming related decision making and have direct access to the traffic related information. Moreover, the proposed combination requires minimal infrastructure changes.

There can be other choices for location management like dynamic DNS or a rendezvous mechanism. These proposals need some additional functionalities to be introduced for providing location management for mobile networks. As the use of dynamic DNS lacks in providing a seamless mobility for local fixed nodes due to their inability to change their network point of attachment for an ongoing connection [56]. NEMO is the only solution that will be able to provide seamless mobility to local fixed nodes with the help of its HA route. Another advantage of NEMO against dynamic DNS solution is that in the case of non-friendly visited networks (NAT, paranoiac firewalls, etc.), a tunnel is mandatory for incoming traffic [78]. This would require a rendezvous mechanism (which a DNS server is not) to open the connection simultaneously from both the ends for, e.g., VPN (with their tunnels). Whereas, NEMO already uses tunnels which can be used for incoming traffic in non-friendly visited networks. Therefore, NEMO provides better location management than dynamic DNS in mobile networks.

There can be other choices for multihoming as well, e.g., CMT-SCTP [73]. However, unlike MPTCP, SCTP is not transparent to the applications. Moreover,

MPTCP performs significantly better than SCTP [74]. Therefore, the combination of NEMO and MPTCP would be a better choice than any other rendezvous mechanism or dynamic DNS with MPTCP to solve network mobility having local fixed nodes and mobile network nodes providing better multihoming support.

Our aim is to investigate an approach that requires minimal infrastructure changes in the Internet. To best of our knowledge, there have not been any attempt to combine NEMO with MPTCP. Our proposal easily overcomes the limitations of NEMO and MPTCP detailed in the following subsection 3.1.1. Section 3.2 describes the proposed architecture with signaling and its benefits. Section 3.3 presents the comparison between classical NEMO and proposed NEMO with MPTCP. Finally, we present our conclusion.

3.1.1 Limitations of NEMO and MPTCP

NEMO and MPTCP provide mobility and multihoming but with some limitations. These limitations are as explained below.

Limitation of NEMO:

- Inefficient Routing: In NEMO, all the incoming and outgoing traffic has to travel through its HA-MR route. That is because, in NEMO, MNN's are not aware of mobility. Therefore, any communication between CN and MNN is done using MNN's home address. This HA-MR route makes the routing inefficient and reduces RTT (round-trip time) and throughput.
- Fault-tolerant: NEMO has very low fault tolerance for mobility because if there is a path disruption between HA and MR, all the incoming and outgoing traffic of mobile network will be disrupted and the whole mobile network will be disconnected from the outside world.
- Tunneling Packet Overhead: There is an additional tunneling overhead in NEMO as the packets have to be routed through tunnels between HA and MR. HA will encapsulate all the incoming traffic for mobile network node and send it to MR's current care-of-address. While MR will encapsulate all the outgoing traffic from MNN and send it towards HA. Therefore, there is an additional packet tunneling overhead in between HA and MR.
- Load-balancing: With the help of its extensions (MCoA and Flow Binding), NEMO tries to use all the existing IP addresses simultaneously. However,

this requires additional tunnels between HA and MR. The flow binding extension of NEMO attempts to manage the traffic distribution of flows over several existing paths. This is an effort to provide an equal distribution of flows over all available interfaces. However, even with the flow-binding extension, it cannot provide a full load balancing as the flow-binding approach will bind one flow to a particular path. That means that for a single flow only one path will be used, so the load-balancing is done on MR level rather than user level.

- Handover delays: To manage mobility, NEMO being a network layer protocol uses “break before make" method to provide mobility. It waits for the old link to break before connecting to the new link which adds a delay during handover.

- User Choice Consideration: The mobile network nodes attached to the mobile router, cannot take part in mobility or multihoming with NEMO. If mobile network nodes are involved in the multihoming, the load from mobile router can be reduced, and each user can manage its connections according to the user and application requirements. Otherwise, there is a requirement of extra signaling from MNN to MR for pushing the user preferences and requirements and make MR select the best access link for each user's stream according to its preferences [59].

Limitation of MPTCP:

- No Network Mobility Support: The transport layer solution MPTCP provides “make before break" mobility to the hosts. However, it needs to have some location management entity. Even with the location management entity, it lacks to provide network mobility which is the requirement of our project.

- No Location Management: MPTCP does not have its location management to support mobility of the host. There are several proposal for location management with MPTCP using dynamic DNS [98] or a rendezvous mechanism. However, these proposals work only for host mobility but not for mobile networks. Therefore, to solve network mobility and multihoming with MPTCP, there is a requirement of location management mechanism.

Considering the above limitations, there is a requirement for an improvement in mobility and multihoming support with NEMO to reach the multihoming goals

optimally, improve routing and reduce tunneling overhead. These enhancements are dealt by our proposed novel combination of the two protocols which overcomes these limitations and supports better multihomed mobility for mobile networks.

3.2 Network Mobility with Host Multihoming

In this section, we describe the procedure to combine NEMO with MPTCP protocol. Their integration can be done without any significant modifications to basic NEMO or MPTCP. As explained above, NEMO is being used for the location management of mobile network for incoming traffic during connection initiation, and afterward, the MPTCP handles the mobility and multihoming. This proposal enables MNNs to participate in mobility and multihoming. For implementing this, the MNNs need to be aware of mobility which requires two minor changes in MR. Firstly, the MR needs to advertise its current network prefixes or Care-of-prefixes to MNNs. After receiving the current network prefixes, MNNs can configure and add the newly acquired IP address to their interfaces. Secondly, MR should be able to differentiate between the packet flows. The packet flow with MNN's home IP address needs to be sent through HA-MR tunnel whereas the packet flow having MNN's newly acquired care-of-address need to be routed towards the Internet.

To illustrate the key points, we consider the following scenario. When a mobile network is outside its home network, and a communicating node (CN) initiates communication with the node which is connected to MR, the communication has to pass through the HA because CN is not aware of MNN's current location in the Internet. The home agent then encapsulates the packets and forwards them towards MR's current care-of-address which is the same as NEMO shown in Fig. 3.1.

During the connection establishment, the mobile network node or communicating node adds MP_CAPABLE option inside the TCP packet header. If both nodes natively support MPTCP, then they establish an MPTCP connection and exchange all the existing IP addresses. If any node does not support MPTCP, there is a proposal to install a lightweight proxy on the node to make it MPTCP-capable, as proposed in [81]. Once the communication is established the mobile network node can set the HA path as BACKUP path with the help of MP_PRIO option and create subflows using the rest of the IP addresses. The mobile router should be able to route the packets directly using its current care-of-address rather than through HA.

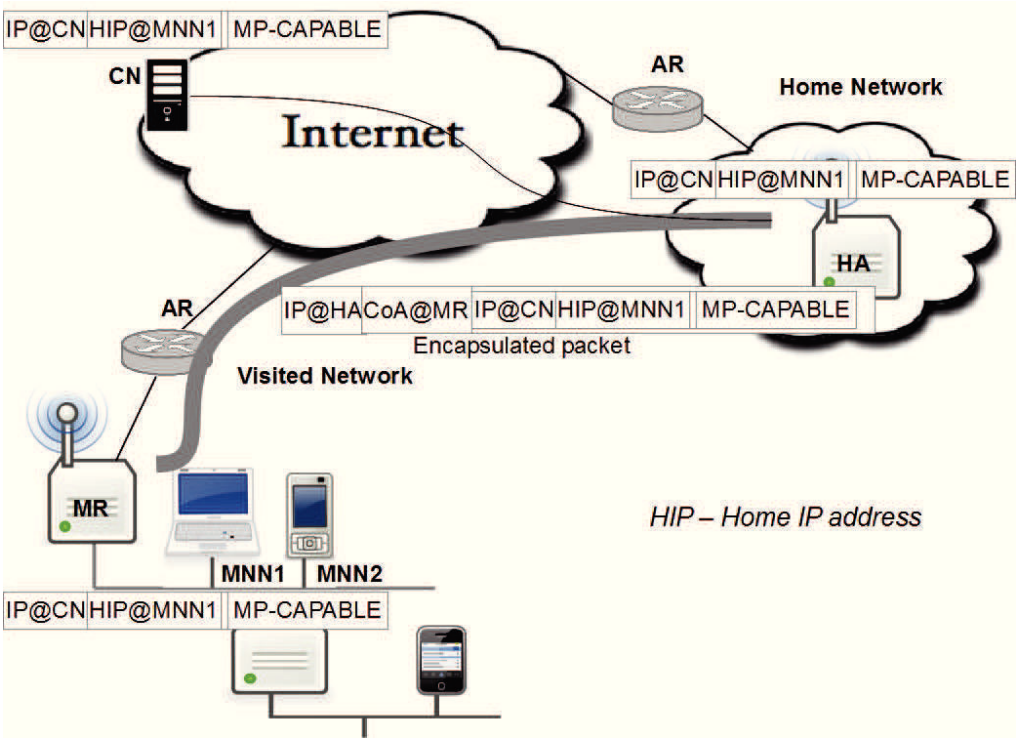

FIGURE 3.1: Connection initiation in proposed architecture

Whenever during mobility, the mobile network attaches to a new point in the Internet, it receives a new network prefix. Using this prefix, it creates a care-of-address and updates the binding with HA. It then advertises the new prefix to the MNNs. Once the nodes receive the new prefix, they can configure the new IP address and communicate it with the communicating node using MPTCP in order to create another subflow as shown in Fig. 3.2. The IPv6 address configuration can be done either with the help of DHCPv6 or stateless address autoconfiguration [99]. However, this may require minor modification of DHCP server (most of them distribute IP within fixed pool) and of DHCP clients (most of them replace the old IP of the interface by the new one).

In the presence of multiple CoAs on MR, HA has to make a choice among available interfaces for forwarding the connection initiation packets. This problem can be solved by implementing policies in between HA and MR with the help of flow binding extension [100] of NEMO.

As MPTCP uses “make before break", the proposed approach makes handover smooth compared to classical NEMO. In the proposed approach, NEMO is used only for starting the communication from the nodes in the rest of the Internet to an MNN. If MNN wants to initiate a connection it can use its care-of-address to send an SYN packet with MPTCP-CAPABLE option added in TCP header (as explained in [75]) to the communicating node. This header also contains the

care-of-address in the destination address field. Once, the communicating node receives the SYN packet it replies with SYN+ACK. On reception, MNN responds with ACK and connection is established. After the connection establishment, MNN can communicate its other available addresses including its home address to the communicating node using MP-JOIN option. Once communicated, MNN has an option to set the HA-MR tunneled path as a backup path using MP-PRIO option. That means it will only be used when none of the other paths works. Due to mobility, when MR moves away towards a new foreign network, MNN can communicate its newly acquired care-of-address to the communicating node.

NEMO is more compatible to IPv6 addresses and works for IPv4 as well [101]. The solution for users having IPv4 addresses requires mobile IPv4 enabled foreign agents (access routers) and an additional tunnel. The HA needs to encapsulate the packets twice first with mobile router's current care-of-address than with foreign agents address. First tunnel's endpoint is mobile IPv4 capable access router and second tunnel's endpoint is the mobile router. Except these differences, NEMO works same for both IPv6 and IPv4 addresses. MPTCP is also compatible with both IPv4 and IPv6 addresses. Therefore, the impact of the proposed approach in the case of IPv4 addresses is similar to the impact in case of IPv6 addresses. It will work the same way with an additional functionality into the mobile IPv4 enabled access router to route the packets with care-of-address towards the Internet.

3.2.1 Signaling

For explaining the signaling in the proposed approach, we consider two different scenarios.

- When MNN initiates the communication with CN, i.e., for outbound traffic
- When CN initiates the communication with MNN, i.e., for inbound traffic.

3.2.1.1 Signaling for Outbound Traffic

In outbound traffic, MNN needs to initiate communication with CN. To establish the communication, the following steps need to be executed.

- MNN creates an SYN packet with the MP_CAPABLE option and routes it toward MR using its CoIP@MR-AR1 as the source address and CN's address as destination address.

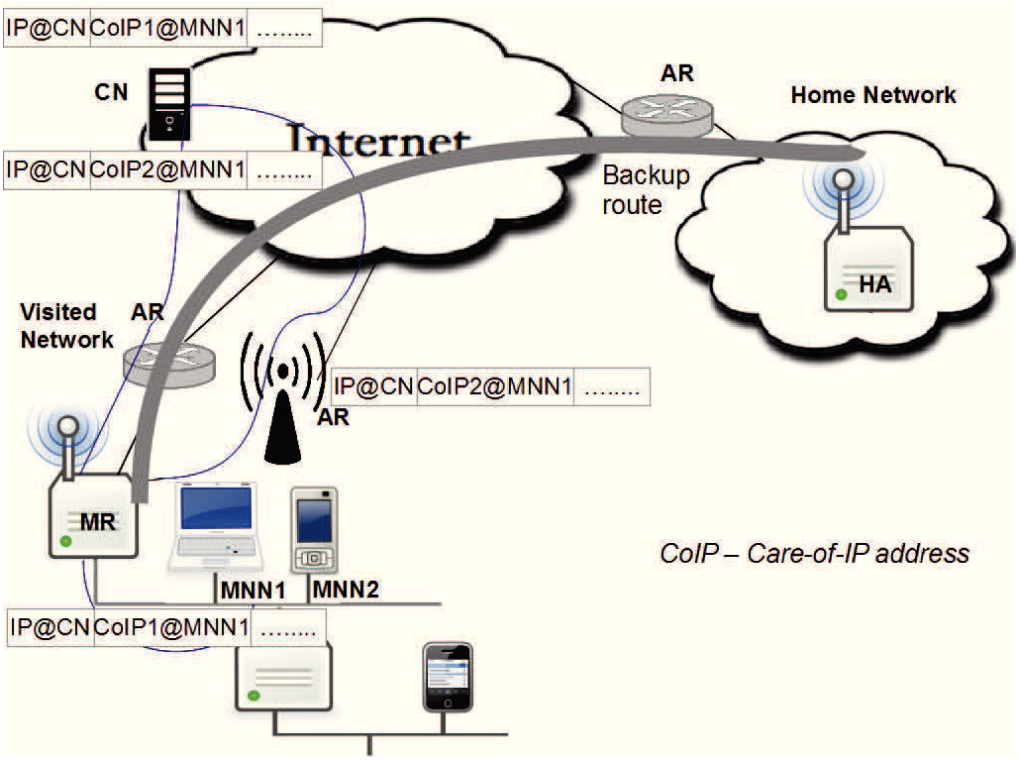

FIGURE 3.2: Communication after connection establishment in proposed architecture

- MR then routes this packet towards the Internet through access point AR1/.
- CN receives the packet and routes the reply SYN-ACK packet towards MNN's CoIP@MR-AR1 supposing that CN support MPTCP.
- On reception of SYN-ACK, MNN sends an ACK packet, and the MPTCP connection is established.

After the connection establishment, MNN can share its existing CoIPs. MNN has an option to share its Home IP address with the CN to keep this path as a backup path, as usually it is not used. If mobility occurs in between, then MNN receives a new prefix from MR and configures a new CoIP. It then shares this new CoIP with CN and creates another subflow. If the communication is lost with the previous access network, MNN sends a request to remove the previous IP address from its IP address list and the communication continues through other subflows. Fig. 3.3 illustrates the above explained signaling.

In the proposed approach, the traffic avoids tunneled route between HA and MR. Therefore compared to classical NEMO, the proposed approach would perform better by reducing transmission delay, avoiding tunneling overhead and improving throughput in case of outbound traffic between mobile network node and

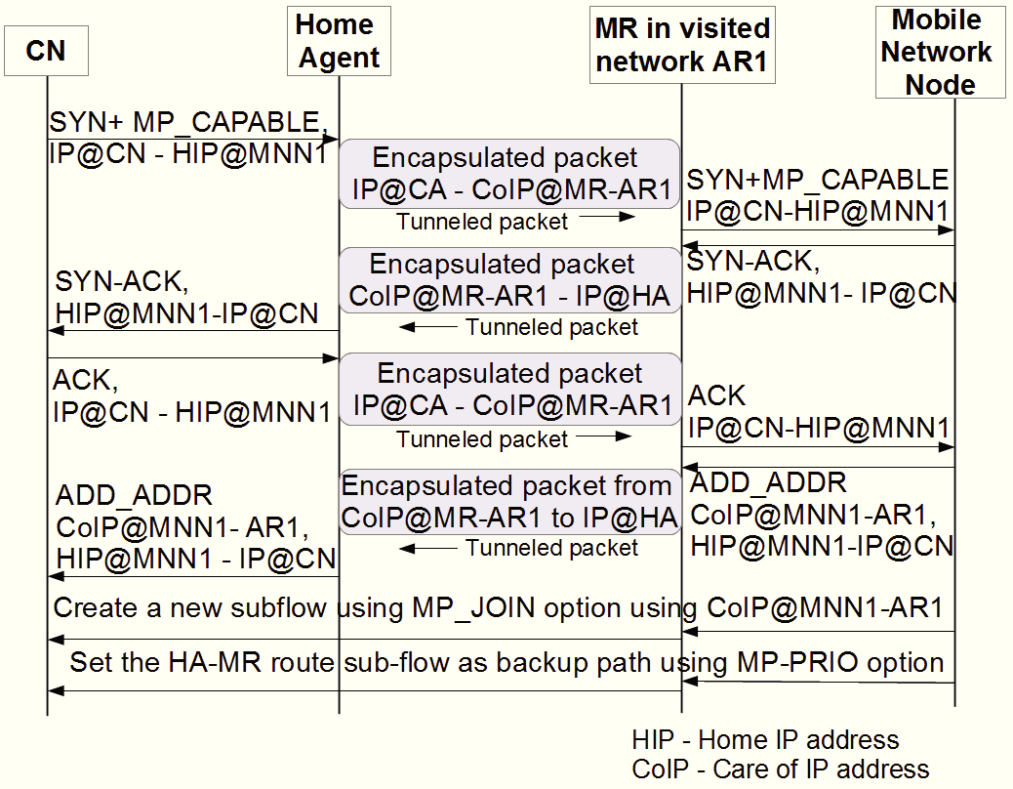

FIGURE 3.3: MPTCP connection establishment for outbound flow in proposed architecture

communicating node. Since, for local fixed nodes, the IP address needs to be preserved for an ongoing communication in order to provide session continuity, the proposed solution falls back to the classical NEMO. Therefore, NEMO is used to support mobility for local fixed nodes and works in a classical way.

3.2.1.2 Signaling for Inbound Traffic

To illustrate the signaling for inbound traffic, we consider the scenario where mobile network is on the move and currently connected to access router 1 (AR1). Once it is connected with AR1, it creates a binding with its HA for its current care-of-address. It then advertises the new prefix to MNN, and it then configures and adds the new IP (CoIP@MNN-AR1) to one of its interfaces. When any communicating node from the outside Internet initiates communication with MNN, the following steps need to be executed to establish a connection.

- CN generates the SYN segment packet with the MP_CAPABLE option for MNN's home IP address and routed towards its home network.

- In the home network, HA intercepts the packets and finds a binding entry for MNN's MR.
- HA then encapsulates the packets using care-of-address of MR@AR1 (CoIP @MR-AR1) and forwards the packet towards mobile network's visiting network.
- Upon the reception of the packet, MR decapsulates it and forwards it inside the mobile network.
- MNN receives the packets and create an SYN-ACK packet segment for IP@CN and route it towards MR.
- MR encapsulates this SYN-ACK packet and send it to HA. On reception of the packet from MR, HA decapsulates it and route it towards CN's network.
- CN receives the packet and generates reply as an ACK packet, and the packet takes the same HA-MR route as before. On reception of ACK packet, the MPTCP connection is established.

After the connection establishment, MNN sends a request to ADD-ADDR providing CoIP@MNN-AR1 and create a subflow using this IP. Once the new subflow is added to the ongoing communication MNN sets the HA-MR route as backup path and continues to communicate through its care-of-address. After this step, a tunneling overhead is gained with the exchange of each packet for the ongoing communication. Fig. 3.4 illustrates the above explained signaling.

The above explained scenario is valid when MNNs and MR are connected to a single access network. There can be multiple available access networks. In that scenario, MNN can create new subflows by adding other available CoIP address to the ongoing communication with CN and communicate using all the subflows.

The only difference between outbound and inbound traffic signaling is during connection initiation. As in the case of inbound traffic the proposed approach use tunnels for connection initiation. After the connection initiation both the scenarios show similar expected gain concerning reduced tunneling overhead and improved routing, load balancing thus improved throughput.

3.2.2 Benefits and Use cases

In order to see the benefits of the proposed architecture, we have to reconsider the limitations of NEMO, which can be easily overcome by the combination of

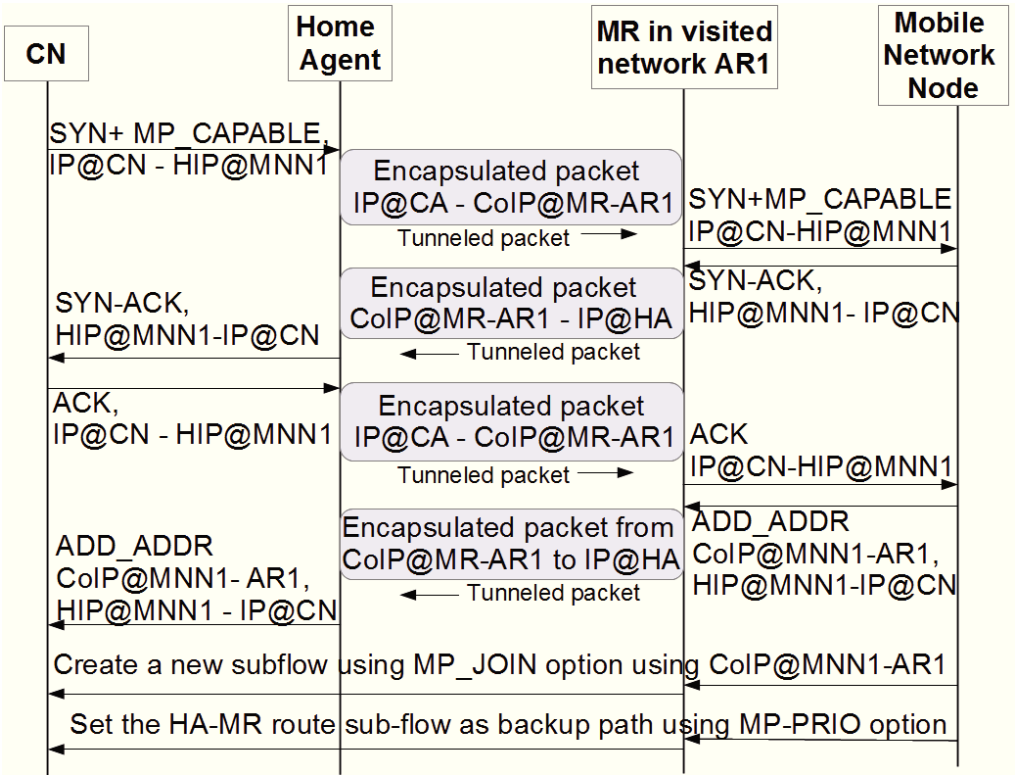

FIGURE 3.4: MPTCP connection establishment for inbound flow in proposed architecture

NEMO and MPTCP. For performing an ideal mobility or “make before break" mobility, any solution for mobility requires access to some path related information from transport layer as discussed in section 3.1. The proposed approach is a collaboration between network and transport layer protocols. Network layer protocol NEMO with the help of transport layer protocol MPTCP provides a better mobility support with the smooth handover.

Multihoming can be supported with the help of its multiple care-of-address registration (MCoA) extension. However, this would add more tunnels between HA and MR. While in the proposed approach, MR does not have to perform multihoming. MPTCP takes over once the connection is established and the rest of the communication happens in a similar way to that of the Internet. The use of MPTCP reduces these additional tunnels and provides multihoming benefits to the host.

The flow binding extension of NEMO attempts to provide an equal distribution of flows over all available interfaces, but it can only be done on MR-HA route as the policies that are introduced in flow binding extension consider only the path characteristics in between the mobile router and the home agent. Optimum load

balancing cannot be achieved. While in the proposed scenario, MPTCP helps to achieve an optimum load balancing over all the available network interfaces.

There can be a scenario where the communicating node is very near to MR. An example of such a scenario in the real world situation can be a boat/ship which resides in France (its home network) and currently sailing near Australian coast. A random user from Australia would want to communicate/transfer a file or video with/to a node on this boat/ship. This situation will cause the traffic to travel through its home network, i.e., France. It can be improved by the proposed architecture as the data transfer takes normal routing path instead of its HA path.

Considering the scenario where two mobile network nodes (inside different mobile networks) want to communicate or exchange data with NEMO, the traffic has to pass through both of their HAs and then tunneled towards MRs. The proposed approach shows a gain in this scenario as after the connection establishment these two nodes can communicate independent of the HAs-MRs route without the requirement of tunnels.

Some other use case scenarios can be considered as in the case of boats; mail-servers can receive any amount of data in real time without requiring to pass through tunnels or by polling a cache server. In the present time, some commercial ship vessels have some limitations of the file size in the onboard mail-servers. This file-size constraint can be removed with the help of the proposed architecture, and onboard email servers can be reached at any time instead of polling.

The proposed approach does not need any significant modification in already implemented NEMO and MPTCP. This makes its deployment manageable. For UDP connections or in the absence of MPTCP proxies, tunnels are still available as a fall-back solution. For non-TCP connections in real-time traffic such as VoIP, IETF is working on standardizing multi-path extension for RTP [78]. This can also be combined with NEMO to limit tunneling, as MPTCP does.

The tunnels of NEMO may have increased overhead in normal scenarios, but they are beneficial for the incoming traffic in non-friendly visited networks for, e.g., NAT, firewall, etc. and for providing seamless mobility to the local fixed nodes inside a mobile network. NEMO's tunnels are also convenient natural fall-back solution in the scenario when there is no MPTCP support. Moreover, the proposed solutions help to avoid tunnels when it is not necessary. This makes the system more flexible and more robust. Therefore, MPTCP with NEMO helps to provide better network mobility with optimum multihoming benefits.

3.3 Comparison between classical NEMO and NEMO with MPTCP

In this section, Table 3.1 demonstrates the comparison in the features of NEMO and the proposed hybridization of NEMO and MPTCP, based on following parameters:

- **Deployment Complexity**: Classical NEMO introduces two new entities in the Internet. A home agent in the home network and a mobile router in the mobile network but no changes to the mobile nodes. These two entities are standard routers with some additional functionalities. Therefore, whenever the mobile network is connected to home network, home agent and mobile router work as any other router to forward packets. However, our proposed architecture inherits all the changes needs to be done for NEMO with additional changes in the mobile node to make them MPTCP compliant. Mobile nodes can either have inbuilt MPTCP support or use the proxy. The proposal also introduces two small variations in the mobile router of classical NEMO and none to the MPTCP. These minor changes make the deployment of our proposal easy and are compatible with the legacy Internet architecture.

- **Fault Tolerance** All the traffic having to go through HA-MR route makes NEMO less fault tolerant. If there is any issue on HA-MR route, the whole traffic of mobile network will be disrupted. However combining NEMO with MPTCP, helps to minimize the use of HA-MR bidirectional tunnel. This tunnel is used only for the connection initiation signaling for incoming traffic. Afterward, all the traffic flows through MR as it flows through any standard router in the Internet. Therefore, the hybridization of NEMO and MPTCP makes system better fault tolerant than HA-MR route in classical NEMO.

- **Routing**: In classical NEMO, all the traffic destined to mobile network nodes has to pass through HA and then it is tunneled towards MR in the foreign network. This is the same case for the outbound traffic which makes the routing inefficient. Whereas, in the proposed approach, for outbound traffic the traffic follows a classical Internet path which makes the routing more efficient. The HA-MR route is used only for signaling for incoming traffic and for providing mobility to LFNs. Once the connection is established for the incoming traffic, MPTCP handles the communication. Both

communicating node and mobile network node can share other existing addresses, i.e., care-of-addresses (one or more) and communicate using them rather than following HA-MR route. Thus, the proposed approach make routing more efficient compared to classical NEMO.

- **Throughput**: The throughput of the system can be almost doubled by using MPTCP compared to TCP in mobile scenario [78]. However, having only one network interface available at a time provides an expected improvement throughput from the proposed architecture due to improved routing compared to classical NEMO. Therefore considering more than one interfaces available at a time with MPTCP will increase the performance.

- **Round Trip Time**: In classical NEMO, as the mobile network moves away from the home network, the length of the HA-MR tunnel increases. This results in increased round-trip time. Whereas, the hybridization of NEMO and MPTCP enables the traffic to follow standard Internet routing path instead of routing it through MR's home network. Thus, the proposed approach reduces round trip time for the packets in the system.

- **Signaling Cost**: The classical NEMO will have signaling cost required for a TCP connection establishment in NEMO. Whereas, the proposed architecture will have NEMO signaling cost with additional signaling cost for adding MPTCP options in TCP header while initiating a connection or adding or removing subflows during mobility. The difference is very less compared to the multihoming benefits provided by the MPTCP into the system.

- **Tunneling packet overhead**: The proposed architecture significantly reduces tunneling cost compared to classical NEMO. As in classical NEMO, the total traffic takes HA-MR route which adds bi-directional encapsulation overhead. Whereas in the proposed architecture, the traffic is routed directly towards the Internet from MR rather than towards HA. In the case of IPv4 addresses, it will reduce the packets for both the tunnels.

- **Transmission Delay**: Inefficient routing, packet encapsulation-decapsulation, regular binding updates, etc. can introduce delays in the path while using classical NEMO. However, the proposed approach improves routing and reduces packet tunneling. Thus, a less transmission delay is expected.

- **User choice consideration**: In classical NEMO, the load balancing is done on the mobile router rather than per user basis. Users can not participate in multihoming related decisions. Whereas the proposed approach

Table 3.1: Classical NEMO vs. NEMO with MPTCP

Parameters	Classical NEMO	NEMO with MPTCP
Deployment Complexity	Low	Low
Fault Tolerance	Low	High
Routing	Inefficient	Efficient
Throughput	Low	High
Round Trip Time	High	Low
Signaling Cost	Low	High
Transmission Delay	High	Low
Tunneling packet overhead	Always	Only for incoming Traffic, local fixed nodes and in non-friendly visited network

provides a way for MNNs to participate in multihoming with the help of MPTCP and helps to improve the throughput of the whole system. This participation also gives the user an opportunity to decide the communication mode concerning cost efficiency, energy efficiency, or best availability of an interface, etc.

3.4 Conclusion

In this chapter, we proposed a highly efficient approach for enhancing the multihoming support in mobile networks by integrating NEMO with MPTCP. The proposed architecture requires very minimal changes in the functionalities of the mobile router in NEMO and none in MPTCP. There are two changes that need to be implemented in the MR. First, it should advertise its care-of-prefixes to mobile network nodes for them to configure their care-of-address. Second, it should be able to route the packets directly using MNNs care-of-addresses instead of routing them towards HA through the tunnel. The other enhanced feature of the proposed solution is that it limits the tunneling overhead. The established connection will survive as long as there is at least one available care-of-address. Moreover, the performance of the communication is also enhanced by using MPTCP when compared to TCP [102]. Therefore, this novel integration of NEMO and MPTCP provides much better network mobility with enhanced multihoming support compared to classical NEMO concerning reduced tunneling overhead, increased throughput and improved load balancing.

Chapter 4

Quantitative Analysis of the proposed approach

4.1 Introduction

In this chapter, a quantitative analysis is performed to demonstrate the effectiveness of the proposed approach over the existing approaches. For this demonstration, a local-testbed architecture is established to carry out a theoretical and experimental study to learn the behavior of NEMO, MPTCP, and NEMO with MPTCP.

The local testbed implementation is a part of TMS-WP6 deliverable v4 [103]. The purpose of this first version was to install NEMO and verify whether it works for some test case scenarios considering cruise ships or merchant vessels etc. in the sea where the travel speed is generally not very high. Through installation and experimental verification, it can be concluded that NEMO is one of the best possible solution for network mobility in case of ships and boats. However, there is room for improvement in a way the NEMO performs routing. It takes a longer route compared to legacy Internet routing. In our approach, we propose to use MPTCP to overcome inefficient routing of NEMO. Thus, the local testbed is extended with the installation of MPTCP. The performance of the proposed approach is evaluated and compared with that of classical NEMO in different network scenarios. For measuring the gain in performance, we consider various network parameters such as throughput/goodput and delay performance. Based on these parameters, a valid conclusion can be derived from the performance of a system. The network performance parameters throughput (Mbits/sec) and

round-trip time(ms) are measured experimentally while transmission delay has been calculated theoretically.

The next section 4.2 presents the testbed architecture followed by review of existing implementations of NEMO and MPTCP in section 4.3. Section 4.4 presents the network scenarios considered for measuring the throughput and round-trip time. In section 4.5 theoretical and experimental measurement results are presented followed by conclusion in section 4.6.

4.2 Testbed Architecture

The local testbed architecture involves following entities:

- Mobile network having a mobile router and a mobile network node connected to it.
- Home network, where mobile network resides when it is not moving. This home network also has the entity called Home Agent for managing the mobility of the mobile network.
- Two visited/foreign networks, to illustrate the mobility scenario when mobile network moves in between foreign networks.
- One communicating Node, which is somewhere inside the Internet to show the communication between the mobile network node and the communicating node.

For simulating the Internet kind of environment, some delay and packet loss is added on the outgoing links on home agent, and foreign networks. This delay is added using "*netem*" tool in linux [104]. In the local test bed, 10ms of delay and 5% of packet loss has been added as shown in the Fig. 4.1. The values of delay and packet loss are chosen arbitrarily.

While considering the scenarios to exhibit network mobility and multihoming, we just "translate" it into Ethernet cables and switches. The local testbed architecture is a cluster of generic-purpose PCs with linux installed as OS, Ethernet cables and switches as shown in Fig. 4.1. The generic-purpose PCs act as different entities in the testbed, whose hardware and software configuration are explained as following:

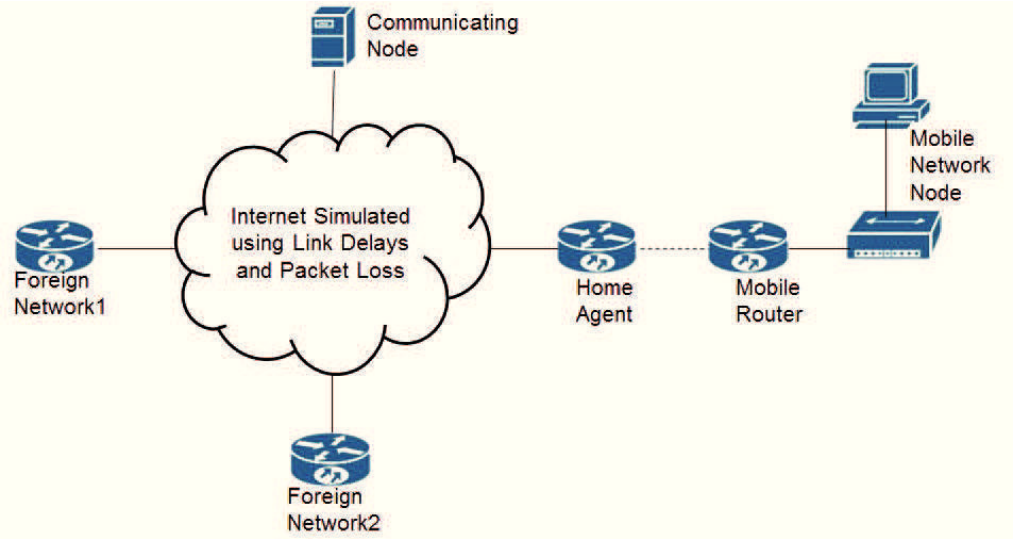

FIGURE 4.1: Testbed implementation architecture

1. Hardware Configuration: The generic-purpose PC which acts as Mobile router has Intel®Core™-i5-4440 CPU @ 3.10GHz × 4 processor and 7.8 GB RAM. The hardware configuration of home agent, foreign networks (access routers), communicating node and mobile network node consists Intel®Core™2 Duo CPU E8400 @ 3.00GHz × 2 processor with 3.8 GB RAM.

2. Software Configuration: Mobile router and home agent has Debian wheezy 7 with Linux 3.8.2 as operating system. Mobile router and home agent has some part of NEMO functionalities installed on it. The access routers have Ubuntu 12.04 with Linux 3.2.0 installed as operating system. These routers have 'radvd' installed on them. Therefore, they can advertise there prefixes and any node connected to these links can generate its own IPv6 address using IPv6 stateless autoconfiguration mechanism. The Communicating node and mobile network node has Debian Wheezy 7 with Linux 3.18.20 installed as operating system. The Communicating node and mobile network node has mptcp version 0.90 installed on it with backup mode functionality. The communicating node is used to verify the reachability of the mobile network node from Internet. The communicating node work as a server and the mobile network node work as a client in order to calculate the throughput of the system.

4.3 NEMO and MPTCP Installation

There are several existing implementations of NEMO based on different operating systems. SHISA is an implementation of Mobile IPv6 and NEMO on BSD. It was part of WIDE project, under which two different implementation of Mobile IPv6 have been developed [105]. NEPL is the implementation of NEMO Basic Support on Linux 2.6 for UMIP. ATLANTIS is the NEMO Basic Support implementation for NetBSD [106]. These work groups have been inactive since 2013.

For the testbed implementation, we have used NEMO implementation for Linux provided by UMIP working group [107]. NEMO functionalities are installed on mobile router and home agent. This installation enabled mobile router to send periodic binding updates to the home agent, when in foreign network. Home agent is enabled to create a mapping between mobile network home prefix and care-of-address and cache these binding entries. In our system these periodic updates are every 60 seconds. Whereas, when mobile router is in home network it notifies the home agent that it is inside home network. Mobile router advertises the network prefix to the connected nodes as it works as a normal router for them. This implementation uses IPv6 addresses. In the local implementation, the home network prefix set on the mobile router is 2001:db8:ffff::1/64. Any mobile network node connected to it can create an IPv6 address using this prefix with the help of IPv6 stateless autoconfiguration mechanism.

There exists several implementation for MPTCP based on different operating systems e.g., for Linux, Android from Universite catholique de Louvain [108], for FreeBSD (IPv4 only) from Swinburne University of Technology [109], for Citrix with Netscaler [110], for Apple iOS [111] (first large scale commercial deployment), for Apple MAC OS X 10.10 [112]. For the testbed implementation, we have used the latest available version v0.90 of MPTCP available for Linux from University catholique de Louvain [108]. The authors of these implementation are still providing different versions of MPTCP and further plan to develop innovative products based on this technology. MPTCP is installed on mobile network node and communicating node. After installation, for enabling MPTCP we need to set the value *Disable/Enable* for *net.mptcp.mptcp_enabled* on the machine. There are other options which can be used like checksum, syn_retries, congestion control etc. MPTCP can be set to use all ports or any number of different ports of the machine using path manager. For the testbed architecture we are going to install MPTCP in backup mode and set *net.mptcp.mptcp_enabled* as 1.

4.4 Network Scenarios

This section presents the network scenarios implemented in the local testbed. These scenarios are taken in consideration to demonstrate mobile network's mobility in between home network and foreign network, and in between two foreign networks. There are three network scenarios based on mobile network's attachment location among home network and foreign networks, as explained in the following sub sections. To demonstrate mobile network's mobility from one network to another network, the Ethernet wire is unplugged from one link switch and then plugged to the switch connected to another link. Here, we should also mention that, the handover being performed is a hard handover. The connection between mobile router and home agent is broken manually i.e., unplugging the wire; and then connecting manually i.e., plugging the wire to the new link in foreign network 1. The three scenarios detailed in following subsections are listed below:

- Network Scenario 0 (NS0): When Mobile Network is directly attached to Home Network
- Network Scenario 1 (NS1): When Mobile Network is attached to a Foreign Network1
- Network Scenario 2 (NS2): When Mobile Network is attached to a Foreign Network2

4.4.1 Network Scenario 0 (NS0): When Mobile Network is in Home Network

In Network Scenario 0 (NS0), mobile router is directly attached to its home agent as illustrated in Fig. 4.2, so there is no requirement of mobility. Mobile router identifies that it is connected to home network and does not require any mobility related functioning. Therefore, home agent behaves as a normal router for the inbound and outbound traffic from mobile network. The traffic between mobile network node and communicating node flows through the classical Internet routing path. We consider, this as the best case scenario, as there is no requirement of tunnels or diverted routing for classical NEMO. Therefore, proposed approach does not provide any improvement in this scenario.

In the logs on the mobile router, it can be verified that the mobile router is connected to home agent and is now in home network, in logs B.1.1. It can also

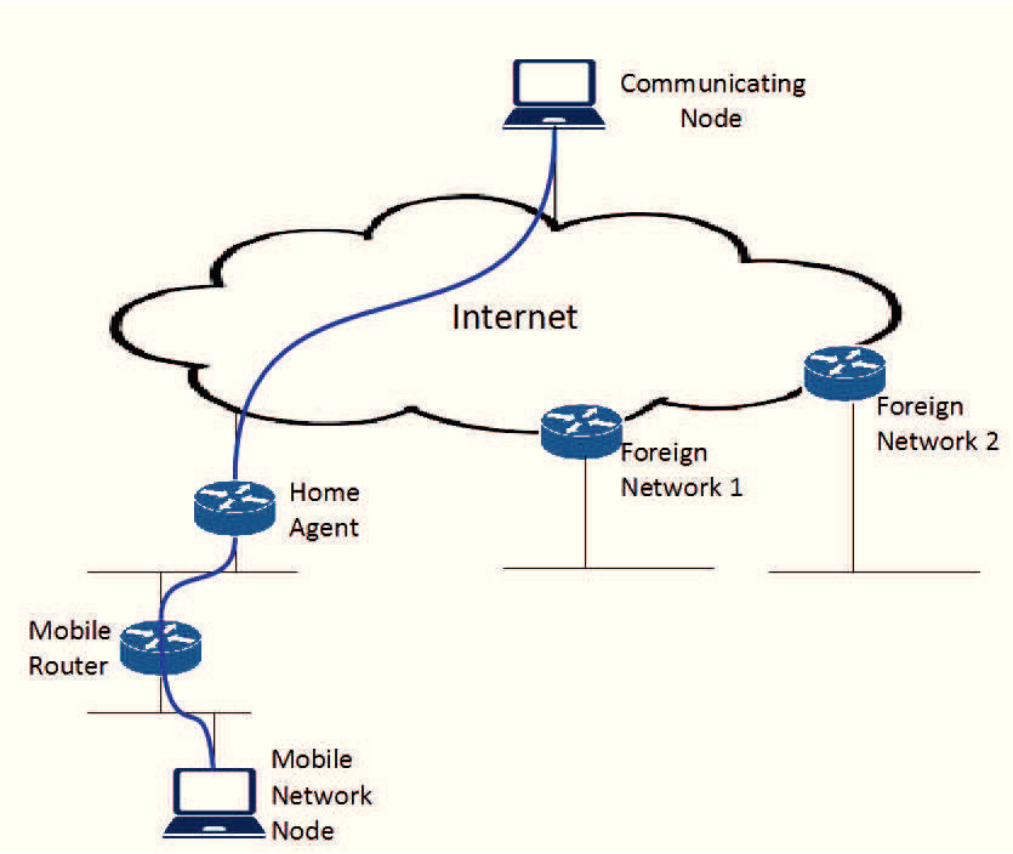

FIGURE 4.2: Testbed implementation architecture - Network Scenario 0

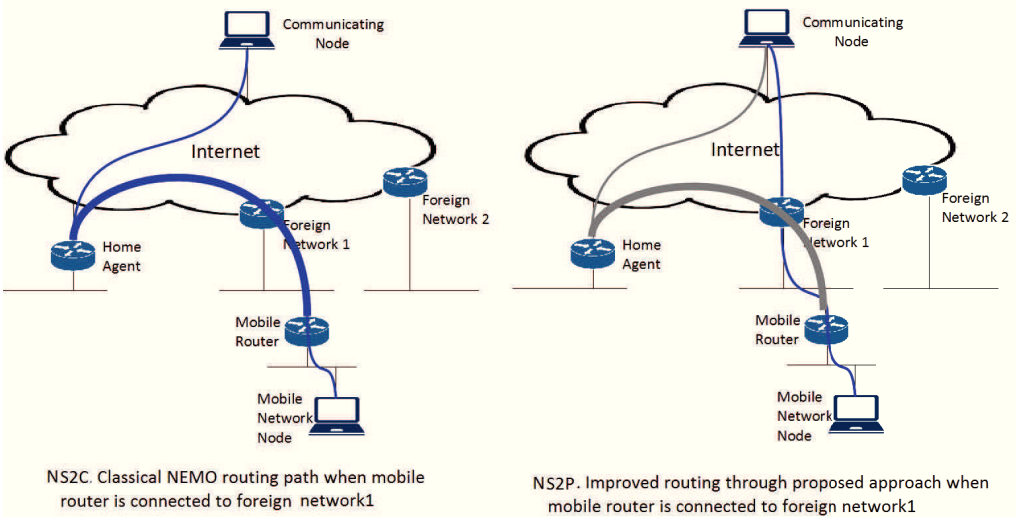

FIGURE 4.3: Testbed implementation architecture - Network Scenario 1

be verified that the mobile router has the information of its address of HA and mobile network prefix etc. When mobile router connects to the home agent, it notices itself to be in home net. Moreover, the binding cache on the home agent and binding update list on the mobile router can also be verified to be found empty in the logs B.1.2.

4.4.2 Network Scenario 1 (NS1): When Mobile Network is in Foreign Network1

In Network Scenario 1 (NS1), mobile router is attached to foreign network1 as shown in Fig. 4.3. This network scenario is used to demonstrate the mobility of the mobile network from home network to foreign network. The access router in foreign network1 advertises a router solicitation message with its network prefix i.e., 2001:db8:0:1::1 in local testbed. On the reception of router solicitation message, mobile router configures a care-of-address with the help of stateless address auto-configuration feature. Let's call this care-of-address as CoA1. Mobile router then sends the binding update to the home agent with its acquired CoA1 and creates a tunnel towards the home agent. The home agent, then creates the binding entry in its cache with the mapping between mobile router's home address and CoA1. This can be verified by looking into binding update list on the Mobile Router and binding cache entry on the home agent.

The only difference between classical and proposed approach is of the routing path in between mobile network node and communication node. In the classical NEMO, the traffic flows through the tunnel as shown in Fig. 4.3 NS1C (network scenario1 for classical approach). Whereas, in the proposed approach, mobile router advertises its new acquired prefix to the mobile network node to make network node aware of mobility. With the help of stateless address auto-configuration feature, mobile network configures its own care-of-address using the prefix of foreign network 1. Afterwards, with the help of MPTCP's multihoming management properties, mobile network node establishes a direct route with the communicating node through foreign network 1 as shown in Fig. 4.3 NS1P (network scenario 1 for proposed approach). After the establishment of direct route, the HA-MR tunnel route is put as a backup path.

In the logs on the mobile router, it can be verified that the mobile router is attached to the foreign network 1, in logs B.2.1. It can also be verified that the mobile router has the information of its care-of-address 1, address of HA and mobile network prefix etc. When mobile router connects to the foreign network, it notices itself to be in foreign net and sends a binding to the home agent. Moreover, the binding cache on the home agent and binding update list on the mobile router can also be verified for its care-of-address 1 in the logs B.2.2. The tunnel is also available on the home agent which can also be verified by its starting point as well as end point at the home agent in the logs B.2.2.

From the logs on mobile router B.2.1 and home agent B.2.2, it can be confirmed that the connection works properly and binding updates are sent and received when mobile router is in foreign network 1. The end points of the tunnel are mobile router's and home agent's addresses.

4.4.3 Network Scenario 2 (NS2): When Mobile Network is in Foreign Network2

Network Scenario 2 (NS2), is almost identical to NS1 apart from the foreign network to which mobile network is connected. In NS2, mobile network is connected to foreign network 2 as shown in Fig. 4.4. This network scenario is to demonstrate the mobility of mobile network in between two foreign networks. The mobile network moves from foreign network 1, connects to foreign network 2, configures a new care-of-address with foreign network's prefix which is 2001:db8:1:1::1, in the local-testbed. Let's call this care-of-address as CoA2. After acquiring this new address mobile router will update the binding cache mapping from CoA1 to CoA2 as by sending the binding update. The end point of the tunnel is also modified from CoA1 to CoA2.

Similar to the previous scenario, the only difference between classical and proposed approach is of the routing path in between mobile network node and communication node. In the classical NEMO, the traffic flows through the tunnel between HoA and CoA2 as shown in Fig. 4.4 NS2C (network scenario2 for classical approach). Whereas, in the proposed approach, mobile network node establishes a direct route with the communicating node using its acquired CoA2 through foreign network 2 as shown in Fig. 4.4 NS2P (network scenario 2 for proposed approach).

In the logs on the mobile router, it can be verified that the mobile router is attached to the foreign network 2, in logs B.3.1. It can also be verified that the mobile router has the information of its care-of-address 1, address of HA and mobile network prefix etc. When mobile router connects to the foreign network, it notices itself to be in foreign net and sends a binding to the home agent. Moreover, the binding cache on the home agent and binding update list on the mobile router can also be verified for its care-of-address2 in the logs B.3.1. The tunnel is also available on the home agent which can also be verified by its starting point as well as end point at the home agent in the logs B.3.1.

From the logs on mobile router B.3.1 and home agent B.3.1, it can be confirmed that the connection works properly and binding updates are sent and received

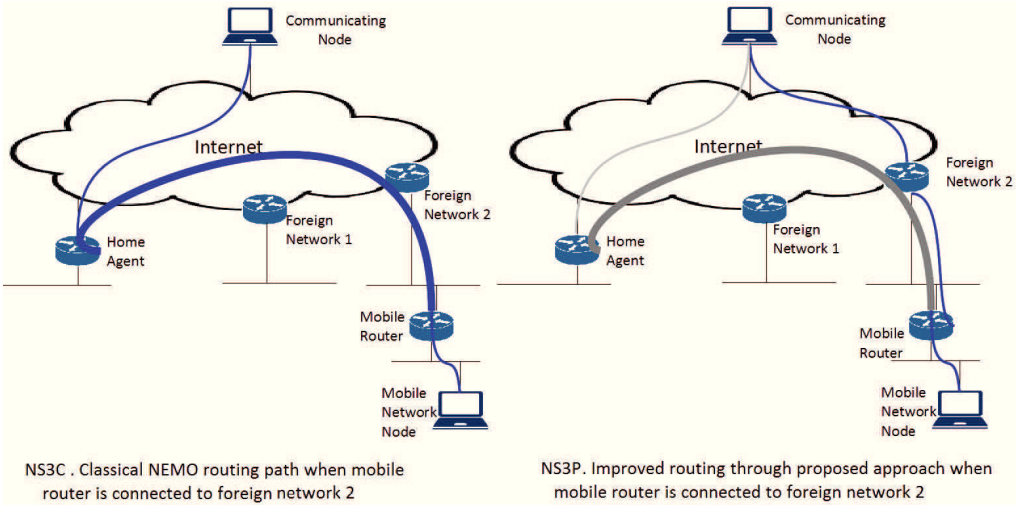

FIGURE 4.4: Testbed implementation architecture - Network Scenario 2

when mobile router is in foreign network 2. The end points of the tunnel are mobile router's and home agent's addresses.

4.5 Results: Classical NEMO vs proposed approach Measurements

This section presents the experimental results. The throughput is measured by using iperf [113] and netperfmeter [114] commands and RTT by using ping6 command on the mobile network node and communicating node. The gain in the transmission delay, RTT and throughput has also been calculated by theoretical equations in the following sub-sections.

4.5.1 Delay Performance

The delay performance is calculated theoretically and measured graphically in the following subsections 4.5.1.1 and 4.5.1.2.

4.5.1.1 Qualitative Analysis

The per hop delay time can be defined by the sum of processing delay time and the delay time at the relevant link, given in following equation.

$$DelayTime = ProcessingDelay + PathDelay \tag{4.1}$$

In classical NEMO, MR sends the packets through MR-HA bidirectional tunnel. Therefore, the traffic between mobile network node and communicating node follows the same route. Thus, we can count the number of hops in the path from mobile network node to communicating node by following the transmission path. In Fig. 4.3NS1C and 4.4NS2C, the transmission path from mobile network node to communicating node is

$$MNN \rightarrow MR \rightarrow AR(FN) \rightarrow Internet \rightarrow HA \rightarrow Internet \rightarrow CN \tag{4.2}$$

However, in the proposed approach the routing path differs from the classical NEMO. Thus, the transmission path is also different from mobile network node to communicating node. From Fig. 4.3NS1P and 4.4NS2P, we can calculate the transmission path as

$$MNN \rightarrow MR \rightarrow AR(FN) \rightarrow Internet \rightarrow CN \tag{4.3}$$

The delay time for the classical NEMO and proposed approach, can be driven from equations (4.1), (4.2) and (4.3) as follows.

$$\begin{aligned} Delay_{classical} = {} & ProcessingDelay@_{(\text{MNN,MR,AR(FN),Internet,HA,Internet,CN})} \\ & + PathDelay_{between\_(\text{MNN,MR,AR(FN),Internet,HA,Internet,CN})} \\ & + TunnelDelay@_{(\text{MR,HA})} \end{aligned} \tag{4.4}$$

Here, the tunnel processing delay over MR and HA is for encapsulating and decapsulating packets.

$$\begin{aligned} Delay_{proposed} = {} & ProcessingDelay@_{(\text{MNN,MR,AR(FN),Internet,CN})} \\ & + PathDelay_{between\_(\text{MNN,MR,AR(FN),Internet,CN})} \end{aligned} \tag{4.5}$$

Here, we are assuming that the average number of hops and transmission delay in the Internet stays same for both the cases.

In classical NEMO, the transmission path between AR(FN1) and CN has to follow more number of hops due to its tunneled routing in between HA and MR. MR encapsulates each packet and tunnels them towards HA and vice versa. Therefore, the distance between HA and MR determines the added transmission delay. Moreover, MR and HA has to encapsulate and decapsulate each packet which

increases the processing delay on these two nodes. However, the proposed approach avoids the use of this bi-directional tunnels. Thus, the transmission path between AR(FN1 or FN2) and CN has to follow less number of hops compared to classical NEMO without any processing delays for encapsulating and decapsulating the packets. The delay for classical and proposed approaches is calculated theoretically in equation (4.4) and (4.5). The quantitative analysis is presented in the section 4.5.1.2.

4.5.1.2 Testbed measurements

The transmission delay can be estimated by calculating round-trip time. Round-trip time is the time taken to send a packet towards the destination and receive the corresponding acknowledgment. Although the packets do not follow the same route in both the directions yet the measurement of round-trip time can approximately be used to confirm the results of the qualitative analysis.

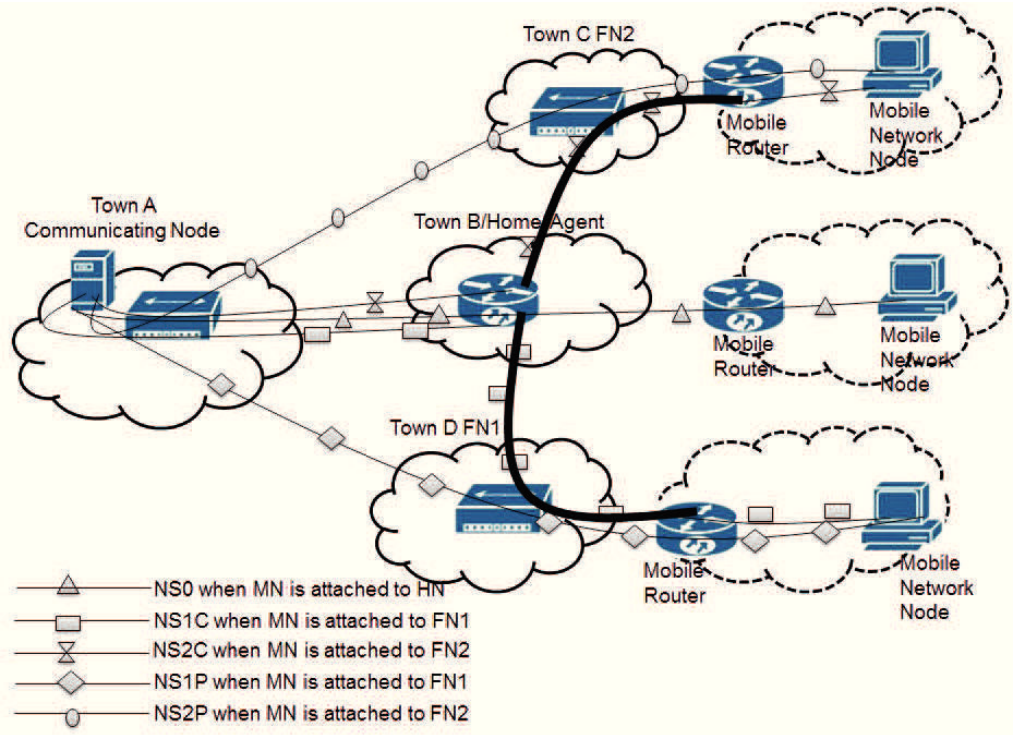

FIGURE 4.5: Network settings for comparing RTT values

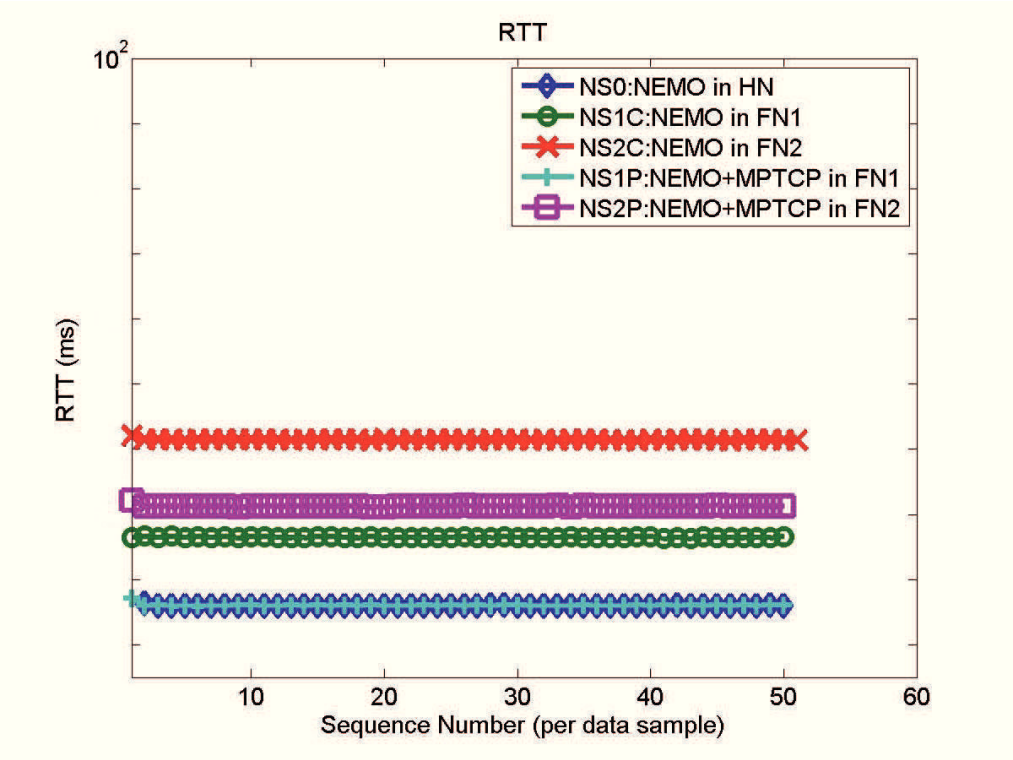

FIGURE 4.6: Round Trip Time measurements for that Network Scenario

In the graph 4.6, we attempt to represent a scenario where the direct distance of communication node from the home agent and the access router in the foreign network 1 is same while the access router in foreign network2 is a little bit closer, as shown in Fig. 4.5. Communicating node and home agent are in town A and town B respectively while foreign network 1 and 2 are in town C and town D respectively. Using the classical approach all the traffic has to travel through town B which increases the round-trip time, whereas, in proposed approach, the traffic flows through legacy Internet route resulting in optimum RTT. The values of round-trip time for classical and proposed approach can be compared for the different scenarios. The curves are produced by measuring round-trip time using "*ping6*" command in the test-bed implementation for each scenario. In this graph, the curve for NS0 and NS2P are overlapping each other while the round-trip time in NS1P is lesser. However, the round-trip time for classical scenarios NS1C and NS2C is higher. In this graph, it can also be seen that the round trip time gain is directly proportional to the distance between the home agent and the mobile network. The distance is simulated by adding some delay with the help of the "*netem*".

4.5.2 Throughput Gain

Throughput is the rate at which any node can process the data. The gain in the throughput is achieved by enhanced routing and by avoiding the tunneling packet overhead, which is calculated in the following subsections 4.5.2.1 and 4.5.2.2.

4.5.2.1 Tunneling Packet Overhead Gain

The bi-directional tunnel in classical NEMO is established by encapsulating the packets. The home agent encapsulates the mobile network's inbound traffic with the mobile router's care-of-address, and the mobile router encapsulates the outbound traffic with the home agent's address. The encapsulation of IPv6 packet of size 1460 bytes, adds 40 bytes of overhead, i.e., 2.74% [115]. Therefore, the classical NEMO adds an overhead of 2.74% on the communication.

However, the proposed approach avoids the use of tunneling except in some scenarios such as in case local fixed node or in a firewall restricted domains. Therefore, for communication, there is a gain of 2.74% in the proposed approach by avoiding tunneling packet overhead.

4.5.2.2 Throughput Gain by Enhanced Routing

Network throughput is directly proportional to the maximum segment size and inversely proportion to the round trip time [116]. Therefore, the increased RTT will result in reduced throughput. In the test-bed experiment, mobile network node receives the data from CN. The throughput is calculated at the mobile network node and the communicating node both with the help of iperf [113] and netperfmeter [114] tools. These two tools provide different throughput measurement options. For the measurement of the throughput, the mobile network node and the communicating node for a client server relation where the mobile network node acts as a client and the communicating node acts as a server. The throughput is measured in three different cases, which are as follows.

1. ***IPERF:*** This utility computes the throughput at the client machine every second by sending 8Mbits data and on the server side,it computes the throughput every 10 seconds on receiving 80 Mbits data. This is the default scenario of the iperf command. Since iperf measures the throughput for a very short duration (10sec), Our purpose from this scenario is to illustrate

the behavior when throughput is measured for a very short duration, as shown in the graphs Fig. 4.7 and 4.8.

2. ***Netperfmeter-Bidirectional:*** This utility measures the throughput when data flows in both the directions in between the client and the server. This is the default scenario provided by netperfmeter for bidirectional data exchange in between client and server. The client is transmitting 10 Mbits and receiving 0.01Mbits per second. Our aim by having this scenario is to demonstrate the throughput for bidirectional communication in between the client and the server for longer duration compared to iperf. The throughput graphs on client and server for this case are shown in Fig. 4.9 and 4.10 respectively.

3. ***Netperfmeter-Unidirectional:*** This feature is used when the client is transmitting 10 Mbits of data in the direction to the server every second. This is the default scenario provided by netperfmeter for uni-directional data exchange in between the client and the server. Our aim by having this scenario is to demonstrate the throughput when measured for longer duration (10 min) in single direction. Fig. 4.11 and 4.12 represent the throughput graphs for this case.

Therefore, iperf provides an assessment of the instantaneous variation of the throughput while netperfmeter provides a long term estimation of the throughput.

The curve NS0 is produced for the scenario when the mobile network is directly connected to the home network. The values for this scenario is same for both the proposed and the classical approach. The curve NS1 and NS2 are produced for the scenarios when the mobile network is connected to the foreign network 1 and the foreign network 2 respectively. NS1C and NS2C are the throughput measurements, when the packets are encapsulated and tunneled via the HA-MR route, i.e., the classical NEMO approach. While the curve NS1P is produced by the throughput when the packets are routed by avoiding the HA-MR bidirectional tunnel with the help of the proposed approach, i.e., the hybridization of NEMO and MPTCP. In the graph, the throughput for the proposed approach scenarios, i.e., NS1P and NS2P, can be compared to the classical approach scenarios, i.e., NS1C and NS2C respectively, considering NS0 as best case scenario.

In all the throughput graphs , i.e., Fig. 4.7, 4.8, 4.9, 4.10, 4.11 and 4.12, the curves for NS0 and NS1P are overlapping each other. The curves NS1C and NS2C can

be compared with the curves NS1P and NS2P respectively. This comparison shows a significant throughput gain by enhancing NEMO with MPTCP.

All the scenarios present fluctuations in the network throughput. One of the contributing factor in the fluctuation of throughput data could be the current version of MPTCP stack, as the throughput measurements for UDP datagrams are consistent. Moreover, it has also been stated that the new versions of MPTCP attempts to reduce latency and jitter compared to the older versions [117].

Using iperf, there are 10 times more number of data sample on client side compared to server side. However, here in the graph Fig. 4.7 we show only limited points in order to avoid congestion in the graph.

From all these throughput graphs, we find that the hybridization of NEMO and MPTCP (NS1P and NS2P) provides better throughput compared to the classical approach (NS1C and NS2C). By considering the average values for each scenario in all the throughput graphs, the throughput gain can be calculated as $15(\pm5)\%$ in case of the foreign network 1 and $30(\pm5)\%$ in case of the foreign network 2. Since the distance of the home agent is more from the foreign network 1 than the foreign network 2, the throughput gain is more in the case of foreign network 2.

The gain by avoiding the tunneling packet overhead with the help of the MPTCP is small, as calculated in the section 4.5.2.1, whereas, the gain by enhanced routing with the help of the MPTCP is significant, as calculated in the section 4.5.2.2. Moreover, the availability of a single available interface shows an improvement in the throughput. Therefore, having more than one interfaces with MPTCP will improve the traffic more as presented in [78].

4.6 Conclusion

In this chapter, a quantitative comparison between the proposed approach and the existing approach has been demonstrated using relevantly chosen scenarios. The novel combination of NEMO and MPTCP, works effectively with the addition of two very small functions in the NEMO functionality on mobile router. With these two small functions mobile router is able to advertise the acquired care-of-prefix in the foreign network 1 and the foreign network 2. This IP address with the acquired prefix is used to route the packets towards the Internet instead of home agent. In the results section, we can see that the proposed approach effectively reduces the round trip time, transmission delay and significantly improves the throughput when compared with the classical approach. This corroborates that

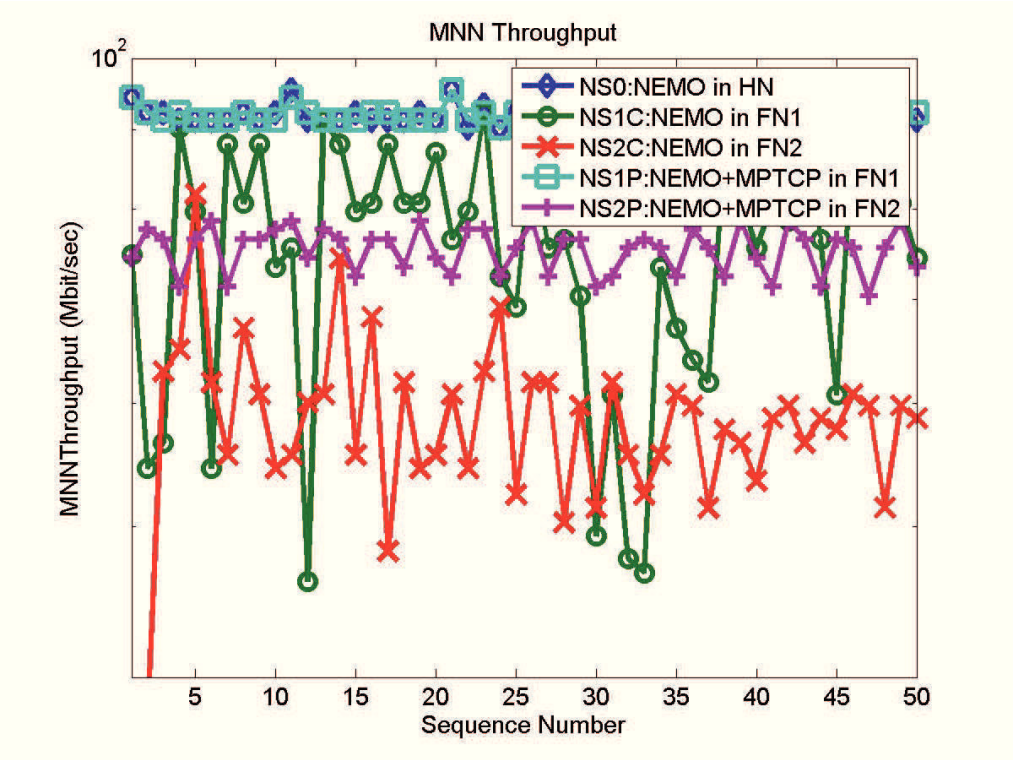

FIGURE 4.7: Throughput over MNN

the novel combination of NEMO and MPTCP indeed provides better network mobility support compared to classical NEMO.

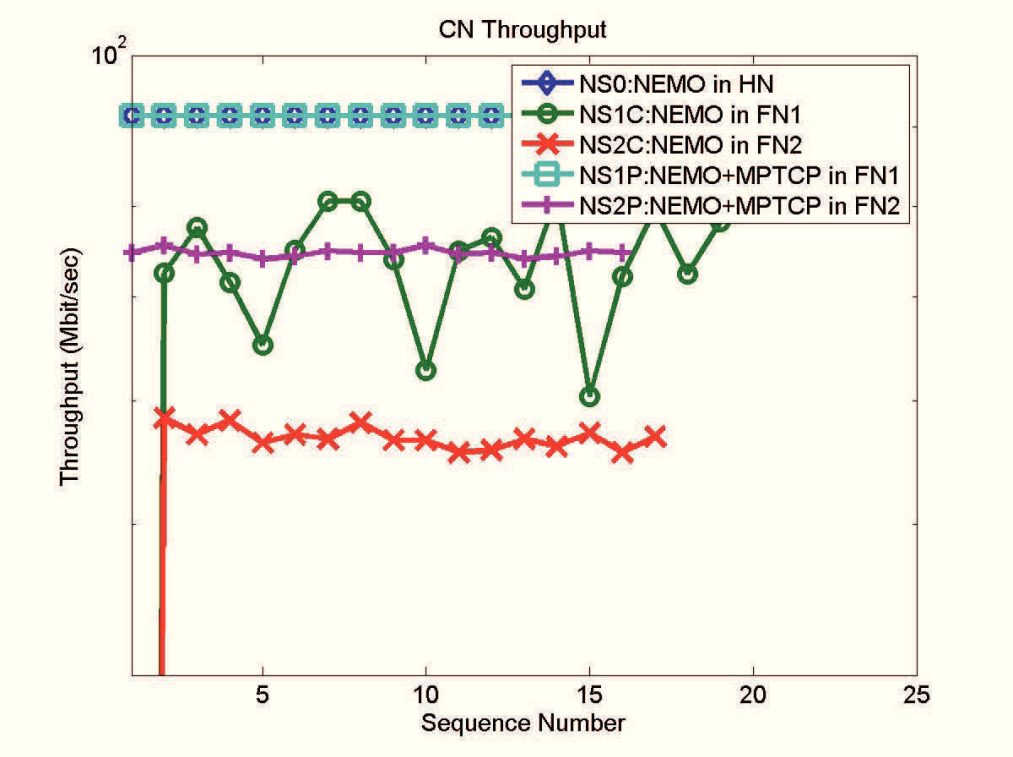

FIGURE 4.8: Throughput over CN

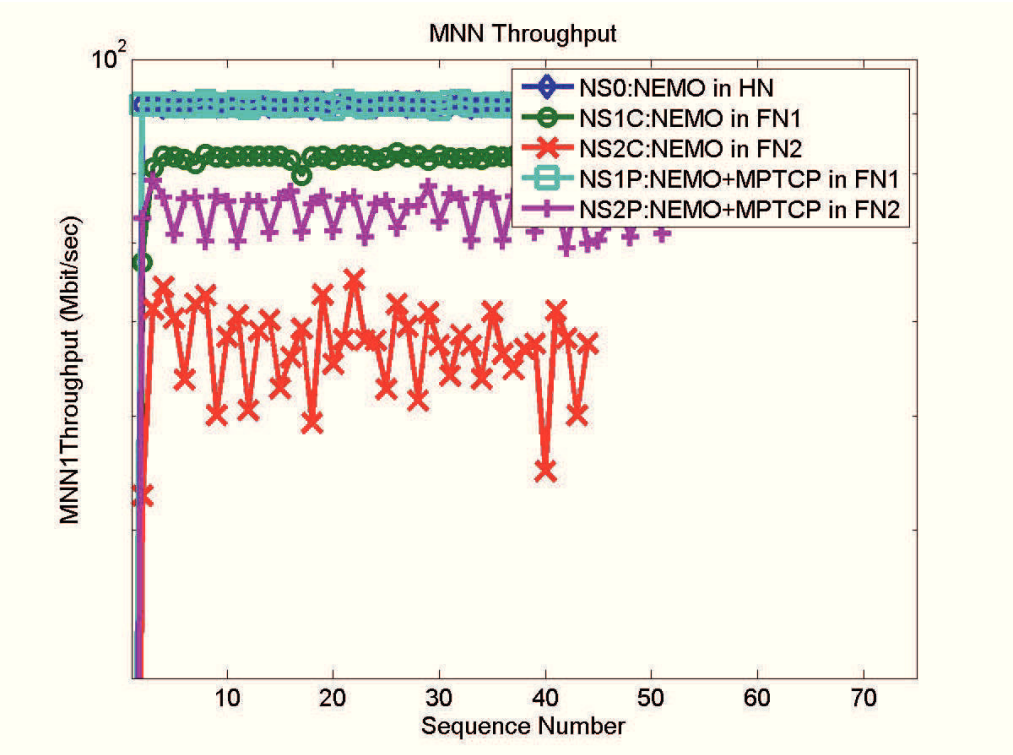

FIGURE 4.9: Throughput over MNN

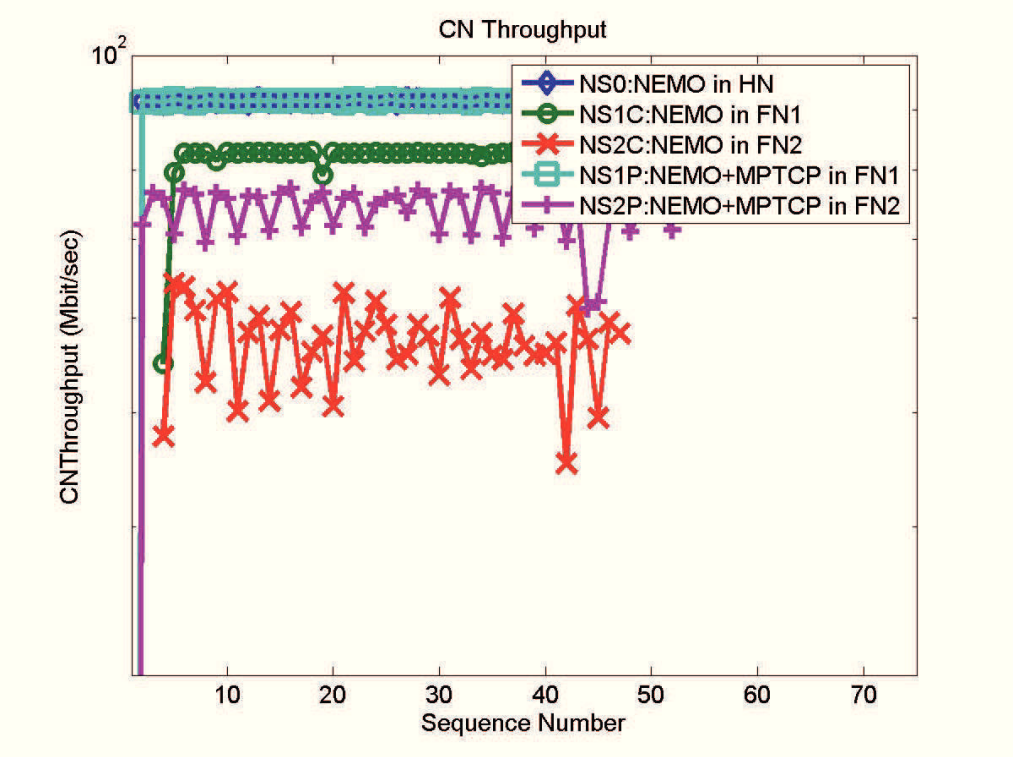

FIGURE 4.10: Throughput over CN

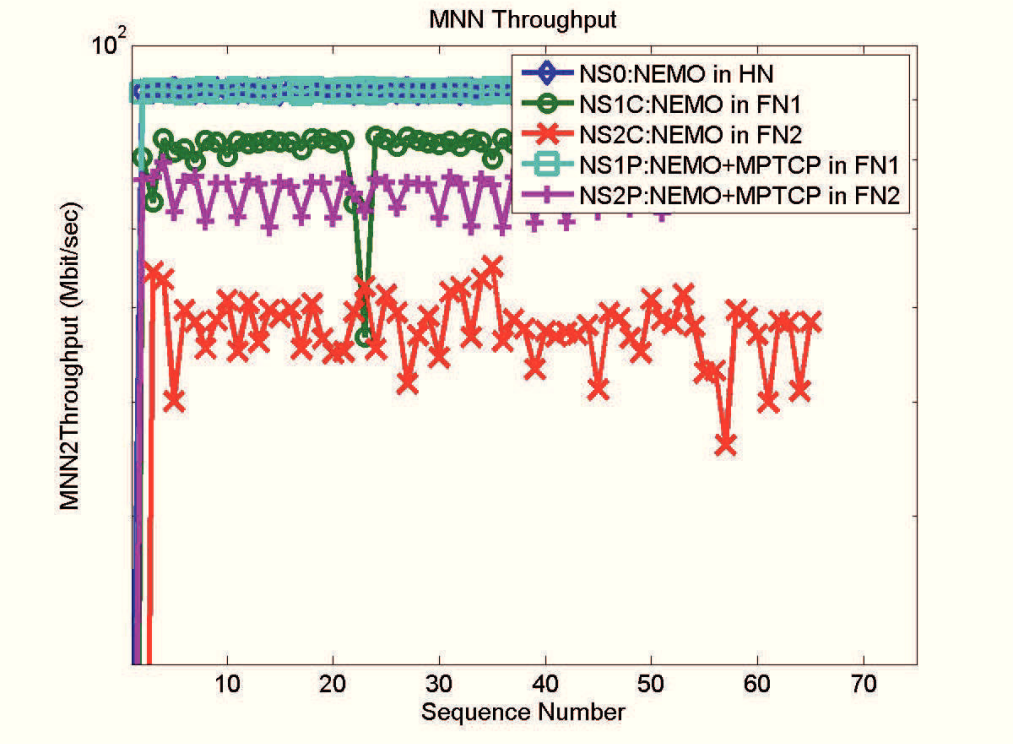

FIGURE 4.11: Throughput over MNN

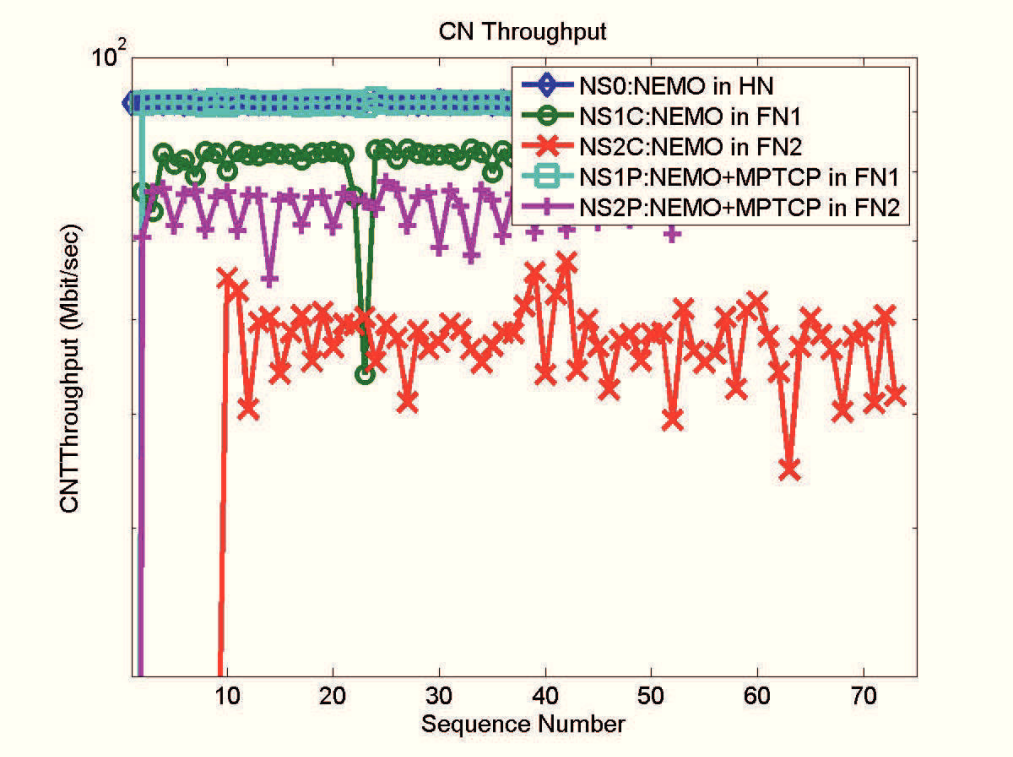

FIGURE 4.12: Throughput over CN

Chapter 5

MultiPath-TCP for Session Continuity in 5G Mobile networks

5.1 Introduction

The reported work is obtained within a close collaboration with my colleague Souheir Eido [118], A. This work has partly been published in [118] and an extended presentation of the reported work is given in Appendix A. My contribution in this work mainly consists analyzing existing multihoming solutions in the context of content distribution in 5G networks and provide a way to use them for solving the mobility issue in 3GPP SIPTO mobility use cases.

The growth of the data traffic has lead to the evolution of the network, technology, handsets, etc. in order to provide better bandwidth, speed, QoS, data and many more attractive technical features. This evolution has made possible to handle the exponential growth in the number of users and the resulting data traffic. This never ending demand and supply chain has lead the current mobile network architecture i.e. 4G to evolve in the next generation network, i.e., 5G. In 5G, this foreseen exponential growth of data traffic has lead to the proposals of putting the IP edge nearer to the user with application servers (e.g., video caches), in 5G [12] [119], as illustrated in Fig. 5.1. In COMBO, the proposed idea is to unify all the gateways of all technologies (i.e., fixed, mobile, and Wi-Fi) within a unified entity known as Universal Access Gateway (UAG), having Next Generation - Point of Presence (NG-POP) where the global IP edge, servers, and data centres are co-located, as shown in Fig. 5.2. This would certainly realize more efficient control

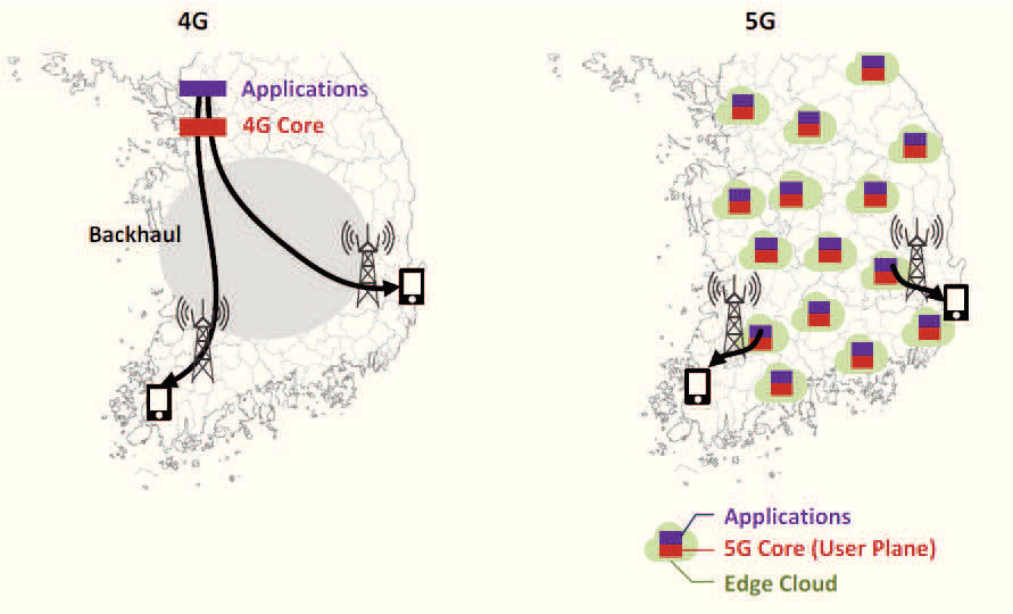

FIGURE 5.1: 5G era envisioned by KT - Core nodes (user plane) distributed to tens of edge nodes nationwide(source [119])

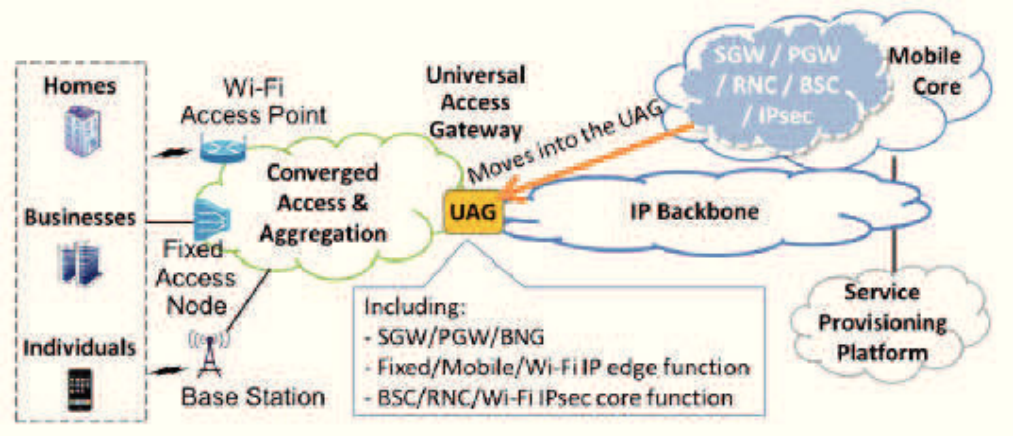

FIGURE 5.2: Convergence of fixed,mobile,and Wi-Fi gateway functionalities. SGW, serving gateway; PGW, packet data network gateway; BNG, broadband network gateway.(source [12])

functionalities and reduce the data traffic in the core network but at the cost of new issues to be taken care, for, e.g., user's mobility in between two locations which requires a gateway relocation. Since a user can only be connected to a single SGW and PGW at any given time, the session preservation becomes an issue during the occurrence of any mobility event requiring gateway relocation.

5.2 Problem Statement and Brief Background

To alleviate the traffic load in the core network, 3GPP has proposed two methods to offload the selected IP traffic using SIPTO (Selected IP Traffic Offload). SIPTO breaks out the part of traffic either at (or above) the radio access network by choosing an SGW/PGW that is geographically closer to the user or at local network within the residential or enterprise IP network [20], [22]. SIPTO at local network allows a UE to directly access the private IP network services using a Local Gateway (LGW) towards the external IP network [120]. LGW supports some PGW and SGW functions such as UE's IP address allocation and DHCP (or DHCPv6 for IPv6) functions, downlink packet buffering as well as direct tunneling towards the eNB respectively. SGW & PGW can be as separate entities (i.e., standalone) or can be co-located. Similarly, LGW can be as an independent entity or co-located with eNB (i.e., Home eNB).

3GPP has defined three use case scenarios for SIPTO, based on the configuration of SGW and PGW or LGW in the network, in [20].

1. Standalone SGW and PGW.
2. Co-located SGW and PGW.
3. LGW co-located with Home enodeB.

These three scenarios are illustrated in Fig. 5.3. In the scenario (a), the user/Alice is accessing the Internet services on its smartphone via eNodeB1. The network is offloading a part of its data using SIPTO scenario 1, i.e., standalone SGW and PGW, e.g., serving a video streaming request from a cache which is geographically closer to Alice's current location. Now, while streaming the video, Alice moves from location 1 to location 2. Location 2 is covered by eNodeB2 which is connected to a different SGW. This movement between eNodeBs raises a need of handover for the SIPTO traffic. However, in this scenario, the IP address of the user does not change as the PGW which allocates the IP address remains same. Therefore, this traffic can be handed over using Intra LTE handover methods with the help of the MME, as explained in [17].

In the scenario (b), the user/Alice is accessing the Internet services while travelling in a bus or train. This time, the network is offloading a part of traffic using SIPTO scenario 2, i.e., SGW co-located with PGW. Since her smartphone is connected to two PGWs, she is having two active IP addresses, e.g., IP_{LTE} and $IP_{SGW/PGW}$. Let's assume that she is playing a game and the network

is offloading this traffic using $IP_{SGW/PGW}$ via eNodeB1. Since the bus is on move, Alice moves from eNodeB1 to eNodeB2 while playing the game. These eNodeBs are connected with different SGWs co-located with PGWs. Therefore, the UE of Alice, will be assigned a new IP address from the new PGW, i.e., $IP_{NEW-SGW/PGW}$. The old IP address $IP_{SGW/PGW}$ will become unreachable now, which would break the ongoing session and disrupt the game.

In the scenario (b), the user/Alice is accessing the Internet services while walking in a big university campus. This time, the network is offloading a part of traffic using SIPTO scenario 3, i.e., LGW co-located with Home eNodeB. Since her smartphone is connected to PGW and LGW both, she is having two active IP addresses, e.g., IP_{LTE} and IP_{LGW}. Let's assume that she is watching a video and the network is offloading this traffic using IP_{LGW} via home eNodeB1. While walking she goes from one building to another building. Since these buildings are having different home eNodeBs which are co-located with LGW. Therefore, Alice's smartphone, will be assigned a new IP address from the new LGW, i.e., $IP_{NEW-LGW}$. The old IP address IP_{LGW} will become unreachable which would break the ongoing session and disrupt the video streaming. Therefore, in order to maintain the session continuity, the traffic should be transferred towards the new acquired address.

Therefore, for SIPTO scenario 2 and 3, there is a need to establish an end-to-end tunnel in between the UE and the server with a solution for handing over the traffic (already transferred packets) from the previous gateway towards the new one. Since the content server is always stationary, the switching of network paths (i.e. IP addresses) is a particular case of multihoming scenario, where the traffic is switched in between two IP addresses due to either traffic characteristics or unavailability of one IP address. Therefore, the problem of transferring the ongoing session from $IP_{SGW/PGW}$ or IP_{LGW} to $IP_{New-SGW/PGW}$ or $IP_{New-LGW}$ can be solved with the help of existing multihoming solutions. However, handover would require some additional functionalities in the mobile network.

5.3 Qualitative Analysis of Multihoming Approaches

As discussed in chapter 2, there are several multihoming solutions. For this problem, we are going to consider only the host multihoming solutions which are host identity protocol (HIP) [121], Site Multihoming by IPv6 Intermediation (SHIM6) [89], Stream Control Transmission Protocol (SCTP) [67] and Multipath

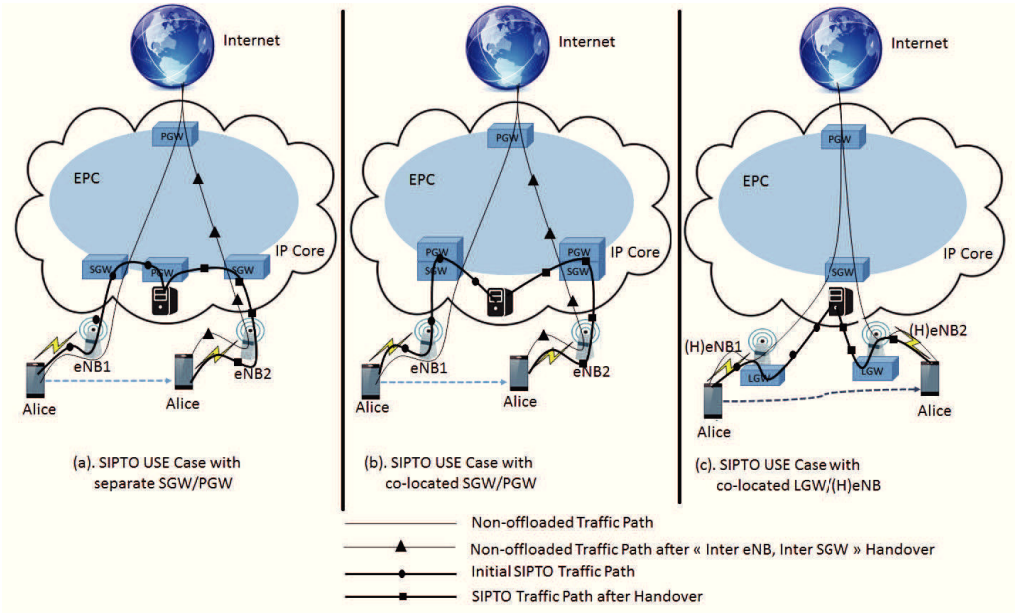

FIGURE 5.3: Selected IP Traffic Offload Use Cases

TCP (MPTCP) [75]. The primary parameter while analyzing the existing multihoming solution is to introduce minimum possible changes to the existing network architecture. The solutions should also be compatible with both IPv4 and IPv6 hosts. Using these parameters, the multihoming approaches are analyzed below. This analysis is summarized in Table 5.1.

- The application of HIP approach will require modification in both host and server host stakes in order to solve multihoming in the discussed scenario, due to its introduction of a new hip layer in between network and transport layer in TCP/IP stack. Moreover, this approach would require an introduction of a new namespace for host identifiers and a rendezvous mechanism which will eventually lead to the additional cost of deployment. To solve multihoming, these host identifiers should also be compatible to 3GPP standards.

- The application of SHIM6 approach would be compatible only with IPv6 hosts whereas, in 3GPP, IPv4 is still the main mode of communication.

- The application of SCTP approach would require the changes in the applications to be compatible with it. This would be included in infrastructure changes as changing all the existing applications is not an easy task. SCTP has an extension for concurrent-multipath streaming (CMT-SCTP) [73] in order to provide load balancing using multiple available paths simultaneously.

Table 5.1: Qualitative Analysis of The Multihoming Approaches

	Modification in the Host Protocol Stack	Transparency to the applications	Compatible with IPv4 and IPv6	Compatible with the Legacy Internet
HIP	Yes	No	Yes	No
SHIM6	Yes	Yes	No	Yes
CMT-SCTP	Yes	No	Yes	Yes
MPTCP	Yes	Yes	Yes	Yes

- The application of MPTCP approach would only require the hosts to support MPTCP to be benefited by multihoming features. MPTCP is also backward compatible with the legacy hosts in the Internet and works for IPv4 & IPv6 both the hosts. Moreover, this approach is also compatible to 3GPP standards.

From Table 5.1, MPTCP appeared to be the most efficient solution to solve mobility in the given scenario. Like TCP and UDP, MPTCP is another transport layer protocol which can create different subflows (i.e., separate TCP connections) for a given session using all the possible combination of IP addresses between two communicating hosts. The use of MPTCP does not require any changes in the legacy routing and the connection initiation. The connection initiation is also compatible with all the legacy host as it performs the same 3-way handshake, i.e., used for establishing a TCP connection with the TCP header. The only difference is that the MP-CAPABLE option is added to the TCP header of SYN packet while initiating an MPTCP connection. Once the connection is established, both the peer host are aware of multiple available addresses. So, the host can initiate another subflow using MP-JOIN option in the TCP header using the same cryptographic key which is generated while initiating the connection. This key is used to create a secure connection. After having more than one subflows, the hosts have an option to decide whether all the subflows to be used or a specific one. The session is identified by a specific sequence number in the TCP header (i.e., Data Sequence Number) of each subflow. This sequence number is also used for packet re-ordering.

The subflows can be created and removed during an ongoing session due to a new active interface or due to an old interface to become inactive respectively. These subflows are seen as a single TCP session to the application layer.

5.4 MPTCP-based solution for Mobility

Initially, UE has an IP address assigned by the global PGW, whenever it attaches to the LTE network. Using this IP address, UE establishes an MPTCP connection with the content server assuming that both UE and content server are MPTCP compliant. Since this IP address is always available whenever the user is attached to LTE, it can be used for MPTCP related signaling such as creating or removing a subflow. After the connection establishment, on behalf of UE, MME requests to establish an SIPTO data path to the content server, thus it receives another IP address from the nearest gateway (co-located SGW&PGW or LGW). This IP address is then communicated with the content server using MP-JOIN option, and a new subflow is created. This new subflow (i.e., SIPTO data path) is used for downstream data traffic and the subflow with the initial IP address is put as a backup path using MP_PRIO option.

5.4.1 Smooth SIPTO Handover

During mobility whenever user moves from one eNodeB (Source eNB) to another eNodeB (Target eNB), Source-eNB sends a signal strength measurement request from UE. On the reception of the reply from UE, Source eNodeB takes a handover decision and sends a ”handover required" message to the MME. The MME then selects a gateway for the UE that is geographically closer to the UE. The UE acquires a new IP address from the current SGW&PGW or LGW it is attached to and a new SIPTO connection is established. Then, it notifies the content server to add this new IP address using MP-JOIN option. Once the content server receives the MP-JOIN option, it can initiate a new subflow using the new IP address. The UE's IP address allocated by the previous LGW (or co-located SGW&PGW) becomes unreachable during the course of connecting to the new gateway (LGW or SGW&PGW), acquiring a new IP address and creating a new subflow with it. During this time, there is some traffic which has been already transferred to the previous gateway (source LGW or source SGW). Therefore, a smooth handover needs to be performed in between source and target gateways.

In the case of co-located SGW&PGW relocation, MME must initiate the handover even when a PGW relocation is required and keep the existing connection active until the handover is finished. An indirect forwarding tunnel is then established between source and target SGWs. The handover is performed similar to the “inter eNB/inter SGW” handover procedure defined in [122].

In the case of LGW relocation, for performing a handover between source and target LGW, the notion of "Proxy-SGW" is proposed by my fellow colleague Souheir in the 3GPP architecture with SIPTO at the local network. This proxy-SGW function is installed on the LGW. HeNB and LGW are only the entities which are aware of its existence. The rest of the network will remain as it is.

The proxy-SGW function performs an inter HeNB/inter Proxy-SGW handover over the S1 interface between the HeNB and the Proxy-SGW. For this, HeNB needs to be enhanced to enforce an S1 based handover for the users with on-going SIPTO@LN sessions. Moreover, MME must be able to select a target LGW/Proxy-SGW. MME then establishes an indirect tunnel between the source and target Proxy-SGW/LGW. For the tunnel establishment, a functionality needs to be added on LGW for forwarding all the messages received from SGW related to an "indirect tunnel establishment" towards proxy-SGW. In the mean time, UE is not connected to the target LGW; therefore, it receives a new IP address.

After the establishment of an end-to-end tunnel in between source and target gateways and the traffic can be handed over. During the handover, UE notifies the server to remove the previous IP address and removes the subflow with the previous IP address. Once the handover is finished, then only the previous connection needs to be deactivated by the MME.

The above explained MPTCP signaling has been illustrated in Fig. 5.4. Here, we should mention that the multihoming ability of MPTCP is used only for providing session continuity. The two subflows are used simultaneously only during handover. After the completion of the handover, the previous subflow is removed. Only the currently active link is used for downstream data. We should also mention that we assume that both UE and content server are MPTCP compliant while explaining the proposition. For the elements which are non-MPTCP compliant the use of proxy MPTCP is explained in the section 5.5

5.5 Non-MPTCP Compliant Elements

There are two ways to enable MPTCP on a host, either by an inbuilt support or by using MPTCP proxy. Using either of these methods, a host can use all the multiple available connections.

MPTCP proxies are the static point in the Internet with respect to the host. Therefore, for solving mobility using MPTCP the host/UE has to be MPTCP

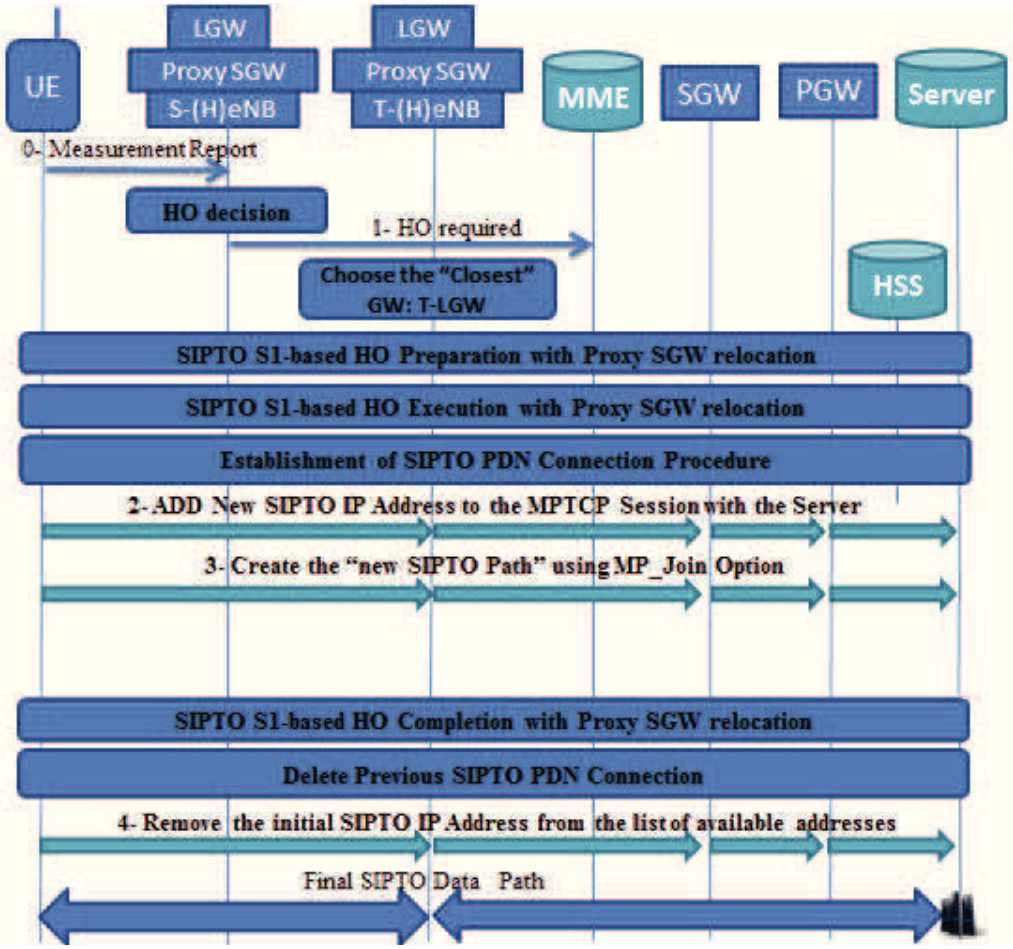

FIGURE 5.4: Session continuity with MPTCP in SIPTO Scenarios

compliant. If UE does not have inbuilt support for MPTCP, a lightweight proxy can be installed on the UE as explained in [81].

If the content server is non-MPTCP compliant, the placement of the proxy MPTCP should be closer to the content server. Therefore, as discussed in the introduction, NG-POP (proposed in [12]) is the ideal place for the placement of proxy MPTCP. This placement ensures no relocation of proxy MPTCP during an ongoing session.

5.6 Conclusion

Thanks to MPTCP, the mobility in both the use cases can be solved with some added functions in 3GPP without modifying anything in the EPC. The proposed MPTCP-based smooth SIPTO solution significantly reduces the handover delay from 500ms to 150ms, during the mobility of UEs having an SIPTO at Local Network and/or SIPTO above RAN services. The ceiling of the delay is set

150 ms for conversational videos and 300ms for non-conversational videos [123], which will allow the user to continue its video streaming session with the delay of 150ms.

This work is in detailed explained in the appended paper A.

Chapter 6

Conclusion and Perspective

6.1 Conclusion

The first contribution in the thesis provides an enhanced solution for multihoming in case of vehicular mobility using MPTCP. We proposed an effective approach for boosting network mobility through a novel combination of NEMO and MPTCP requiring minimal changes in their existing functionalities. These two new functionalities will enable mobile router to advertise its acquired care-of-address and route the packets using it. The proposed approach has also been analyzed theoretically and using a local testbed implementation. The implementation of local testbed gives a clear advantage of the existing approach and problems associated with these.

The existing solution for network mobility i.e., NEMO introduces an inefficient routing, additional packet tunneling overhead, increased transmission delay, increased round-trip time and reduced fault tolerance. Moreover, it does not take user choices dynamically into account while performing interface selection in case of multihoming. Our proposal of hybridizing NEMO with MPTCP, has effectively improved the existing solution. From theoretical and quantitative analysis, it can be concluded that the proposed approach shows the enhanced features discussed below:

1. Significant improvement in the routing compared to classical NEMO by following the legacy Internet routing path.
2. Significant amount of throughput gain, i.e. $15(\pm 5)\%$ minimum is shown in our local testbed implementation. Moreover, the gain keeps on increasing as mobile networks travels farther from home network.

3. Significant reduction in delay performance by reducing transmission delay and round-trip time by taking the shortest possible route in the Internet. The gain in round-trip time will also increase with the distance between mobile network and home agent (home network).

With all the above enhancement, the proposed approach also reduces tunneling packet overhead by 2.75%, increases fault tolerance, allows mobile node to participate in mobility and multihoming related decisions.

The proposed approach enables the established connection to survive as long as there is available a single active path. Moreover, it enhances the performance of the communication by using MPTCP when compared to TCP [102]. Therefore, this novel integration of NEMO and MPTCP provides much better network mobility with enhanced multihoming support compared to classical NEMO.

The other contribution of this work is providing a solution for session continuity in context of content distribution in 5G networks. In 5G network, the IP edges will be closer to the host nodes in order to improve the user experience and reduce traffic load in the core network. Moreover, a part of traffic is offloaded into the access network by putting the video caches locally or near to Home(eNBs). The fact that a host can only be connected to a single gateway (SGW&PGW or LGW) at a time, would break the ongoing sessions for real time applications like video streaming or gaming during an occurrence of mobility event requiring gateway relocation. The thesis presents the solution for session continuity with the help of MPTCP. Since, the content servers are stationary only the user is mobile, this makes the switching of network paths similar to multihoming. The use of multipath TCP enables a user to switch in between available network paths with session continuity.

6.2 Perspective

In this thesis, we present a unification of network layer protocol NEMO and transport layer protocol MPTCP. This unification improves the routing and throughput for the nodes in the mobile networks, e.g., car, or bus or boat etc. It would also be useful in the real-time scenario to avoid tunnels. However, the proposition requires HA-MR tunnel for all the incoming connection requests. This HA-MR bi-directional tunnel is also used for the exchange of binding updates. Therefore, as a future work it would be interesting to study if Proxy Mobile IPv6 (PMIPv6) can be extended to support mobility for a network and how its unification with

MPTCP can be used to enhance the mobility support. PMIPv6 reduces the length of tunnels compared to NEMO. Moreover, PMIPv6 will provide a network oriented and hierarchical solution for network mobility. In PMIPv6, there is a local mobility anchor which handles the host mobility inside a domain, instead of HA. The application of PMIPv6 is expected to avoid tunnels between the home network & the foreign network and enhance the routing during the connection establishment for outbound traffic. However, PMIPv6 is a solution for host mobility therefore, it needs to be enhanced in order to support network mobility. This can further be extended by the distributed mobility management in all IP network where the home agents or local mobility anchors are distributed.

In the Internet of things, where machine to machine communication is one of the features of the network, also the nodes will be mobile and multihomed; it would be interesting to study the vehicular interconnection in respect of IP networking by applying this unification of the network and the transport layer approaches. The current thesis contains the study of a mobile network with respect to a fixed node in the Internet, when applying NEMO with MPTCP. This study can be enhanced to observe the behavior of the communication between two mobile networks (e.g., cars or boats) having NEMO and MPTCP. In this scenario also, it is expected that the unification of NEMO and MPTCP will be able to improve the routing, the quality of service etc. Since the communication is initiated by a node inside the mobile network, the fixed point in the Internet, i.e., the home agent can be avoided for this communication. This communication can be done in ad-hoc way. However, there is always a fixed point in the Internet for the incoming traffic. The impact of this study is useful for with respect to mobile ad hoc networking for automating the future communication [124], [125], [126]. If we consider the examples of ships in the deep sea, it would be beneficial to receive the information such as current weather reports or streaming the international news from the peers rather than via satellite. Also, the communication between the cars makes it useful for automating the driving such as in google self-driving car. The enhancement of NEMO by combining MPTCP will make the communication between two vehicles faster by reducing the delay.

Mobility poses security threats as discussed in [127]. Since the IP address of the host changes and there are no ways to identify the host which makes the communication vulnerable to security threats. There exists several type of security threats such as address spoofing, man-in-middle attack or denial-of-service etc. In man-in-middle attack, the attacker tries to modify the packets. While in address spoofing, the attacker injects the packets claiming that these are coming from the communicating node. Another type of attack, Denial of Service, where

the attacker is trying to make the system slow or paralyze rather than taking control of the system. The proposed solution fails to provide a higher degree of security than already exists in the Internet. Therefore, in order to improve the security standards, the mobility solutions need some additional features such as some signature or some cryptographic key may be added to the binding updates between the mobile router and its home agent. This is also an interesting direction to explore.

Publication

Journal

1. Souheir Eido, Pratibha Mitharwal, Annie Gravey and Christophe Lohr. "Smooth Handover with SIPTO-Based Mobile Access." (submitted)

Conference

1. Mitharwal, Pratibha, Christophe Lohr, and Annie Gravey. "Survey on Network Interface Selection in Multihomed Mobile Networks." Advances in Communication Networking. Springer International Publishing, 2014. 134-146.

2. Mitharwal, Pratibha, Christophe Lohr, and Annie Gravey. "Boosting NEMO with multi-path TCP." Network of the Future (NOF), 2015 6th International Conference on the. IEEE, 2015.

3. Souheir Eido, Pratibha Mitharwal, Annie Gravey and Christophe Lohr. MPTCP solution for seamless local sipto mobility. HPSR : 16th International Conference on High Performance Switching and Routing, 01-04 july 2015, Budapest, Hungary, 2015.

4. Mitharwal, Pratibha, Christophe Lohr, and Annie Gravey. "Quantitative Analysis of Boosting Network Mobility through the Hybridization of NEMO and MPTCP." (submitted)

Appendix A

Smooth handover with SIPTO-Based Mobile Access

A.1 Abstract

In this article, we propose a novel approach for a “Smooth handover with SIPTO-based Mobile Access" supporting seamless mobility. Session continuity and data path selection have been considered as key issues to be solved within 3GPP, as none of the solutions proposed for Mobile IP directly apply in the context of LTE. As in some cases, typically when SIPTO relies on using Local Gateways or a Packet Data Network Gateway that is closer to the user's location, it is necessary to change the IP address allocated to a User Equipment, an active session may be interrupted. We propose an MPTCP based solution within the LTE architecture to maintain a single session, initially carried over a given SIPTO connection, and then carried over another SIPTO connection initiated due to the mobility of the user. We identify how MPTCP operates over the LTE architecture, and estimate whether the corresponding delay is compatible with session continuity.

A.2 Introduction

Data traffic is going through an exponential growth, which is expected to become, within the next few years, dominant in both fixed and mobile networks. As a result of this tremendous pace of expansion, network operators are increasing their network capacity by deploying a distributed content distribution architecture with data centers (DC) and Video-on-Demand (VoD) servers located closer

to the users, typically in every large or medium town. The deployment of such Content Distribution Network (CDN) would help reducing both CAPEX and OPEX costs [128] as well as server loads and latency delays for end-users.

The current Long Term Evolution/System Architecture Evolution (LTE/SAE) or the so-called “4G" mobile architecture is based on routing user’s traffic through an end-to-end tunnel starting from the User Equipment (UE) and ending into a Packet Data Network GateWay (PDN-GW or PGW), which allows the UE to access the IP backbone and the Internet [122].

The use of an end-to-end tunnel secures the connection and allows a seamless mobility with high QoS for mobile users. However, even when a user requests a content that is available in a geographically close server, the requested traffic must first be sent to the PGW in the Evolved Packet Core (EPC) network and then be tunneled and sent toward the UE. This sub-optimal routing leads to a loss of network resources [128].

3GPP has proposed the Selected IP Traffic Offload (SIPTO) approach in [20] in order to selectively breakout some of the mobile IP traffic either directly at the local network using femtocells or above the Radio Access Network (RAN) using macrocells. One of the main objectives of using SIPTO is to ensure a better mobile connectivity service; i.e. a UE shall always use the best available data path towards the external IP network. SIPTO re-assigns new PGWs that are geographically closer to the current UEs locations, either co-located with the radio base station or represented as separate entities. Consequently, non-offloaded traffic could be routed towards the EPC network while SIPTO traffic would be offloaded within the access/metro segment of the network. According to [128], the use of SIPTO could save more than 30% of bandwidth used in backbone and up to 15% of bandwidth used in the metro/core segment of the network.

In [12] and [119], the authors present the idea to distribute several IP edge nodes closer to the users within the access and/or aggregation segments of the network, having application servers (e.g., video caches) also distributed closer to the IP edge nodes. In [12] Gosselin et al. propose to integrate the IP edges of fixed, mobile, and Wi-Fi access networks within a functional entity known as Universal Access Gateway (UAG), in future converged fixed and mobile networks. The co-location of such a UAG with application servers and data centers within a so-called Next Generation Point of Presence (NG-PoP) would allow a more efficient control of network resources.

3GPP has identified, in the framework of SIPTO ([20] and [22]), some mobility use cases where session continuity is not supported due to the fact that mobility of UE's with PGW relocation implies modifying the UEs IP address.

In the present article, we propose a solution to provide seamless mobility during PGW relocation. This solution relies on the Multi-Path Transmission Control Protocol (MPTCP) proposed recently by IETF [75].

MPTCP enables any host to use multiple available network interfaces simultaneously for a single TCP session. Each interface carries a subflow of a single TCP session presented to the application layer. The use of multiple available network interfaces can hopefully improve throughput by spreading data traffic over different data paths. Our main idea is to associate the multiple addresses obtained through different PGWs to a given session in order to provide mobility support.

The rest of the paper is organized as follows. Section A.3 presents the state of the art for classic LTE, SIPTO, MPTCP and discusses SIPTO mobility use cases with respect to session continuity. Section A.4 outlines related works. Section A.5 presents a Smooth handover for users with SIPTO connection relying on MPTCP for providing session continuity. Section A.6 evaluates the interruption time of the Smooth handover solution for SIPTO connections. Section A.7 outlines mapping the proposed SIPTO handover solution on a fixed and mobile converged topology. Finally, Section A.8 concludes the paper.

A.3 State of Art

This section presents an overview of classic LTE architecture and SIPTO for mobile data offloading. It then presents some mobility use cases where session continuity for users with multiple IP addresses can be an issue. Finally, the basic architecture of MPTCP protocol is outlined.

A.3.1 Classical Mobile Architecture

Mobile networks rely on IP to support both signalling traffic (control plane) and user data traffic (data plane).

Figure A.1-a shows the classical mobile signalling and data paths. The latter uses an end-to-end tunnel between the UE and the PGW. Considering the example when a user is using his phone to access an application server, first an IP

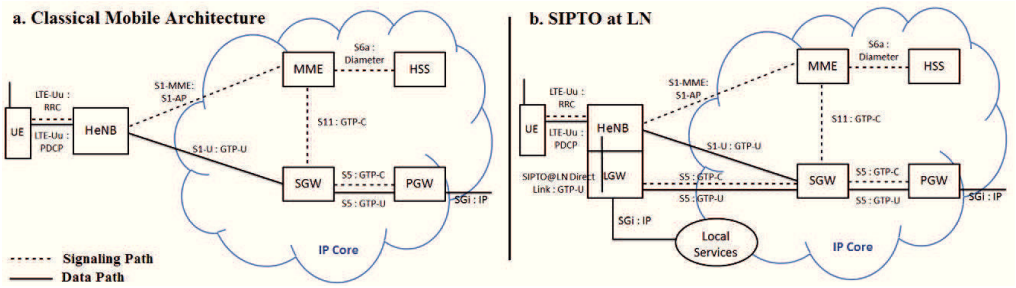

FIGURE A.1: Evolution of Mobile Network's Signaling and Data Paths

packet would be created at the UE's level. This packet consists of actual data by application, TCP or UDP header for transport and then IP field information which has source address of UE and destination address of application server (e.g. Youtube). The IP packet is routed from the UE to the radio base station (eNB) or Home eNB (HeNB) over the LTE-User Universal-Mobile-Telecommunications-System (LTE-Uu) air interface with Packet Data Convergence Protocol (PDCP). Once received, the IP packet would be encapsulated inside a GTP header which has information related to tunnel identifications (TEIDs) and then encapsulated inside a UDP and IP header and forwarded as ethernet frame towards the SGW over the (S1-U) interface with General-Packet-Radio-Service Tunnelling Protocol (GTP-U) of user plane. The IP header of the packet will now contain (H)eNB IP as a source address and SGW IP as a destination address. Finally, the SGW encapsulates the packet inside a GTP header and then inside a UDP and IP header and forwards it to the PGW over the S5 interface with the GTP-U protocol. Furthermore, signaling paths are built with:

- Radio Resource Control (RRC) protocol on the LTE-Uu air interface between the UE and the (H)eNB.
- S1 Application Protocol (S1-AP) on the S1-MME interface between the (H)eNB and the MME.
- GTP-Control (GTP-C) protocol on the S11 interface between the MME and the SGW and the S5 interface between SGW and PGW.
- Diameter protocol on the S6a interface between the MME and the HSS.

In the currently deployed mobile architecture, network operators typically deploy a small number of SGWs and PGWs. This makes sense as long as the amount of data traffic carried over LTE is small. However, this shall not probably be true in the near future as mobile data traffic is expected to grow at a compound annual growth rate of 53% from 2015 to 2020, reaching 30.6 exabytes per month in 2020

[129]. This traffic growth includes the growth in traffic for video applications such as video streaming, video conferencing, etc., which is expected to reach 75% of the overall mobile data traffic, by 2020. In order to accommodate this growth, 3GPP has considered a distributed LTE architecture, as a key solution for a future 5G network. The basic idea is to distribute small radio base stations within the local residential network and mobile IP edges (SGWs and PGWs) within access and metro segments of the network under Selected IP Traffic Offloading approach. These proposals are presented in more details in the next subsection.

A.3.2 SIPTO Architecture

SIPTO was first defined within 3GPP SA2 group in [20] in order to alleviating traffic load on the mobile core, aggregation and access networks. In particular, SIPTO allows breaking out a selected IP traffic (e.g., Internet) above the RAN, i.e., beyond the eNB. The basic idea is to select a SGW and a PGW that are topologically/geographically close to the UE.

According to 3GPP in [122], a UE can only be connected to one SGW at a time. Therefore, at the establishment of a SIPTO connection, the Mobility Management Entity (MME) selects its preferred SGW. SIPTO above RAN architecture relies on the same architecture model and concepts of LTE network described in [122]. Consequently, the selected SGW and PGW might either be co-located together in a single gateway or separated (standalone) from each other within different equipment. 3GPP uses the term "standalone" for this latter case. SIPTO has been extended by 3GPP in [22] in order to support breaking out a selected IP traffic within the residential or enterprise IP network, or at local network (LN). SIPTO at LN allows a UE to directly access the private IP network services using a HeNB with a co-located or a separated (standalone) Local Gateway (LGW) [120]. The LGW is also the gateway towards the external IP network. It supports especially PGW functions such as UEs IP address allocation and DHCP (or DHCPv6 for IPv6) functions. Moreover, LGW supports some of the SGWs functions such as downlink packet buffering as well as direct tunneling towards the HeNB, although it is not a full SGW since the UE is already linked to a different SGW for its non-SIPTO traffic. For the user's uplink packets, traffic is first routed towards the HeNB and then filtered by its destination's IP address and tunnel ID to be sent to its adequate destination (LGW or SGW).

SIPTO at LN network architectures introduce new signaling and data paths using the existing protocols defined in mobile architecture [122]. An S5 interface

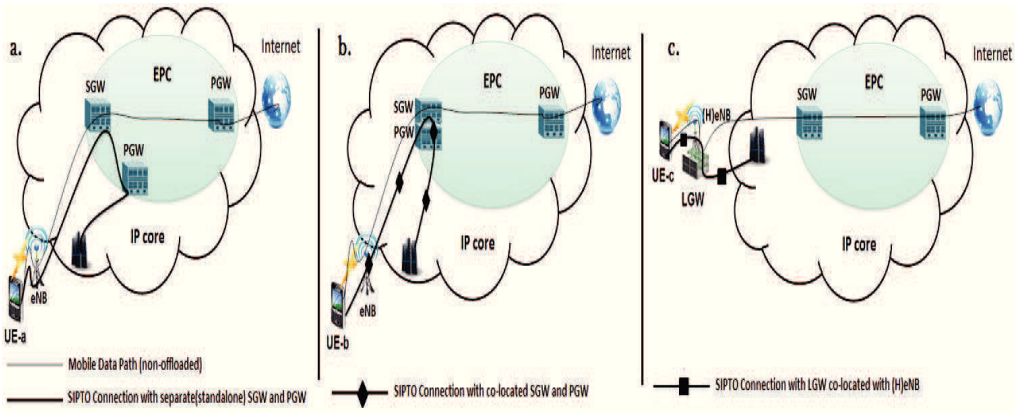

FIGURE A.2: Selected IP Traffic Offload Architecture

is introduced between SGW and LGW and built over user and control plane with GTP-U and GTP-C protocols for tunnel management. Also, a direct link is built between HeNB and LGW with GTP:U protocol over the user plane. Fig. A.1-b illustrates the new paths standardized in 3GPP in [122] for the SIPTO at LN architecture. We should mention here that the introduction of new interfaces for SIPTO at LN architecture does not affect mobile signaling and data traffic routing.

The different SIPTO use cases are illustrated in Fig. A.2, where UEs (a, b and c) are having part of their IP traffic routed towards EPC, while another part is offloaded towards different VoD servers, located within the IP network closer to the user. In the first use case, UE-a (Fig. A.2-a) is traversing the SGW for all the traffic. The UE-a is using a standalone PGW to access the server. Similarly to use case 1, in the second use case, UE-b (Fig. A.2-b) is traversing the SGW for all the traffic. However, UE-b is accessing the local server using co-located SGW and PGW. Finally, for the third use case, UE-c (Fig. A.2-c) is traversing the SGW only for the non-offloaded traffic. Since the LGW includes functionalities of both PGW and SGW, this implies that UE-c is virtually connected to two SGWs simultaneously: the standard SGW, which is used by the non-offloaded traffic and the LGW, which is used by the traffic offloaded thanks to SIPTO.

A.3.3 SIPTO Mobility Use Cases

Since LTE does not support smooth handover when the PGW is changed [122], depending on the type of gateways used to access the external IP network for SIPTO, 3GPP has distinguished three different mobility use cases (MC):

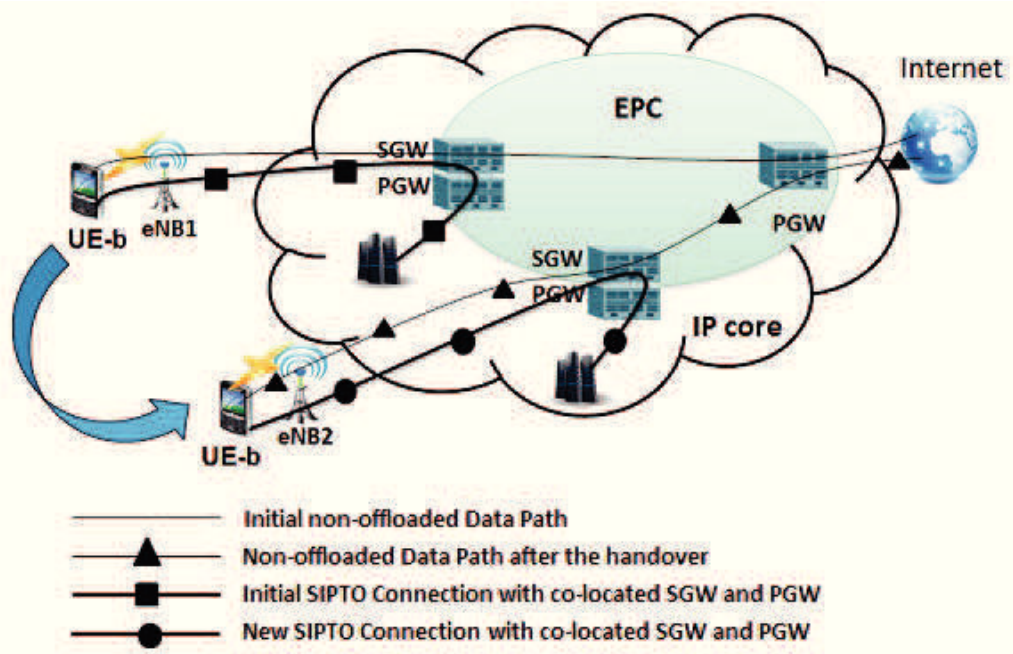

FIGURE A.3: MC2: Mobility of UE having SIPTO above RAN Session with co-located SGW and PGW

A.3.3.1 MC1: SIPTO above RAN with standalone SGW and PGW

According to [22], session continuity for users with "SIPTO above the RAN with standalone SGW and PGW session" is supported using the existing mobility procedures defined in 3GPP specifications for LTE mobile architecture. This is due to the fact that even if a SGW relocation is required, the user's IP address allocated by the PGW remains the same during the whole handover procedure. This includes UEs mobility within Macro network, Femto network and between Macro and Femto cellular networks.

However, if SGW and PGW are quite close to one another (e.g., located in the same building) there would be a potential relocation of PGW whenever SGW is relocated.

A.3.3.2 MC2: SIPTO above RAN with co-located SGW and PGW

As result of UE mobility having an ongoing SIPTO above RAN session, a SGW relocation procedure might be provided by the MME. For SIPTO with co-located SGW and PGW, the gateway relocation decision would affect both SGW and PGW. Then, the relocation of SIPTO PGW will result in losing the IP address allocated for the UE by PGW. Consequently, the MME must disconnect the impacted SIPTO connection with reconnection cause required [122]. This procedure

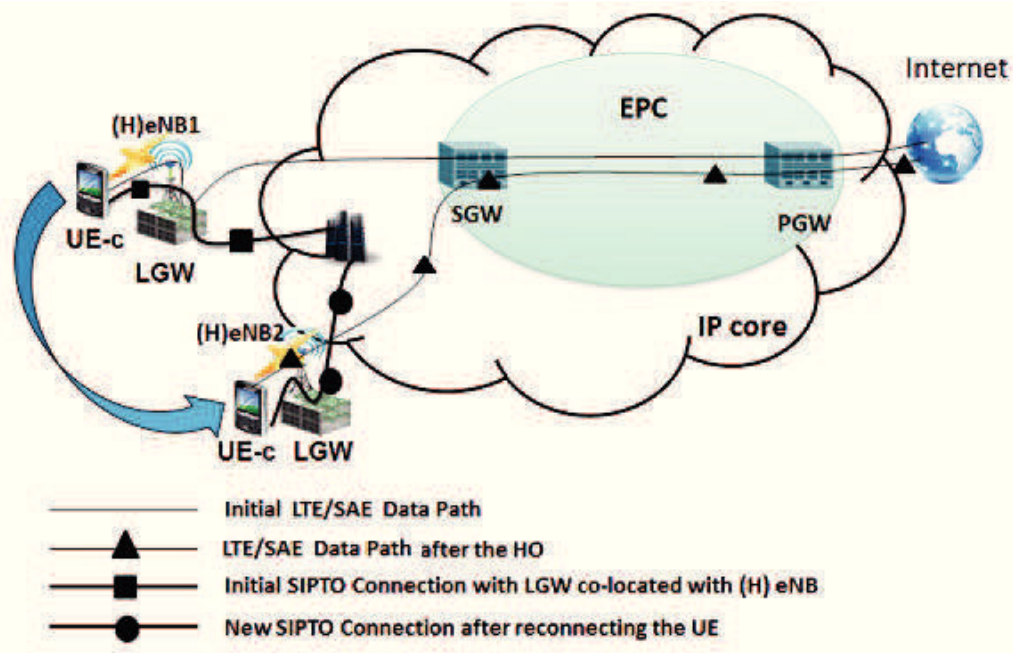

FIGURE A.4: MC3: Mobility of a UE having SIPTO at LN session with LGW co-located with HeNB

will probably be seamless to users having short-lived applications such as SMS texting. However, the deactivation of SIPTO connection will affect the sessions which require the currently used IP address to be maintained, e.g., real time video streaming and online gaming. We illustrates this mobility use case in Fig. A.3 when UE-b shown previously in Fig. A.2-b moves from eNB1 to eNB2 and relocates from source co-located SGW and PGW towards new co-located SGW and PGW. As shown in this figure, local services are interrupted during all the UEs mobility procedure. Only, after the activation of the new SIPTO connection, the UE can request those services again.

A.3.3.3 MC3: SIPTO with LGW co-located with HeNB

Similarly to SIPTO with co-located SGW and PGW, mobility of UEs with ongoing SIPTO sessions with either eNB or HeNB co-located with LGW will affect the continuity of sessions requiring the same IP address to be maintained. Considering the initial scenario shown in Fig. A.2-c, we now illustrates in Fig. A.4 the mobility use case when UE-c moves from HeNB1 to HeNB2. Due to the user's mobility, the MME decides to perform LGW relocation. Consequently, the offloaded data traffic requiring the same IP address to be maintained, is interrupted and a deactivation procedure with type of reactivation is performed by the MME on SIPTO traffic during the change of LGW.

In the mobility use cases discussed above, we see that SIPTO mobility is not supported due to multiple data paths to a single UE which has multiple IP addresses. Multiple data paths issue can be solved with the help of multihoming protocols provided by IETF, which is discussed in the following subsection.

A.3.4 MultiPath Transmission Control Protocol (MPTCP)

MPTCP is an extension of TCP standardized in RFC 6824 [75]. It was originally proposed to provide support for multi-homed hosts. It enables a mobile host to use multiple available interfaces simultaneously and thus allows multi-path streaming [130]. Its target benefit is load balancing. The traffic is distributed over different interfaces of a mobile host, which potentially results in improved throughput. MPTCP is backward compatible to TCP and uses the standard socket API used by most Internet applications, which makes it compatible to existing application and network.

MPTCP connection establishment starts as a standard TCP connection with SYN segment included with MPTCP option MP-CAPABLE in the TCP packet header as discussed in [75], to know whether the receiving host supports MPTCP or not. If the receiving host or remote host supports MPTCP, it will add the MP-CAPABLE option in SYN-ACK reply. The two hosts also include cryptographic tokens to these packets to uniquely identify this connection. If there are more than one network interfaces available at the start of the connection the additional sub-flows can be added to this MPTCP connection with the final ACK. These sub-flows behave as separate TCP connections inside the network. The sub-flows in any MPTCP ongoing communication can be added and removed at any point of time with the help of ADD_ADDR option and REMOVE_ADDR option for any interface. These options can be helpful during mobility of a mobile host when it moves from one network to another network i.e., it receives or configures a new IP address through new network attachment.

Fig. A.5 demonstrates full mesh created by sub flows between two MPTCP enabled nodes each having two active IP addresses. The mobile Host (MH) can represent user equipment here and Remote Host (RH) represents any peer node (e.g., content server).

MPTCP provides different handover modes, namely full handover mode, backup mode and single-path mode [76]. In full handover mode all the sub-flows are used simultaneously between two communicating hosts. Whereas, in backup mode MPTCP opens sub-flows over all the existing interfaces but uses only a

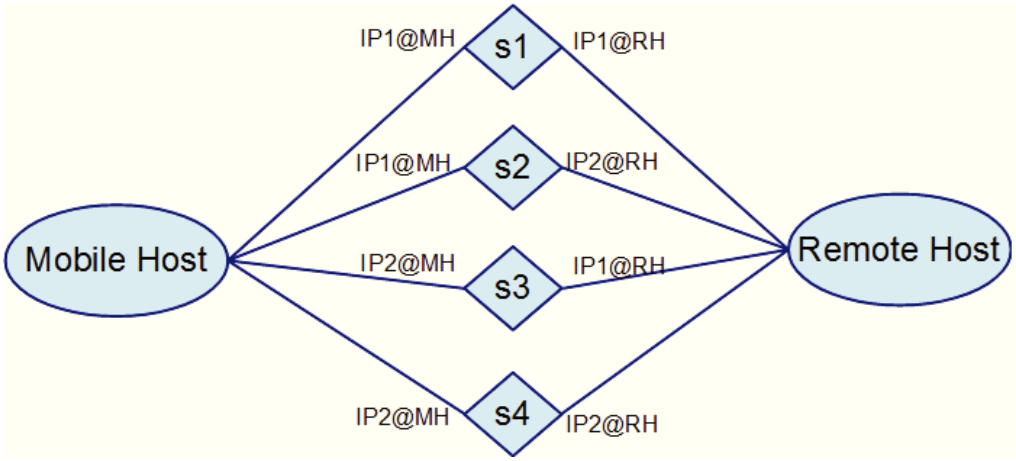

FIGURE A.5: Full Mesh Architecture for MPTCP communication

subset of sub flows for transmission of data packets. MPTCP uses MP-PRIO option to specify any sub-flow as backup mode. The sub-flow which is defined in MP-PRIO option will be used only when rest of the other addresses are not working. In the single-path mode only one TCP sub-flow is used at any time. If this interface goes down then another sub-flow can be created and used for packet forwarding.

IETF has proposed the use of proxy MPTCP for non-MPTCP compliant clients, in [80]. When a MPTCP compliant client (for example UE) initiates a communication with a server using MPTCP-capable option in SYN packet, the proxy MPTCP server intercepts the packets and creates a temporary entry consisting of UE IP, Server IP, UE port number and server port number for this connection. Then, the proxy forwards this SYN packet to the server. If server replies with MP-CAPABLE option in SYN+ACK packet then proxy removes the temporary entry for this connection, otherwise the proxy initiates an MPTCP connection with the UE and sustains the temporary entry to record all the sub-flows. Proxy MPTCP is transparent to the UE and all the TCP applications on both the hosts.

There can be other choices for multihoming as well for eg. CMT-SCTP [73]. However, unlike MPTCP, CMT-SCTP is not transparent to the applications. Moreover, MPTCP performs significantly better than CMT-SCTP [74]. Therefore, the paper focuses on the application of MPTCP for solving session continuity.

A.4 Related Work

As shown in Section A.3, session continuity is not maintained during mobility cases 2 and 3. Most of the current studies focusing on offloading mobile data

traffic with seamless mobility are considering IP address maintenance as key issue for SIPTO approach.

3GPP have considered in [131], three different use cases under the Change for SIPTO (C-SIPTO) approach. C-SIPTO first use case relies on performing deactivation procedure with reactivation cause only for short-lived traffic, while keep routing the ongoing long-lived traffic towards the EPC. On the meantime, a new SIPTO PDN connection is being established with a target PGW, closer to the user's new location, to be used for future long-lived sessions. C-SIPTO second and third use cases have introduced always-on dual connection and on-demand dual connection concepts. Herein, C-SIPTO proposes redirecting all short-lived sessions towards a shorter data path using a selected LGW while keep routing all real time streaming traffic which requires the same IP address to be maintained, towards the initial PGW in the EPC network. As a result, for all three uses cases, C-SIPTO has allowed a smooth mobility for users with ongoing short-lived sessions. However, none of these cases allowed a smooth mobility with gateway relocation for users with ongoing long-lived sessions requiring the same IP address to be maintained.

Taleb T. et al. have introduced the Follow Me Cloud framework [132] for seamless users mobility using interworking federated clouds with distributed mobile networks. Follow Me Cloud enables mobile users to access cloud services using always the most optimal path by migrating services to the nearest available DC and/or data anchor gateway with no session interruption. However, to allow a smooth mobility of users in this solution, the authors propose to replace data anchoring at the network layer by service anchoring and IP addressing by service/data identification. Moreover, a Follow Me Cloud controller and a DC/GW mapping entity have also been introduced to the network architecture in order to allow an optimum session migration from one location to another during users mobility. Consequently, even though Follow Me Cloud has allowed a best data path selection while ensuring a smooth session migration when a user changes its network point of attachment; it has also added more complexity to the current 3GPP architecture.

A lightweight Mobile Cloud Offloading Architecture (MOCA) has also been introduced by authors in [133] in order to offload part of users IP traffic using cloud infrastructure and SDN capabilities. The basic idea of MOCA is to introduce a cloud platform, inside the mobile network, in which operators can instantiate a software instance of SGW, PGW and Content Server engine. Even though,

MOCA have enabled the adoption of SDN and cloud technologies in a new mobile data offloading architecture, MOCA realization has included extensions to signaling protocols and modifications to the MME and the new cloud based SGW. Additionally, the use of an SDN middle-box for packet interception and the additional routing rules added into the eNBs and SGWs, introduce supplement delays and complexity to the standardized mobile architecture. Finally, similar to the other solutions, session continuity during mobility between core EPCs was not considered in MOCA.

The present article differs from the existing methods by introducing an MPTCP-based solution allowing a Smooth handover for mobile users with either SIPTO short-lived or long-lived sessions.

A.5 Smooth handover for SIPTO Connections with MPTCP

In this section, we focus on providing smooth handover in the two mobility use cases (MC2 and MC3), presented in section A.3 for users with either SIPTO at or above RAN with co-located SGW and PGW or SIPTO at LN with LGW co-located with HeNB ongoing sessions.

A.5.1 SIPTO Data Path Connection Setup

In order to realize a Smooth handover solution for SIPTO, we first need to enhance the 3GPP SIPTO mechanism by setting up an MPTCP connection between the UE and the server. The enhancement of SIPTO with MPTCP connection will allow at least two data paths between the UE and the server: one towards the PGW within the EPC and the second towards the SIPTO IP edge. In this solution we also propose to exchange all MPTCP signaling messages over the EPC-routed mobile data path. The “always available" feature of this data path will ensure that MPTCP connection will not be broken even during user’s mobility.

Fig. A.6 illustrates the MPTCP connection establishment signaling procedure with the initiation of the initial SIPTO connection for the user. First, at the attachment to the network, the UE receives an IP address by the default PGW within the EPC. Then, using this IP address, the UE connects to an appropriate server. Here, we assume that the server is MPTCP-capable. The data path built

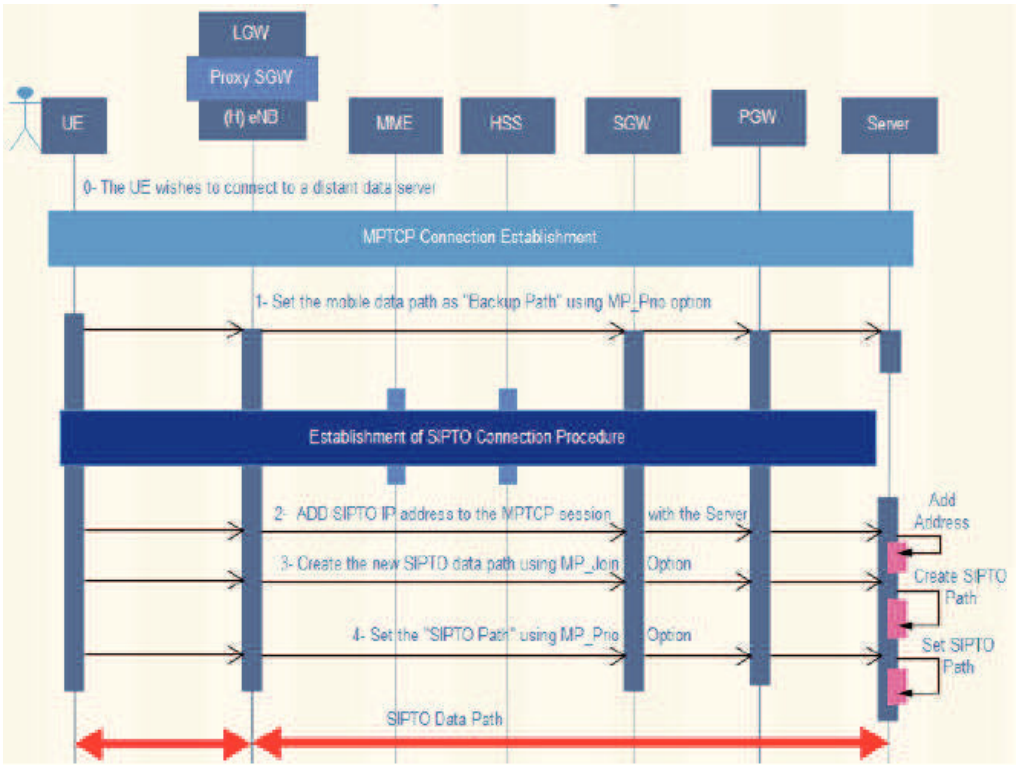

FIGURE A.6: SIPTO Data Path Setup using MPTCP Connection

between the UE and the server is an EPC-routed data path. This data path shall be used for all signaling messages related to the MPTCP connection. The UE then establishes an MPTCP connection over the EPC-routed data path. Next, the UE requests the establishment of a SIPTO data path to the same server, and thus obtains another IP address, called local IP address. This address is then communicated to the server by the UE, for updating the server's list of addresses it uses to communicate with the UE. After that, using the MP-Join option of MPTCP, the UE requests the creation of an MPTCP sub-flow between the server and this local IP address. Finally, with the MP-PRIO option of MPTCP, the UE declares the subflow over the EPC-routed data path as backup path and the subflow over the non-EPC-routed data path as SIPTO path. All downstream traffic from the server arrives to the UE through the SIPTO path.

A.5.2 Smooth SIPTO Handover

In this subsection we present how the mobility issues are solved with the help of MPTCP multihoming features. MPTCP enables the user to manage the traffic over various available data paths (subflows) between the UE and the server.

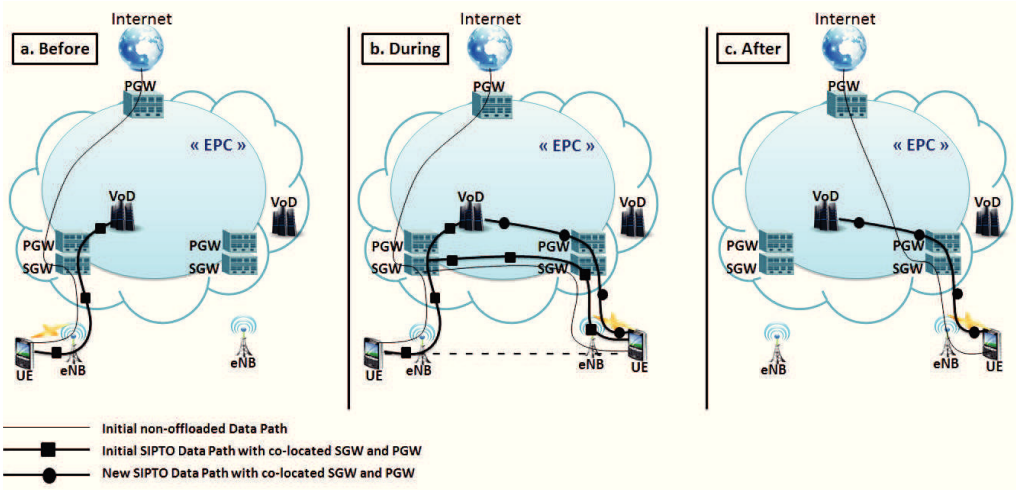

FIGURE A.7: Proposed Mobility Scenario for UE having non-offloaded session and SIPTO session with co-located SGW and PGW

A.5.2.1 MC2: SIPTO above RAN with co-located SGW and PGW

Let us assume the scenario in Fig. A.7-a where a UE is accessing the centralized IP services (e.g., internet) through a PGW located within the backbone while the network is breaking out part of its IP traffic (e.g., real time video streaming) above the RAN using co-located SGW and PGW as described in section A.3 (see Fig. A.2-b). This could e.g., correspond to a user, which is traveling from one town to another town by train.

In order to maintain the UE's session continuity for the offloaded traffic, Smooth SIPTO handover solution proposes to handover the current SIPTO data to the target selected SGW while establishing a new SIPTO data path towards the co-located target SGW and PGW. For that, new behaviours have been introduced to the MME while other network equipments behaviours remain unchanged. These behaviours have to fulfil the following requirements:

- Requirement 1: The MME must not deactivate the initial SIPTO connection when a PGW relocation decision is taken. Instead, it must start a handover procedure.
- Requirement 2: During this handover, the MME must request the establishment of new SIPTO connection towards the target PGW.
- Requirement 3: Once the handover procedure is completed and the new SIPTO connection is established, the MME must deactivate the initial SIPTO connection.

Now that we have cited the requirements, let us see how they can be applied in a Smooth SIPTO handover: ¨In mobile networks, eNBs are setup to send time mode RRC requests to UEs for measurement control. Upon receiving the RRC request, a UE performs neighbour cell measurement and replays to the eNB with an RRC response message including a measurement report. According to the information received in this message (i.e. a neighbour cell has a better signal), the source eNB could decide that a handover of user's traffic towards another eNB is required. As stated in [122], the handover process is subdivided in to three phases: Preparation, Execution and Completion.

Typically, as pointed out in section A.3.2 in 3GPP SIPTO architecture, whenever the MME receives a handover required message from the source eNB, the MME must deactivate the intended SIPTO connection with reactivation cause required. This article differs from existing 3GPP solution by proposing, whenever SGW/PGW relocation is required for a SIPTO connection, to handover user's traffic built on the same steps of the "inter eNB/inter SGW" handover procedure defined in [122]. The Smooth SIPTO handover procedure is shown in Fig. A.7-b).

In the proposed handover preparation phase, when a handover decision is made by source eNB, the latter sends a handover required message to the MME. Once received, the MME must prepare the network for the handover. The MME selects the target SGW and PGW and an Indirect Forwarding Tunnel is then established between source and target SGWs. Now that the two eNBs are ready to perform a handover, the handover execution phase starts by detaching the UE from the old cell and synchronize it to the new one. This step is done aligned with the transfer of source eNB's status towards target eNB via the MME. At this stage the uplink traffic forwarding between source and target eNBs over the indirect SIPTO forwarding tunnel begins and the target eNB starts buffering all received packets until users synchronization is completed. Finally, the downlink packets are then sent to the UE.

As pointed out above, to realize a Smooth SIPTO handover during users mobility, a new SIPTO data path must be established before performing the handover completion phase of the initial SIPTO data path. The basic idea here is to ensure that both initial and new SIPTO data paths would be used at the same time to transfer packets between the UE and the server, and thus, no traffic interruption would be realized.

Usually, the handover is interrupted only within the execution phase of the process. In order to allow minimum interruption time during the handover process

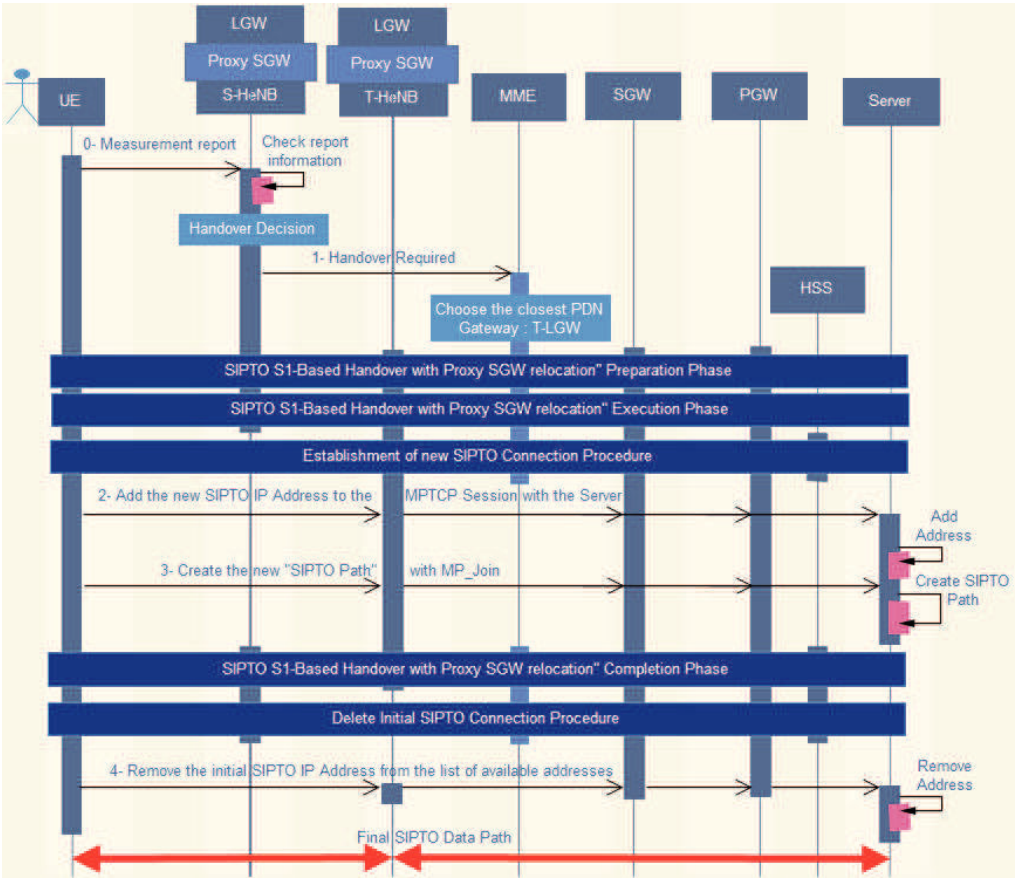

FIGURE A.8: Proposed Smooth handover procedure for SIPTO Connections

of the initial SIPTO traffic, we propose not to establish the new SIPTO path before the execution phase of the initial SIPTO traffic handover is completed. Moreover, to ensure that the initial SIPTO data path will not be broken before the establishment of the new data path, the handover completion phase of the initial SIPTO data path must be delayed until the new SIPTO data path establishment procedure is completed. In that aim, we propose to modify the standard handover process by delaying the resource release timer at the MME level. For the best result, the resource release timer delay must not be less than the delay required for the establishment of the new SIPTO connection.

Consequently, after the handover execution phase is completed and before starting the handover completion phase of the initial SIPTO connection, the new SIPTO data path establishment procedure towards the selected co-located target SGW and PGW is performed. This can be done using the established MPTCP connection presented in section A.5.1. The UE then communicates its new IP address with the content server and creates new MPTCP subflow, using MP-JOIN option of MPTCP, as “new SIPTO path". The UE will now have at least three data paths at a time: the default (backup) data path towards the EPC, the

initial SIPTO data path towards the co-located source SGW using the indirect data forwarding tunnel between (target and source SGWs) and PGW and the new SIPTO data path towards the co-located target SGW and PGW (see Fig. A.8).

At the handover completion phase, the MME sends a UE Context Release Command to the source eNB and then deletes the indirect data forwarding tunnel of the initial SIPTO path. Later on, we use MPTCP features to delete the MPTCP subflow originally set up for the initial SIPTO path. Finally, a deactivation procedure for the initial SIPTO connection will be requested by the MME. Then, With the help of MPTCP, all IP addresses allocated by the source PGW for this UE will be deleted from the list of addresses stored within the content server.

At the end, the user will only have two MPTCP subflows : the Backup data path towards the EPC and the SIPTO data path towards the new co-located SGW and PGW. The final user's Offloaded and non-offloaded data paths are shown in Fig. A.7-c.

Accordingly, in Smooth SIPTO handover support, both the first and second handover phases (preparation and execution) are performed similarly to 3GPP standardization. However, the handover completion phase would be delayed in order to ensure the multiple simultaneous SIPTO paths to guarantee non-breaking the traffic. After the completion of Smooth handover for SIPTO connections, the server used by the UE may not be the optimum due to the server distribution closer to the user, as proposed in [12] and [119]. Smooth handover for SIPTO connections allows UEs to keep the ongoing communication with the original server, i.e., the server with which the UE started the communication in the first place. However, the server relocation would break the ongoing communication as the IP address of the server would change, which can not be solved with Smooth SIPTO handover.

A.5.2.2 MC3: SIPTO with LGW co-located with HeNB

To support user's local mobility, our Smooth SIPTO handover proposal introduces the notion of Proxy-SGW to the 3GPP architecture with SIPTO at LN. A Proxy-SGW is a functionality which is going to be included into the LGW entity. As shown in Fig. A.9, Proxy-SGW is a purely internal function that is only seen by the co-located HeNB and LGW and unseen by the rest of the network equipments. Proxy-SGW is, thus, seen as HeNB to the LGW and as an LGW to the HeNB. In order to maintain the compatibility to 3GPP architecture, we

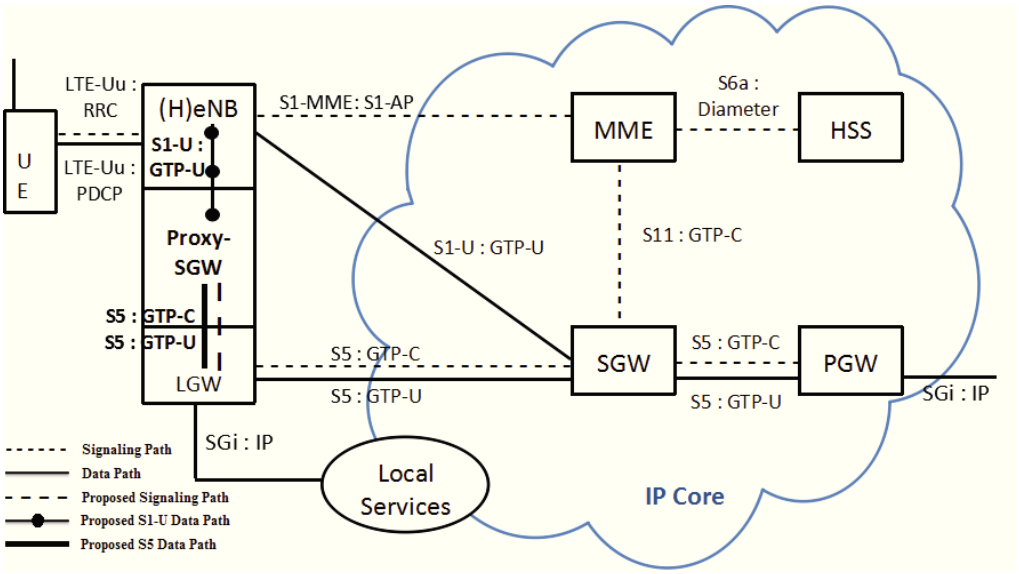

FIGURE A.9: Smooth SIPTO handover with LGW Co-located with HeNB Signaling and Data Path

propose to connect Proxy-SGW to the HeNB over an S1-U interface with GTP-U protocol and to the LGW over an S5 interface with GTP-U protocol on the user plane and GTP-C protocol on the control plane.

To allow a seamless user's mobility support, Smooth SIPTO handover solution for SIPTO at LN, differs from standards 3GPP by introducing new behaviours to MME, LGW and HeNB equipments while keeping other equipment's behaviours (SGW, PGW, etc.) unchanged. The MME new behaviours for SIPTO at LN mobility fulfill the same requirements defined in the subsection A.5.2.1. However, LGW's and HeNB's new behaviours have to fulfill the following requirements:

- Requirement 4: Source HeNB must enforce an "inter HeNB/inter Proxy-SGW" handover procedure whenever a UE, which is having a SIPTO at LN session moves from one cell to another.
- Requirement 5: LGW must forward all the "indirect tunnel establishment related signalling messages" received from default SGW (within the EPC) to the Proxy-SGW.

Let us assume a scenario where a UE is having an IP session towards the Internet, while another session (e.g., video) is offloaded towards a content (or VoD) server using a HeNB co-located with LGW including Proxy-SGW function as illustrated in Fig. A.10-a. We also assume that this UE is handing over towards another

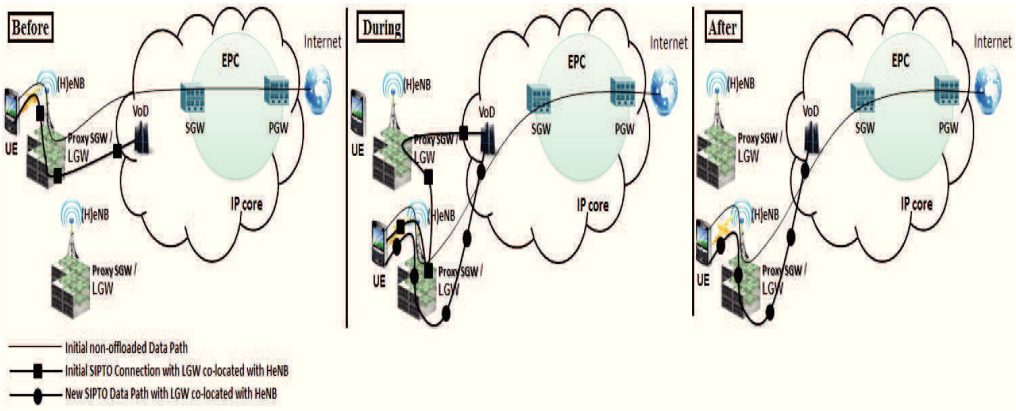

FIGURE A.10: Proposed Mobility Scenario for UE having non-SIPTO session and SIPTO session with Proxy SGW function included in LGW

HeNB, which is also co-located with a LGW including Proxy-SGW functionality (for example, one can consider a student walking around a large University Campus, and attaching its UE to different HeNBs). Due to this mobility, the MME may decide to relocate the current LGW towards the new co-located LGW. The Smooth SIPTO handover procedure is illustrated in Fig. A.8.

The Proxy-SGW function, in Smooth handover with SIPTO scenarios, is used to perform an “inter HeNB/inter Proxy-SGW" handover over the S1 interface between the HeNB and the Proxy-SGW. To achieve this, the interface selection function within the HeNB, must be enhanced to enable an always S1-based handover for users with ongoing SIPTO at LN sessions. Moreover, whenever a LGW relocation decision is made by the MME, a gateway selection function must be performed by the MME to select the target LGW/Proxy-SGW using either RAN-based alternative or DNS-based alternative proposed by 3GPP in [20]. Following this selection, the MME performs an indirect tunnel establishment between the initial Proxy-SGW/LGW and the target Proxy-SGW/LGW. This tunnel is then used to forward the SIPTO at LN’s uplink and downlink data traffic from and towards the UE as shown in Fig. A.10-b. Parallel to the current SIPTO traffic handover, the MME initiates a new SIPTO connection towards the server using its new local IP address, which is allocated by the target LGW. Similar to the previous section, the network must delay the resource release timer to ensure the establishment of new SIPTO path before releasing the resources allocated during the initial SIPTO handover procedure.

With the help of the MPTCP, the session continuity can be maintained after the the old local IP address becomes unreachable. This new SIPTO connection using the new local IP address can be added to the ongoing session using MP-JOIN option of MPTCP. Also, the subflow with the old SIPTO connection can

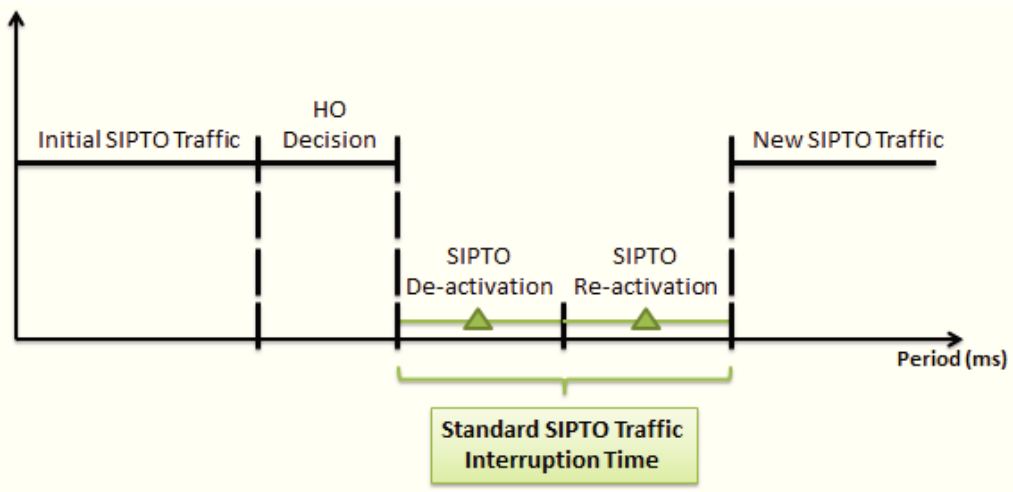

FIGURE A.11: Period Graph for Standard SIPTO Interruption Time

be removed from the session after the handover is completed, as illustrated in Fig. A.8.

The Fig. A.10-c illustrates the user's new route towards EPC and SIPTO at LN data paths.

A.6 Evaluation of Interruption Time with Smooth handover for SIPTO Connections

In this section, the performance of our proposed Smooth handover with SIPTO scenarios is evaluated in terms of interruption time duration. The evaluation is focused on finding out whether the proposed scenarios can reduce the interruption time of SIPTO traffic during mobility of UEs between two cells when a PDN gateway (PGW or LGW) relocation decision triggered by the MME. Let PD and LD respectively represent the processing delay of the nodes and the link transmission time between different nodes. Let also SDD and SED respectively represent the SIPTO connection deactivation delay and SIPTO connection establishment delay.

The period graph shown in Fig. A.11 illustrates the standard SIPTO traffic interruption time during user's mobility scenarios (MC2 and MC3) with no possible handover. As pointed out in the section A.3, when PGW or LGW is relocated, the interruption time is given by:

$$IT_{standardS} = SDD + SED + X \tag{A.1}$$

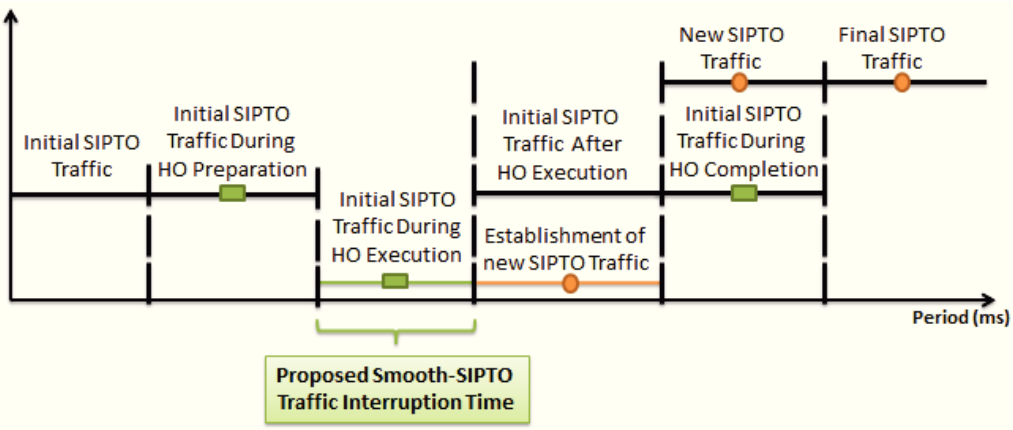

FIGURE A.12: Period Graph for Proposed SIPTO Interruption Time

where, X is a constant which represents the total propagation and processing delay from MME to HSS, MME to DNS and PGW to PCRF. Typical values for these delays are respectively 100ms, 50ms and 100ms [123].

Thanks to the transition diagram for activation and deactivation procedures in [22] and [123], SDD and SED can be driven. Therefore, for MC2: SIPTO above RAN with co-located SGW and PGW, the interruption time can be calculated as follows:

$$IT_{standardMC2} = 2\{PD_{(2\text{UE},3\text{E}\text{NB},2\text{MME},2\text{SGW},\text{PGW})} + LD_{(3\text{UE\_E}\text{NB},3\text{E}\text{NB\_MME},2\text{MME\_SGW},2\text{SGW\_PGW})}\} + X \tag{A.2}$$

Furthermore, with the help of the transition diagram for activation and deactivation procedures in [122], [22] and [134], SDD and SED for MC3: SIPTO at LN with LGW co-located with HeNB can also be derived, yielding:

$$IT_{standardMC3} = 2\{PD_{(2\text{UE},3\text{H}\text{E}\text{NB},2\text{MME},2\text{SGW},\text{LGW})} + LD_{(3\text{UE\_H}\text{E}\text{NB},3\text{H}\text{E}\text{NB\_MME},2\text{MME\_SGW},2\text{SGW\_LGW})}\} + X \tag{A.3}$$

..

For proposed MC2 and MC3 scenarios, the interruption time of SIPTO traffic illustrated in Fig. A.12 is given by:

TABLE A.1: Delay Budget for processing and links (in ms)

	UE	eNB	MME	SGW	Proxy SGW	LGW
UE	3	2	-	-	-	-
eNB	2	4	7.5	3.75	0	0
MME	-	7.5	15	3.75	7.5	-
SGW	-	3.75	3.75	10	-	3.75
Proxy SGW	-	0		-	10	0
LGW	-	0	-	3.75	0	10

$$IT_{proposedMC2} = PD_{(4UE,2SeNB,TeNB,MME)} + LD_{(SeNB\_UE,\ 2MME\_SeNB,MME\_TeNB,UE\_TeNB)} \tag{A.4}$$

and

$$IT_{proposedMC3} = PD_{(4UE,2SHeNB,THeNB,MME)} + LD_{(SHeNB\_UE,\ 2MME\_SHeNB,MME\_THeNB,UE\_THeNB)} \tag{A.5}$$

We used values from 3GPP [135] for the processing delay on different nodes and the link delay between two different nodes. The propagation delay between different nodes is taken to be equal to 5µsec/km. In SIPTO at LN the LGW and Proxy-SGW must be co-located with the base station (HeNB) while in SIPTO above RAN, the co-located SGW and PGW must be located within the metro/-core segment of the network (inside the EPC network). Based on this information, we assume that the distance from the eNB to the default SGW (co-located with PGW) and distance from the SGW to the MME equals 150km. We also assume that the distance from the co-located HeNB and LGW to the SGW and the distance from the HeNB to the MME equals 180km. Therefore we obtain the results reported in Table A.1. The diagonal entries in Table A.1 represent the processing delay of nodes whilst the rest of the values correspond to the link delays.

Given the numbers in Table. A.1, applied to equations A.2, A.3, A.4 and A.5, we obtain the following results:

- the interruption time for standard scenarios ($IT_{standardMC2} = IT_{standardMC3}$) approximately equals to 500ms.

- the interruption time for proposed scenarios ($IT_{proposedMC2}$/$IT_{proposedMC3}$) is approximately 65ms.

From these results, we can state that our proposed MPTCP-based Smooth handover solution for SIPTO enables operators to significantly reduce delay during the mobility of UEs having a SIPTO at LN and/or SIPTO above RAN services. This allows seamless session continuity for users having ongoing video-streaming data taking into consideration that the delay budget for conversational video is estimated by 150ms and non-conversational video is estimated by 300ms [123]. Thus, obtained results using our method are fully compliant with the level of quality of service required for this kind of traffic.

With an exponential growth of total mobile and fixed IP traffic, reaching up to 168.4 exabytes per month by 2019 ([129], [136]), network operators in [12] and [119] have decided to alleviate the load off the different segments of the network (core, aggregation and access) by deploying distributed IP edges and services closer to the user's location within a Fixed and Mobile Converged (FMC) network. The following section presents how the proposed Smooth handover scenarios for SIPTO could be mapped on such FMC network architecture.

A.7 Mapping Smooth handover SIPTO solution on a Fixed and Mobile Converged Network Topology

As pointed out in Section A.2, the main idea for future FMC network is to integrate IP edges of different access networks within a UAG on the one hand and co-locate them with application servers and data centers within a NG-PoP on the other hand. A NG-PoP could be located in the network either at the Main Central Office's (CO) level or at the Core CO's level. The location of the NG-PoP would depend mostly on the population density of the region; e.g., NG-PoP is placed within the Core-CO for the industrial areas and within the Main-CO for the residential areas. Further, the mobile IP core (EPC) would be replaced by a converged IP core.

Having PGWs functions within UAGs very low in the network (i.e., at the access network or beyond the RAN) is unpractical to manage users mobility as potential loss of user's IP address is more frequent. A UE would then need to have a connection towards an anchor PDN gateway to ensure an "always-on mobile connectivity" in case their actual connection towards the distributed UAG or HGW breaks. This connection could be setup at the attachment of the UE to

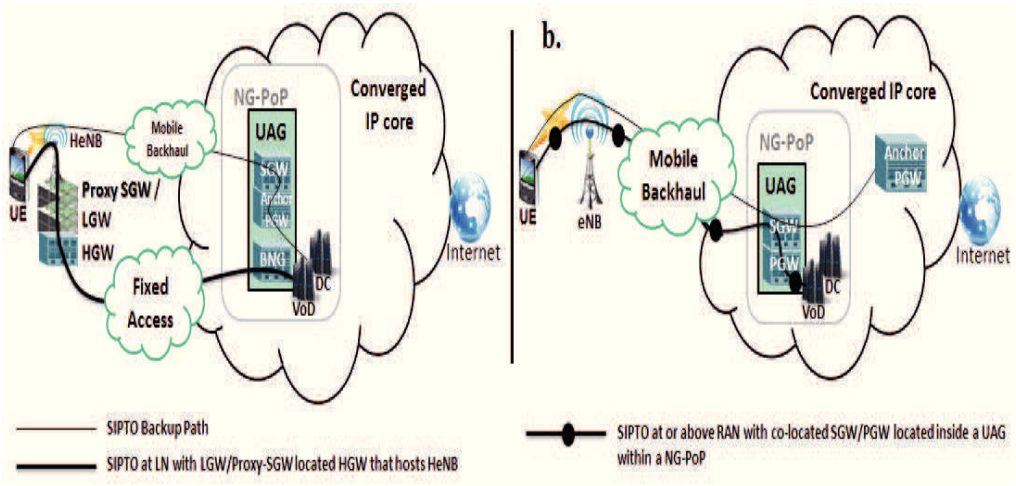

FIGURE A.13: Mapping Smooth handover SIPTO solution on FMC Network Topology

the network where an anchor PGW for the user would be selected. The latter then allocates a permanent IP address to the FMC user. This IP address could then be used to establish a backup data path ensuring the data re-transmission. The location of the selected anchor PGW depends on the user's location.

By deploying such converged network topology with respect to Smooth handover solution for SIPTO presented in section A.5, we would be able to consider two reference models for a next generation of the mobile network architecture.

1. The first reference model is based on SIPTO at LN architecture shown in Fig A.2-c. In this scenario, the breakout point from the mobile architecture is quite close to the UE, which takes advantage of LGWs/Proxy-SGWs located e.g. within Home Gateways (HGWs) that host HeNBs. As shown in Fig A.13-a, the use of co-located HGWs with femto-cells (HeNBs) instead of macro-cells (eNBs) allows reaching the network services located within the NG-PoP using the fixed access network instead of the mobile back-haul. This allows saving bandwidth at all segments of the network (access, aggregation and core) [128]. A typical mobility use case for SIPTO at LN scenario could be represented when a UE is playing an online game while walking and changing it's LGW. In this case, the selected anchor PGW could be located within the closest UAG in the Main CO.

2. The second reference model is based on SIPTO at or above RAN architectures shown in Fig A.2-b and A.2-c. In this scenario, in order to access the required services, the user's data traffic must be routed through the mobile back-haul towards the co-located SGW and PGW integrated inside

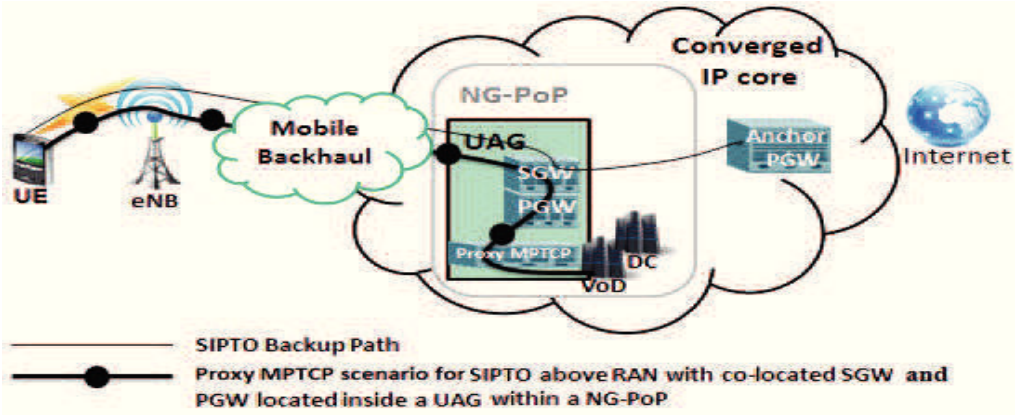

FIGURE A.14: Proxy MPTCP placement for proposed scenarios.

the UAG, which is located within the NG-PoP (see Fig A.13-b). Unlike the first scenario, this reference model allows alleviating the load only at the core segment of the network. Traffic handover for this scenario could be performed for e.g. when children are sitting in a car and watching an IPTV video on their tablet while their father is driving. As the distributed PGW within the UAG does not change so often in this case, the selected anchor PGW could be located within the Core CO.

The proposed Smooth handover SIPTO scenario is applicable as long as both the UE and the servers are MPTCP capable. If the UE or the servers are non-MPTCP compliant, we propose to use proxy MPTCP as a solution for a Smooth handover support for SIPTO. Proxy MPTCP is a fixed anchor which is used to enable the UE to initiate an MPTCP connection with the server. Fig. A.14 illustrates the placement of proxy component in the proposed Smooth handover SIPTO solution for FMC scenarios. Depending on the non-MPTCP client type, we propose the two scenarios explained below.

1. UE: In context of Smooth SIPTO, UE has to be MPTCP compliant to achieve seamless mobility. This is due to the fact that changing the proxy MPTCP would break the ongoing session. Therefore, the proxy MPTCP has to be fixed relative to the UE. Thus, either a UE has inbuilt MPTCP support or it has installed the proxy such as a lightweight proxy MPTCP proposed in [81].

2. Server: If the server is non-MPTCP compliant, the placement of the proxy MPTCP should be closer to the server. Therefore, the ideal place for the placement of proxy MPTCP would be within the NG-PoP (e.g. inside the

UAG). This placement ensures no relocation of proxy MPTCP during an ongoing session.

A.8 Conclusion

In this present article, we have addressed the session continuity issue in SIPTO at LN and SIPTO above RAN reference models. We have proposed an MPTCP-based solution for a smooth mobility of users having ongoing sessions requiring IP address maintain. Moreover, we enhanced the LGW with a Proxy SGW function for a seamless local mobility.

The MPTCP protocol is used to maintain the ongoing session even after the previous IP address becomes unreachable and UE acquires a new address. We have described how to maintain MPTCP signaling for creating new subflows and discarding old ones, relying on LTE mobile architecture. This enhancement goes beyond the 3GPP study in [131] by using the LGW to offload both long-lived and short-lived data sessions. We also proved that our Smooth handover SIPTO solution allows a seamless mobility by significantly reduce the handover delay compared to the standard 3GPP SIPTO architectures. Finally, we mapped the proposed Smooth handover SIPTO architecture models on a FMC network topology and we considered a proxy MPTCP scenario for UEs that are unable to support an MPTCP connection. In future works, the proposed solutions can be evaluated in an experimental setup in order to verify their feasibility for a real time scenario.

Appendix B

Log Entry

B.1 When Mobile router is attached to its Home Network

In the logs on the mobile router, it can be verified that the mobile router is connected to home agent and is now in home network.

B.1.1 Logs on Mobile Router

rootMobileHost:/home/tmsproject# mip6d -c /usr/local/etc/mip6d.conf
mip6d[4647]: UMIP Mobile IPv6 for Linux v1.0 started (Mobile Node)
main: UMIP NEMO for Linux started in debug mode, not detaching from terminal
.....
conf_home_addr_info: HoA address 2001:db8:ffff:0:0:0:0:1
conf_home_addr_info: ***is Mobile Router***
conf_home_addr_info: ***Mobile Network Prefix 2001:db8:ffff:1:0:0:0:0/64***
conf_home_addr_info: ***HA address 2001:db8:ffff:0:0:0:0:1000***
conf_home_addr_info: Home address 2001:db8:ffff:0:0:0:0:1
flag_hoa: set HoA 2001:db8:ffff:0:0:0:0:1/128 iif 8 flags 12 preferred_time 4294967295 valid_time 4294967295
conf_home_addr_info: Added new home_addr_info successfully
__md_discover_router: discover link on iface (3)
md_change_default_router: add new router fe80:0:0:0:222:19ff:fe06:d2e1 on interface (3)

md_update_router_stats: Adding CoA 2001:db8:ffff:0:12fe:edff:fe05:ed2e on interface (3)
mn_addr_do_dad: DAD succeeded!
mn_addr_do_dad: address = 2001:db8:ffff:0:0:0:0:1
mn_move: 1874
mn_move: ***in home net***
mv_hoa: move HoA 2001:db8:ffff:0:0:0:0:1/64 from iface 8 to 3

As shown in the logs above, mobile router has the information of its address of HA and mobile network prefix etc. When mobile router connects to the home agent, it notices itself to be in home net.

B.1.2 Binding Cache on Home Agent

The binding cache on the home agent and binding update list on the mobile router can also be verified to be found empty, as shown in the following logs:

rootHomeAgent:/home/tmsproject# telnet localhost 7777
Trying ::1...
Connected to localhost.
Escape character is '^]'.
mip6d> verbose yes
yes
mip6d> bc
mip6d>

Binding Update List on Mobile Router:
rootMobileHost:/home/tmsproject# telnet localhost 7777
Trying ::1...
Connected to localhost.
Escape character is '^]'.
mip6d> verbose yes
yes
mip6d> bul
mip6d>

B.2 When Mobile router is attached to Foreign Network 1

While NEMO components are running, mobile router moves from home network to foreign network1. In this case, we receive the update logs described in following sub sections.

B.2.1 Logs on Mobile Router

__md_discover_router: discover link on iface (3)
md_change_default_router: add new router fe80:0:0:0:222:19ff:fe06:db71 on interface (3)
md_update_router_stats: ***Adding CoA***
2001:db8:0:1:12fe:edff:fe05:ed2e on interface (3)
mn_move: 1874
mn_move: ***in foreign net***
mv_hoa: move HoA 2001:db8:ffff:0:0:0:0:1/128 from iface 3 to 8
mn_send_home_bu: 829
mn_get_home_lifetime: CoA lifetime 86399 s, HoA lifetime 86390 s, BU lifetime 60 s
process_first_home_bu: New bule for HA
bul_add: Adding bule
******Binding Update List Entry*****
== BUL_ENTRY ==
Home address 2001:db8:ffff:0:0:0:0:1
Care-of address 2001:db8:0:1:12fe:edff:fe05:ed2e
CN address 2001:db8:ffff:0:0:0:0:1000
lifetime = 60, delay = 1500
flags: IP6_MH_BU_HOME IP6_MH_BU_ACK IP6_MH_BU_MR
mn_send_home_bu: New bule for HA
mh_send: sending MH type 5 from 2001:db8:ffff:0:0:0:0:1 to 2001:db8:ffff:0:0:0:0:1000
mh_send: local CoA 2001:db8:0:1:12fe:edff:fe05:ed2e
bul_update_timer: Updating timer
******Tunnel between HA and MR*****
tunnel_mod: modifying tunnel 8 end points with from
2001:db8:0:1:12fe:edff:fe05:ed2e to 2001:db8:ffff:0:0:0:0:1000
******Binding Acknowledgement*****
mn_recv_ba: ***Got BA (status 0) from 2001:db8:ffff:0:0:0:0:1000***

to home address 2001:db8:ffff:0:0:0:0:1 with coa 2001:db8:0:1:12fe:edff:fe05:ed2e.

As shown in the logs above, mobile router creates a new care-of-address with the new prefix advertised from the access router in foreign network 1. Mobile router then identifies itself to be in foreign net and sends a binding update to the home agent and receives an acknowledgment for it. The lifetime of this binding update is 60 second. Afterwards, mobile router creates a tunnel whose end points are home agent's address and mobile router's acquired address. This tunnel entry can also be verified from the interface list of the mobile router.

rootMobileRouter:/home/tmsproject# ifconfig
ip6tnl1 Link encap:UNSPEC HWaddr 20-01-0D-B8-00-00-00-01-00-00-00-00-00-00-00-00
inet6 addr: 2001:db8:ffff::1/128 Scope:Global
inet6 addr: fe80::12fe:edff:fe05:ed2e/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MTU:1460 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

B.2.2 Logs on Home Agent

mh_bu_parse: Binding Update Received
__tunnel_add: created tunnel ip6tnl1 (6) from 2001:db8:ffff:0:0:0:0:1000 to 2001:db8:0:1:12fe:edff:fe05:ed2e user count 1
mh_send_ba: status Binding Update accepted (0)
remote CoA 2001:db8:0:1:12fe:edff:fe05:ed2e

From the logs on the home agent, the care-of-address can be verified. The home agent sends a binding ACK reply to mobile router for each successful reception. The tunnel is also available on the home agent can also be verified by its starting point as well as end point at the home agent by using "ifconfig".
rootHomeAgent:/home/tmsproject# ifconfig
ip6tnl1 Link encap:UNSPEC HWaddr

```
20-01-0D-B8-FF-FF-00-00-00-00-00-00-00-00-00-00
inet6 addr: fe80::222:19ff:fe06:d2e1/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MTU:1460 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

The binding update list entries (bul) on the mobile router and binding cache entry (bc) on the home agent in the network scenario when mobile router is attached to foreing network are as follows:

```
    mip6d >bc
hoa 2001:db8:ffff:0:0:0:0:1 nonce 0 status registered
coa 2001:db8:0:1:12fe:edff:fe05:ed2e nonce 0 flags AH–
local 2001:db8:ffff:0:0:0:0:1000 tunnel ip6tnl1 link eth0
lifetime 54 / 60 seq 49849 unreach 0 mpa 383 / 619 retry 0


    mip6d >bul
== BUL_ENTRY ==
Home address 2001:db8:ffff:0:0:0:0:1
Care-of address 2001:db8:0:1:12fe:edff:fe05:ed2e
CN address 2001:db8:ffff:0:0:0:0:1000
lifetime = 60, delay = 57000
flags: IP6_MH_BU_HOME IP6_MH_BU_ACK IP6_MH_BU_MR
ack ready
dev eth0 last_coa 2001:db8:0:1:12fe:edff:fe05:ed2e
lifetime 11 / 60 seq 34513 resend 0 delay 57(after 8s) expires 11
mps 77650 / 77701
```

All of the above logs confirm that the connection works properly and binding updates are sent and received when mobile router is in foreign network. The end points of the tunnel are mobile router's and home agent's addresses.

B.3 When Mobile router is attached to Foreign Network 2

While NEMO components are running, mobile router moves from foreign network 1 to foreign network2. In this case we receive different update logs as shown below, which demonstrates the successful connection establishment in foreign network2 and binding establishment in between Home network and foreign network 2.

B.3.1 Logs on Mobile Router

******Disconnection from foreign network1 *****
md_expire_router: expiring router fe80:0:0:0:222:19ff:fe06:db71 on iface (3)
__md_discover_router: discover link on iface (3)
******Connection with foreign network2 *****
md_change_default_router: add new router fe80:0:0:0:201:2ff:fe77:3088 on interface (3)
md_update_router_stats: ***Adding CoA 2001:db8:1:1:12fe:edff:fe05:ed2e on interface (3)***
mn_move: in foreign net
mn_get_home_lifetime: CoA lifetime 86398 s, HoA lifetime 85009 s, BU lifetime 60 s
mn_send_home_bu: ***Moved to foreign network***
mn_send_home_bu: Bule for HA exists. Updating it.
mh_send: sending MH type 5 from 2001:db8:ffff:0:0:0:0:1 to 2001:db8:ffff:0:0:0:0:1000
mh_send: local CoA 2001:db8:1:1:12fe:edff:fe05:ed2e
bul_update_timer: Updating timer
******Binding Update List *****
== BUL_ENTRY ==
Home address 2001:db8:ffff:0:0:0:0:1
Care-of address 2001:db8:1:1:12fe:edff:fe05:ed2e
CN address 2001:db8:ffff:0:0:0:0:1000
lifetime = 60, delay = 1000
flags: IP6_MH_BU_HOME IP6_MH_BU_ACK IP6_MH_BU_MR
****** Tunnel end point modified *****
tunnel_mod: modified tunnel 8 end points with from 2001:db8:1:1:12fe:edff:fe05:ed2e to 2001:db8:ffff:0:0:0:0:1000
mn_recv_ba: Got BA (status 0) from 2001:db8:ffff:0:0:0:0:1000 to home

address 2001:db8:ffff:0:0:0:0:1 with coa 2001:db8:1:1:12fe:edff:fe05:ed2e.

mh_bu_parse: Binding Update Received
tunnel_mod: modifying tunnel 6 end points with from 2001:db8:ffff:0:0:0:0:1000
to 2001:db8:1:1:12fe:edff:fe05:ed2e
__tunnel_mod: modified tunnel iface ip6tnl1 (6)from 2001:db8:ffff:0:0:0:0:1000
to 2001:db8:1:1:12fe:edff:fe05:ed2e
mh_send_ba: status Binding Update accepted (0)
mh_send: sending MH type 6 from 2001:db8:ffff:0:0:0:0:1000 to 2001:db8:ffff:0:0:0:0:1
mh_send: remote CoA 2001:db8:1:1:12fe:edff:fe05:ed2e

Binding Update List on mobile router and Binding Cache on home agent

mip6d> bul
== BUL_ENTRY ==
Home address 2001:db8:ffff:0:0:0:0:1
Care-of address 2001:db8:1:1:12fe:edff:fe05:ed2e
CN address 2001:db8:ffff:0:0:0:0:1000
lifetime = 60, delay = 57000
flags: IP6_MH_BU_HOME IP6_MH_BU_ACK IP6_MH_BU_MR
ack ready
dev eth0 last_coa 2001:db8:1:1:12fe:edff:fe05:ed2e
lifetime 15 / 60 seq 34539 resend 0 delay 57(after 13s) expires 15 mps 76217 /
77701

mip6d> bc
hoa 2001:db8:ffff:0:0:0:0:1 nonce 0 status registered
coa 2001:db8:1:1:12fe:edff:fe05:ed2e nonce 0 flags AH–
local 2001:db8:ffff:0:0:0:0:1000 tunnel ip6tnl1 link eth0
lifetime 43 / 60 seq 34540 unreach 0 mpa -1513 / 0 retry 0 MNP: 2001:db8:ffff:1:0:0:0:0/64

Bibliography

[1] A Ben Nacef and N Montavont. A generic end-host mechanism for path selection and flow distribution. In *IEEE, PIMRC*, 2008.

[2] A Hurson. *Connected computing environment*, volume 90. Academic Press, 2012.

[3] A Mihailovic, G Leijonhufvud, and T Suihko. Providing multi-homing support in ip access networks. In *IEEE, PIMRC*, 2002.

[4] Alexander Gladisch, Robil Daher, and Djamshid Tavangarian. Survey on mobility and multihoming in future internet. *Wireless personal communications*, 74(1):45–81, 2014.

[5] Antoine Boutet, Benoit Le Texier, Julien Montavont, Nicolas Montavont, and Guillaume Schreiner. Advantages of flow bindings: an embedded mobile network use case. In *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, page 14. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[6] J Ylitalo, T Jokikyyny, T Kauppinen, Antti J Tuominen, and J Laine. Dynamic network interface selection in multihomed mobile hosts. In *IEEE, HICSS*, 2003.

[7] Wesley M Eddy. At what layer does mobility belong? *Communications Magazine, IEEE*, 2004.

[8] D Le, X Fu, and D Hogrefe. A review of mobility support paradigms for the internet. *IEEE Communications Surveys and Tutorials*, 2006.

[9] R Wakikawa, E Paik, C Ng, K Kuladinithi, and T Noel. Goals and benefits of multihoming draft-ernst-generic-goals-and-benefits-01. *Internet-Draft*, 2005.

[10] Convergence of fixed and mobile broadband access/aggregation networks). http://ict-combo.eu/data/uploads/review_files/combo_d7_1_wp7_09may2013_jcp_v1.0.pdf, Accessed: 2016-04-21.

[11] Convergence of fixed and mobile broadband access/aggregation networks). http://ict-combo.eu/data/uploads/pdf-combo-v2/combo_d3.1_wp3_20june2014_orange_v2.0_sec.pdf, Accessed: 2016-04-21.

[12] Stéphane Gosselin, Anna Pizzinat, Xavier Grall, Dirk Breuer, Eckard Bogenfeld, Sandro Krauß, Jose Alfonso Torrijos Gijón, Ali Hamidian, Neiva Fonseca, and Björn Skubic. Fixed and mobile convergence: Which role for optical networks? *Journal of Optical Communications and Networking*, 7 (11):1075–1083, 2015.

[13] Magdalena Nohrborg. 3gpp a global initiative: Lte. http://www.3gpp.org/technologies/keywords-acronyms/98-lte, Accessed: 2016-04-09.

[14] SNSTelecom. Lte encyclopedia. https://sites.google.com/site/lteencyclopedia/home, Accessed: 2016-04-09.

[15] Alcatel Lucent. The lte network architecture—a comprehensive tutorial. *Strategic Whitepaper*, 2009.

[16] Bart Barton. Lte, 4g, epc, mme, pgw, sgw, interfaces and beyond tech-blog by bart barton. http://www.lteandbeyond.com/2012/01/functions-of-main-lte-packet-core.html, 2012. Accessed: 2016-04-09.

[17] Lead Engineer V. Srinivasa Rao, Senior Architect & Rambabu Gajula. Interoperable ue handovers in lte. http://go.radisys.com/rs/radisys/images/paper-lte-interoperable.pdf, Accessed: 2016-04-25.

[18] 3GPP, "Mobile IPv6 vendor specific option format and usage within 3GPP," Technical specification, Release 8, TS 29.282, 2014.

[19] Proxy mobile ipv6 (pmipv6) based mobility and tunnelling protocols. www.3gpp.org/DynaReport/29275.htm, Accessed: 2016-05-08.

[20] 3GPP, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)," Technical report, Release 10, TR 23.829, 2011.

[21] Sipto/lipa deployment architecture. http://tech.queryhome.com/26718/sipto-lipa-deployment-architecture, Accessed: 2016-05-08.

[22] 3GPP, "Local IP Access (LIPA) mobility and Selected IP Traffic Overload (SIPTO) at the local network," Technical report, Release 12, TR 23.859, 2013.

[23] Margaret Rouse. Ip address (internet protocol address) ip address. http://searchwindevelopment.techtarget.com/definition/IP-address, 2006. Accessed: 2016-04-09.

[24] Wikipedia. Ip address. https://en.wikipedia.org/wiki/IP_addresse, Accessed: 2016-04-09.

[25] Yakov Rekhter and Tony Li. An architecture for ip address allocation with cidr. *RFC 1518*, 1993.

[26] Wikipedia. Classless inter-domain routing. https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing, Accessed: 2016-04-09.

[27] Margaret Rouse. Cidr (classless inter-domain routing or supernetting). http://searchnetworking.techtarget.com/definition/CIDR, 2015. Accessed: 2016-04-09.

[28] Stephen E Deering. Internet protocol, version 6 (ipv6) specification. *RFC 2460*, 1998.

[29] Thomas Narten, Susan Thomson, and Tatuya Jinmei. Ipv6 stateless address autoconfiguration. *RFC 2462*, 2007.

[30] Wikipedia. Ipv6. https://en.wikipedia.org/wiki/IPv6, Accessed: 2016-04-09.

[31] Chakchai So-In, Raj Jain, Subharthi Paul, and Jianli Pan. Future wireless networks: key issues and a survey (id/locator split perspective). *International Journal of Communication Networks and Distributed Systems*, 8 (1-2):24–52, 2012.

[32] Pekka Nikander and Robert Moskowitz. Host identity protocol (hip) architecture. *RFC 4423*, 2006.

[33] Alberto García-Martínez, Marcelo Bagnulo, and Iljitsch Van Beijnum. The shim6 architecture for ipv6 multihoming. *Communications Magazine, IEEE*, 48(9):152–157, 2010.

[34] Yangyang Wang, Jun Bi, and Jianping Wu. Empirical analysis of core-edge separation by decomposing internet topology graph. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5. IEEE, 2010.

[35] Ali Hurson. *Connected computing environment*, volume 90. Academic Press, 2012.

[36] Dino Farinacci, V Fuller, David Meyer, and D Lewis. The locator/id separation protocol (lisp). *RFC 6830*, 2013.

[37] J Abley, K Lindqvist, E Davies, B Black, and V Gill. Rfc 4116: Ipv4 multihoming practices and limitations. *Network Working Group*, 2005.

[38] Margaret Wasserman and Fred Baker. Rfc 6296: Ipv6-to-ipv6 network prefix translation. *Internet Engineering Task Force (IETF)*, 2011.

[39] Ole Troan, David Miles, Satoru Matsushima, Tadahisa Okimoto, and Dan Wing. Ipv6 multihoming without network address translation. *IETF draft, March*, 18, 2013.

[40] Takayuki Tomonari and Shunji Kimura. Mobility support in ipv6 networks with dynamic dns servers. In *Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), 2013 International Joint Conference on*, pages 729–735. IEEE, 2013.

[41] Andreas Pappas, Stephen Hailes, and Raffaele Giaffreda. Mobile host location tracking through dns. In *Proceedings of IEEE London Communications Symposium, IEEE*, 2002.

[42] Alex C Snoeren and Hari Balakrishnan. An end-to-end approach to host mobility. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 155–166. ACM, 2000.

[43] Bashir Yahya and Jalel Ben-Othman. Achieving host mobility using dns dynamic updating protocol. In *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, pages 634–638. IEEE, 2008.

[44] Brian Wellington. Secure domain name system (dns) dynamic update. Technical report, RFC 3007, November, 2000.

[45] P Vixie, S Thomson, Y Rekhter, and J Bound. Rfc 2136 dynamic updates in the domain name system (dns update), internet engineering task force, 51 pages, 1997.

[46] C Perkins. Ip mobility support for ipv4. *RFC 3344*, 2002.

[47] D Johnson, C Perkins, and J Arkko. Mobility support in ipv6. *RFC 3775*, 2004.

[48] Mobile ip networks: An overview. http://searchunifiedcommunications.techtarget.com/feature/Mobile-IP-networks-An-overview, Accessed: 2016-04-17.

[49] Hesham Soliman, Ludovic Bellier, Karim Elmalki, and Claude Castelluccia. Hierarchical mobile ipv6 (hmipv6) mobility management. *RFC 5380*, 2008.

[50] R Koodli. Mobile ipv6 fast handovers. *RFC 5568*, 2009.

[51] S Gundavelli, K Leung, V Devarapalli, K Chowdhury, and B Patil. Proxy mobile ipv6. *RFC 5213*, 2008.

[52] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. Rfc 3963 network mobility (nemo) basic support protocol, 2005.

[53] Carlos J Bernardos, Antonio De La Oliva, María Calderón, Dirk von Hugo, and Holger Kahle. Nemo: Network mobility. bringing ubiquity to the internet access. *demonstration at IEEE INFOCOM*, 2006.

[54] Kent Leung, Gopal Dommety, Vidya Narayanan, and Alexandru Petrescu. Network mobility (nemo) extensions for mobile ipv4. *IFTF RFC5177. April*, 2008.

[55] Thierry Ernst. Network mobility support terminology. *Network*, 2007.

[56] Sangheon Pack, Taekyoung Kwon, Yanghee Choi, and Eun Kyoung Paik. An adaptive network mobility support protocol in hierarchical mobile ipv6 networks. *Vehicular Technology, IEEE Transactions on*, 58(7):3627–3639, 2009.

[57] R Wakikawa, V Devarapalli, G Tsirtsis, T Ernst, and K Nagami. Multiple care-of addresses registration. *RFC 5648*, 2009.

[58] C Ng, Thierry Ernst, E Paik, and Marcelo Bagnulo. Analysis of multihoming in network mobility support, 2007.

[59] G Tsirtsis, H Soliman, N Montavont, G Giaretta, and K Kuladinithi. Flow bindings in mobile ipv6 and nemo basic support. *RFC 6089*, 2011.

[60] T Ropitault and N Montavont. Implementation of flow binding mechanism. In *IEEE PerCom*, 2008.

[61] K Mitsuya, R Kuntz, S Sugimoto, R Wakikawa, and J Murai. A policy management framework for flow distribution on multihomed end nodes. In *ACM/IEEE international workshop on Mobility*, 2007.

[62] L Iannone, D Saucez, and O Bonaventure. Implementing the locator/id separation protocol: Design and experience. *Computer Networks*, 2011.

[63] D Saucez, L Iannone, O Bonaventure, and D Farinacci. Designing a deployable internet: the locator/identifier separation protocol. *Internet Computing, IEEE*, 2012.

[64] Chris White, Darrel Lewis, David Meyer, and Dino Farinacci. Lisp mobile node. *draft-meyer-lisp-mn-14.txt, Internet Engineering Task Force, Work in Progress*, 2016.

[65] F Coras, L Jakab, D Lewis, J Domingo-Pascual, and A Cabellos-Aparicio. Lisp network element deployment considerations. *RFC 7215, Internet Engineering Task Force*, 2014.

[66] S Fu and M Atiquzzaman. Sctp: state of the art in research, products, and technical challenges. *Communications Magazine, IEEE*, 2004.

[67] R Stewart. Stream control transmission protocol. *RFC 4960*, 2007.

[68] Randall Stewart and Chris Metz. Sctp: new transport protocol for tcp/ip. *Internet Computing, IEEE*, 5(6):64–69, 2001.

[69] Dsl router diagnostics (voip/sip, dect, pots). http://grauonline.de/wordpress/?page_id=546, Accessed: 2016-04-17.

[70] Sctp association establishment and termination. http://www.masterraghu.com/subjects/np/introduction/unix_network_programming_v1.3/ch02lev1sec8.html#ch02fig09, Accessed: 2016-04-17.

[71] M Tuexen, S Maruyama, and M Kozuka. Cisco systems, inc. category: Standards track q. xie motorola, inc. *Network Working Group R. Stewart Request for Comments: 5061*, 2007.

[72] R Stewart, Q Xie, L Yarroll, J Wood, K Poon, and M Tuexen. Sockets api extensions for stream control transmission protocol (sctp). *RFC 6458*, 2006.

[73] J Janardhan Iyengar. Concurrent multipath transfer using sctp multihoming. *Multihomed Communication with SCTP (Stream Control Transmission Protocol)*, page 99, 2012.

[74] Martin Becke, Hakim Adhari, Erwin P Rathgeb, Fu Fa, Xiong Yang, and Xing Zhou. Comparison of multipath tcp and cmt-sctp based on intercontinental measurements. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 1360–1366. IEEE, 2013.

[75] A Ford, C Raiciu, M Handley, and O Bonaventure. Tcp extensions for multipath operation with multiple addresses, 2013.

[76] Christoph Paasch, Gregory Detal, Fabien Duchene, Costin Raiciu, and Olivier Bonaventure. Exploring mobile/wifi handover with multipath tcp. In *Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design*, pages 31–36. ACM, 2012.

[77] Mptcp and product support overview. http://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html, Accessed: 2016-04-17.

[78] Costin Raiciu, Dragos Niculescu, Marcelo Bagnulo, and Mark James Handley. Opportunistic mobility with multipath tcp. In *Proceedings of the sixth international workshop on MobiArch*, pages 7–12. ACM, 2011.

[79] C Raiciu, M Handley, and D Wischik. Coupled congestion control for multipath transport protocols. *RFC6356, October*, 2011.

[80] L. Deng, D. Liu, T. Sun, M. Boucadair and G. Cauchie. Use-cases and requirements for mptcp proxy in isp networks, 2014.

[81] Georg Hampel, Anil Rana, and Thierry Klein. Seamless tcp mobility using lightweight mptcp proxy. In *Proceedings of the 11th ACM international symposium on Mobility management and wireless access*, pages 139–146. ACM, 2013.

[82] R Moskowitz and P Nikander. Host identity protocol architecture. *RFC 4423*, 2006.

[83] R Moskowitz, P Nikander, P Jokela, and T Henderson. Host identity protocol. *RFC 5201*, 2008.

[84] P Nikander, A Gurtov, and Thomas R Henderson. Host identity protocol (hip): Connectivity, mobility, multi-homing, security, and privacy over ipv4 and ipv6 networks. *Communications Surveys & Tutorials, IEEE*, 2010.

[85] Hip for linux. http://infrahip.hiit.fi/index.php?index=how, Accessed: 2016-04-17.

[86] J Laganier and L Eggert. Host identity protocol (hip) rendezvous extension. *RFC 5204*, 2008.

[87] M Komu, M Bagnulo, K Slavov, and S Sugimoto. Rfc 6316: Sockets application program interface (api) for multihoming shim. *Request for Comments*, 6316, 2011.

[88] Geoff Huston. Architectural commentary on site multi-homing using a level 3 shim. *draft-ietf-shim6-arch-00 (work in progress)*, 2005.

[89] E Nordmark and M Bagnulo. Shim6: level 3 muhihoming shim protocol for ipv6: Rfc5533, 2008.

[90] Md Sazzadur Rahman and Mohammed Atiquzzaman. Semo6-a multihoming-based seamless mobility management framework. In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pages 1–7. IEEE, 2008.

[91] SIP RFC3261. Session initiation protocol. *J. Rosenberg, H. Schulzrinne et al*, 2002.

[92] Abdullah Azfar, A Hossen, and Razib Hayat Khan. Sip mobility modes: Application layer and data link layer. *International Journal of Computer Science and Network Security, IJCSNS 2009*, 9(12):258–264, 2009.

[93] Wesley M Eddy. At what layer does mobility belong? *Communications Magazine, IEEE*, 42(10):155–159, 2004.

[94] Marcelo Bagnulo, Phil Eardley, Alan Ford, Alberto García-Martínez, Alexandros Kostopoulos, Costin Raiciu, and Francisco Valera. Boosting mobility performance with multi-path tcp. In *Future Network and Mobile Summit, 2010*, pages 1–8. IEEE, 2010.

[95] Matthieu Coudron, Stefano Secci, Guy Pujolle, Patrick Raad, and Pascal Gallard. Cross-layer cooperation to boost multipath tcp performance in cloud networks. In *Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on*, pages 58–66. IEEE, 2013.

[96] Pratibha Mitharwal, Christophe Lohr, and Annie Gravey. Survey on network interface selection in multihomed mobile networks. In *Advances in Communication Networking*, pages 134–146. Springer, 2014.

[97] Pulak K Chowdhury, Mohammed Atiquzzaman, and William Ivancic. Sinemo: An ip-diversity based approach for network mobility in space.

In *Space Mission Challenges for Information Technology, 2006. SMC-IT 2006. Second IEEE International Conference on*, pages 7–pp. IEEE, 2006.

[98] Yonghao Sun, Yong Cui, Wendong Wang, Tianze Ma, Yuri Ismailov, and Xin Zheng. Mobility support in multi-path tcp. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pages 195–199. IEEE, 2011.

[99] Wikipedia. Dynamic host configuration protocol version 6 (dhcpv6). https://en.wikipedia.org/wiki/DHCPv6, Accessed: 2016-02-24.

[100] Tanguy Ropitault and Nicolas Montavont. Implementation of flow binding mechanism. In *Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on*, pages 342–347. IEEE, 2008.

[101] Kent Leung, Gopal Dommety, Vidya Narayanan, and Alexandru Petrescu. Rfc5177: Network mobility (nemo) extensions for mobile ipv4. *IFTF RFC5177. April*, 2008.

[102] M Scharf and A Ford. Multipath tcp (mptcp) application interface considerations. Technical report, RFC 6897, March, 2013.

[103] Tms deliverable (version 4). http://tms-project.eu, Accessed: 2016-04-21.

[104] The Linux Foundation. Netem. http://www.linuxfoundation.org/collaborate/workgroups/networking/netem, Accessed: 2016-03-18.

[105] Nautilus6 working group. Nautilus6 - implementation. http://www.nautilus6.org/implementation/index.html, Accessed: 2016-03-18.

[106] Nautilus6 working group. Atlantis: Nemo basic support implementation. http://www.nautilus6.org/implementation/atlantis.html, Accessed: 2016-03-18.

[107] UMIP group. How to setup a nemo basic support testbed with ipsec static keying). http://umip.org/docs/umip-nemo.html, Accessed: 2016-02-24.

[108] Fabien Duchêne Sébastien Barré, Christoph Paasch and Gregory Detal. Multipath tcp - linux kernel implementation. http://www.multipath-tcp.org/, Accessed: 2016-03-18.

[109] Lawrence Stewart. Multipath tcp for freebsd v0.1. http://lists.freebsd.org/pipermail/freebsd-net/2013-March/034882.html, Accessed: 2016-03-25.

[110] John Gudmundson. Maximize mobile user experience with netscaler multipath tcp. https://www.citrix.com/blogs/2013/05/28/maximize-mobile-user-experience-with-netscaler-multipath-tcp/, Accessed: 2016-03-18.

[111] Olivier Bonaventure. Apple seems to also believe in multipath tcp. http://perso.uclouvain.be/olivier.bonaventure/blog/html/2013/09/18/mptcp.html, Accessed: 2016-03-25.

[112] Patrick Thomas and Kate Pearce. Mptcp roams free (by default!) – os x yosemite. http://labs.neohapsis.com/2014/10/20/mptcp-roams-free-by-default-os-x-yosemite/, Accessed: 2016-03-25.

[113] openmaniak. Iperf. http://openmaniak.com/fr/iperf.php, Accessed: 2016-02-24.

[114] Thomas Dreibholz. Netperfmeter : A network performance metering tool. http://blog.multipath-tcp.org/blog/html/2015/09/07/netperfmeter.html, Accessed: 2016-02-24.

[115] Encapsulation overhead calculator. http://baturin.org/tools/encapcalc/, Accessed: 2016-05-04.

[116] Wikipedia. Transmission time. https://en.wikipedia.org/wiki/Transmission_time, Accessed: 2016-02-24.

[117] Multipath tcp - linux kernel implementation: Release 91. http://multipath-tcp.org/pmwiki.php?n=Main.Release91, Accessed: 2016-11-09.

[118] Souheir Eido, Pratibha Mitharwal, Annie Gravey, and Christophe Lohr. Mptcp solution for seamless local sipto mobility. *HPSR : 16th International Conference on High Performance Switching and Routing , 01-04 july 2015, Budapest, Hungary*, 2015.

[119] J. Son Dr. Harrison and Dr. Michelle M. Do. 5g network as envisioned by kt - analysis of kt's 5g network architecture, November 2015.

[120] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)," Technical report, Stage 2, Release 12, TS 36.300, 2014.

[121] Robert Moskowitz, Pekka Nikander, Petri Jokela, and Thomas Henderson. Host identity protocol. *RFC5201, April*, 2008.

[122] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," Technical specification, Release 13, TS 23.401, 2014.

[123] Z Savic. "LTE Design and Deployement Strategies," Cisco, 2011.

[124] J Mackar and S Corson. Rfc 2501,". *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF*, 1999.

[125] E Baccelli and M Townsley. Ip addressing model in ad hoc networks. Technical report, RFC 5889, September, 2010.

[126] IETF. Manet working group. https://tools.ietf.org/wg/manet/, Accessed: 2016-05-31.

[127] Damien Saucez, Luigi Iannone, and Olivier Bonaventure. Locator/id separation protocol (lisp) threat analysis. *RFC 7835*, 2016.

[128] Souheir Eido and Annie Gravey. How much lte traffic can be offloaded? In *Advances in Communication Networking*, pages 48–58. Springer, 2014.

[129] Cisco Visual Networking Index Cisco. Global mobile data traffic forecast update, 2015–2020. *white paper*, 2016.

[130] Pratibha Mitharwal, Christophe Lohr, and Annie Gravey. Survey on network interface selection in multihomed mobile networks. In *Advances in Communication Networking*, pages 134–146. Springer, 2014.

[131] 3GPP, "Study on co-ordinated Packet data network GateWay (PGW) Change for Selected IP Traffic Offload (C-SIPTO)," Technical report, Release 13, TR 22.828, 2014.

[132] Tarik Taleb and Adlen Ksentini. Follow me cloud: interworking federated clouds and distributed mobile networks. *Network, IEEE*, 27(5):12–19, 2013.

[133] Arijit Banerjee, Xu Chen, Jeffrey Erman, Vijay Gopalakrishnan, Seungjoon Lee, and Jacobus Van Der Merwe. Moca: a lightweight mobile cloud offloading architecture. In *Proceedings of the eighth ACM international workshop on Mobility in the evolving internet architecture*, pages 11–16. ACM, 2013.

[134] R. Gupta and N. Rastogi. "LTE Advanced – LIPA and SIPTO," White Paper, 2012.

[135] 3GPP, "Feasibility study for evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)," Technical report, Release 12, TR 25.912, 2014.

[136] Cisco Visual Networking Index. Forecast and methodology, 2014-2019 white paper. Technical report, Technical Report, Cisco, 2015.

[137] SN Bhatti and RJ Atkinson. Identifier-locator network protocol (ilnp) architectural description. *RFC6740, April*, 2012.

[138] Charles E Perkins. Mobile networking through mobile ip. *Internet Computing, IEEE*, 2(1):58–69, 1998.

Résumé en français

L'architecture de TCP/IP avait été conçue historiquement pour des ordinateurs lourds, difficilement déplaçables, et dotés d'une seule interface réseau. Le fait d'être stationnaire les rendait facilement identifiables au moyen de leur unique adresse IP. Avec l'évolution de la technologie, les choses ont radicalement changé. Les ordinateurs (tels que les ordinateurs portables, tablettes, etc.) peuvent être facilement déplacés et peuvent être connectés par plus qu'une interface réseau, alors que dans le même temps l'architecture d'Internet reste sensiblement la même.

Mobilité et multi-homing partagent une exigence commune, c.à.d. devoir gérer un flux donné au via différentes interfaces réseau. Au cours de la mobilité, le point de raccordement Internet change, il faut donc changer d'adresse IP. De manière similaire, grâce au multi-homing, le flux peut changer d'IP si un chemin est rompu ou si l'on souhaite multiplexer la connexion sur toutes les interfaces réseau disponibles. L'utilisation simultanée de toutes les interfaces réseau disponibles peut améliorer le débit, l'équilibrage de charge et de rendre le système plus résilient. Avec une demande accrue de la connectivité, il y a une demande accrue de la bande passante ainsi que du débit. C'est pourquoi, lorsque l'on combine la mobilité avec le multi-homing, cela peut être bénéfique pour l'amélioration de la mobilité elle-même, rendre plus fluide la période de transition, et augmenter les débits.

Mobilité et multi-homing

La *mobilité* fait référence à une situation où un hôte terminal change son point d'attache topologique à Internet. Chaque fois qu'un hôte se déplace, son adresse de couche réseau change. Ainsi, afin de continuer à communiquer, l'hôte doit être en mesure de signaler les changements de ses adresses à ses pairs avec lesquels il a des communications actives. Si c'est un terminal utilisateur qui est mobile,

cela est appelé "*host mobility*", c.à.d. mobilité d'un seul hôte. En revanche, si les hôtes sont raccordés à un routeur et que celui-ci est mobile avec tout son réseau interne, on parle alors de "*network mobility*".

Le *multi-homing* se réfère à une situation où un point terminal dispose de plusieurs chemins parallèles pour la communication avec le reste de Internet [2]. Cette situation peut être caractérisée comme le fait que l'hôte est accessible par plusieurs chemins topologiques (avec plusieurs adresses de couche réseau) qui sont complètement indépendants les uns des autres. Quand un hôte est connecté à plusieurs réseaux d'accès différents, il est connu comme un "*hôte multi-homé*". Lorsqu'un réseau de bordure est interconnecté au réseau de cœur de manière redondante par plusieurs connexions via plusieurs routeurs de bordure ou par un routeur de bordure disposant de plusieurs interfaces, on parle alors de "*site multi-homé*".

Le multi-homing aide à gérer la redondance et la tolérance aux pannes, augmente la bande passante, équilibre la charge sur le réseau d'accès et permet une gestion du trafic en aiguillant les flux sur tous les chemins, en utilisant les règles définies par l'utilisateur [3].

Questions concernant la mobilité et le multi-homing

Le rôle double d'identifiant et de localisateur que joue l'adresse IP devient le principal problème pour résoudre la mobilité et le multi-homing.

Chaque fois que l'adresse IP change en raison de l'occurrence d'un événement de mobilité, la gestion de la localisation de l'utilisateur devient la difficulté première. Ce changement de localisation exige également la gestion du transfert pour les sessions en cours.

Cependant, le multi-homing a besoin de traiter un ensemble de questions différentes pour s'articuler avec l'architecture historique d'Internet, comme le transport de données par trajets multiples et des mécanismes pour la sélection d'interface.

Contexte et exigences

Le principal travail de cette thèse liée à la mobilité et au multi-homing est de proposer des solutions aux problèmes spécifiques rencontrés par deux projets de recherche présentés ci-dessous.

Terminal Marine Stabilisé (TMS)

Cette thèse a été réalisée dans le cadre du projet TMS[1] qui a pour but de concevoir un terminal stabilisé pour la communication marine. Ce terminal facilitera l'accès à haut débit IP pour les utilisateurs sur différents types de bateaux (par exemple des pêcheurs, des plaisanciers, les garde-côtes, des navires de sauvetage, des bateaux de croisière, etc.) en mer et dans les zones portuaires. L'objectif principal est de fournir un accès Internet, des cartes météorologiques, des cartes portuaires, des plans de bateaux (sauvetage), les documents médicaux, photos/vidéos, lectures scientifiques, rapports d'observations de la mer, transmission vidéo pour des grutiers sur le port, etc.

Toutes les activités du projet de TMS, de l'étude aux mises en œuvre et la validation, sont partagées entre ses partenaires THALES, Alcatel-Lucent (ALU), SATIMO, Déti, Télécom-Bretagne et TES Electronique.

La principale contribution de notre travail porte sur les problèmes de routage IP dans les réseaux mobiles et multi-homés. Sur un bateau, l'infrastructure réseau entière est soumise à la mobilité (réseaux, sous-réseaux, équipements, terminaux, etc.).

Cependant, l'accès à Internet peut être sporadique ou encore multi-homé avec des connexions multiples (satellite, LTE, 3G, WiFi). Par conséquent, le projet TMS nécessite une solution pour la gestion de réseaux mobiles et multi-homés, avec un routage efficace.

COnvergence of fixed and Mobile BrOadband access/aggregation networks (COMBO)

L'objectif principal du projet COMBO est d'étudier et de proposer de nouvelles approches intégrées pour la convergence fixe-mobile et l'intégration du réseau fixe-mobile dans les réseaux d'accès et d'agrégation large bande, et ceci pour différents scénarios tels que urbain, urbain dense, ou rural. COMBO vise une qualité optimale et transparente de l'expérience utilisateur avec une infrastructure de réseau optimisée assurant une performance accrue.

L'intégration de réseau mobile fixe permettrait un contrôle plus efficace sur les différents éléments de réseau, un gain de bande passante dans le réseau de cœur et métropolitain au moyen de technique de *offloading*, c.à.d. délestage des données

[1] Le projet est soutenu par le gouvernement français (Direction Générale des Entreprises)

mobiles, partage des ressources réseau, etc. La convergence fixe-mobile a été étudiée en considérant différents cas d'utilisation tels que l'utilisation simultanée de réseaux WiFi et mobiles, la commutation transparente du trafic entre les deux interfaces (à savoir, le multi-homing), ou encore un système de cache intégré pour l'optimisation de la distribution de contenu, etc.[12] COMBO introduit l'idée de Passerelle d'Accès Unifiée (c'est-à-dire, une passerelle unifiée pour fixe, mobile et WiFi) avec le Next Generation Point of Presence (NG-POP) pour avoir une meilleure répartition de toutes les fonctions essentielles, équipements et infrastructures de convergence réseaux. L'objectif de notre travail et d'obtenir une continuité de service sans coupure, dans le contexte de la distribution de contenus pour les réseaux 5G. Les serveurs de contenu distribuent les données dans des caches au plus près de l'utilisateur pour satisfaire un trafic élevé. Par ailleurs, dans 5G, les "bords" d'IP seront également mis près de l'utilisateur. Seulement, un utilisateur ne peut se connecter qu'à une passerelle unique (SGW) à la fois.

Par conséquent, chaque fois qu'un événement de mobilité se produit, ce qui exige un transfert de passerelle, la communication en cours est rompue. Malheureusement, certaines applications en temps réel comme le streaming vidéo ou les jeux ont besoin que la continuité de la session soit préservée.

État de l'art

Il y a plusieurs propositions pour résoudre la mobilité et le multi-homing.

La mobilité et le multi-homing de réseaux est pris en charge par NEMO [52, 53], Locator/Identifier Separation protocol (LISP) [36], Identifier Locator Networking protocol (ILNP) [137], etc. D'autre part, la mobilité et multi-homing pour un hôte seul est pris en charge par Mobile IP [138], Multi-Path TCP (MPTCP) [75], Host Identity Protocol [121]. Toutes les solutions existantes pour la mobilité et le multi-homing fournissent la gestion de la localisation de l'hôte ou du réseau avec des avantages et des inconvénients en ce qui concerne le déploiement, les changements d'infrastructure, le délai de transfert, le débit, un surcoût causé par des tunnels, etc.

Les approches suivies pour gérer la mobilité et le multi-homing peuvent être classés en fonction de la couche sur laquelle elles sont mises en œuvre. Les approches de la couche réseau pour résoudre la mobilité et le multi-homing fournissent facilement la gestion de la localisation, mais exigent des informations

relatives au trafic de la part de la couche de transport, afin de fournir un meilleur support de la mobilité.

D'autre part, les approches de la couche transport fournissent un meilleur support du multi-homing grâce au fait qu'elles peuvent facilement accéder aux informations concernant le temps aller-retour ou de la congestion. Cependant elles nécessitent une collaboration avec la couche réseau afin de fournir une gestion de la localisation efficace au lieu de déployer des mécanismes de rendez-vous encombrant. Il devient alors intéressant d'évaluer comment des approches de couche réseau et des approches de couche transport peuvent être mélangées.

Aussi, nous avons proposé une combinaison des approches réseau et transport en combinant NEMO et MPTCP. NEMO offre une gestion de localisation pour les réseaux mobiles (*Mobile Networks* – MN), et MPTCP permet de gérer des nœuds de réseau mobiles (*Mobile Network Nodes* – MNN), c'est-à-dire que les hôtes à l'intérieur du MN vont pouvoir participer aux prises de décision concernant la situation de multi-homing. Cette nouvelle combinaison de NEMO et MPTCP devrait fournir un meilleur support à la mobilité avec une meilleure prise en charge du multi-homing vis-à-vis du débit, du coût et l'équilibrage de charge pour les réseaux mobiles.

NEMO et MPTCP

NEMO [52, 53] a été conçu pour assurer la gestion de la mobilité pour MNs en permettant à un MN de se déplacer et recevoir le trafic lors de son itinérance. Ceci est réalisé avec l'aide d'une part d'un point d'ancrage fixe dans le réseau de résidence du MN, le *Home Agent* (HA), et d'autre part avec un *Mobile Router* (MR) à l'intérieur du MN. Le routeur mobile à l'intérieur du MN informe le HA de son point d'attache actuel au réseau, à savoir son adresse d'accueil (*Care-Of-Address* – CoA), en envoyant au HA des mises à jour d'information concernant son raccordement, et ceci à chaque fois qu'il s'attache à un nouveau réseau visité. Le HA intercepte tous les paquets entrants à destination du MN, encapsule ces paquets, et les retransmet vers la CoA du MN. À la réception, le MR décapsule ces paquets et les achemine à l'intérieur du MN. Pour le trafic sortant, le MR encapsule les paquets et les retransmet au HA; le HA décapsule alors les paquets reçus et les achemine reçus à l'intérieur d'Internet. Grâce à ce tunnel entre l'AP et le MR, le nœud du réseau mobile (*Mobile Network Node* – MNN) et le nœud de communication distant (*Communicating Node* – CN) n'ont pas à se préoccuper de la mobilité du MN.

MPTCP [75] permet à un hôte d'utiliser plusieurs chemins de données disponibles simultanément pour une session donnée. MPTCP est rétrocompatible avec TCP et ne nécessite donc pas de modification dans les infrastructures de réseau existantes. Un hôte compatible MPTCP démarre une session MPTCP comme une session TCP avec un drapeau SYN portant l'option supplémentaire MP_CAPABLE. Si l'hôte avec qui il communique supporte également MPTCP, il répond avec l'option MP_CAPABLE dans le SYN-ACK. Une fois la connexion établie, les hôtes peuvent s'informer de toutes les adresses disponibles et initier d'autres sous-flux MPTCP en utilisant ces adresses.

NEMO augmenté avec MPTCP

La combinaison proposée de NEMO et MPTCP n'exige aucune modification majeure dans le fonctionnement NEMO ou MPTCP. Deux modifications mineures sont proposées pour NEMO afin de rendre les MNNs conscients de la mobilité. Le premier changement est que le MR doit annoncer le préfixe du réseau actuel visité ou les préfixes d'accueil pour les MNNs. Après avoir reçu les préfixes du réseau d'accueil, les MNNs peuvent configurer leurs interfaces avec de nouvelles adresses IP par le mécanisme d'autoconfiguration IP sans état [29]. Le deuxième changement est que le MR doit être en mesure de router vers Internent les paquets portant des adresses IP du réseau d'accueil, et router dans le tunnel vers le HA les paquets portant des adresses IP du réseau de résidence.

Comme NEMO est utilisé pour la gestion de la localisation, le trafic entrant doit passer par le HA. Le CN ne connaît que l'adresse de résidence du MNN lorsqu'il envoie sa demande d'établissement de connexion. Le HA reçoit ce paquet et le transmet via le tunnel vers le MR à son point d'attache réseau actuel. À la réception, le MNN génère un SYN-ACK avec l'option MP_CAPABLE. Si le CN supporte également MPTCP, les deux nœuds peuvent établir une connexion MPTCP. Une fois que la connexion est établie pour une session donnée, d'autres sous-flux peuvent être ajoutés à cette session et utiliser les interfaces disponibles. Le sous-flux avec l'adresse IP de résidence du MNN peut être mis comme un chemin "de secours" avec l'aide de l'option MP_PRIO. Le chemin de secours est utilisé seulement quand aucune des autres interfaces réseau n'est disponible. Le MR est capable de router vers Internet les paquets portant les adresses IP du réseau d'accueil. Par conséquent, après la mise en place de la connexion MPTCP, le tunnel n'est plus utilisé. Cependant, les tunnels NEMO peuvent toujours être

utilisés dans les cas où les réseaux visités sont “inamicaux” à cause de NATs, pare-feu, etc.

Lorsqu'au cours de la mobilité, le MR perd son point de raccordement et se rattache à un nouveau point de raccordement réseau, il annonce le préfixe du réseau nouvellement acquis vers les MNNs. En utilisant ce nouveau préfixe, les MNNs peuvent configurer leurs interfaces avec une nouvelle adresse IP (CoA). Cette adresse IP acquise peut alors être communiquée au CN en utilisant l'option ADD_ADDR, et l'adresse IP indisponible peut être retirée en utilisant l'option REMOVE_ADDR. Dans la proposition présente, le tunnel construit par NEMO est utilisé uniquement pour initier des communications depuis les nœuds extérieurs vers les MNNs. Pour le trafic sortant, les MNNs peuvent utiliser leur CoA pour établir une connexion MPTCP. Ceci est la seule différence entre la signalisation pour le trafic sortant et le trafic entrant.

Une fois la connexion établie, les adresses IP peuvent être ajoutées ou supprimées en utilisant les options de MPTCP; les trafics entrants et sortants prennent la même route.

L'approche proposée améliore ainsi le routage, réduit l'utilisation de tunnels, améliore potentiellement l'équilibrage de charge et le débit. Ces améliorations ont été mises en lumière à l'aide de la réalisation d'un banc de test en laboratoire.

MultiPath-TCP pour la continuité de session dans les réseaux mobiles 5G

Ceci est la seconde contribution de la thèse.

Les travaux présentés ici ont été obtenus en étroite collaboration avec ma collègue Souheir Eido. Ce travail a été partiellement publié dans [118], et une présentation plus complète est donnée à l'annexe A. Ma contribution à ce travail consiste principalement en l'analyse des solutions pour le multi-homing dans le cadre de la distribution des contenus dans les réseaux 5G, et à fournir un moyen de les utiliser pour résoudre le problème de la mobilité pour les cas d'utilisation de mobilité 3GPP SIPTO.

Description de la problématique et du contexte

Dans 3GPP, l'adresse est assignée par la passerelle de paquets de données (*Packet Data Gateway* – PGW). Dans l'architecture actuelle 3GPP, il y a très peu PGWs et la plupart d'entre eux sont centralisés. Cela provoque une latence élevée pour certains services en temps réel tels que les jeux, et consomme une bande passante élevée pour les services de distribution de contenu.

Pour alléger la charge de trafic dans le réseau de cœur, 3GPP a proposé deux méthodes pour décharger du trafic IP sélectionné en utilisant SIPTO (*Selected IP Traffic Offload*), et en distribuant plus de passerelles placées plus proche de l'utilisateur. SIPTO extrait une partie du trafic, soit après le réseau d'accès radio en choisissant une SGW/PGW qui soit plus proche géographiquement de l'utilisateur, soit au niveau du réseau local dans le cas de réseau IP résidentiel ou d'entreprise [20]. SIPTO dans un réseau local admet qu'un équipement utilisateur (*User Equipment* – UE) puisse accéder directement aux services du réseau IP privé en utilisant une passerelle locale (*Local Gateway* – LGW) qui soit raccordée également au réseau IP externe [120]. Une LBV comporte certaines des fonctions des PGW et des SGW, telle que des fonctions d'allocation d'adresse IP pour le UE de type DHCP (ou DHCPv6 pour IPv6), la mise en buffers des paquets descendants, ou encore la mise en tunnel direct vers le eNodeB. Les SGW et PGW peuvent des entités séparées (c'est-à-dire, autonomes) ou peuvent être co-localisées. De même, une LGW peut être une entité indépendante ou co-localisée avec le eNB (qui est alors un Home-eNB).

Le déploiement de passerelles co-localisées nécessite la gestion de la mobilité pour les sessions en cours, comme expliqué dans les cas d'utilisation suivants.

Dans le premier scénario, l'utilisatrice Alice accède aux services Internet alors qu'elle voyage dans un bus ou un train. À ce moment-là le réseau se décharge d'une partie du trafic en utilisant la SGW co-localisée avec la PGW. Puisque son smartphone est connecté à deux PGWs, elle a deux adresses IP actives, par exemple IP_{LTE} et $IP_{SGW/PGW}$. Supposons qu'elle joue à un jeu et que le réseau déroute ce trafic en utilisant l'$IP_{SGW/PGW}$ via eNodeB1. Le bus étant en mouvement, Alice se déplace d'eNodeB1 à eNodeB2 tout en continant son jeu. Ces eNodeB sont reliés à différentes SGWs co-localisées avec des PGWs. Par conséquent, le UE d'Alice se verra attribuer une nouvelle adresse IP par la nouvelle PGW, par exemple $IP_{NEW-SGW/PGW}$. L'ancienne adresse IP $IP_{SGW/PGW}$ deviendra alors inaccessible, ce qui va briser la session en cours et perturber le jeu.

Aussi, pour maintenir la continuité de session, le trafic devrait être transféré vers la nouvelle adresse acquise, en poursuivant le trafic en cours avec la précédente passerelle (paquets déjà transférés) vers la nouvelle passerelle.

Étant donné que le serveur de contenu est fixe, la commutation de chemins réseau (c.à.d. entre adresses IP) est un cas particulier de scénario de multi-homing, comme lorsque le trafic est commuté entre deux adresses IP en raison des caractéristiques du trafic ou en raison de l'indisponibilité d'une adresse IP.

Par conséquent, le problème du transfert de la session en cours de $IP_{SGW/PGW}$ ou IP_{LGW} vers $IP_{New-SGW/PGW}$ ou $IP_{New-LGW}$ peut être résolu à l'aide de solutions existantes de multi-homing. Cependant, le transfert va nécessiter des fonctionnalités supplémentaires dans le réseau mobile.

Solution de mobilité basée sur MPTCP

Initialement, le UE se voit assigné une adresse IP par la PGW globale lorsqu'il s'attache au réseau LTE. En utilisant cette adresse IP, le UE établit une connexion MPTCP avec le serveur de contenu, en supposant que le UE tout comme le serveur de contenu supportent MPTCP. Puisque cette adresse IP est valide lorsque l'utilisateur est sur le réseau LTE, elle peut être utilisée pour la signalisation MPTCP, comme la création ou la suppression de sous-flux. Après l'établissement de la connexion, le UE fait une demande pour établir un chemin de données SIPTO vers le serveur de contenus. Il reçoit alors une autre adresse IP de la passerelle la plus proche (co-localisée SGW/PGW ou LGW). Cette adresse IP est ensuite indiquée au serveur de contenu en utilisant l'option MP_JOIN de MPTCP, et un nouveau sous-flux est créé. Ce nouveau sous-flux (c'est-à-dire, le chemin de données SIPTO) est utilisé pour le trafic de données entrant, et le sous-flux avec l'adresse IP initiale est annoncé comme un chemin de secours utilisant l'option MP_PRIO.

Transfert SIPTO sans heurt

Au cours de la mobilité, chaque fois que l'utilisateur se déplace d'un eNodeB (eNB-source) à un autre eNodeB (eNB-cible), l'eNB-source envoie à l'UE une demande de mesure de la force de signal. À la réception de la réponse de l'UE, l'eNB-source prend une décision de transfert et envoie un message "*handover required*" au MME (*Mobility Management Entity*). Le MME sélectionne alors une

passerelle pour l'UE qui est géographiquement plus proche de l'UE. L'UE acquiert une nouvelle adresse IP de la SGW/PGW ou de la LGW à laquelle il se rattache, et une nouvelle connexion SIPTO est établie. Ensuite, il notifie le serveur de contenu pour ajouter cette nouvelle adresse IP en utilisant l'option MP_JOIN. Une fois que le serveur de contenu reçoit l'option MP_JOIN, il peut lancer un nouveau sous-flux en utilisant la nouvelle adresse IP. L'adresse IP de l'UE allouée par la passerelle SGW/PGW co-localisée précédente devient inaccessible au cours de la connexion à la nouvelle passerelle, passerelle qui permet d'acquérir une nouvelle adresse IP et de créer un nouveau sous-flux avec elle. Pendant ce temps, il y a une partie du trafic qui a déjà été transféré à la passerelle précédente. Par conséquent, afin d'effectuer une transition en douceur entre passerelle source et passerelle cible, le MME doit initier le transfert même quand une délocalisation PGW est nécessaire et maintenir la connexion active existante jusqu'à ce que le transfert soit terminé. Un tunnel de transfert indirect est alors établi entre les SGWs source et cible. Ce transfert est effectué selon la procédure de transfert "inter eNB/inter SGW" défini dans [122].

Après la mise en place d'un tunnel de bout en bout entre les passerelles source et cible, le trafic peut être repris. Pendant le transfert, le UE notifie le serveur pour supprimer l'adresse IP précédente, et supprime le sous-flux avec l'adresse IP précédente. Une fois que le transfert est terminé, alors seulement la connexion précédente est désactivée par la MME.

Ici, il convient de mentionner que la capacité de multi-homing de MPTCP est utilisée uniquement pour assurer la continuité de la session. Les deux sous-flux sont utilisés simultanément seulement pendant le transfert. À l'issue de l'opération de transfert, le premier sous-flux est supprimé. Seul le lien actuellement actif est utilisé pour les données entrantes. Il faut aussi mentionner que pour expliquer la proposition, nous supposons que le UE et le serveur de contenu doivent supporter MPTCP. Pour les éléments qui ne supportent pas nativement MPTCP, on peut avoir recours à des proxys MPTCP.

Conclusion et perspectives

La caractéristique commune à la mobilité et au multi-homing repose dans la capacité à transporter un flux donné par différentes interfaces réseau.

Dans la première contribution de la thèse, le protocole de multi-homing MPTCP permet d'améliorer la mobilité de réseau dans le contexte des réseaux mobiles

multi-homés tels que les voitures, les bus, les bateaux, les personnes, etc. À l'avenir, il y aura certainement de plus en plus véhicules avec un réseau installé à bord, et les personnes aussi seront aussi des réseaux avec de multiples terminaux sur eux, par exemple le smartphone, tablette, montre, pacemaker, etc. Par conséquent, NEMO augmentée avec MPTCP offre une solution à faible coût et peu complexe pour les réseaux mobiles multi-homés. La solution proposée améliore aussi le routage fourni par NEMO et augmente le débit. Son niveau de sécurité est celui d'Internet en général.

Dans la deuxième contribution de la thèse, le protocole de multi-homing MPTCP contribue à assurer la continuité de la session dans le contexte de la distribution de contenu dans 5G. Dans le réseau 5G, les bords d'IP seront plus proche des nœuds terminaux hôtes pour améliorer l'expérience utilisateur et réduire la charge de trafic dans le réseau de cœur.

La solution actuelle pour la mobilité nécessite un point fixe quelque part dans le réseau de résidence habituel du réseau mobile. Supposons un scénario en temps réel où quelqu'un a besoin de communiquer depuis une voiture avec une personne voyageant dans la voiture devant ou derrière lui. Le trafic doit voyager par ce nœud fixe quelque part dans Internet avant d'atteindre à l'autre voiture. Cela provoque des retards inutiles. Par conséquent, il serait intéressant d'étudier la communication inter-véhicules sans un nœud fixe. En outre, cela sera utile dans le cas des voitures autonomes où les voitures devront communiquer entre elles avec l'exigence un délai minimum.

Dans le contexte de la distribution de contenu, il y a des propositions intéressantes telles que HTTP2, QUIC etc. Le protocole QUIC vise à multiplexer le trafic UDP sur toutes les interfaces réseau disponibles. HTTP2 essaye de résoudre les besoins de multi-homing au niveau applicatif, mais il n'est pas possible d'ajouter une nouvelle interface pendant une session en cours. Aussi, il serait intéressant d'étudier HTTP2 sur QUIC par rapport à MPTCP.

Résumé

Cette thèse présente une solution pour améliorer la mobilité des réseaux, dans le cadre de communications véhiculaires ainsi que pour la distribution de contenu. Les solutions actuelles pour les communications véhiculaires (c'est-à-dire lorsqu'un réseau est mobile) reposent sur la mise en place de tunnels, permettant également d'utiliser simultanément les différentes interfaces disponibles sur le véhicule (multi-homing). Même avec des tunnels, ces solutions ne sont pas en mesure d'équilibrer le trafic sur les interfaces réseau disponibles, elles ne parviennent pas à tirer partie du multi-homing. De plus, certaines des solutions existantes pour la mobilité de réseau cachent la mobilité aux hôtes connectés au routeur mobile. De fait, cela empêche les hôtes de participer aux décisions relatives au multi-homing, telles que le choix de l'interface réseau à utiliser, ce qui est pourtant utile pour réaliser du routage à moindre coût. Dans cette thèse, nous proposons de combiner un protocole de mobilité réseau (tel que NEMO) avec le protocole de TCP-multivoies (MPTCP), ce qui permet aux nœuds hôtes de participer à la mobilité et au multi-homing. Cette nouvelle combinaison améliore significativement le routage et l'encapsulation de paquets causée par les tunnels. En outre, cela augmente le débit, la tolérance de panne, le temps d'aller-retour et réduit le délai de transmission.

La deuxième contribution de ce travail propose une solution de continuité de session pour la distribution de contenu dans les réseaux 5G. Dans le réseau 5G, les équipements d'accès IP seront au plus proche des nœuds terminaux afin d'améliorer l'expérience utilisateur et de réduire la charge de trafic dans le réseau central. Le fait est qu'à un instant donné un terminal ne peut être raccordé qu'à une seule passerelle (SGW/PGW) à la fois. Et comme la passerelle change lors de la mobilité, les sessions en cours seront rompues, impactant les applications temps réelle, le streaming vidéo, les jeux, etc. Pour cela, la thèse présente une solution de continuité de session avec l'aide de TCP-multivoie en bénéficiant du fait que les serveurs de contenu sont stationnaires.

Mots clefs : Mobilité de réseau, NEMO, Mobilité automobile, MultiPath TCP, Multihoming, 5G, Continuité de session, Trafic Offload

Abstract

This thesis presents a solution for boosting network mobility in the context of vehicular communications and content distribution in fixed network. Existing solutions for vehicular communications (i.e., network mobility), relies on tunneling in order to use multiple available interfaces on a vehicle. Even with tunnels, these solutions are unable to balance the traffic over available network interfaces thus do not reach the goal to provide optimum multi-homing benefits. Moreover, some of the existing solutions for network mobility, hide the mobility from the hosts connected to the mobile router. This in result inhibits the host nodes from participating in multi-homing related decisions such as interface selection which can be helpful in performing least cost routing. In this thesis, we propose to combine network mobility protocol with MPTCP which enables the host nodes to participate in mobility and multi-homing. This novel combination significantly improves routing and tunneling packet overhead. Moreover it increases throughput, fault tolerance, round-trip time and reduces transmission delay.

The second contribution of this work is providing a solution for session continuity in context of content distribution in 5G networks. In 5G network, the IP edges will be closer to the host nodes in order to improve the user experience and reduce traffic load in the core network. The fact that a host can only be connected to a single gateway (SGW/PGW) at a time, would break the ongoing sessions for real time applications like video streaming or gaming during an occurrence of mobility event requiring gateway relocation. The thesis presents the solution for session continuity with the help of multipath TCP by benefiting from the fact that the content servers are stationary.

Keywords: Network Mobility, NEMO, Vehicular Mobility, MultiPath TCP, Multihoming, 5G, Session continuity, Traffic Offload

TELECOM Bretagne

n° d'ordre : 2016telb0407

Télécom Bretagne

Technopôle Brest-Iroise - CS 83818 - 29238 Brest Cedex 3

Tél : + 33(0) 29 00 11 11 - Fax : + 33(0) 29 00 10 00