A NEW NEMO ROUTE OPTIMIZATION SCHEME USING NEMO CORRESPONDENT REGISTRATION PROCEDURE

SAMER SAMI HASAN AL-RAMMAHI

THESIS SUBMITTED IN FULFILMENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2013

SKEMA PENGOPTIMUMAN PEROUTAN NEMO BARU MENGGUNAKAN PROSEDUR PENDAFTARAN SEPADAN NEMO

SAMER SAMI HASAN AL-RAMMAHI

TESIS YANG DIKEMUKAKAN UNTUK MEMPEROLEH IJAZAH
DOKTOR FALSAFAH

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2013

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries, which have been duly acknowledged.

October 2013

SAMER SAMI HASAN AL-RAMMAHI
P54907

ACKNOWLEDGMENTS

First and foremost praise be to Almighty Allah for all his blessings for giving me patience and good health throughout the duration of this PhD research.

I would like to express my deep gratitude to my main supervisor Associate Professor Dr. Rosilah Hassan for her support, encouragement, and guidance during this research. I would also like to express my special thanks to all those who have helped me with my work by invaluable suggestions, and comments on my work.

Also, My deepest gratitude and appreciation to my wife Aseel and my kids Ali and Lara for their helps and support in difficult times. Your love, understanding and patience sustained me through to the end of my Ph.D.

Moreover, I cannot thank my parents enough for their love and sacrifice throughout my whole life. Over the years they have continued to support and encourage me. I would like to thank them for everything.

DEDICATION

I dedicate this thesis to my late dad who passed away on Thursday, 22 September 2011.

ABSTRACT

Network mobility basic support protocol (NEMO BSP) is an important requirement for internet networks to reach the goal of ubiquitous connectivity. NEMO basic support protocol handles the mobility of multiple nodes in an aggregate way as a mobile network. The standard NEMO suffers from a number of problems and limitations, such as inefficient route due to pinball problem, link drop problem, and long handoff latency; however, most previous studies attempting to solve such problems impose an extra signaling load and/or modify the functionalities of the main entities. To overcome such problems: Firstly, a new architecture for infrastructure-based route optimization in NEMO (FRON) that uses a correspondent firewall with new filtering rules to support the route optimization in NEMO BSP been proposed. In order to further improve the correspondent registration, a more secure and lightweight enhanced return routability procedure (ERRP) extended from the original correspondent registration option headers within FRON infrastructure also been developed. Furthermore, instead of employing ERRP in stateless environments, a new route optimization scheme for NEMO stateless DHCPv6 using the proposed ERRP with the DHCPv6PD (DHCPv6 prefix delegation) protocol been implemented. Finally, to overcome the bursts of re-registration signaling due to dropping links in the binding cache of the correspondent entities; correspondent node, correspondent router, and correspondent firewall; a new cache replacement policy is proposed to solve such problem. The results shows that the proposed mechanisms provides secure communications by making an authorized decision about the mobile router (MR) home of address (HoA), care of address (CoA), and the complete mobile network prefixes (MNPs) underneath the MR. In addition, it reduces the total signaling required for NEMO handoffs, especially when the number of mobile network nodes (MNNs) and/or CNs is increased. Moreover, the proposed mechanisms can be easily deployed without modifying the mobility protocol stack of CNs.
A thorough analytical model and network simulator (NS-2) are used for evaluating the performance of the proposed mechanisms compared with NEMO BSP and state-of-the-art of route optimization schemes. Numerical and simulation results demonstrate that our proposed design and mechanisms outperforms other route optimization schemes in terms of security considerations, handoff latency, and total signaling load on wired and wireless links.

ABSTRAK

Protokol sokongan asas mobiliti rangkaian (NEMO BSP) adalah satu syarat penting rangkaian internet agar rangkaian berada di mana-mana (ubiquitous connectivity). NEMO BSP mengendalikan mobiliti nod berbilang secara agregat sebagai rangkaian mobil. NEMO piawai mengalami beberapa masalah dan kekangan, seperti laluan tidak cekap akibat masalah *pinball*, masalah kemerosotan sambungan, dan kependaman pengalihan yang panjang. Namun, kebanyakan kajian lepas yang cuba menyelesaikan masalah tersebut meningkatkan beban pengisyaratan dan/atau mengubah kefungsian entiti-entiti utama. Untuk mengatasi masalah-masalah ini, pertamanya dicadangkan senibina baru untuk pengoptimuman laluan berasaskan prasarana dalam NEMO (FRON). Ia menggunakan dinding api perantara dengan petua penapisan baru untuk menyokong pengoptimuman laluan dalam NEMO BSP. Untuk membaiki pendaftaran perantara, satu prosedur kebolehroutan kembali lanjutan (*ERRP*) yang lebih selamat dan ringan. Turut dicadangkan ia lanjutan kepada kepala pilihan pendaftaran perantara (correspondent registration option headers) yang asal dalam prasarana FRON. Seterusnya, skim baru pengoptimuman laluan bagi NEMO DHCPv6 yang *stateless* menggunakan ERRP yang dicadangkan dengan protokol perwakilan awalan DHCPv6 (DHCPv6 prefix delegation, DHCPv6PD). Telah dilaksanakan akhir sekali, untuk mengatasi letusan pengisyaratan pendaftaran semula (bursts of re-registration signalling) yang berlaku akibat kemerosotan sambungan di jadual cache mengikat (binding cache) entiti perantara (iaitu nod perantara, penghala perantara, dan dinding api perantara); satu polisi penggantian jadual cache dicadangkan untuk mengatasi masalah ini. Keputusan menunjukkan bahawa mekanisme-mekanisme yang dicadangkan menyediakan komunikasi yang selamat dengan membuat keputusan yang dibenarkan (authorized) mengenai alamat rumah (home of address, HoA) dan alamat penjaga (care of address, CoA) penghala mobil (mobile router, MR), serta awalan rangkaian mobil (mobile network prefixes, MNP) yang lengkap di bawah MR. Tambahan pula, ia mengurangkan jumlah pengisyaratan yang diperlukan untuk pengalihan NEMO, terutamanya apabila bilangan nod rangkaian mobil (mobile network nodes, MNN) dan/atau nod perantara (corresponding nodes, CN) meningkat. Selain itu, mekanisme-mekanisme cadangan ini boleh dilaksana dengan mudah tanpa mengubah tindanan protokol mobiliti CN. Satu model analitikal menyeluruh dan simulator rangkaian (NS-2) digunakan untuk menilai prestasi mekanisme-mekanisme cadangan berbanding NEMO BSP dan skim pengoptimuman penghala yang terkini. Keputusan berangka dan simulasi menunjukkan bahawa rekabentuk dan mekanisme yang cadangan mengatasi skema pengoptimuman laluan lain dari segi pertimbangan keselamatan, kependaman pengalihan, dan jumlah beban pengisyaratan pada sambungan berwayar dan tanpa wayar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	Ad hoc On Demand Vector
AR	Access Router
BA	Binding Acknowledgment
BC	Binding Cache
BSP	Basic Support Protocol
BU	Binding Update
CGA	Cryptographically Generated Address
CN	Correspondent Node
CR	Correspondent Router
CoA	Care-of Address
CoT	Care-of Test
CoTi	Care-of Test Init
DAD	Duplicate Address Detection
DHCPv6	Dynamic Host Control Protocol version 6
DHCPv6PD	Dynamic Host Control Protocol Prefix Delegation version 6
ERRP	Enhanced Return Routability Procedure
FRON	Firewall Route Optimization for NEMO
FW	Firewall
HA	Home Agent
HIMPv6	Hierarchical MIPv6
HMAC-SHA1	Hashing Message Authentication Code based on Secure HAsh algorithm version 1
HoA	Home-of Address
HoT	Home Test
HoTi	Home Test Init
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
IPSec ESP	IPSec Encapsulating Security Payload
LFN	Local Fixed Node

LMN	Local Mobility Node
MIP	Mobile IP
MIPv6	MIP version 6
MNN	Mobile Network Node
MNP	Mobile Network Prefix
MR	Mobile Router
NEMO	NEtwork MObility
NEMO ES	NEMO Extended Support
ORC	Optimized Route Cache
PANA	Protocol for Carrying Authentication for Network Access
PCH	Path Control Header
PDA	Personal Digital Assistant
PF	Prefix
RA	Router Advertisement
RO	Route Optimization
RR	Return Routability
TCP	Transmission Control Protocol
TLMR	Top Level Mobile Router
VMN	Visited Mobile Node
QoS	Quality of Services
xHoT	extended HoT

LIST OF SYMBOLS

t_{L2}	Link layer (L2) switching delay
t_{RD}	Router discovery delay in MIPv6
t_{DAD}	Duplicate address detection delay
β	Wireless link failure probability
$R_{wireless}$	Wireless link bandwidth
R_{wired}	Wired link bandwidth
λ_{wired}	Wired link delay
$\lambda_{wireless}$	Wireless link delay
$d\ x\text{-}y$	Number of hops between X and Y
α	Simple processing delay unit for each entry
Nc	Number of CNs
n	Number of prefixes
D_{queue}	Average queuing delay
S_c	Control packet size
S_d	Data packet size
γ	Packet arrival rate
ϖ	HA lifetime
υ	CN lifetime
μ	Wight factor for tunneling effect
K	Wight factor for dropping effect
$p^{HoTi}_{MR,HA}$	HoTi control packet size from MR to HA
$p^{HoTi}_{HA,CN}$	HoTi control packet size from HA to CN
$p^{HoT}_{CN,HA}$	HoT control packet size from CN to HA
$p^{HoT}_{HA,MR}$	HoT control packet size from HA to MR
$p^{CoTi}_{MR,CN}$	CoTi control packet size from MR to CN

$p_{CN,MR}^{CoT}$	CoT control packet size from CN to MR
$p_{MR,HA}^{BU}$	BU control packet size from MR to HA
$p_{MR,CN}^{BU}$	BU control packet size from MR to CN
$p_{HA,HA}^{BU}$	BU control packet size from HA to HA
$p_{HA,MR}^{BA}$	Binding Acknowledgement control packet size from HA to MR
$p_{CN,MR}^{BA}$	Binding Acknowledgement control packet size from CN to MR
$p_{PF+KeyToken}$	Prefix option with its key token size
p_{PF}	Prefix option size
$rtAdvInterval$	Router advertisement interval
t_{L2}	Link switching delay
t_{ll}	Link-local IPv6 address configuration delay
$t_{DHCPv6PDConfig}$	Stateful address auto configuration with prefix delegation
X_{proc}	Processing time consumed by entity X
t_h	Total IP handoff delay
t_d	Movement detection time
t_a	CoA configuration time
t_o	Total RO delay
$t_{prefAdvCoA}$	MR CoA prefix advertisement delay
$t_{MRCoAddrConfig}$	Time required by the MN to employ the address configuration rule (EUI64)
ω	Verification delay consumed by CNs
μ_t	Reallocate time threshold

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

Our mobile lifestyle is currently reflected in the importance of mobile communications. However, in some situations, devices (or hosts, as we will refer to them) move as a group, for example, when travelers commute in the same train or coach for the same distance. Such cases are not efficiently covered by considering the mobility of individual devices because this involves increased signaling overhead and power consumption. A more efficient solution is required for the aggregate mobility (or network mobility) of devices using at least one mobile router. The Internet Engineers Task Force (IETF) developed a protocol named Mobile IPv4 (MIP) (Perkins 2002), and for IPv6 communication environments, MIPv6 (Johnson et al. 2004) was developed to support fast and smooth connectivity to the mobile node. Currently, Internet users may own more than one mobile device, and these devices feature multiple interfaces that can be connected to each other as well as to other networks. This includes the set of Internet-connected devices found in vehicles. IETF extends MIPv6 to the design of NEMO BSP (Devarapalli et al. 2005) to handle node mobility in an aggregate way using a dedicated router. In NEMO BSP, there are four main entities, which are defined as follows: Correspondent Node (CN), Mobile Router (MR), Home Agent (HA), and Mobile Network Node (MNN) as shown in Figure 1.1. CN is any IPv6 node that communicates with the MNN. MR is a router that handles all movement transparently for all MNN underneath. HA is a router usually located in the home network of MNN that acts on behalf of the mobile node while away from the home link. The MNN is described as a mobile node that has the ability to move through different networks with seamless connectivity. When MNN leaves its home link and enters a new subnet, it notifies its home agent on its home link. After

updating the HA with the new address acquired from the foreign link, which is based on the foreign prefix and called the Care-of Address (CoA), the MNN can then be reached through its HA. In this case, network overheads and handoff latency will be increased due to an insufficient route (i.e., Pinball Routing problem). The IETF developed an optimization procedure to address this problem. A direct connection is established between the MNN and the CN. To alleviate the performance penalty, Mobile IPv6 includes a mode of operation that allows the mobile node and its peer, a CN, to exchange packets directly, bypassing the home agent completely after the initial setup phase (i.e., return routability procedure). This mode of operation is called route optimization (RO). When RO is used, the mobile node sends its current care-of address to the CN, using binding update (BU) messages. The CN stores the binding between the home address and care-of address into its Binding Cache (Nikkander et al. 2005).

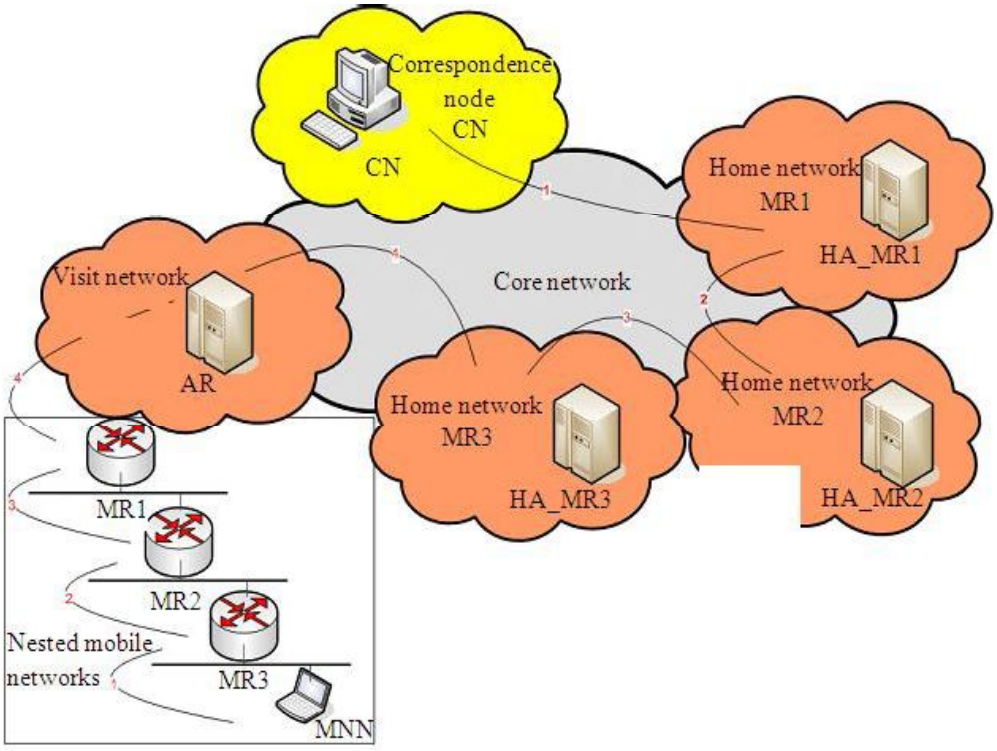

Figure 1.1 NEMO basic entities

RO typically requires the MNN and CN to have certain capabilities, such as the possibility to execute a Return Routability procedure (RRP) - MNN transmitting

Home Test Init (HoTI), Care-of Test Init (CoTI) and direct Binding Update messages to CN, with the CN responding with respective Home Test (HoT), Care-of Test Init (CoT), and Binding Acknowledgement messages to the MN. If the CN is a basic IP node without support for RO, the MNN with support for RO cannot set up RO with this CN because RFC 3775 (Johnson et al. 2004) specifies *"If a mobile node attempts to set up route optimization with a node with only basic IPv6 support, an ICMP error will signal that the node does not support such optimizations and communications will flow through the home agent"*.

The nodes involved in performing RO would be expected to exchange additional signaling messages to establish RO. The required amount of signaling depends on the solution but is likely to exceed the amount required in the home Binding Update procedure defined in NEMO Basic Support. The amount for signaling is likely to increase with the increasing number of Mobile Network Nodes and/or CNs and may be amplified with the nesting of mobile networks. It may scale to unacceptable heights, especially to the resource-scarce mobile node, which typically has limited power, memory, and processing capacity (Koodli et al. 2007). This may lead to an issue that impacts NEMO RO known as the phenomenon of "Binding Update Storm", or more generally, "Signaling Storm". This occurs when a change in the point of attachment of the mobile network is accompanied with a sudden burst in signaling messages, resulting in temporary congestion, packet delays, or even packet loss. This effect will be especially significant for wireless environments where bandwidth is relatively limited. It is possible to moderate the effect of Signaling Storm by incorporating mechanisms such as spreading the transmissions burst of signaling messages over a longer period of time or aggregating the signaling messages. Even then, the amount of signaling required might be overwhelming because large mobile networks (such as those deployed on a train or plane) may potentially have a large number of flows with a large number of CNs. This might suggest the need to have some adaptive behavior that depends on the amount of signaling required versus the effort needed to tunnel home (Watari et al. 2007).

1.2 PROBLEM STATEMENT

Network mobility (NEMO) handles mobility of multiple nodes in an aggregate manner as a mobile network. The standard NEMO suffers from a number of limitations, such as inefficient route and increased handoff latency. Most previous studies attempting to solve such problems impose an extra signaling load and/or modify the functionalities of the main entities. Due to the diversity of the locations of different nodes that a Mobile Network Node may signal with and the complexity of NEMO Route-Optimization procedures, which may cause several rounds of signaling messages, a NEMO Route-Optimization procedure may take a longer time to finish its handoff than that in NEMO Basic Support. This may exacerbate the overall delay during handoffs and cause a further degradation in the performance of the applications running on Mobile Network Nodes (Shahriar 2012; Qureshi 2010). Such problems from Correspondent Node side are:

i. Correspondent entities suffer from a problem of establishing route optimization between the CNs and mobile network nodes associated with NEMO.

   To support NEMO RO, some nodes need to be changed or upgraded. A smaller number of nodes required to be changed will allow for easier adoption of the NEMO Route-Optimization solution in the Internet and create less of an impact on the existing Internet infrastructure. The number and the types of nodes involved in new functionalities also affect how much of the route is optimized. In addition, it may also be beneficial to reuse existing protocols (such as Mobile IPv6) as much as possible (Watari et al. 2007; Shahriar, Atiquzzaman, et al. 2010). It may prove to be difficult to introduce new functionalities at CNs because, by definition, any IPv6 node can be a CN. This might mean that only those CNs that are modified can enjoy the benefits of RO. If the CN is a basic IP node without support for RO, the MN with support for RO cannot set up RO for this CN because RFC 3775 (Johnson et al. 2004). This will lead to performance degradation. The question here is how the initiator of RO knows whether the correspondent entity supports the functionality required to establish a RO session. Typically, the initiator attempts RO with the correspondent entity. Depending on the protocol specifics, the initiator may receive (a) a reply from the correspondent entity indicating its

capability, (b) an error message from the correspondent entity, or (c) no response from the correspondent entity within a certain time period. This serves as an indication of whether the correspondent entity supports the required functionality to establish RO. This form of detection may incur an additional delay as a penalty when the correspondent entity does not have a RO capability.

ii. High signaling cost of RO in NEMO Lacks of protects against changes or inserts options in mobile network prefixes option by attackers.

The authentication portion for the initialization of the optimization procedure for verifying the Home-of address (HoA) and Care-of address (CoA) to the mobile node in mobile IPv6 is inadequate. This verification does not support the link prefix to make an authorized decision about the Mobile Router (MR) HoA, CoA, and the complete prefixes before the MR, nor does it check whether it is handled by the mobile entity inside the NEMO.

iii. The size of correspondent binding cache is finite.

CN may choose to drop any entry that exists in its BC if it is substantially insufficient in order to make space for a new entry. When entries are deleted from the CN, as a result packet loss will be increased. At that time the CN will pass a packet without destination option set and routed through HA of MNN to inform them that the CN needs a new Binding Update (BU) with its Return Routability Procedure (RRP). The new BU will lead to increase additional overhead and latency in delivering packets to the mobile node.

1.3 RESEARCH AIM AND OBJECTIVES

The aim of this research is to improve the efficiency as well as security and management of RO in IP-based mobility protocol. To restrict the scope of the discussion, this thesis is limited to an improvement in the IPv6 network mobility protocol (NEMO). The reasons for choose network mobility are: firstly, our mobile lifestyle is currently reflected in the importance of mobile communication. Secondly, ubiquitous mobile devices and services supporting IPv6/MIPv6 have recently proliferated widely, it is expected that IPv6/MIPv6 and its extensions replace the current IPv4/MIP in the next couple of years. Thirdly, simulation packages such as NS-2 (McCanne et al. 1997), OMNET++ (Varga 2001, 2006) and OPNET (Modeler 2009) implement MIPv6 as a base work for other extensions in order to simulate and evaluate the existing works as well as the proposed work.

The themes of this research, and hence this thesis, are:

i. To identify the weakness prevalent in the existing RO schemes for NEMO and MIPv6.

ii. To propose a new lightweight and secure route optimization scheme based on correspondent network in both stateless and stateful address auto-configuration.

iii. To propose a new binding cache replacement policy using prioritizing algorithm in correspondent entities.

iv. To validate and evaluate the performance of the new architecture with a new return routability procedure as integrated scenario.

1.4 THESIS CONTRIBUTION

This thesis explores mechanisms to deploy RO in a secure mode, with low deployment cost and without modifying the main entities. The main contributions of this thesis are as follows:

i. A new architecture (FRON) has been developed using the correspondent Firewall to support the RO in NEMO BSP. Also, a more secure and reliable return routability procedure (ERRP) as an extension from the original one has been proposed. This mechanism provides a more secure and lightweight communications. Moreover, the integration of the proposed return routability procedure (ERRP) with FRON architecture combined with the prefix delegation protocol (DHCPv6PD) to produce a new RO scheme with new option headers for stateless DHCPv6 NEMO.

ii. A new cache replacement policy is implemented to alleviate the link drop problem in correspondent Entity (i.e. CN, correspondent router, and correspondent firewall) cache table. This policy uses user class prioritizing mechanism. This mechanism guarantees that the user with higher amount of traffic not suffers from link drop problem.

iii. A new Firewall agent with its classifier is generated using NS-2 network simulator. The validation and the evaluation of the new architecture using new proposed model are tested with different mobility scenarios.

iv. A new return routability procedure message format is produced for ERRP in NS-2 simulator. The integration of the ERRP with new FRON architecture provides a new route optimization scheme.

1.5 THESIS RESEARCH METHODOLOGY

The methodology of this research work as shown in Figure 1.2 can be explained as follows:

i. Review the Literature
   In this step, an excessive investigation has been done on the main topics which constitute the research.

ii. Design Architecture for reducing the signaling load on CN and shortening the communication path.

iii. Design a new option header in return routability procedure to validate and authenticate the list of prefixes delegated to the NEMO mobile router.

iv. Design a scheme for optimizing the communication path in stateless and stateful scenarios, in this stage a low cost route optimization scheme is proposed by using the FRON architecture with the ERRP to reduce the communication path between the communicating entities.

v. Design new rules for binding entries in CN binding cache table depends on the priorities of the binding update message according to user class priority.

vi. Implementation, The system modeling refers to an act of representing an actual system in a simply way. System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented. With modeling, the parameters of the system can be changed, tested, and analyzed. More importantly, modeling, if properly handled, can save costs in system development. To model a system, some simplifying assumptions are often required. It is important to note that too many assumptions would simplify the modeling but may lead to an inaccurate representation of the system. Traditionally, there are two modeling approaches: analytical approach and simulation approach.

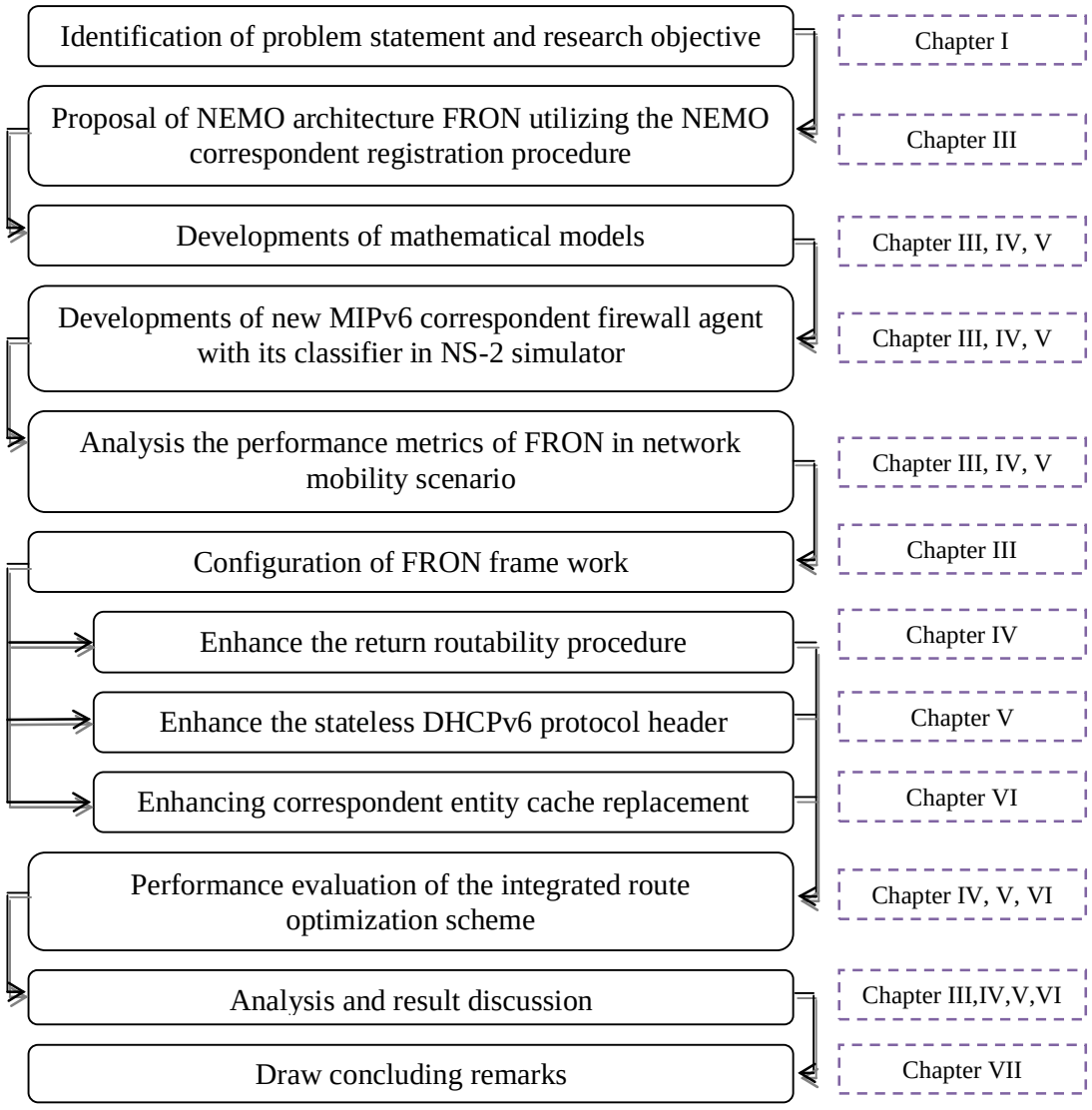

Figure 1.2 Methodology of New NEMO RO Scheme

1.6 THESIS ORGANIZATION

This thesis is organized into seven chapters. The first chapter briefly introduces the definition, advantages, weakness and history of NEMO. This chapter also states the objectives and contributions of this thesis.

Chapter II contains the back ground of IP and its mobility. This chapter also covers the literature review and the basic principles of MIPv6 and its extension NEMO BSP. This chapter reviews the peak problems and its reduction techniques. The adaptive schemes and definitions are also explained in details in this chapter.

Chapter III describes the design of new infrastructure base RO scheme using correspondent firewall (FRON).

Chapter IV proposes a new secure and lightweight return routeability procedure (ERRP) using FRON structure.

Chapter V develops the ERRP to provide return routeability in stateless DHCPv6 network scenario.

Chapter VI proposes a new cache replacement policy to overcome the link drop problems.

Lastly, Chapter VII contains the conclusions from the thesis, and recommendations for follow-on research.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter gives an insight into the current specification of the Mobile IPv6 protocol and its extension NEMO. In detail, Section 2.2 It first presented an overview of the basic concepts related to the Internet Protocol. Section 2.3 it then focused on IP mobility and presented problems caused by node and network mobility. Subsequently, gives an overview of the host mobility protocol, its main components, and the communications between the mobile node and a CN. Then describe protocol problems and limitations. In addition, network mobility (NEMO BSP) protocol presented with its optimization and all of its benefits and limitations. Moreover, this subsection classifies the RO schemes proposed in the literature over the last five years. We classify the schemes based on the basic approach for RO. Finally, Section 2.4 summarizes the chapter.

2.2 IP ADDRESS

The Internet Protocol (IP) address is part of the TCP/IP network suite that is widely deployed on the Internet. This numerical label is used to provide addresses to distinctly identify devices, so that theses devices can communicate with each other. An IP address divided in to two parts: host or network interface, where as (Postel 1981) characterize these interfaces as "*A name indicates what we seek. An address indicates where it is. A route indicates how to get there*". The current form of IP, IPv4, has remained relatively unchanged since it was adopted in the late 1970 by ARPAnet. Unfortunately, the enormous growth of smart mobile devices and unprecedented need for IP addresses has indicate that there has been a rapid decline in the number of IP addresses available for allocation. The way in which the addresses

were distributed originally, classed based networks, also contributed to this shortage because large numbers of addresses were allocated but remained useless. The designers in Internet Engineering Task Force (IETF) formally approved the new version of the protocol, IPv6, on 1995 (Deering et al. 1995). IPv6 was standardized as RFC in 1998 (Deering et al. 1998). The main objectives of this new version were to expand the address space sufficiently for future use and also to make improvements to IPv4 where necessary; particularly in the areas of security, network scalability and quality of service. The IETF workgroups developing this new version of the protocol decided that the address size should be expanded from the IPv4 (32-bit addresses) to the new version of IPv6 with (128-bit addresses). It is hoped that this will provide enough addresses for all devices that connected to the Internet within this couple of years such as: smart mobile phones, pocket PCs, printers, scanners, routers, fridges, toasters etc (McGann et al. 2005; Blanchet 2006).

The IPv6 header is generally based on the IPv4 header with dropping of some IPv4 header fields such as (Header Length field, Checksum field, an the fields used for Fragmentation) or made as optional fields and new extension options supported for more efficient forwarding, greater flexibility for introducing new options in the future, and less stringent limits on the length options (see Figure 2.1). There are still fields for the source and destination addresses, but they have been expanded to accommodate the larger addresses and the version field is set to six instead of four. All the optional fields were removed from the main IPv6 header and made into "*Extension Headers*". The other changes that were made were more of a restructuring nature. The functionality of the Type-of-Service (ToS) field in the IPv4 header was replaced by the Quality of Service (QoS) fields to provide support for real time traffic such as (Traffic Class field and the Flow Label field) (Deering et al. 1995). The Payload Length field has replaced the Total Length field, as the length of the IPv6 header is fixed there is no longer any need for this to be taken into account when calculating the length of the packet (the optional headers in IPv4 were of variable length, thus so was the overall header). The Payload Length field can register a data payload of up to 64kB, or more if the Jumbogram (Borman et al. 1999) (i.e. setting the payload length and next header fields to zero it means IPv6 jumpogram, the next header will be hop-by-hop options header) option is specified. The Time-To-live field was replaced by

the Hop Limit field. It operates in the same way as in IPv4, with each router the packet passes through decrementing the field by one, indicating each “hop” in an end-to-end route. The old Protocol Type field has been replaced by the Next Header field; this contains the code that indicates whether an extension header follows the main header. The Next Header field is also used to specify the transport layer protocol of the packet payload, just as in IPv4. These codes are the same as they are in IPv4: TCP (Carpenter 2000), UDP (Deering et al. 1998) and ICMPv6 (Dupont et al. 2004). A Next Header value of “59” means there is no next header in the packet as shown Table 2.1. This restructuring has resulted in a much simpler header compared to its IPv4 counterpart; the IPv4 header has thirteen fields in it whereas the IPv6 header has only eight. Even though the new addresses are four times the size of the IPv4 addresses, the restructuring has resulted in a new header that is only twice the size of its predecessor. This is intended to offset the bandwidth cost of using these larger addresses and it should help to make routing these packets more efficient (Kafle 2006).

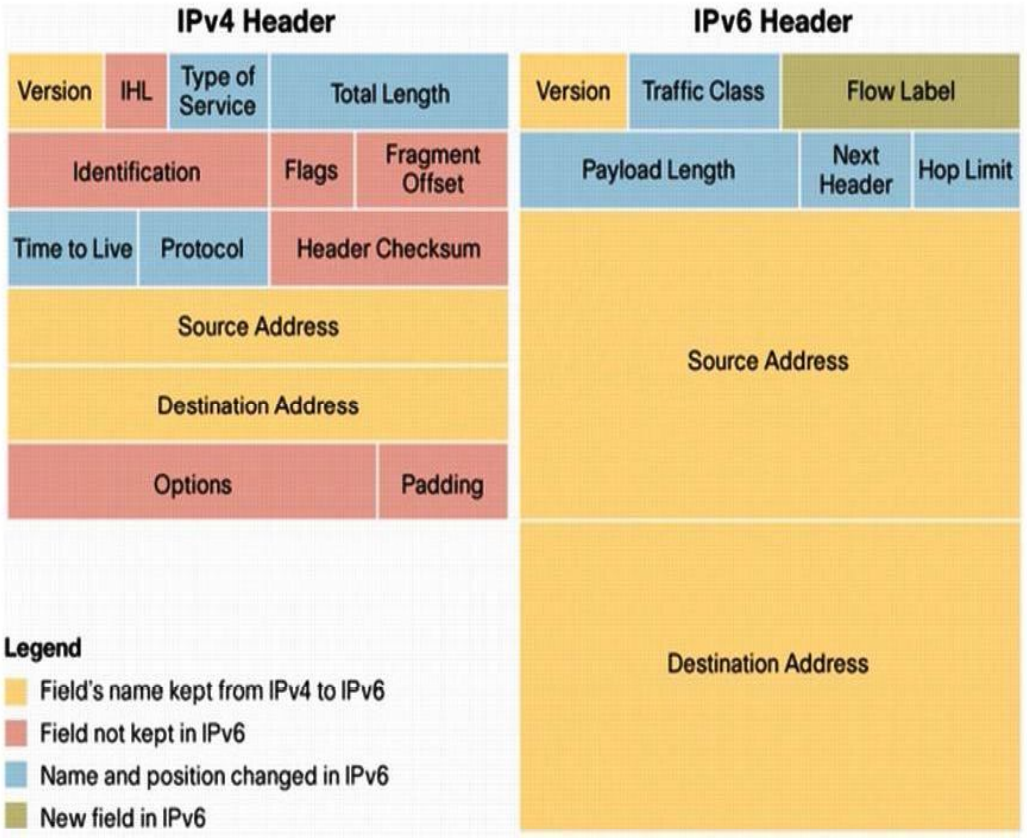

Figure 2.1 IPv4 and IPv6 Headers

2.2.1 Extension Headers

As previously mentioned, all the options fields of the IPv4 header are not present in the main IPv6 header and flexible extension headers that are placed in between the IPv6 header and the transport layer header were created instead. These extension headers provide support in IPv6 for features, such as security (in the form of IPsec), source routing, network management and fragmentation. There are six Extension Headers: Hop-by-Hop option, Destination option, Routing, Fragment, Authentication and Encapsulation Security Payload. Different extension headers can be chained together in a packet. Each extension header also has a Next Header field, which is used to identify the header following it.

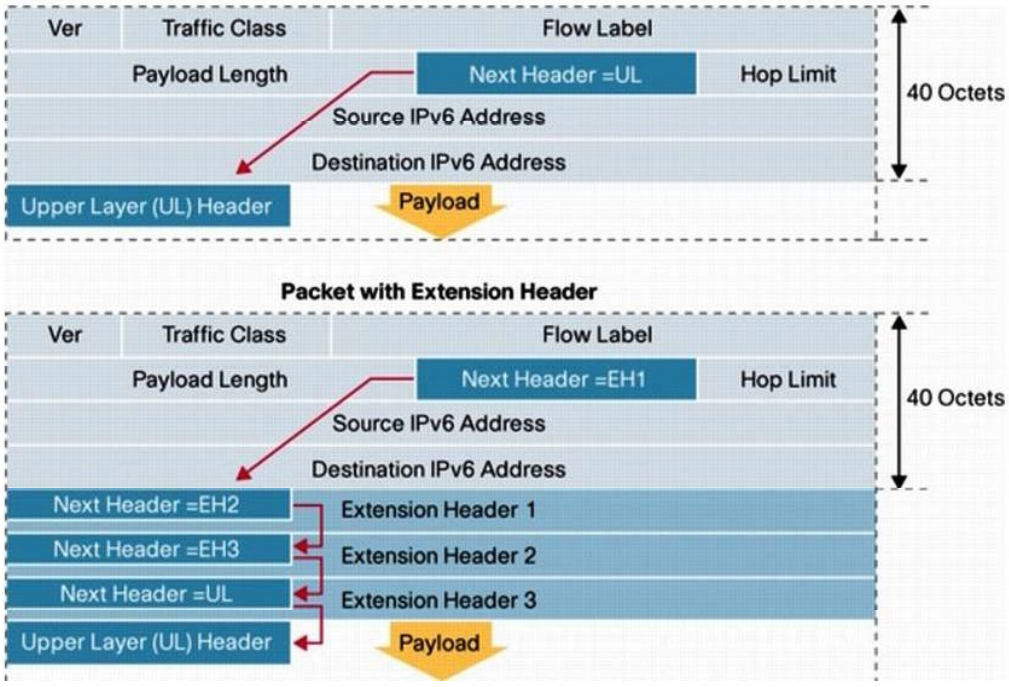

Figure 2.2 Chaining Extension Headers in IPv6 Packets

Figure 2.2 shows this chaining process and table 2.1 contains the next header codes. Extension headers should always be chained together in the order they are listed above. This is to facilitate the processing of these headers at the destination. The Hop-by-Hop options header must always follow the main IPv6 header, as it is the only extension header that must be examined by intermediate nodes. The Jumbogram and Router Alert options are part of the Hop-by-hop extension header. Jumbograms are

used to send packets with a larger data payload than the 64 KB specified by the Payload Length field in the IPv6 header. To implement this, the value of the Payload length field should be set to zero and the Jumbogram extension header attached; then a much larger payload of up to 4GB can be sent in the one IPv6 datagram (on links with a high enough MTU). The router alert Hop-by-Hop option is used to notify transit routers that they should examine the contents of the packet more thoroughly before forwarding it on. This option is used to specify that the datagram requires special processing by the nodes route. Each extension header only occurs once per packet at most, except the destination options header. The first instance of the destination option is used to carry information to the destinations listed in the destination address field in the IPv6 header and the addresses in the routing header, and the second is for optional information that is only to be read by the final destination (Deering et al. 1998).

Table 2.1 IPv6 Extension Headers and their Recommended Order in a Packet (Johnson et al. 2004)

Order	Header Type	Next Header Code
1	**Basic IPv6 Header**	-
2	**Hop-by-Hop Options**	0
3	**Destination Options (with Routing Options)**	60
4	**Routing Header**	43
5	**Fragment Header**	44
6	**Authentication Header**	51
7	**Encapsulation Security Payload Header**	50
8	**Destination Options**	60
9	**Mobility Header**	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

The routing header is used to specify intermediate nodes the packet must pass through on the way to the destination. Different types of routing headers may be used. The “type 0” routing header is similar to IPv4’s loose source routing option. Its header comprises of a next header field, which identifies the header following it; the Hdr Extn Length, which gives the length of the routing header (in the type 0 case, the Header Extension Length is twice the number of addresses given in the header); the routing header type; the Segments Left field, which identifies how many nodes must still be visited by the packet; a 32-bit reserved field that is to be ignored; and finally the addresses that must be visited en-route by the packet.

In IPv6, fragmentation of a packet is only permitted when it is performed by the source node. Routers are not allowed to fragment a packet. If a packet is received by a router that is too big for the link, it must be discarded and an Internet Control Message (ICMPv6) must be sent back to the source of the packet to inform them the packet was dropped. Removing the option to fragment packets en-route should result in fewer problems for hosts and routers, such as crack attempts using overlapping fragments and broken path MTU. If a source wishes to fragment a packet it uses the Fragment extension header. The original packet that is too large is divided up into two sections: the “unfragmentable part”, which contains the IPv6 header and all extension headers which must be processed by nodes en-route to the final destination (i.e. the Hop-by-Hop option, and the destination option and routing header where specified); and the “fragmentable part”, which consists of the rest of the extension headers (if there are any) and the payload data. The fragmentable part is divided into fragments of multiples of 8-octets long, except possibly the final fragment, and each fragment is pre fixed by the “unfragmentable part” and the fragment header. Security was also a major concern of the IETF when it was designing IPv6. They aimed to establish three important security services: packet authentication, packet integrity, and packet confidentiality. These security features are provided by IPsec (Kent et al. 1998) via the Authentication (AH) and Encapsulation Security Payload (ESP) extension headers as shown in Figure 2.3. The AH provides integrity validation, which guarantees that a packet comes where it claims to have come from. This is achieved by the exchange of cryptographic keys, either manually or automatically (using Internet Key Exchange (IKE)). Before each packet is sent, the header creates a checksum based on the key

agreed by both hosts (typically a MD5 hash). This hash is then re-run on the receiving end and is compared to the original checksum. The AH is used to prevent host spoofing attacks and packet modification attempts, but it does not provide any protection against packet sniffing. The ESP extension header is used to provide packet confidentiality as well as the same security services that AH provides. This high level of privacy and integrity for packets was unheard of in IPv4, except in the case of Secure Socket Layer (SSL) applications or where the IPv4 implementation of IPsec was deployed; IPsec was back-ported to IPv4, but was not made an integral part of the protocol as in IPv6. ESP can be deployed in two ways: transport mode or tunnel mode. In transport mode the encryption is applied to the transport layer and other upper layer protocols but not the IPv6 header or any other extension headers that come before the AH and ESP headers. With Tunnel mode ESP, the entire packet is encrypted including the entire IPv6 header, and a new header prefixes the encapsulated encrypted packet. (Kent et al. 1998) describes the difference between AH and ESP as: "*The primary difference between the authentication provided by ESP and AH is the extent of the coverage; ESP does not protect the IP header fields unless those fields are encapsulated by ESP (tunnel mode).*"

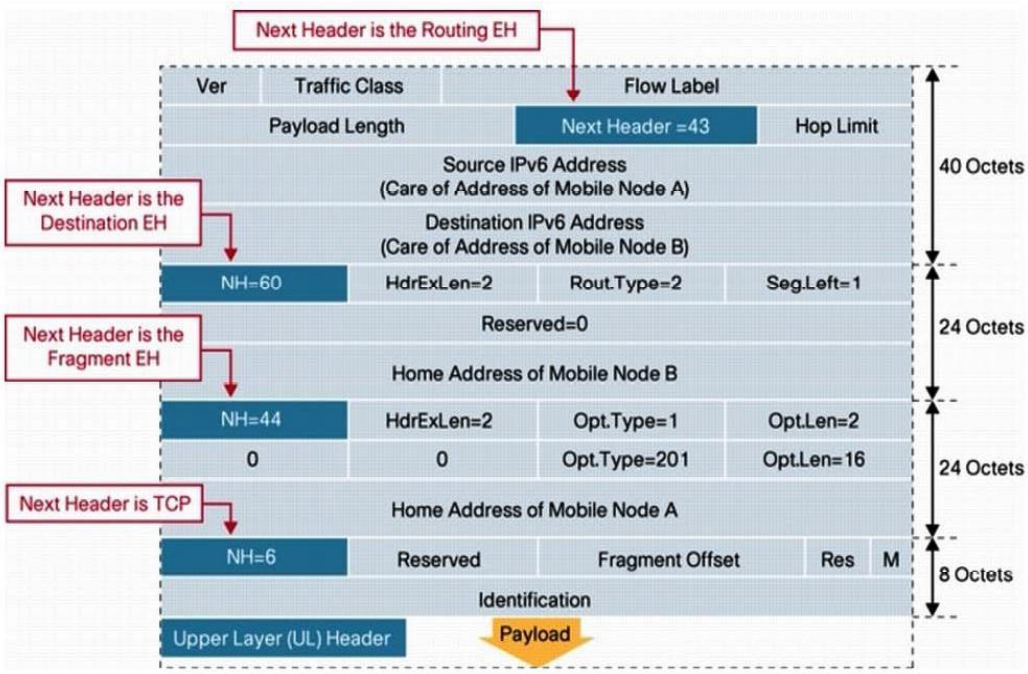

Figure 2.3 Data Traffic between Two Mobile Nodes over the Route optimized Path