ENHANCING THE QUALITY OF SERVICE IN MOBILE NETWORKS BASED ON NEMO BASIC SUPPORT PROTOCOL

BADIEA ABDULKAREM MOHAMMED AL-SHAIBANI

UNIVERSITI SAINS MALAYSIA

2018

ENHANCING THE QUALITY OF SERVICE IN MOBILE NETWORKS BASED ON NEMO BASIC SUPPORT PROTOCOL

by

BADIEA ABDULKAREM MOHAMMED AL-SHAIBANI

Thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

January 2018

DEDICATION

To:

My Father

My Mother

My Wife

My Sons

ACKNOWLEDGEMENT

I would like to express my deep gratitude to the Associate Professor Wan Tat Chee for his invaluable insights, countless reviews and guidelines that made this thesis possible; as well as Universiti Sains Malaysia and the School of Computer Sciences who gave me the opportunity to do this work. I would also like to thank Hodeidah University for the financial support. I would also like to thank my dear wife Yusra Mohammed and my beloved sons for their patience and support; I apologize for all those evenings that I have spent in front of a monitor instead of being with them. I would also like to acknowledge the passion and the support provided by my father, my mother and the rest of my family.

Badiea Abdulkarem Mohammed

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3G	Third Generation
4G	Fourth Generation
AR	Access Router
ARO	Access Router Option
ARP	Address Resolution Protocol
BA	Binding Acknowledgment
BS	WiMAX Base Stations
BSHO-RSP	WiMAX Base Station Handover Respond
BU	Binding Update Message
BWA	Broadband Wireless Access Networks
BWR	WiMAX Bandwidth Request
CN	Corresponding Node
CoA	Care-of Address
DAD	Duplicate Address Detection Algorithm
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DL-MAP	WiMAX MAC First Message (Mapping DownLink)
DUID	DHCPv6 Server DUID is a Unique Server Identifier
DVB	Digital Video Broadcast
ertPS	A WiMAX Traffic Type
EUI-64	The IEEE-Defined 64-bit Extended Unique Identifier
FA	Foreign Agent
FBAck	Fast Binding Acknowledgment Message

FBU	Fast Binding Update Message
FH802.16e	NEMO fast handover over IEEE802.16e
FINEMO	Fast Integrated NEMO Handover Scheme
FMIPv6	Fast Mobile IPv6
HA	Home Agent
HAck	Handover Initiation Acknowledgment Message
HI	Handover Initiation Message
HMIP-RO	Hierarchical MIPv6 based Route Optimization
HMIPv6	Hierarchical Mobile IPv6
HoA	Home Address
HO-IND	WiMAX handover “Indicate Message”
IETF	Internet Engineering Task Force
IMR	Intermediate Mobile Router
IP	Internet Protocol
IPMN	Interactive Protocol for Mobile Networking
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
L2	The Data Link Layer
L3	The Network Layer
LGD	Link Going Down Trigger
LUP	Link UP Trigger
MAC	Media Access Control in WiMAX
MAP	Mobility Anchor Point
MFINEMO	Proposed Modified Fast Integrated NEMO Handover.
MIPv6	Mobile IPv6

MN	Mobile Network
MNN	Mobile Network Nodes
MNP	Mobile Network Prefix
MONAMI6	Mobile Nodes and Multiple Interfaces
MR	Mobile Router
MR-HA RO	Proposed Route Optimization Scheme.
MSHO-REQ	WiMAX Handover Request
NAR	New Access Router
NBF	Neighbor Found Trigger
NBR_Adv	The WiMAX Neighbour Advertisement Message
NCoA	New Care-of Address
NEMO	Network Mobility
NEMO BS	NEMO Basic Support Mobility
nrtPS	A WiMAX Traffic Type
OAR	Old Access Router
PAR	Previous Access Router
PCoA	Previous Care-of Address
PDSN	Packet Data Serving Node
QFNEMO	Proposed Qualified Fast NEMO Handover and Route Optimization Scheme
QoS	Quality of Service
RA	IPv6 Router Advertisement Message
RBU+	Recursive Binding Update
REG-REQ	WiMAX Registration Request
REG-RSP	WiMAX Base Station Registering Response

RINEMO	Proposed Rapid Integrated Fast NEMO Handover Scheme
RNG-REQ	Ranging Request Message in WiMAX Entry Procedure
RNG-RSP	Ranging Respond Message in WiMAX Entry Procedure
RO	Route Optimization
RRH	Reverse Routing Header
RtAdv	Solicited IPv6 Router Advertisement Message
rtPS	A WiMAX Traffic Type
RtSol	Router Solicitation
SAA	IPv6 Stateless Autoconfiguration
SBC-REQ	WiMAX Scanning Request to Get Basic Capabilities
SBC-RSP	WiMAX Base Station’s Response to the Basic Capabilities Request
SCN-REP	WiMax Scanning Report
SCN-RSP	WiMax Scanning Respond or Grants
TCP	Trancefere Control Prorocol
TLAR	Top Level Access Router
TLMR	Top Level Mobile Router
UGS	WiMAX Unsolicited Grant Service
UL-MAP	WiMAX MAC Second Message (Mapping UpLink)
UNA	Unsolicited Neighbor Advertisement Message
VOIP	Voice Over IP
WiFi	The Commercial Name of Networks and Various Types of Equipment that are Conformant to the IEEE 802.11.
WiMAX	The Commercial Name of Networks and Various Types of Equipment that are Conformant to the IEEE 802.16.

xNEMO	Implemented Simulation Model to Evaluate NEMO Basic Support Scheme

MENINGKATKAN KUALITI PERKHIDMATAN DALAM RANGKAIAN BERGERAK BERDASARKAN PROTOKOL SOKONGAN ASAS NEMO

ABSTRAK

Bagi memenuhi keperluan capaian Internet tanpa gangguan di samping pergerakan dalam rangkaian bergerak sebagai suatu alternatif bagi kebolehgerakan / mobiliti perumah hujung (end-host), maka kumpulan kerja IETF NEMO dicipta untuk mengembangkan sokongan kebolehgerakan perumah hujung dalam Mobile IPv6 (MIPv6). Kumpulan ini mempiawaikan Protokol Sokongan Asas NEMO (Basic Support Protocol, NEMO BS) untuk menyokong kebolehgerakan rangkaian. Namun demikian, ke serahan (handover latency) dalam NEMO BS adalah tinggi dan rangkaian terowong dalam rangkaian NEMO tidak diambil kira dalam spesifikasi protokol ini. Isu yang memberi impak terhadap jaminan QoS semasa proses serahan dalam NEMO BS adalah keperluan untuk merendahkan kependaman serahan, masa gangguan, dan kegagalan lepas-tangan hampir-sifar (near-zero handoff failure) dan kadar kehilangan paket. Banyak skema dicadangkan bagi menyelesaikan masalah ini melalui pengoptimuman prosedur isyarat serahan (handover signaling procedure) dan skema pengoptimuman penghala bagi NEMO. Penyelidikan ini mencadangkan suatu rangka kerja baru yang menggabungjalinkan prosedur isyarat serahan dioptimum yang lebih baik dan skema pengoptimuman penghala yang dicadangkan sebagai penyelesaian bagi kekurangan masalah rangkaian terowong. Keputusan analitik tunjukkan kepentingan skema yang dicadang untuk dibandingkan dengan skema lain yang ada, menunjukkan bahawa skema yang dicadang mampu mengurangkan kependaman serahan dan masa gangguan perkhidmatan. Eksperimen yang disimulasikan menggunakan OMNeTt++ 4.3.1 peralatan simulasi dijalankan untuk menilai rangka kerja yang dicadangkan. Keputusan eksperimen menunjukkan bahawa kependaman serahan, masa gangguan, dan kehilangan paket dalam rangka kerja yang dicadang mampu dikurangkan masing-masing sebanyak 24.34%, 91.88% dan 99.28% berbanding dengan NEMO BS.

ENHANCING THE QUALITY OF SERVICE IN MOBILE NETWORKS BASED ON NEMO BASIC SUPPORT PROTOCOL

ABSTRACT

To fulfil the need for an uninterrupted Internet access along with the move in mobile networks as an alternative to the end-host mobility, the IETF NEMO working group was created to extend basic end-host mobility support in Mobile IPv6 (MIPv6). This group standardizes NEMO Basic Support Protocol (NEMO BS) to support network mobility. However, the handover latency in NEMO BS is high and the nested tunnels' problem in the nested NEMO networks is not considered in the main specification of this protocol. Issues affecting the provision of QoS guarantees during the handoff process in NEMO BS are the handover latency, the disruption time, and the handoff failure and the packet loss. Many schemes have been proposed to solve these issues by optimizing the handover signalling procedure and by proposing routing optimization scheme for NEMO. This research proposes a new framework that combines a better optimized signalling handover procedure, and a proposed Routing Optimization scheme as a solution for the lack of the nested tunnels' problem. Mathematical results highlight the importance of the proposed schemes compared to the related recent schemes are provided, revealing that the proposed scheme has reduced the handover latency and the service disruption time. Simulated experiments using OMNeTt++ 4.3.1 simulation tools have been carried out to evaluate the proposed framework. The results of the experiments showed that the handover latency, the

disruption time, and the packets lost in the proposed framework has been reduced by 24.34%, 91.88% and 99.28% respectively compared to NEMO BS.

CHAPTER 1 - INTRODUCTION

1.1 Background Information

The Mobile Devices (or the Mobile Nodes/the Mobile Network Nodes (MNNs)) which are able to connect to the Internet via the wireless technologies have become available and more popular (Perkins, 2015). The demand for being seamlessly connected to the Internet even while moving between cities or countries results in new challenges in the addressing system and the mobility support (Sathiaseelan & Crowcroft, 2013). Historically, Internet Protocol version 4 (IPv4) has been deployed to address all the interconnected nodes in the Internet, however, the growth of interconnected nodes has led to the depletion of IPv4 and a new version of addressing scheme called Internet Protocol version 6 (IPv6) was developed (Wu, Cui, Wu, Liu, & Metz, 2013). The addressing size was extended from 32-bit in IPv4 to 128-bit in IPv6 to provide flexibility in allocating addresses and routing traffic and to eliminate the primary need for Network Address Translation (NAT). The new features that have been added to IPv6 have made it more comfortable to be used for the mobility support (Wu et al., 2013).

To provide mobility support in IP-based networks, Internet Engineering Task Force (IETF) has standardized Mobile IPv4 (MIPv4), and Mobile IPv6 (MIPv6) to manage the mobility of the MNNs and ensure the IP services connectivity during the movement (Bolla & Repetto, 2014). The Home Agent (HA) concept and global (called Home Address (HoA)) and local (called Care-of Address (CoA)) IP addresses are created and deployed in MIPv6 to provide a good solution for both the mobility management and the connection ubiquity. The HA is located in the Home Network (HN) and responsible for managing the communications between the Mobile Network Node (MNN) and the Corresponding Nodes (CNs) in the Global Network. HoA is an IPv6 address that is assigned to the MN by its home Network, while CoA is an IPv6 address that is assigned to the MNN by the foreign network while it's being visited by the MNN (Johnson, Perkins, & Arkko, 2004). However, when an MNN moves from one link to another link in the IP infrastructure, new CoA needs to be configured and the HA needs to be updated by the new CoA. As a result of this, the connection ubiquity is harmed and a high disruption time is caused. This procedure of configuring new CoA and updating the HA by the new CoA is referred to as the Handover Procedure (Abdullah, Zukarnain, Farzaneh, & Abdullah, 2015).

Mobile IPv6 is an upgrade, which utilized the expertise obtained from the development of Mobile IPv4. Therefore, several features of the Mobile IPv6 are shared with Mobile IPv4, although upgraded with additional enhancements (Johnson et al., 2004). As future networks are envisaged to be based on IP, MIPv6 based protocols are anticipated to be the best choice for the mobility management in these future networks (Bhagwat, Perkins, & Tripathi, 1996; Bolla et al., 2014). Therefore, there are extensions defined for Mobile IPv6 were intended to make it more flexible, scalable, and capable of resolving different application scenarios. Examples of these extensions include Fast MIPv6 (FMIPv6) (Koodli, 2008), Hierarchical MIPv6 (HMIPv6) (Soliman, Castelluccia, ElMalki, & Bellier, 2008), Mobile Nodes and Multiple Interfaces (MONAMI6) (Wakikawa, Devarapalli, Tsirtsis, Ernst, & Nagami, 2009), Proxy Mobile IPv6 (PMIPv6) (Gundavelli, Leung, Devarapalli, Chowdhury, & Patil, 2008), and Network Mobility basic support protocol (NEMO / NEMO BS)

(Devarapalli, Wakikawa, Petrescu, & Thubert, 2005). More information, comparative analysis and performance for most of these extensions are presented in Jong-Hyouk, Bonnin, You, & Chung (2013).

If a group of MNNs moved together (e.g. in a public transport vehicle) each of them has to perform the handover procedure at the same time resulting in a serious extra unnecessary overhead and traffic inefficiency at the visited network (SamuelRaj, Jayapal, & Varadharajan, 2014). IETF has standardized the Network Mobility support (NEMO) (also referred to as NEMO Basic Support Protocol) to enable the group of nodes that move together (e.g. in a public transport vehicle) to handoff as a single network by linking them to a serving router called Mobile Router (MR) (SamuelRaj et al., 2014; Ernest, Falowo, & Chan, 2016). In NEMO, MR is the only entity which needs to perform the handover procedure and MNNs in MR's MN will not be involved with the handover procedure; this is referred to as the mobility transparency (Goswami, Das, & Joardar, 2013). Thus, NEMO supports network mobility while MIPv6 supports node mobility.

Using NEMO to manage groups' mobility should meet some requirements which are reduced transmission power at MNNs, reduced handover events and overhead, reduced complexity, and reduced bandwidth consumption (Céspedes, Shen, & Lazo, 2011). The maintenance of the data flow in NEMO is explained in the following paragraph.

The HA is located in the home network where the global address of the mobile network is topologically correct. All the traffics addressed to the global address of the mobile network are delivered to the HA, which in turn, forwards them towards the MR through a pre-created bidirectional tunnel. Next, the MR forwards each one to its destination within the mobile network. The traffics that are started in the mobile network are forwarded by the MR towards the HA through the bidirectional tunnel, the HA in turn forwards each of them to their destination. These operations are reflected in Figure 1.1 which adapted from Bernardos, et al. (2007).

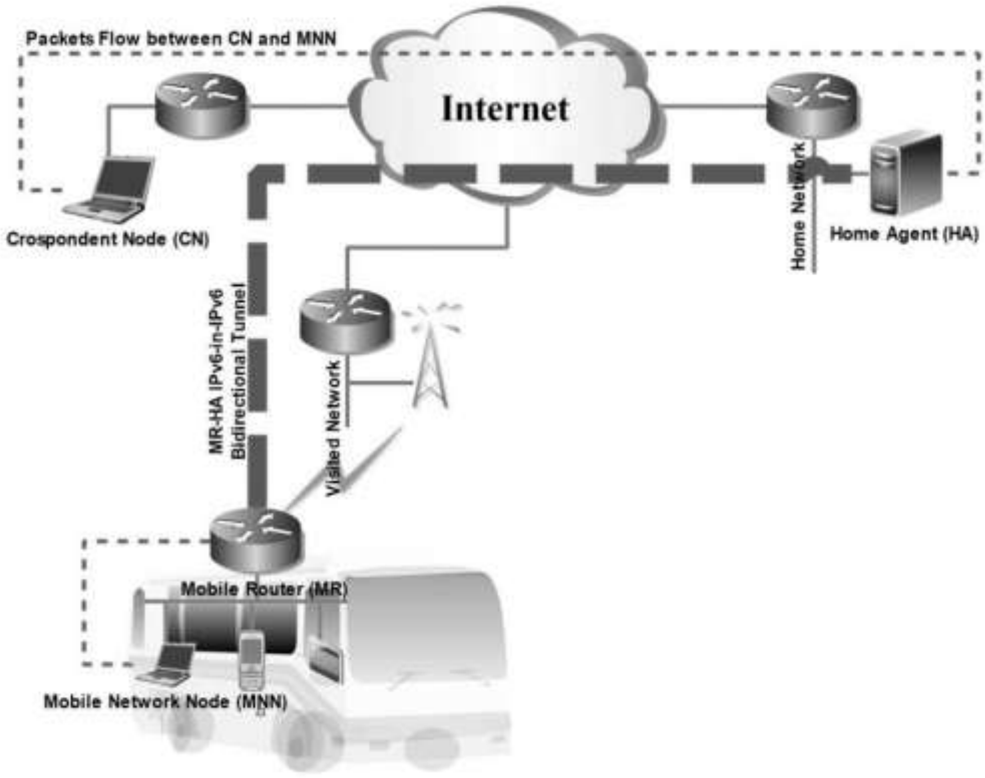

Figure 1.1: Data Flow in NEMO Basic Support Protocol (adapted from Bernardos, et al. (2007))

The time consumed by applying the handover procedure named as the Handover Latency (Manner & Kojo, 2004). The handover latency in NEMO is still high and is not adequate to QoS-demanded and real time applications (Do & Kim, 2012). This high handover latency is from the result of sequential signalling parts for the handover procedure which starts with the physical link switching part followed by the IP re-configuration (Zhong, Liu, Wang, & Ji, 2007a; Zhong, Liu, & Ji 2007b). Route Optimization and multi-hop (sometimes called hierarchical or nested) mobile networks are not considered in the basic description of NEMO and this is another challenge needs to be solved in NEMO. These challenges have their direct impact on the provision of Quality of Service (QoS) services in NEMO based networks (Akyildiz, Altunbasak, Fekri, & Sivakumar, 2004; Sen, 2010; Chen, Zheng, Liu, Huang, & Sun, 2013).

Internet regularly encountered perceptible quality degradation due to the huge amount of data transmitting. Quality of Service (QoS) is a resource reservation control mechanism that is used to overcome this degradation. Quality of Service mechanisms ensures a certain level of data flow performance is required for an application program or offered by the Internet Service Provider (ISP). QoS is significant if the network capacity is limited. QoS covers all aspects of a connection, which may include time of service provision, voice quality, echo, loss, and reliability (Xiao & Ni, 1999; Menascé, 2002; Khairi & Berqia, 2015).

Providing Quality of Service in Packet Switched Networks discussed in details in Towsley (1993); and Marosits (2011). The main drawbacks of NEMO BS that affect the Quality of Service (QoS) are the handoff latency, the hierarchical nesting networks (multi-hop mobile networks) and the lack of routing optimization (Akyildiz et al., 2004; Sen, 2010; Goswami et al., 2013; Khairi & Berqia, 2015). The main purpose of carrying out this study is providing solutions to these drawbacks.

Several schemes have been proposed in the literature to optimize the signalling parts and parallelizing them to get minimum possible handover latency. Other schemes in the literature were also proposed to optimize the routes in NEMO and reduce the multi-hop mobile network mobility overhead. However, it has been revealed that all these schemes have disadvantages that restrict their utility (Ryu, Park, & Choi, 2014). Taking this into account, this study proposes schemes that overcome these disadvantages and can lead to better utility and enhanced QoS services.

1.2 The Problem Statement

NEMO provides a solution to reduce group mobility overhead of MIPv6 and provides connectivity to all the mobile nodes that moving together as a single unit. The mobility management and the handover procedure are carried out by a mobile router (MR) that serves the moving group of nodes. However, the handover latency in this protocol is high and not compatible with real-time and multimedia applications that require QoS guarantees such as streaming video (Ojanperä, Luoto, Majanen, Mannersalo, & Savolainen, 2015), Voice over IP (VoIP) (Amarsinh & Satish, 2014) and music downloads (Goldman, 2001). This high handover latency is resulted from sequential signalling parts for the handover procedure which start with the physical link switching part followed by the IP re-configuration. Another problem is the lack of scalability and multi-level communications in on-the-move hierarchical (multi-hop or nested) networks (Chen, Hsu, & Cheng, 2014; Ernest et al., 2016). This particular problem, also referred to as pinball problem (Mousa, Abdalla, Al Khateeb, Khalifa, & Adibah, 2014; Qiang, Li, Guizani, & Ji, 2014), instigates a sub optimal end-to-end delay in the MR-HA tunnel. The available solutions in the literature have disadvantages (do not consider the lack of the heretical mobile networks or not provide efficient signalling parallelisation to the handover procedures of the link and the network layers) that limit their ability to provide the required QoS by real-time and multimedia applications. To overcome these disadvantages, an efficient, low handover latency protocol that is capable of optimizing the routing procedure should be incorporated into a suitable network model that provides a good solution for the scalability problems. This must be resulted in a better Quality of Service (QoS) in the future networks.

1.3 Research Objectives

The main aim of this study is to decrease the negative influences of the issues in group mobility solutions for QoS-Sensitive Applications that hinders QoS support in moving packet-switched networks. Three specific objectives were developed to achieve this main aim. These specific objectives are:

- To reduce the network overhead in the mobile networks due to group mobility.
- To improve QoS performance for hierarchical mobile networks during the handover process.
- To evaluate and compare the proposed solutions against the existing handover and route optimization techniques.

1.4 Scope and Limitations

The focus of this study is to propose and design a new NEMO extension, which takes into consideration the drawbacks in NEMO BS as a centralized mobility management protocol and the existed solutions in the literature to provide better services to QoS demanded applications. This study also focuses on reducing the network layer handover latency because it has been reported that it consumes the biggest part of the handover latency. The solution proposed in this study intends a minimum change to the original NEMO specification; due that, The Distributed Mobility Management (DMM) is not considered in this thesis. The performance of the proposed extension will be evaluated based on the general requirements for real-time/multimedia applications. However, it does not focus on specific real-time/multimedia applications which may require specific specifications and specific QoS requirements. Thus, only general factors consisting of handover latency, service disruption time, and packet loss will be investigated in this study.

Furthermore, although the proposed solution does not put emphasis on a specific media access or wireless technology, homogeneous wireless networks based on WiMAX IEEE802.16e will be used in the simulation due to its wide range and mobility support (Zubairi, Erdogan, & Reich, 2015). Compared to 4G Long Term Evolution (LTE), WiMAX Base Station (BS) has wider per-cell coverage and enter-system roaming is not required (Hafez, Fahmy, & Khairy, 2013). This makes WiMAX more suitable for fast moving mobile networks. Furthermore, the frame duration in WiMax is shorter than LTE (Hafez et al., 2013). As IEEE802.16m based on IEEE802.16e with more enhancements that does not affect the mobility support (Mhiri, Sethom, & Bouallegue, 2013), this will not be among the concerns of this study.

This study considers only the intra-system roaming technology, and focusses in the handoff management rather than the location management. Power management in the mobile nodes and the multiple registrations (multi-homing) are not considered. Although this study considers cross-layer solution for the handoff management, it gives more attention to the network layer solutions. Although the micro-mobility is not discussed much in this thesis, the macro-mobility is considered when the mobile nodes handoff between different domains. Though Mobile IP and its extensions are briefly discussed in this thesis, the NEMO basic support and its extensions are investigated in details. While security is one of the major QoS issues in mobile networks, but it is out of the scope of the designed objectives of this thesis.

1.5 Organization

This thesis consists of six chapters. Chapter one comprises a concise review of the study background, including outline presentation of the problem statement, objectives and scope of the study. Related work on the subject matter is reviewed in Chapter two, while Chapter three provides a detailed description of the methodology, mathematical modelling, Simulation Implementation and computations utilized in the study. Chapter four entails the proposed work and the schemes carried out in the study. Mathematical modelling and analysis are also presented in this Chapter. The results of the simulated experiments are discussed in chapter five. Deductions from the results are presented in the concluding chapter as well as future work related to the study area.

CHAPTER 2 - LITERATURE REVIEW

2.1 Introduction

This chapter provides a detailed review about the mobile networks and the handover related issues. Justification of the area of study selection is also provided along with some additional background information. The objectives of this study are also clearly defined in this chapter. As convenience to non-expert readers of this dissertation, a short introduction describing WiMAX, IPv6, DHCPv6 and Mobile IPv6 protocols is also provided. This chapter provides a brief review about the wireless technologies, followed by an introduction about the mobility and the handoff management. Next to that, Mobile IPv6 and its extensions are discussed briefly. The chapter then gives a brief details about NEMO basic support protocol as a group mobility solution and highlights the issues in this protocol. Finally, the solutions for these issues that are available in the literature are discussed.

2.2 Wireless Network Technologies Overview

Wireless network technologies allow mobile communications to provide connectivity to the entities while moving. In a heterogeneous network environment, there are typically multiple overlapping networks technologies, which cover any single place. The most recognized technologies in the literature involve the satellite services technologies (i.e. Globalstar, Spaceway, and Iridium) (Ibnkahla et al., 2004), cellular mobile phone technologies that comprising the second generation cellular General Packet Radio Service (GPRS) networks (Bettstetter, Vogel, & Eberspacher, 1999), the third generation Universal Mobile Telecommunications Service (UMTS) technologies

(Holma & Toskala, 2000), the fourth generation Long Term Evolution technologies (LTE/LTE-Advanced) (Cox, 2012; Sesia, Toufik, & Baker, 2015), CDMA2000 technology (Knisely, Sarath, Subhasis, & Sanjiv, 1998), WiMAX technologies (i.e. IEEE802.16-2004 (Eklund, Marks, Stanwood, & Wang, 2002) and IEEE802.16e (IEEE80216e-committee, 2004)), Wireless Local Area Networks (WLANs) technologies (i.e. IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n) and Wireless Personal Area Networking (WPAN) technologies (i.e. Bluetooth and IEEE 802.15.3 based Ultra-Wide Band (UWB)) (Aiello & Rogerson, 2003). These wireless technologies are descriptively clarified in Kuran & Tugcu (2007). These wireless technologies overlap as shown in Figure 2.1 which is adapted from Akyildiz, Mcnair, Ho, Uzunalioglu, and Wang (1999).

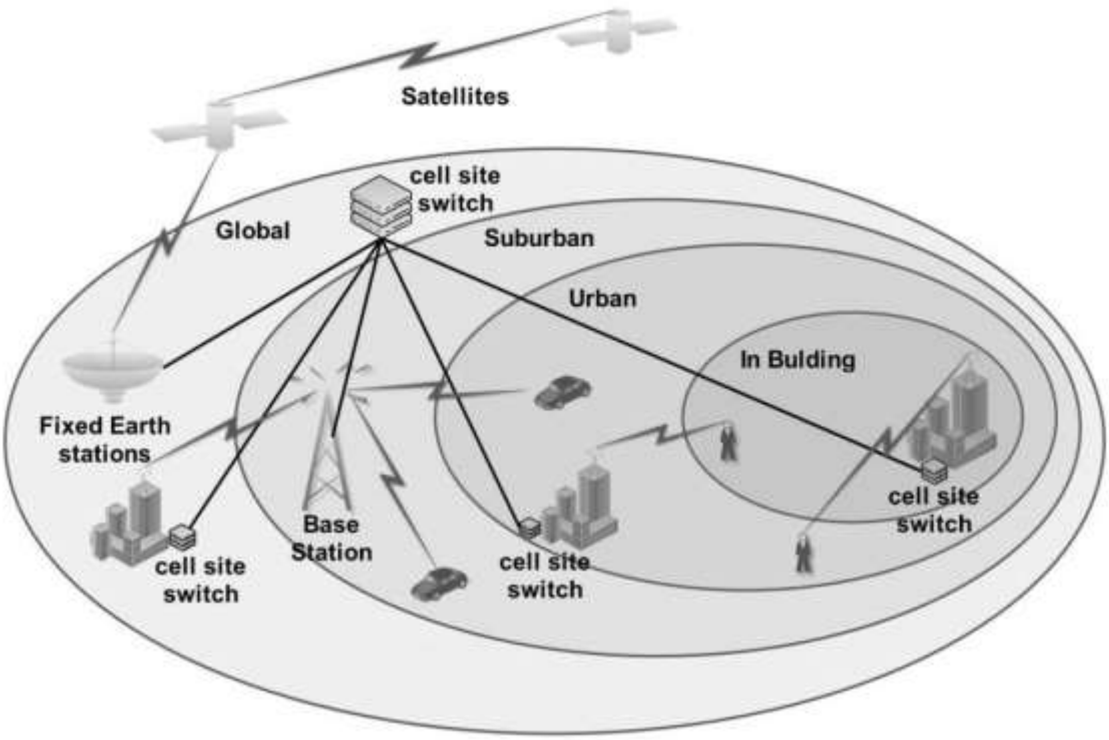

Figure 2.1: Heterogeneous Network Services (Akyildiz et al., 1999)

2.3 Handoff Management

Handoff or handover is the process that enables a mobile entity to move from one point of attachment to another. Handoff management ensures the active connection of a mobile entity to be kept during the handoff process. The handoff process comprises three stages. In the first stage, the handoff initiation is triggered by a mobile device, a network agent, or a changing of the network conditions. In the second stage, the new connection generation stage, the targeted network has to find new resources for the coming mobile entity and perform any required routing operations. In the third stage, the data-flow control, the data delivery is maintained from the old connection path to the new connection path in accordance with the agreed QoS guarantees.

Depending on the network system, there are two types of the handoff process: intra-system handoff (horizontal handoff) and inter-system handoff (vertical handoff). Intra-system handoff is the handoff process in homogeneous networks. The need for intra-system handoff arises when a mobile entity detects that the serving Base Station (BS) services is no longer required. In contrast, the inter-system handoff is the handoff between heterogeneous networks. The need for inter-system handoff may arise in the following scenarios: when a mobile entity moves from the serving network to an overlying network; when a mobile entity chooses to handoff to an underlying or overlaid network for specific service requirements and when there is need to distribute the overall load on the network among different systems (Akyildiz, Xie, & Mohanty, 2004; Mohanty, 2006).

Depending on the network domain, there are also two types of the handoff process: intra-domain handoff (horizontal handoff) and inter-domain handoff (vertical handoff). Intra-domain handoff is the handoff between base stations governed by the same operator. This type does not require change in the IP address. Inter-domain handoff is the handoff between base stations belonging to different operators. However, this kind of handoff requires the re-configuration of the IP Address (Khasawneh, BenMimoune, Kadoch, & Osama, 2014).

Designing the handoff management is encumbered by several challenges. These challenges may include minimizing the signaling and the power overhead; the need for QoS guarantees during the handover process which needs low handoff latency, low disruption time, and near-zero handoff failure and packet loss rate (Figure 2.2); efficiency in the use of network resources, and the need for enhanced scalability, reliability, and robustness (Akyildiz et al., 2004; Sen, 2010; Vikram Raju et al., 2014).

Figure 2.2: QoS Guarantees During the Handoff Process

2.3.1 WiMAX Overview

Mobile entities are usually found in wireless environments where mobile entities move across overlapping wireless systems. An overlapping wireless system could be like the one shown in Figure 2.1 on Page 11. WiMAX is chosen as the wireless media in the experiments carried out in this study due to its wide range and mobility support as has been addressed before in Section 1.4. WiMAX is discussed in detail in Andrews, Ghosh, & Muhamed (2007). WiMax offers a range of up to 50km, with throughput up to 70Mbps and good handling of NLOS (none line of sight) scenarios, hence it is the perfect network solution for urban, suburban and rural areas. A WiMAX network consists of several base stations and a large number of subscriber stations, both fixed and mobile. An extension, designated 802,16e, was selected for this study because it is capable of providing support for mobility. It is also commonly referred to as "mobile WiMAX".

There are two entities in a WiMAX network: subscriber stations, and base stations (BSs). Subscriber stations are small devices installed at the customer's premises or connected to customers' hardware, in the experiments performed in the study, connected to mobile routers and mobile network nodes. A subscriber station must be connected to the wireless link of a controlling BS. Network entry is the process of connecting a subscriber station to its serving BS. Subscriber station may be within range of several BSs. These BSs are called the neighboring BSs. To access a neighboring BS and evaluate the signal quality, the subscriber station may initiate a procedure called the Scanning procedure. When a subscriber station detects that the serving BS no longer offers required connection limits, handover procedure may be initiated. After completing the detachment from serving BS, radio adjustment and the network re-entry procedure must be performed by the subscribe station. One or more MAC messages are included in each WiMAX transmission. Data transmission is organized in radio frames typically each frame spans 5ms interval (Mrugalski, 2009). WiMAX has over 50 types of control messages. These messages used to signal and control different aspects of WiMAX operation such as ranging, scanning, and various stages of network entry. A convergence sublayer was defined to transmit user data over MAC messages.

2.3.1(a) WiMAX MAC messages

DL-MAP and UL-MAP MAC mapping messages are the first two in each radio frame. Allocations for specified Subscribers and general opportunities for various requests such as ranging or bandwidth requests are included on each map. Data Pane Activities are all operations related to data processing.

Several service flows for each subscriber station attached to a BS, including Basic, Primary, and Secondary service flows for control traffic. There are also at least one uplink and one downlink user data connections. There is a traffic type defined for each service flow. Best Effort is the worst type because it offers no QoS guarantees. In this traffic type, every time the Subscriber wants to transmit any data, it has to send Bandwidth Request (BWR) message to request bandwidth for this data. The Unsolicited Grant Service (UGS) is another common traffic type. In this traffic type, the Subscriber and the BS agree on service parameters during service flow creation. Thus, the BS offers transmission opportunities for that subscriber on a regular basis. Other, less commonly used traffic types include Non-Real Time Polling Service (nrtPS), Real-Time Polling Service (rtPS), and Extended Real Time Polling Service (ertPS).

2.3.1(b) WiMAX Network Entry

Ranging is the first operation on the network entry. In this operation, the subscriber station sends Code Division Multiple Access (CDMA) code or Ranging Request Message (RNG-REQ) message to adjust and tune the radio. BS replies with Ranging

Response Message (RNG-RSP). Information about the signal strength and quality are included in this reply. The second operation is the basic capabilities negotiation. The subscriber station sends Scan Basic Capabilities Request (SBC-REQ) message that contains list of all supported features. The BS removes unsupported and disabled features from the list. Then, it responds to the subscriber station by sending Scan Basic Capabilities Response (SBC-RSP) message. Regarding the capabilities of the subscriber and the base station, the security negotiation may follow. The Privacy Key Management protocol handles this security negotiation. As security is a very broad topic, issues related to cryptographic protection are left out of scope of this study. The third operation is the network registration. Registration Request (REG-REQ) message is sent by the subscriber station. BS decides the ability to log into the network and sends Registering Response (REG-RSP) message as a reply. The fourth operation is the service flows creation. After the subscriber station logs into the network, the service flows are created to transmit user data. Dynamic Service Add Request (DSA-REQ) message is sent with all intended parameters for each requested service flow. BS responds with Dynamic Service Add Response (DSA-RSP) message. Finally, the subscriber station acknowledges this message by sending Dynamic Service Add Acknowledgement (DSA-ACK) message.

2.3.1(c) WiMAX Handover Procedure

The handover procedure in WiMAX contains various mechanisms that make such handover possible. First, the serving BS periodically announces the list of possible targets BSs. This operation called Neighbor Advertisements. Second, the Scanning procedure starts by sending SCN-REQ request to the serving BS. The serving BS grants requested scanning periods to the subscriber station using SCN-RSP message and suspends support for this subscriber during the time of scanning. Third, after the scanning procedure is complete, the subscriber station may send a scanning report to its Serving Base Station using SCN-REP message. The scanning periods can be arbitrary long. In practice, the scanning periods seldom exceed 20ms. After successful scanning, the handover procedure may be initiated. The subscriber station informs its intent by sending a Handover Request (MSHO-REQ) message with one or more intended handover targets. BS may amend this list by the BSs negotiation process and may send it back to the subscriber by using a Handover Respond (BSHO-RSP) message. The last transmitted message is the Handover Indication (HO-IND) message that indicates the actual detachment and concludes handover operation at serving Base Station. The subscriber station, then, performs ranging and continues with network re-entry at target BS. Figure 2.3 shows the WiMAX Handover Procedure. After re-entry is complete, the mobile subscriber may start to reconfigure network layer, i.e. IPv6.

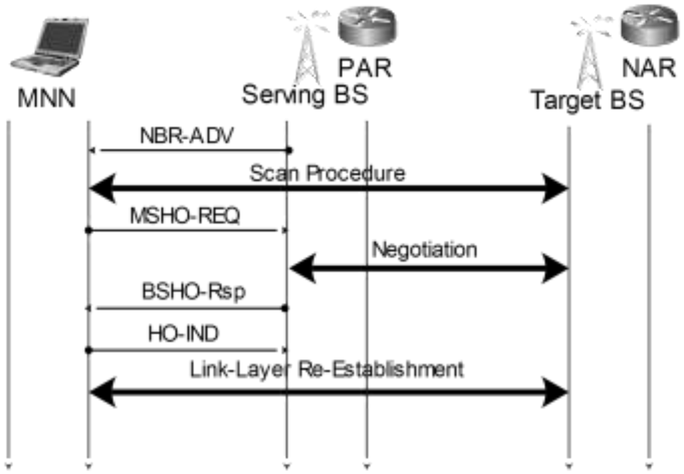

Figure 2.3: WiMAX Handover Procedure

2.3.2 IPv6 Overview

IPv6 was developed in 1996 (Deering & Hinden, 1998) to solve addresses shortage encountered in IPv4. Comparison of IPv4 and IPv6 from the mobility perspective is available in Wozniak, Nowicki, & Mrugalski (2004). Each entity that has IPv6 stack implemented is called a node. There are two types of nodes. The first type accepts traffic that is not directed to them (called routers). The second type does not accept traffic that is not directed to them (called hosts). Each IPv6 address is 128 bits long and is divided into two parts. The first part leads n bits which are called the prefix, while remaining $(128 - n)$ bits is the second part that is called host address.

Although there are no specified rules regarding n value, in most cases involving end users, an even split $(n = 64)$ is used. This is particularly true with the initial steps of node bring-up. Each node's network interface contains fixed, globally, and unique link layer address. In case of Ethernet, 802.11 (WiFi), Bluetooth and 802.16 (WiMAX) networks, it is called MAC address. This 48 bit address is extended to form a 64 bit node address (EUI-64). It is prepended with a well-known (fe80::) link-local prefix. Together, they form a link-local address that can be used for communication with other nodes available on the link. Unfortunately, due to its scope limited to a single link, it is not sufficient to maintain communication at a larger distance. Therefore the global address is usually required.

2.3.2(a) IPv6 Re-Configuration

The network layer must be re-configured when the data link layer changes a point of attachment. In the best and only case when intra-domain handover takes place, routing strategies can be adjusted and the ability to send and receive IP datagrams does not need to change the IP address. However, this case not always reasonable due to the fact that with a large number of subscribers the routing table is more complicated. This may degrade the routing manageability and efficiency. Therefore, operators may desire to limit excessive routing modifications.

Inter-domain handover is a more complicated case. This study focuses on Intra-domain handover. In the intra-domain handover, once a subscriber completes network re-entry, the network layer must be reconfigured. According to IPv6 standards (Johnson et al., 2004; Narten, Nordmark, Simpson, & Soliman, 2007; R. Droms et al., 2003; Thomson, Narten, & Jinmei, 2007), these steps are necessary. After attaching the new network, the IPv6 node must get a new IPv6 address and configure routing parameters. To obtain these new parameters, Stateless and usually stateful autoconfiguration are used. The IP address assists, two goals: equipment identity (unique identifier to the nodes) and designate location (determines the node's location). Therefore the corresponding nodes must be informed by the new location. This re-configuration process is designed without concerned about mobility; therefore, they introduce significant delays.

2.3.2(b) IPv6 Interface Re-Initialization

When IPv6 interface which is capable of multicasting is re-initialized, the node must join all-nodes multicast group and the node multicast address corresponding to its link-local address must be solicited (Narten et al., 2007) Mentioned operations must be performed after the node associated with new BS, because this is considered as interface re-initialization. Fortunately, multicast groups joining may be carried in parallel with other operations, thus do not increase the handover delay.

2.3.2(c) Automatic configuration in IPv6

There are two ways to acquire global IPv6 addresses. The first way uses the RA messages mechanism. These messages are being periodically broadcasting by routers to announce a list of available networks and services, and information about them. RA also can be initiated by any node via sending Router Solicitation message for this purpose. This kind of messaging is usually called ‘Router Discovery”. In each RA one or more prefixes that belong to each listed network are contained. The prefixes of the chosen network can be used together with the host link-local address to acquire a global IPv6 address. Such way can be autonomous. In other words, the hosts can generate global addresses by using one of these prefixes and their link-local addresses. This way is commonly referred to as Stateless Autoconfiguration (or SAA). For more details on this topic reference to Thomson et al. (2007).

2.3.2(d) Dynamic Host Control Protocol version 6 (DHCPv6)

The second way of obtaining the global IPv6 address is by way of Dynamic Host Configuration Protocol for IPv6 (Droms et al., 2003), commonly abbreviated as DHCPv6. When IPv6 stack of a node is initialized, the configuration parameters may be obtained from DHCPv6. Contrary to the first way, closely monitoring the node state and all granted parameters, (especially addresses, delegated prefixes, assigned fully qualified domain names, and temporary addresses), are required as they may vary in time. Therefore, the DHCPv6 configuration is called Stateful autoconfiguration.

The first solicit message is transmitted, once IPv6 node initializes its IPv6 stack. To avoid network congestion after the detachment period, this message should be delayed by a random time from 0 to 1 second. All servers and relays must listen to a well-known multicast address used for this message. The message contains a list of requests options. As multiple servers are allowed to present and be active on a single link at the same time in DHCPv6 protocol, one or more solicits are expected to be sent, each of them contains a set of proposed options, prefixes and addresses. All available servers respond by RAs containing their proposed addresses and configuration parameters. A client waits one second to allow all servers to generate and send answers, this waiting time specified in Droms et al. (2003). Options specified in RAs are not granted, but rather they are provided as advertisements. The client asks for actual assignment, and once it chooses the server that best suits its needs, this will be processed by sending a request message. This message is also sent to the same multicast address as before, but it also contains a unique server identifier (Server DUID). Such message is processed by one server and ignored by the others depend on the server DUID. The selected server grants the requested options. A reply message that contains the assigned parameters is sent to the client. This concludes the DHCPv6 configuration. Clearly, the DHCP basic configuration delay time is over 1000 ms, which is a major area for possible improvement.

2.3.2(e) Duplicate Address Detection (DAD)

Disregarding of its source, each new obtained address must be checked to verify its uniqueness. This verification process is called Duplicate Address Detection (DAD). A neighbour solicitation message is sent by the node to a multicast group that is generated from the address which needs to be verified. If any other nodes use this address, the message may reach them and they may respond with a Neighbour Advertisement message. From the mobility perspective, it is essential to note that the minimum waiting time for such improbable responses is one second. This waiting time can be more when a given interface type defines repeated transmissions. More details about DAD operation are specified in Narten et al. (2007) and Thomson et al. (2007). More specific details about the message structures and the operation of IPv6, Neighbour Discovery, Stateless Autoconfiguration, Addressing architecture, and other related topics are included in Loshin (2004).

This procedure is compulsory for all IPv6 nodes configuring a new address by either stateful or stateless auto-configurations. Once the handover is accomplished, DAD procedure must be initiated bringing out another 1000 ms delay. In reality, address duplications are extremely rare; therefore, DAD delay is an excellent candidate for improvement.

2.3.2(f) Optimistic DAD

Optimistic Duplicate Address Detection (Optimistic DAD) (Moore, 2006) is a modification of Neighbour Discovery (Narten et al., 2007) and Stateless Autoconfiguration (Thomson et al., 2007) processes. The main purpose of the Optimistic DAD is to minimize address configuration delays in the successful case, and to reduce disruption as far as possible in the failure case which are very rare cases.

A new address state OPTIMISTIC is introduced. It may be considered a mixture of TENTATIVE (being verified, only DAD related packet can be sent or received) and DEPRECATED (assigned to an interface, all packets can be sent or received) states. A newly obtained address is assigned in OPTIMISTIC state. This address cannot be used for sending Neighbour Solicitation or Router Solicitation messages. This seriously limits Optimistic Node (i.e. node that supports Optimistic DAD) capability for communicating with its neighbours in a regular way (i.e. discovering them using Neighbour Discovery mechanism). Optimistic node sends packets to its default router instead. The router is expected to respond by standard ICMP by redirect message that contains all necessary information for direct communication.

Moore (2006) provides interesting analysis of necessary conditions for the DAD procedure to fail, using Birthday Paradox. When randomly generated host addresses are used, the probability of collision in 500 node network is $5.4e^{-14}$. For the theoretical network consisting of 500,000 nodes the probability raises to $5.4e^{-8}$, which is still extremely unlikely to happen. Also, it should be noted that host addresses are usually generated from unique L2 addresses, which in turn are expected to be unique. For 802 network family hardware, each is assigned one or more 3 octet identifier that is supposed to be appended with 3 octets of unique values. The general observation is that this approach offers unique L2 addresses on a global scale, except in rare cases when low-end vendors try to further limit its manufacturing costs and mass producing multiple network cards with the same address.

Optimistic DAD assumes that address duplication is very unlikely. As such, benefits of DAD speed up outweigh the cost of failed cases, i.e. when the address is detected to be duplicated. That is a reasonable assumption and as such, the proposal may be used in various scenarios. There are, however, several aspects that may hinder the deployment and usefulness of the scheme. As pointed out in Moore (2006), Section 2.4, a node with only Optimistic Address is unable to determine router's Link-Layer Address. In such case, Optimistic Node may not be able to communicate with the router until at least one of its addresses is no longer optimistic (i.e. classic DAD procedure is completed). Also, in a negative case, when the address is proven to be duplicated, consequences are quite severe. While optimistic DAD still take place, the Mobile Node is allowed to use its new optimistic address (e.g. using it to send Binding Update message). This may lead to broken connections, as the data sent by the Correspondent Nodes and Home Agent may be received by the actual owner of the address in question, rather than Mobile Node. Incoming packets may not be recognized by this unknown node and either be dropped (e.g. UDP packets) or the connection be closed (e.g. RST packet in TCP connections).

2.4 Mobile IPv6

Mobile IP (Perkins, Johnson, & Arkko, 2011) is a network layer protocol to provide host mobility among the Internet. It is scalable, reliable and secure and it can support the continuity of ongoing communications when hosts switch their link (Amgahd & Yadav, 2016). Currently, the Mobile IP primarily refers to the Mobile IPv4 (MIPv4) and Mobile IPv6 (MIPv6), MIPv6 provided more and better features than MIPv4. It can supply the address needed by the large number of mobile terminals along with IPv6's function and equipment. Most of the additional enhancements in Mobile IPv6 over Mobile IPv4 are summarized in Jia, Wang, & Zhao (2011).

MIPv6 Mobile nodes (MNN) in their Home Network dealing like a normal IPv6 nodes. The access router in the home network which connects MNN to the global network named as Home Agent (HA). The configured IPv6 address for a MNN in its home network named as Home Address (HoA). However, when a MNN is away from its home network, its HoA becomes topologically invalid. To continue its connectivity a new IPv6 address named as Care-of Address (CoA) must be configured on the visited link and a bidirectional tunnel to connect the MNN with the HA located in its home network, must be constructed by updating the HA with this new CoA. Thus, the HA can bind the HoA and the CoA of the MNN and forward packets meant to MNN via this bidirectional tunnel.