# UNIVERSITI PUTRA MALAYSIA

# SECURITY ENHANCEMENT OF ROUTE OPTIMIZATION IN MOBILE IPv6 NETWORKS


**ABBAS MEHDIZADEH ZARE ANARI**



**FK 2008 39**

# SECURITY ENHANCEMENT OF ROUTE OPTIMIZATION IN MOBILE IPv6 NETWORKS

By

**ABBAS MEHDIZADEH ZARE ANARI**

**Thesis Submitted to the School of Graduate Studies, University Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science**

**June, 2008**

## DEDICATION

This thesis is dedicated to

*MY BELOVED PARENTS*

*MOHAMMAD MEHDIZADEH AND ZEINAB SADEGHI*

*FOR THEIR ENDLESS CARE AND COMFORT*

*AND MY DEAR HAMIDEH*

*FOR HER CARE AND LOVE IN MY LIFE*

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

**SECURITY ENHANCEMENT OF ROUTE OPTIMIZATION IN MOBILE IPv6 NETWORKS**

By

**ABBAS MEHDIZADEH ZARE ANARI**

**June 2008**

**Chairman: Associate Professor Sabira Khatun, PhD**

**Faculty: Engineering**

Mobile IPv6 is an IP-layer protocol that is designed to provide mobility support. It allows an IPv6 node to arbitrarily change its location in the IPv6 network while maintaining the existing connection by handling the change of addresses at the Internet layer.

Route optimization is standard in Mobile IPv6 to eliminate inefficient triangle routing. Several methods were proposed to secure route optimization. Return routability was adopted by Internet Engineering Task Force (IETF) with its security protocol based on RFC 3775. Return routability is an infrastructureless, lightweight procedure that enables a Mobile IPv6 node to request another IPv6 node to check and test the ownership of its permanent address in both home network and current visited network. It authorizes a binding procedure by the use of cryptographically token exchange. However, return routability protocol in route optimization is to protect messages and is not able to detect or prevent an attacker which tampers against data.

In this thesis, focus is given on Mobile IPv6 route optimization test-bed with enhanced security in terms of data integrity. The proposed method can be performed on top of the return routability procedure to detect and prevent Man-In-The-Middle attack by using encryption if any attack is detected. This also eliminates the additional delay compared to using encryption from the beginning of a connection.

A real-time experimental test-bed has been set up, which is comprised of hardware, software and network analysis tools to monitor the packet flow and content of data packets. The test-bed consists of four computers acting as Mobile Node, Home Agent, Correspondent Node, and Router, respectively. To ensure the accuracy and integrity of the collected data, the Network Time Protocol (NTP) was used between the packet generator (Mobile Node) and packet receiver (Correspondent Node) to synchronize the time.

The results show that the proposed method is able to work efficiently, maintaining 99% data security of route optimization in Mobile IPv6 (MIPv6) networks. The overall data integrity (by means of security) is improved 72% compared to existing MIPv6 by at a cost of 0.1 sec added overall delay, which is within the tolerable range by the network.

.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master of Sains

**PENINGKATAN KESELAMATAN UNTUK MENGOPTIMUMKAN LALUAN DALAM RANGKAIAN MOBIL IPv6**

Oleh

**ABBAS MEHDIZADEH ZARE ANARI**

**June 2008**

**Pengerusi: Profesor Madya Sabira Khatun, PhD**

**Fakulti: Kejuruteraan**

Rangkaian IPv6 bergerak ialah satu protokol lapisan IP yang direka khas bagi tujuan membenarkan pergerakan nod IPv6. Ia membenarkan setiap nod IPv6 untuk bertukar lokasi di dalam rangkaian IPv6 sambil mengekalkan hubungan dengan menguruskan pertukaran alamat pada lapisan *Internet.*

Laluan optimum adalah piawai di dalam IPv6 bergerak untuk menghapuskan penghalaan tigasegi. Beberapa kaedah dicadangkan untuk memastikan perlaksanaan laluan optimum. Sebagai contoh, *Return Routability* telah diadaptasi daripada *Internet Engineering Task Force (IETF)* bersama-sama dengan protokol keselamatan berdasarkan RFC 3775. *Return Routability* mempunyai ciri-ciri tanpa infrastrukutur, prosedur yang tidak terlampau kompleks. Ia membenarkan nod IPv6 bergerak untuk memohon nod IPv6 yang lain untuk menyemak dan memeriksa hakmilik alamat tetapnya di dalam rangkaian rumah dan juga rangkaian terkini yang dilawatinya. Ia membenarkan prosedur pengikatan dengan menggunakan kaedah pertukaran token secara kriptologi. Walau bagaimanapun, protokol *Return Routability* di dalam laluan

optimum adalah untuk mengawal risalah dan ia tidak mampu untuk mengesan dan mengelak serangan yang akan mengubah data.

Tesis ini memfokuskan kepada tapak uji untuk laluan optimum di dalam IPv6 bergerak bagi meningkatkan keselamatan dari segi integriti data. Kaedah yang dicadangkan boleh dilakukan sebagai tambahan ke atas prosedur *Return Routability* untuk mengesan dan menghalang serangan *Man-In-The-Middle* dengan menggunakan enkripsi jika serangan dikesan. Ini juga dapat mengurangkan kelengahan tambahan jika dibandingkan dengan penggunan enkripsi pada permulaan perhubungan.

Satu tapak uji eksperimen masa nyata telah dibangunkan, yang merangkumi perkakasan, perisian dan alat analisis rangkaian untuk mengawasi pengaliran paket dan kandungan data paket. Tapak uji terdiri dari empat buah komputer sebagai *Mobile Node, Home Agent, Correspondent Node* dan juga penghala,mesing mesing untuk memastikan ketepatan dan integriti data yang dikumpulkan, *Network Time Protocol (NTP)* telah digunakan di antara penghasil paket *(Mobile Node)* dan penerima paket *(Correspondent Node)* untuk menyegerakkan masa.

Hasil keputusan menunjukkan kaedah yang dicadangkan boleh bekerja dengan berkesan, dengan memastikan keselamatan data untuk laluan optimum di dalam rangkaian IPv6 bergerak pada tahap 99%. Integriti data keseluruhan (dari segi keselamatan) bertambah baik sebanyak 72% berbanding dengan MIPv6 yang sedia ada dengan kos penambahan 0.1 saat pada kelengahan keseluruhan, ia itu masih berada di dalam jeda toleransi rangkaian.

# ACKNOWLEDGEMENTS

There are lots of people that I'd like to thank for their help and guide, if I miss some of them here, they have my sincere apologies.

First, I'd like to thank Assoc.Prof Dr.Sabira Khatun for her support, encouragement, and excellent comments that made this work possible.

I'm deeply indebted to Prof.Dr. Borhanuddin Mohd Ali for his support in general and in particular for his efforts in professional reviewing the thesis making extremely useful remarks that have improved the quality of this research.

I extend my deepest gratitude to Dr. Raja Syamsul Azmir Raja Abdullah and Dr. Gopakumar Kurup for their great effort and support during my study period.

The greatest acknowledgment I reserve for my family members especially, my father, my mother, my brothers and sisters, who endured this long process with me always offering support and patience.

My special thanks to Shariq Haseeb, Yong Chu Eu, Dr.Sahar Al-Talib, and Rozaidi Rahmad, who really help me a lot in getting my test-bed done.

Finally, I'd like to thank all of my friends especially, Amin Malek, Nidhal, Fazirul, Dr.Chee Kyun, and Aus with our unforgettable memories.

## APPROVAL

I certify that an Examination Committee has met on **12/06/2008** to conduct the final examination of **Abbas Mehdizadeh Zare Anari** on his Master of Science thesis **“Security Enhancement of Route Optimization in Mobile IPv6 Networks”** in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

**Abdul Rahman Ramli, PhD**
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

**Mohd. Fadlee A. Rashid, PhD**
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

**Nor Kamariah Noordin, PhD**
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

**Rahmat Budiarto, PhD**
Associate Professor
Faculty of Computer Science
Universiti Sains Malaysia
(External Examiner)

**HASANAH MOHD GHAZALI, PhD**
Professor and Deputy Dean
School Of Graduate Studies
University Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science.
The members of the Supervisory Committee were as follows:

**Sabira Khatun, PhD**
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

**Borhanuddin Mohd. Ali, PhD**
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

**Raja Syamsul Azmir Raja Abdullah, PhD**
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

**Gopakumar Kurup, PhD**
Head, Communication Networks & Solutions Lab
MIMOS Berhad
Technology Park, Malaysia
(Member)

______________________
**AINI IDERIS, PhD**
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

## DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

**ABBAS MEHDIZADEH ZARE ANARI**

Date: June 12, 2008

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| 1xEV-DO | 1x Evolution-Data Only |
| 3G | Third Generation |
| 4G | Fourth Generation |
| AAA | Authentication, Authorization, Accounting |
| AH | Authentication Header |
| BA | Binding Acknowledgment |
| BC | Binding Cache |
| BU | Binding Update |
| BUL | Binding Update List |
| BWA | Broadband Wireless Access |
| CDMA | Code Division Multiple Access |
| CGA | Cryptographically Generated Address |
| CMU | Carnegie Mellon University |
| CN | Correspondent Node |
| CoA | Care-of Address |
| CoT | Care-of Test |
| CoTI | Care-of Test Init |
| D&P | Detection and Prevention |
| DAD | Duplicate Address Detection |
| DH | Diffie-Helman |
| DHCPv6 | Dynamic Host Configuration Protocol version 6 |
| DoS | Denial-of Service |
| EDGE | Enhanced Data rate for GSM Evolution |

| | |
|---|---|
| ECC | Elliptic Curve Cryptography |
| ESP | Encapsulating Security Payload |
| ESSID | Extended Service Set IDentifier |
| ETSI | European Telecommunication Standard Institute |
| FA | Foreign Agent |
| FR | Foreign Router |
| FTP | File Transfer Protocol |
| GNU | GNU's Not Unix |
| GPL | GNU Public License |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile communications |
| GUI | Graphical User Interface |
| HA | Home Agent |
| HMAC | Hash-based Message Authentication Code |
| HoA | Home Address |
| HoT | Home Test |
| HoTI | Home Test Init |
| HSPDA | High-Speed Downlink Packet Access |
| HUT | Helsinki University of Technology |
| ICMPv6 | Internet Control Message Protocol version 6 |
| ID | IDentifier |
| IESG | Internet Engineering Steering Group |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |

| | |
|---|---|
| IP | Internet Protocol |
| IPng | Internet Protocol next generation |
| IPsec | Internet Protocol Security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IRDP | ICMP Router Discovery Protocol |
| ISAKMP | Internet Security Association and Key Management Protocol |
| Kbm | Key binding management |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MD5 | Message Digest Algorithm |
| MH | Mobility Header |
| MHAE | Mobile Home Authentication Extension |
| MIPL | Mobile IPv6 for Linux |
| MIPv6 | Mobile IPv6 |
| MITM | Man-In-The-Middle |
| ML-IPsec | Multi-Layered IPsec |
| MML-IPsec | Mobile Multi-Layered IPsec |
| MN | Mobile Node |
| MTU | Maximum Transmission Unit |
| NAT | Network Address Translation |
| NDP | Neighbor Discovery Protocol |
| NTP | Network Time Protocol |
| PC | Personal Computer |

| | |
|---|---|
| PDA | Personal Digital Assistant |
| QoS | Quality-of-Service |
| RA | Router Advertisement |
| RADVD | Router ADVertisement Daemon |
| RFC | Request For Comment |
| RO | Route Optimization |
| RR | Return Routability |
| RS | Router Solicitation |
| SA | Security Association |
| SAD | Security Association Database |
| SG | Security Gateway |
| SPD | Security Policy Database |
| SPI | Security Parameter Index |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TR | Triangle Routing |
| UDP | User Datagram Protocol |
| USAGI | UniverSAl playGround for Ipv6 |
| UMTS | Universal Mobile Telecommunications System |
| UWB | Ultra-Wide Band |
| Wi-Fi | Wireless Fidelity |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WLAN | Wireless Local Area Network |
| WPAN | Wireless Personal Area Network |

# CHAPTER 1

# INTRODUCTION

## 1.1 Background

The Internet Protocol (IP) is the chosen platform for converged communication in future 3G cellular wide area networks, wireless local area networks, personal area networks, and emerging wireless broadband networks often referred to as 802.16 WiMAX, 802.20, or as 4G technologies. Wireless technologies are beginning to co-exist and emerge as Cellular/Bluetooth, Cellular/Wi-Fi, and Cellular/Ultra-Wideband (UWB) devices. Wireless technology includes:

- Wireless local area networks (WLAN) Wi-Fi 802.11a/b/g technologies.
- Wireless wide area networks cellular technologies such as GSM, GPRS, EDGE, UMTS, HSDPA, CDMA2000, and 1xEV-DO.
- Wireless personal area networks (WPAN) technologies including 802.15.1 Bluetooth, 802.15.3c, 802.15.4 ZigBee, 802.15.4a UWB, and 802.15.5 Mesh Networks.
- Broadband wireless access (BWA) network technologies such as 802.16 and 802.20.

Deployment of high-speed wireless networks, emergence of 3G wireless networks that support packet data services, and availability of 802.11 wireless LANs in homes and public places have made un-tethered wireless computing more attractive to a very large number of users.

Mobile IP is the underlying technology for supporting various mobile data and wireless networking applications. Mobility is becoming an increasingly critical need because of the inclusion of IP stacks in PDAs, mobile phones, and various forms of notebooks and PCs. The goal of mobility is to perform intended service anytime, anywhere, anyhow.

The Mobile IPv6 (MIPv6) allows nodes to be reachable by a static IP address which is called Home Address (HoA) [1]. The Home Agent (HA) tunnels packets to and from the Mobile Node (MN), and intercept the packets when Correspondent Node (CN) sends to MN, then forward them. When the MN moves to another network it will inform the HA about its new address called Care-of-Address (CoA).

When the MN is far away from HA, the packets between MN and CN have to travel via the HA. This inefficient routing is called Triangle Routing. To rectify this problem, MIPv6 introduces a Route Optimization (RO) mechanism. When the MN receives a tunnelled packet, it must decide to establish RO. MN sends Binding Update (BU) message to CN containing mobile home address and CoA. The CN stores this information in its binding cache to use to send packets to CoA instead of HoA. Unfortunately, BUs can be used by the attackers to launch the attack. However, MIPv6 uses IPsec to protect signalling between MN and HA [2], it includes a set of facilities that support security services such as authentication, integrity, confidentiality and access control at the IP layer. MIPv6 also uses Return Routability (RR) procedure for protection of the signalling between MN and CN in RO [3]. The RR procedure authenticates BUs, using cryptographic signature to prevent the attackers from sending false BUs.

## 1.2 Problem Statement and Motivation

The Internet Protocol (IP) is a connectionless network layer protocol that uses datagram (data-oriented) to communicate over a packet-switched network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. All data traffic, signalling, real time services, and circuit switched services should be carried in IP packets in the near future, so “All-IP approach” will become reality.

The current version of IP that is widely used is IPv4. A new version, called IPv6 formerly IPng, is the next-generation network layer protocol and now widely implemented and deployed in many networks. The main reason to move toward IPv6 includes the exponential growth of the internet and limitation in IPv4 address space; simpler and more automatic configuration of addresses and other settings; security requirement at IP layer; the need for better support for real-time data delivery; and emergence of IP-capable mobile devices.

Since mobile computing is getting more widespread with the inclusion of IP stacks in PDAs, notebooks, PCs and mobile phone, mobility support for Internet devices is becoming more important. IP mobility is designed to allow mobile device users to move from one network to another while maintaining reachability via their permanent/home IP address [4].

MIPv6 is designed to handle the mobility management on the IP-layer for the emerging IPv6 protocol. One major component in MIPv6 that is needed to be considered is security for most messages used between MNs, HAs, and CNs. The Internet Engineering Task Force (IETF) has developed the IPsec protocol suite as an extension to the basic IP protocol [2] based on modern cryptographic technologies making possible strong data authentication and encryption. The IPsec eliminates the network security problems associated with the IP protocol. It works on the network level, layer three on the protocol stack that is invisible to applications. This feature sets IPsec apart from other Internet security technologies that run at other layers, such as e-mail and web browser encryption. IPsec is compatible with current Internet standards in both IPv4 and IPv6, but in IPv6, IPsec is defined as mandatory feature [3], [5], [6], [7].

There is a concern regarding the performance of IPsec. The required processing power is large for security functions, especially for IPsec. Many users would not have enough throughputs for many applications when very large processing power is required. We can deploy the secure and reliable information infrastructure cost effectively when the ordinary PC platform can handle the IPsec for major applications. Even with IPsec, the majority of vulnerabilities on the internet today are in the application layer, something that IPsec will do nothing to prevent. In Route Optimization when considering authentication of messages between MN and some unknown CNs, no pre-shared secret key can be used, and there is not existing global public key infrastructure, therefore

IPsec is not usable for authentication between MN and CN [8]. Another problem to use IPsec is that Quality-of-Service does not work with it.

There is a serious challenge for securing RO, which is standard in MIPv6 and occurs when MN moves to another network to eliminate inefficient triangle routing. MIPv6 uses return routability procedure to authenticate and secure BUs [1], [3], [9]. There is no authentication and data protection method in RO when MN moves from one network to another, in RFC 3775, standard for MIPv6.

In this thesis, we propose a new security method in terms of data integrity that overcomes the problem of unprotected data in MIPv6 RO where there are problems and limitations of using IPsec. An enhanced security algorithm is developed on top of MIPv6 RO to secure data and prepare safe communication between MN and CN. This algorithm is able to detect and prevent the attacker from modifying the data, using an encryption algorithm at a cost of a small increased tolerable delay. MN starts encryption when attack is detected, not from the beginning of the session because some of the applications are delay sensitive, including real time services such as streaming media or interactive multimedia, as well as data services requiring low latency. In addition, when MN and CN are located in the private or secured network, they do not need to use encryption from the beginning. When MN is sending packets, it copies and save some packet randomly by a flag to inform CN to return those packets. Therefore MN is able to compare these two packets (saved before and received back from CN), whether they are same or not.