UNIVERSITI PUTRA MALAYSIA

SEAMLESS AND SECURE HANDOVER SCHEME IN MOBILE WiMAX

HAMZAH FAREED RASHID

FK 2015 124

SEAMLESS AND SECURE HANDOVER SCHEME IN MOBILE WiMAX

By

HAMZAH FAREED RASHID

© COPYRIGHT UPM

Thesis Submitted to the School Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

December 2015

COPYRIGHT

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia

© COPYRIGHT UPM

قال تعالى:
{ إن أريد إلا الإصلاح ما استطعت وما توفيقي إلا بالله عليه توكلت وإليه أنيب }
هود 88

DEDICATION

To my dear mother, Fadheelah Zmezm, for her love and endless support

To my brothers and sisters for their extraordinary love, their endless care and encouragement

To all those who stand by me

Thank you

© COPYRIGHT UPM

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

SEAMLESS AND SECURE HANDOVER SCHEME IN MOBILE WiMAX

By

HAMZAH FAREED RASHID

December 2015

Chairman : Shaiful Jahari Bin Hashim, PhD
Faculty : Engineering

Handover performance plays an essential role in ensuring that an excellent result is realized for most of the real-time applications in WiMAX networks. Generally, the entire interruption found in the handover process exists in three categories: i) link layer handover delay, ii) IP network layer handover delay, iii) security sub-layer handover delay.

According to research the large portion of the delay associated with the handover process originates from user authentication and network entry and re-entry. Some types of soft real-time applications which include media streaming, however, require the smallest interruption for effective service.

Unfortunately the existing design of the handover scheme lacks the ability to provide a seamless and secure connection [8][9]. Therefore, making use of this conventional technique will be unsuitable [22]. This thesis introduces an efficient design that can provide a seamless and secure communication especially over the subsequent handover; we named it (**S**eamless & **S**ecure Subsequent Handover) 3SHO for short.

This approach considers the use of a pre-authentication method and prior backhaul inter-communication, to generate a minimum delay that is suitable for some types of soft real-time application. Results obtained from analytical comparison and simulation; indicate that 3SHO approach achieves 72% improvement when compared to the standard [8][9], and 38% improvement over the enhanced scheme in [40].

When it comes to packet loss, the simulation results show that 3SHO approach achieves 76% improvement over the standard [8][9], and 56% improvement over the enhanced scheme in [40]. Parallel to the seamless handover, the proposed pre-authentication scheme proves to be a fine addition to our approach towards achieving a seamless handover with backward/forward secrecy characteristic. Furthermore,

© COPYRIGHT UPM

3SHO approach is verified using Automated Validation of Internet Security Protocols and Applications (AVISPA).

© COPYRIGHT UPM

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

SKIM PENGESAHAN LEPAS TANGAN LANCAR DAN SELAMAT DALAM WiMAX MUDAH ALIH

Oleh

HAMZAH FAREED RASHID

Disember 2015

Pengerusi : Shaiful Jahari Bin Hashim, PhD
Fakulti : Kejuruteraan

Prestasi lepas tangan memainkan peranan penting di dalam memastikan keputusan cemerlang untuk kebanyakan aplikasi masa nyata di dalam rangkaian WiMAX. Secara umumnya semua gangguan yang dijumpai di dalam proses lepas tangan berada di dalam tiga kategori: i) lengah lepas tangan lapisan pautan ii) lengah lepas tangan lapisan rangkaian IP iii) lengah lepas tangan sublapisan keselamatan.

Berdasarkan kepada penyelidikan, sebahagian besar daripada lengah yang berkaitan dengan proses lepas tangan adalah berasal daripada proses pengesahan pengguna dan masukan rangkaian serta masukan semula rangkaian. Walaubagaimanapun, sebahagian daripada jenis aplikasi masa nyata yang lembut iaitu pengaliran media memerlukan gangguan minima untuk perkhidmatan yang berkesan.

Malangnya reka bentuk skema lepas tangan yang sedia ada kekurangan keupayaan untuk menyediakan sambungan yang selamat dan lancar [8][9]. Justeru itu, penggunaan teknik konvensional ini adalah tidak sesuai. Tesis ini memperkenalkan rekabentuk cekap yang boleh menyediakan komunikasi yang lancar dan selamat terutamanya untuk lepas tangan berikutan; yang kami namakan (Lepas Tangan Lancar dan Selamat) 3SHO secara ringkas.

Pendekatan ini mempertimbangkan penggunaan kaedah pra-pengesahan dan komunikasi terlebih dahulu antara angkut balik, untuk menjana lengah minima yang sesuai untuk sebahagian jenis aplikasi masa nyata yang lembut. Keputusan yang diperolehi dariapada perbandingan beranalisis dan simulasi menunjukkan pendekatan 3SHO mencapai peningkatan sebanyak 72% berbanding piawai [8][9], dan peningkatan 38% berbanding skema yang telah diperbaiki di dalam [40].

Untuk kehilangan paket, keputusan simulasi menunjukkan pendekatan 3SHO mendapat 76% peningkatan ke atas piawai [8][9], dan 56% peningkatan berbanding skema yang telah diperbaiki di dalam [40]. Selari kepada lepas tangan secara lancar,

© COPYRIGHT UPM

cadangan skema pra-pengesahan tersebut terbukti sebagai penambahan yang baik kepada pendekatan kami ke arah mencapai ciri kerahsiaan kebelakang/kehadapan. Tambahan pula, pendekatan 3SHO telah disahkan dengan menggunakan Pengesahsahihan Berautomat Protokol dan Aplikasi Keselamatan Internet (AVISPA).

© COPYRIGHT UPM

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Almighty Allah (S.W.T) for giving me the strength, patience, courage, and determination to complete this work. All grace and thanks belongs to Almighty Allah (S.W.T)

Many special thanks go to my supervisor Associate Professor Dr. Shaiful Jahari bin Hashim, for his incredible guidance, continuous support, and encouragement. He always has time for me and readily providing his technical expertise throughout the period of my study. I owe more than I can ever repay. The completion of this work becomes possible due to his supervision. His high stance of diplomatic power and professionalism set a great model for me to follow.

I would also like to thank Associate Professor Dr. Aduwati Sali for serving on my thesis committee. Her helpful suggestions and advices on various aspects of my research work have certainly been very constructive. Without Her kind cooperation and support, my graduate study would not have been accomplished.

Thanks to everyone at the Faculty of Engineering and all those who asked "how is your thesis going?" These memories at the Faculty of Engineering will always be cherished.

© COPYRIGHT UPM

I certify that a Thesis Examination Committee has met on 1 December 2015 to conduct the final examination of Hamzah Fareed Rashid on his thesis entitled "Seamless and Secure Handover Scheme in Mobile WiMAX" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Fakhrul Zaman bin Rokhani, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Fazirulhisyam bin Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

R. Badlishah bin Ahmad, PhD
Professor Ir.
Universiti Malaysia Perlis
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 25 May 2016

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

Shaiful Jahari Bin Hashim, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Aduwati Sali, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work
- quotations, illustrations and citations have been duly referenced
- the thesis has not been submitted previously or comcurrently for any other degree at any institutions
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be owned from supervisor and deputy vice –chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature:____________________________ Date: _________________________

Name and Matric No: Hamzah Fareed Rashid, GS26974

© COPYRIGHT UPM

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: ______________________________
Name of Chairman of Supervisory Committee: Associate Professor Dr. Shaiful Jahari Bin Hashim

Signature: ______________________________
Name of Member of Supervisory Committee: Associate Professor Dr. Aduwati Sali

© COPYRIGHT UPM

TABLE OF CONTENTS

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF TABLES

© COPYRIGHT UPM

LIST OF FIGURES

© COPYRIGHT UPM

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization, Accounting
ABS	Anchor BS
AES-CCM	Advanced Encryption Standard in Counter with Cipher Block Chaining (CBC)-MAC
AHOP	Actual Handover Phase
AM	Amplitude Modulation
AMPS	Advanced Mobile Phone System
AOD	Angle of Divergence
AP	Access Point
AR	Access Router
ARPANET	Advanced Research Projects Agency Network
ASN	Access Service Network
ASN-GW	ASN Gateway
ATM	Asynchronous Transfer Mode
BBM	Break-Before-Make
BE	Best Effort
BS	Base Station
BSS	Basis Service Set
CBC	Cipher Block Chaining
CDMA	Code Division Multiplexing Access
CDT	Connection Disruption Time
CID	Connection Identifiers
CL	Current Load
CMAC	Cipher-based Message Authentication Code
CS	Candidate Set
CSN	Connectivity Service Network
DCD	Downlink Channel Descriptor
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DL	MAP_IE - Downlink Map Information Element
DS	Diversity Set
DS	WCDMA - Direct Sequence Wideband CDMA
EAP	Extensible Authentication Protocol
ETSI	European Telecommunication Standards Institute
FA	Foreign Agent
FBSS	Fast Base Station Switching
FDD	Frequency-Division Duplex

© COPYRIGHT UPM

FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FM	Frequency Modulation
FMIPv6	Fast Handover for MIPv6
FTP	File Transfer Protocol
4G	Fourth Generation
GHz	Gigahertz
GSM	Global System for Mobile Communication
HHO	Hard Handover
HMAC	Hash-based Message Authentication Code
HMIPv6	Hierarchical Mobile IPv6
HSPA	High-Speed Packet Access
Hz	Hertz
IETF	Internet Engineering Task Force
IMT-Advanced	International Mobile Telecommunications-Advanced
IP	Internet Protocol
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union's Recommendation
LAN	Local Area Network
LBS	Load-Based Score
LBS	Location-based Services
LOS	Line-of-Sight
LTE	Long Term Evolution
LTE-A	LTE-Advanced
L2	Layer-2
L3	Layer-3
MA	Mobility Agent
MAC	Media Access Control
MANET	Mobile Adhoc Networks
MBB	Make-Before-Break
MBS	Broadcast and Multicast Services
MDHO	Macro-Diversity Handover
MD5	Message-Digest 5
MIMO	Multiple Input / Multiple Output
MITM	Man in the Middle attack
MIPv6	Mobile Internet Protocol version 6
MOB_ASC-REP	Mobile Association Result Report

© COPYRIGHT UPM

MOB_BSHO-REQ	Base Station Handover Request
MOB_BSHO-RSP	Base Station Handover Response
MOB_HO-IND	Mobile Handover Indication
MOB_HO-REP	Mobile Handover Report
MOB_MS-REP	Mobile Report Message
MOB_MSHO-REQ	Mobile Station Handover Request
MOB_NBR-ADV	Mobile Neighbour Advertisement
MOB_RNG-IND	Mobile Ranging Indication
MOB_SCN-REQ	Scanning Interval Allocation Request
MOB_SCN-RSP	Scanning Interval Allocation Response
MOB_SCN-REP	Scanning Result Report
MPDU	MAC protocol data units
MRPLM	Minimum Required Period of Linear Motion
MSC	Mobile Switching Centres
MSDU	MAC service data units
MS	Mobile Station
MHz	Megahertz
NAP	Network Access Providers
NBS	Neighboring Base Stations
NLOS	Non-line-of-sight
NRM	Network Reference Model
NSP	Network Service Providers
NTAP	Network Topology Acquisition Phase
NWG	Network Working Group
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSI	Open Systems Interconnection
PHY	Physical Layer
PKM-REQ	Privacy Key Management Request
PKM-RSP	Privacy Key Management Response
PKMv2	Privacy and Key Management Protocol Version 2
PMP	Point-to-multipoint
PTBS	Potential TBS
QoS	Quality of Service
RAN	Radio Access Network
RNG-REQ	Ranging Request
RNG-RSP	Ranging Response
RR	Radio Resource
RRM	Radio-resource Management

© COPYRIGHT UPM

RSS	Received Signal Strengths
RSSI	Received Signal Strength Indicator
SBC-REQ	SS Basic Capability Request
SBC-RSP	SS Basic Capability Response
SBS	Serving Base Station
SC-FDMA	Single Carrier-Frequency Division Multiple Access
SCR	Spare Capacity Reports
SHO	Soft Handover
SNR	Signal-to-Noise Ratio
SOFDMA	Scalable OFDMA
3SHO	Seamless and Secure Subsequent Handover
TBS	Target Base Station
TCP	Transmission Control Protocol
TDD	Time-Division Duplex
THz	Terahertz
TDM	Time Division Multiplexing
TMDB	Temporary Movement Database
3G	Third Generation
3GPP	Third Generation Partnership Project
UCD	Uplink Channel Descriptor
UGS	Unsolicited Grant Service
UL	Uplink
UMTS	Universal Mobile Telecommunication Services
UMTS	Universal Mobile Telephone Systems
VoIP	Voice-over-IP
WAS	Weighted Average Score
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networking
WiMAX	Worldwide Interoperability for Microwave Access

© COPYRIGHT UPM

CHAPTER 1

INTRODUCTION

1.1 Background

Increasing demand for mobile Internet and wireless multimedia applications has enhanced the development of broadband wireless access technologies.

Fourth generation (4G) mobile communication systems are required to support advanced services over a wide variety of operating environments. A considerably higher peak transmission rate and spectral efficiency than legacy third generation (3G) systems are required in 4G systems.

Two existing technologies have been identified as necessary upgrades to implement the proposed 4G wireless systems at an early date [1]. These technologies are Worldwide Interoperability for Microwave Access (WiMAX), a standard of the Institute of Electrical and Electronics Engineers (IEEE), and Long-Term Evolution (LTE), a standard of the Third Generation Partnership Project (3GPP).

In addition, to satisfy all the requirements of International Mobile Telecommunications Advanced (IMT-Advanced) of the International Telecommunication Union's (ITU) recommendation (ITU-R), both WiMAX and LTE have performed necessary upgrades in their standards to become well-recognized 4G systems [2].

WiMAX (IEEE 802.16), the IEEE standard for Wireless Metropolitan Area Networking (WMAN), was amended to become 802.16m, also known as WiMAX 2.0 [2]. Similarly, 3GPP LTE was augmented to LTE-Advanced to become 4G-compliant [2]. Both WiMAX 2.0 and LTE-A were designed with different QoS parameters to enhance delivery of evolving Internet applications.

1.2 Overview of the WiMAX Network

WiMAX is the broadband network technology for WMAN. The WiMAX family of standards was developed by the IEEE 802.16 Working Group [3] and adopted by the IEEE organization, the European Telecommunication Standard Institute (ETSI), and High Performance Radio Metropolitan Area Network (HiperMAN). The salient features of this technology include a carrier frequency less than 11 GHz (currently at 2.5, 3.5, and 5.7 GHz), orthogonal frequency-division multiplexing (OFDM) [4], and the Orthogonal Frequency-Division Multiple Access (OFDMA). In addition, the technology has scalable OFDMA-based transmission techniques [4], very high data rates of approximately 75 Mbps or higher, and an outdoor coverage range (distance)

© COPYRIGHT UPM

of up to 20 km. Since the inception of IEEE 802.16-2001 in 2001 until the establishment of recent Mobile WiMAX versions of IEEE 802.16e and 802.16m, the WiMAX family of standards has traversed through different stages. Table 1.1 provides a good a comparison of the different IEEE 802.16 versions [5] [6].

Mobile WiMAX supports three types of handover techniques. Among these techniques, hard handover (HHO) is the default. Both fast base station switching (FBSS) and macro-diversity handover (MDHO) are optional techniques [5].

At present, security issues in wireless networks have become a growing concern with the spread of wireless communication. In particular, wireless systems face more security threats than wired systems. IEEE 802.16, which is the standard for WMAN, has integrated a preexisting standard referred to as Data Over Cable Service Interface Specifications (DOCSIS), which is intended to be used for cable networks but not for wireless networks. Consequently, IEEE 802.16 security was unsuccessful in protecting the IEEE 802.16 link [7] and exhibited several major changes in its Privacy and Key Management (PKM) protocol with the most recent standard, i.e., IEEE 802.16e-2005 [8].

1.3 WiMAX Network Security Features

The latest IEEE 802.16 systems were designed by considering advanced security features. Support is available for shared user validation, along with flexible key management protocol, strong traffic encryption, control and management plane message shield, and security protocol optimizations for speedy handovers. The other features of these systems are listed as follows [9].

- Key management protocol: PKM protocol version 2 (PKMv2) forms the basis of WiMAX protection. This protocol manages media access control (MAC) security, traffic encryption control, handover key exchange, and authentication and broadcast/multicast security messages.
- Device/user authentication: WiMAX supports device and user authentication using the Extensible Authentication Protocol (EAP) of the Internet Engineering Task Force (IETF). A diversity of identification authentication schemes, such as username/password, digital certificates, and smart cards, are supported.
- Traffic encryption: The Advanced Encryption Standard (AES) that counters Cipher Block Chaining (CBC) MAC (AES–CCM) is the cipher used to protect all user data over the WiMAX MAC interface. The keys used to drive the cipher are generated via EAP authentication.
- Control message protection: Control data are protected using the AES cipher-based message authentication code (CMAC), or the message-digest 5 algorithms (MD5)-based or hash-based message authentication code (HMAC) schemes [5].
- Fast handover support: To support fast handovers, WiMAX allows the MS to use a pre-authentication scheme with a particular target base station (BS) to facilitate accelerated reentry. A three-way handshake scheme is supported by

© COPYRIGHT UPM

WiMAX to optimize the reauthentication mechanisms for supporting fast handovers.

Table 1.1 Features of Different Versions of IEEE 802.16

Standards	802.16-2001	802.16a	802.16-2004, 16d	802.16e	802.16m
Frequency	10 ~ 66 GHz, LOS	10 to 66 GHz, LOS and 2 to 11 GHZ, NLOS	10 to 66 GHz, LOS and 2 to 11 GHZ, NLOS (mainly in 3.5 and 5.8 GHz)	2 to 11 GHz (mainly in 2.3 and 2.5 GHz), NLOS	2 to 11 GHz, NLOS
Physical Layer	SC	SCa, OFDM, OFDMA	SC, SCa, OFDM, OFDMA	SCa, OFDM, OFDMA	SCa, OFDM, OFDMA
Duplex	TDD, FDD	TDD, FDD	TDD, FDD	TDD, FDD	TDD, FDD
Mobility Features	none	none	none	Mobile (Vehicular up to 120 Km/hr)	Mobile (walking speed up to 10 Km/hr; Vehicular speed up to – 120 Km/hr; High Speed up to 350 Km/hr)
Standardization Date	April 2002	April 2003	October 2004	February 2006	2011
Maximum Data Rate	-	-	Up to 75 Mb/s	63 Mb/s	100 Mb/s for mobile stations and 1 GB/s for fixed stations
Coverage	-	-	~ 50 Km	Up to 10 Km (optimal: 2 to 4 Km)	1 to 30 Km (optimal: 5 Km)
Handover Latency	-	-	-	~ 50 ms	< 30 ms

© COPYRIGHT UPM

1.4 Motivation and Problem Statement

The impressive development of wireless mobile communication and networking was evident during the first decade of this millennium. Wireless mobile networking and cellular networking have exerted the most profound influence on the exceptional growth of wireless mobile networks.

- **Lengthy handover:** One of the biggest issues that confronts any wireless mobile network, including mobile WiMAX, is handover. Thus, the need for seamless handover is essential to exhibit reliable network performance.

Extensive research indicates that most delays associated with the handover process originate from the following categories:

1- Delay associated with the link layer.
2- Delay associated with the IP layer.
3- Delay associated with the security sublayer.

- **Security vulnerability:** During the handover process, the network will be exposed to numerous attacks. Thus, finding a balance between seamless handover and a secure communication line is vital to overall network performance.

1.5 Research Aim and Objectives

The objectives of this research involve several aspects of handover in mobile WiMAX. The various desirable performance criteria of a handover algorithm are as follows.

1. Handover must be seamless and highly reliable such that no call is dropped in the ongoing connection. Unreliable handover may cause further unnecessary handovers that may impede the performance of the network.
2. A secure communication line among TBS, SBS, and MS, as well as forward and backward secrecy in the network are essential.

Providing seamless and secure handovers in different wireless and cellular networks, such as Wi-Fi, WiMAX, UMTS, and LTE, has become a challenge. Individually, these technologies have different kinds of personalized requirements to enable handover activities to occur successfully. Among these networks, the focus of this thesis is to devise newly improved handover techniques for WiMAX networks.

1.6 Study Scope

Mobility is an important feature of a wireless cellular communication system. In general, continuous service is achieved by supporting handover from one cell to another. The IEEE standard 802.16e-2005 enhances IEEE standard 802.16-2004 to support mobile stations that are moving at vehicular speeds. One of the most

© COPYRIGHT UPM

challenging research issues in investigating broadband wireless access technologies, such as WiMAX, is providing smooth and seamless support for mobility.

Continuous services of multimedia streaming data are essential when a mobile station undergoes handover. Although the IEEE 802.16e standard proposes to address this problem, the disruption time of handover remains too long to overcome the maximum delay of some types of soft real-time services, such as media streaming.

This study focuses on micromobility handover or intra-ASN handover environment. In micromobility handover and intra-ASN handover environments, a mobile terminal moves between two BSs that belong to the same ASN, while preserving the same foreign agent at the ASN. A railway train or an express highway network is considered an excellent example of this research environment.

In this study, a network simulator 2 (NS2) was used to measure and evaluate the performance of our design based on the following parameters.

- Handover delay/latency: Handover latency is defined as the time interval from the last packet received from the serving BS to the new packet received from the target BS.
- Packet loss: Packet loss is counted from the MS disconnecting from the serving BS to receiving new packets from the target BS.

This study aims to reduce handover delay and packet loss to realize a seamless connection. Parallel to the seamless handover, the Automated Validation of Internet Security Protocols and Applications (AVISPA) is used to verify and analyze the security performance of our seamless and secure subsequent handover (3SHO) design.

1.7 Thesis Organization

This thesis is organized into five chapters. Chapter 1 includes the background and motivation of the research, the problem statement, the challenges at hand, the research aim and objectives, and the study scope.

Chapter 2 presents a background of the subject related to the methodology proposed in this thesis and discusses other literature related to this work, particularly those on the intra-ASN handover and authentication protocol in mobile WiMAX. Chapter 3 presents the methodology, protocol analysis, and validation of our 3SHO approach. Chapter 4 explains the results and the analysis obtained from our simulation and security validation tool. Chapter 5 presents the conclusion of this study and offers suggestions for future work.

© COPYRIGHT UPM

REFERENCES

[1] Third Generation Partnership Project (3GPP); URL: http://www.3gpp.org/ [As of date: 13.05.2015].

[2] A-E. M. Taha, H. S. Hassanein and N. A. Ali, "LTE, LTE-Advanced and WiMAX: Towards IMT-Advanced Networks", John Wiley and Sons, 2012.

[3] The IEEE 802.16 Working Group on Broadband Wireless Access Standards; URL: http://wirelessman.org/ [As of date: 13.04.2015].

[4] B. G. Lee and S. Choi, "Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi", Artech House, 2008.

[5] J. G. Andrews, A. Ghosh and R. Muhamed, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", Prentice Hall, 2007.

[6] W. Kim, "Mobile WiMaX, the Leader of the Mobile Internet Era", IEEE Communications Magazine, Vol. 47, Issue 6, June 2009, pp. 10-12.

[7] Johnston, D. and Walker, J., 2004. Overview of IEEE 802.16 security, IEEE Security & Privacy Magazine, vol. 2, 2004, Issue: 3, 40 – 48.

[8] IIEEE Std 802.16e-2005, 2006. Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE, New York, USA, 2006.

[9] WiMAX Forum, "Mobile WiMAX: Part 1 – A Technical Overview and Performance Evaluation", White paper, August 2006; URL: http://www.wimaxforum.org/news/downloads/Mobile WiMAX Part1 Overview and Performance.pdf ,As of date: 12.01.2015.

[10] A. S. Tanenbaum, "Computer Networks", Pearson Education Inc., 2003.

[11] IEEE Std 802.16-2004, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, revision of IEEE Std 802.16-2001, October 2004.

[12] IEEE 802.16 Task Group m (TGm); URL: http://www.ieee802.org/16/tgm/ ,As of date: 12.11.2015.

[13] V. Genc etc al, "IEEE 802.16j Relay-Based Wireless Access Networks: An Overview", in IEEE Wireless Communications Magazine, Vol. 15, Issue 5,Oct 2008, pp. 56-63.

[14] T. Jiang, L. Song and Y. Zhang, "Resource allocation in IEEE 802.16 Mobile WiMAX", in Orthogonal Frequency Division Multiple Access (OFDMA), Auerbach Publications, CRC Press, 2010.

© COPYRIGHT UPM

[15] L. Nuaymi, “WiMAX: Technology for Broadband Wireless Access”, Wiley, 2007.[16]S. Das et al., “System Aspects and Handover Management for IEEE 802.16e”, Bell Labs Technical Journal, Vol. 11, No. 1, 2006, pp. 123-142.

[17] Y. Zhang and H. H. Chen, “Mobile WiMAX: Towards Broadband Wireless Metropolitan Area Networks”, Auerbach Publications, 2008.

[18] WiMAX Forum, “Mobile WiMAX-Part II: A Comparative Analysis”, White Paper,May 2006; URL: http://www.wimaxforum.org/news/downloads/ Mobile WiMAX Part2 Comparative Analysis.pdf, as of date: 12.01.2015.

[19] A. S. Tanenbaum, “Computer Networks”, Pearson Education Inc., 2003.

[20] WMF-T33-001-R010v05 - WiMAX Forum® Network Architecture - Stage 3: Detailed Protocols and Procedures - Release 1.0; Document Number: WMF-T33-001- R010v05.

[21] W. Jiao, P. Jiang and Y. Ma, “Fast Handover Scheme for Real-Time Applications in Mobile WiMAX”, in Proc. of IEEE International Conference on Communications (ICC), Glasgow, Scotland, 24-28 June 2007, pp. 6038-6042.

[22] Sayan K. Ray, K. Pawlikowski and H. Sirisena, "Handover in Mobile WiMAX Networks: The State of Art and Research Issues", in IEEE Communications Surveys and Tutorials Magazine, No. 3, August 2010, pp. 376-399.

[23] L. Harte, “Introduction to Mobile Telephone Systems”, Althos Publishing, 2006.

[24] H. Kaaranen, “UMTS Networks: Architecture, Mobility and Services”, John Wiley and Sons, 2005.

[25] E. Dahlman, “3G Evolution: HSPA and LTE for Mobile Broadband”, AcademicPress, 2008.

[26] K. Etemad and M. Riegel, “Topics and Updates on 4G Technologies”, IEEE Communications Magazine, Vol. 48, Issue. 8, 2010, pp. 38-39.

[27] Third Generation Partnership Project (3GPP); URL: http://www.3gpp.org/ ,As of date: 13.05.2012.

[28] A-E. M. Taha, H. S. Hassanein and N. A. Ali, “LTE, LTE-Advanced and WiMAX: Towards IMT-Advanced Networks”, John Wiley and Sons, 2012.

[29] The IEEE 802.16 Working Group on Broadband Wireless Access Standards; URL: http://wirelessman.org/ ,As of date: 11.04.2015.

© COPYRIGHT UPM

[30] D.H. Lee, K. Kyamakya, and J. P. Umindi, "Fast Handover Algorithm for IEEE 802.16e Broadband Wireless Access System," Proceedings of IEEE WPCC 2006, Jan. 2006, pp.1-6.

[31] L. S. Lee and K. Wang, "A Network Assisted Fast Handover Scheme for IEEE 802.16e Networks," Proceedings of IEEE PIMRC 2007, Athens, Greece, Sept. 2007, pp.1-5.

[32] Y. H. Han et al., "A Crossing-Layering Design for IPv6 Fast Handover Support in an IEEE 802.16e Wireless MAN," IEEE Network, vol. 21, no. 6, Nov.-Dec. 2007, pp. 54-62.

[33] H. J. Jang, J. H. Jee, Y. H. Han, S. D. Park, and J. S. Cha, "Mobile IPv6 Fast Handoffs over IEEE 802.16e Networks," IETF draft, draft-ietf-mipshop-fh80216e-05.txt, Nov. 16, 2007.

[34] L. Chen et al., "A Cross-Layer Fast Handover Scheme for Mobile WiMAX," Proceedings of IEEE VTC 2007, Baltimore, MD, USA, Sept.-Oct. 2007, pp.1578-1582.

[35 Y. W. Chen and F. Y. Hsieh, "A Cross Layer Design for Handoff in 802.16e Network with IPv6 Mobility," Proceedings of IEEE WCNC 2007, Kowloon, Mar. 2007, pp.3844-3849.

[36] C. K. Chang and C. T. Huang, "Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks," Proceedings of ICPPW 2007, Xian, China, Sept. 2007, pp.46-46.

[37] Elgembari, E.S., Seman, K.B., A study on the effect of different velocities on the handover delay in WiMAX systems, (2013) International Review on Computers and Software (IRECOS), 8 (1), 2013, pp. 115-119.

[38] Wenhua Jiao, Pin Jiang, Yuanyuan Ma, "Fast Handover Scheme for Real-Time Applications in Mobile WiMAX" ICC '07. IEEE International Conference on Communications, June 2007.

[39] H-M.Sun, S-Y.Chang, Y-H.Lin and S-Y.Chiou, Efficient Authentication Schemes for Handover in Mobile WiMAX," Proc. of 8th Int'l Conf. on Syst. Design and Applications, 2008.

[40] Junbeom Hur, Hyeongseop Shim, Pyung Kim, Hyunsoo Yoon, Nah-Oak Song, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE, Las Vegas, USA, March 31 2008-April 3 2008, pp. 2531 – 2536.

[41] Hua Cai, et al., "Measurement-Based Low-Level Performance Analysis of IEEE 802.16e/WiBro Networks," Proc. International Conference on Information Networking, Busan, Korea, Jan. 27- 29, 2010.

© COPYRIGHT UPM

[42] C. K. Chang and C. T. Huang, "Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks,"Proceedings of ICPPW 2007,Xian, China, Sept. 2007, pp.46-46.

[43] Kihun Hong, Souhwan Jung, Ki Jun Lee, Brian Lee, Jungwook Wang, "Secure Roaming of Key Association for Fast handover," IEEE C802.16e-04/407, 2004.

[44] Hung-Min Sun; Shih-Ying Chang; Yue-Hsun Lin; Shin-Yan Chiou, "Efficient Authentication Schemes for Handover in Mobile WiMAX," Intelligent Systems Design and Applications, 2008. ISDA '08. Eighth International Conference, Kaohsiung., 26-28 Nov. 2008, pp.235,240.

[45] T.Shon, B.Koo, J.Park, H.Chang, "Novel approaches to enhance mobile WiMAX security," EURASIP Journal on Wireless Communications and Networking, vol. 2010, pp. 1-11, July 2010.

[46] Alezabi, K.A.; Hashim, F.; Hashim, S.J.; Ali, B.M., "A new tunnelled EAP based authentication method for WiMAX networks," *Communications (MICC), 2013 IEEE Malaysia International Conference on* , vol., no., pp.412,417, 26-28 Nov. 2013 doi: 10.1109/MICC.2013.6805864

[47] B Aboba, L Blunk, J Vollbrecht and J Carlson, “Extensible Authentication Protocol, EAP,” RFC 3748, June 2004.

[48] Chen-Hua Shih and Yaw-Chung Chen, “A FMIPv6 Based Handover Scheme for Real-Time Applications in Mobile WiMAX,” JOURNAL OF NETWORKS, vol. 5, pp. 929- 936, August 2010.

[49] Christoforos Ntantogian, Christos Xenakis, and Ioannis Stavrakakis,"A generic mechanism for efficient authentication in B3G networks", Computers & Security, vol. 29, pp. 460-475, 2010.

[50] A. Rai, V. Kumar, and S. Mishra, “An efficient password authenticated key exchange protocol for wlan and wimax,” in Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp. 881–885, ACM, 2011.

[51] Zmezm, Hamzah, Hashim, S. J., Sali, Aduwati, Alezabi, Kamal Ali. "Seamless and Secure Design for Subsequent Handover in Mobile WiMAX Networks"(2014) International Review on Computers and Software (IRECOS), 9(8),pp 1399 – 1407.

[52] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/.

[53] Seamless and Secure Handover, http://www.nist.gov/itl/antd/emntg/ssm_tools. cfm

[54] S.-Y. Tang, P. Muller, and H. Sharif, WiMAX security and quality of service: an end-to- end perspective. Wiley. com, 2011.

© COPYRIGHT UPM

[55] F. Yang and P. Zhu, "An eap-ttls-spekey method for single eap-based auth mode of ieee 802.16e pkmv2," in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, pp. 1– 4, 2010.

[56] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cu´ellar, P. H. Drielsma, P.-C. H´eam, O. Kouchnarenko, J. Mantovani, et al., "The avispa tool for the automated validation of internet security protocols and applications," in Computer Aided Verification, pp. 281– 285, Springer, 2005.

[57] D. Stanley, J. Walker, and B. Aboba, "Extensible authentication protocol (eap) method requirements for wireless lans," Request for Comments, vol. 4017, 2005.

[58] A. K. Rai, V. Kumar, and S. Mishra, "Strong password based eap- tls authentication protocol for wimax," Anjani K. Rai et al./(IJCSE) International Journal on Computer Science and Engineering, vol. 2, no. 02, pp. 2736–2741, 2010.

[59] S. K. Ray, "On the design of fast handovers in Mobile WiMAX networks", Ph.D Thesis, University of Canterbury, Christchurch, New Zealand, 2012.

[60] B. Meandzija and P. Iyer, "Minimizing IP Connectivity Delay during Network Re- Entry", IEEE 802.16 Broadband Wireless Access Working Group Project, IEEE C802.16e-04/151r1, 25 June 2004. URL: http://wirelessman.org/tge/contrib/ C80216e-04 151.pdf As of date: 13.9.2014.

[61] T. Casey, N. Veselinovic and R. Jantti, "Base Station Controlled Load Balancing with Handovers in Mobile WiMAX", in Proc. of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Cannes, France, 15- 18 September 2008, pp. 1-5.

[62] H. Kang, C. Koo and J. Son, "Resource Retain Time for Handover or Ping Pong Call Recovery", IEEE 802.16 Broadband Wireless Access Working Group Project, IEEE C802.16e-04/55r2, 17 May 2004. URL: http://wirelessman.org/tge/contrib/C80216e-0455r2.pdf ,As of date: 11.9.2014.

[63] X. Li, "A Fast Handover Scheme for WiMAX System", in Proc. of 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, China, 23-25 Sept. 2010, pp. 1-4

[64] Zmezm, H. F., Hashim, S. J., Sali, A., & Alezabi, K. A. (2015). Pre-authentication design for seamless and secure handover in Mobile WiMAXNetworks.International Review on Computers and Software (IRECOS), 2015, 10(7), 764-772.

[65] D.H. Lee, K. Kyamakya, and J. P. Umindi, "Fast Handover Algorithm for IEEE 802.16e Broadband Wireless Access System," Proceedings of IEEE WPCC, Jan. 2006, pp.1-6.

© COPYRIGHT UPM

[66] Ray, S.K., et al. Self-Tracking Mobile Station Controls Its Fast Handover in Mobile WiMAX. in Wireless Communications and Networking Conference (WCNC), 2010 IEEE. 2010
.

[67] Shurman, Mohammad M., Mamoun F. Al-Mistarihi, and Shehab A. Nasser. "Hard handover optimization in mobile WiMAX networks." Communications, Computers and Applications (MIC-CCA), Mosharaka International Conference on. IEEE, 2012.

[68] Zhang, Zhenxia, et al. "Reducing handoff latency for WiMAX networks using mobility patterns." Wireless communications and networking conference (WCNC), IEEE. IEEE, 2010.

[69] Poolnisai, Pongtep, and Prawit Chumchu. "Seamless handover for high velocity mobile station in WiMAX." Communications and Information Technologies (ISCIT), 13th International Symposium on. IEEE, 2013.

[70] Pahal, Sudesh, Brahmjit Singh, and Ashok Arora. "Cross layer based fast handover for IEEE 802.16 e networks." Optik-International Journal for Light and Electron Optics 125.15 (2014): 4108-4112.

[71] Ben-Mubarak, Mohammed A., et al. "Movement direction-based handover scanning for mobile WiMAX." Communications (APCC), 2011 17th Asia-Pacific Conference on. IEEE, 2011.

[72] Lu, Qi, and Maode Ma. "Achieving faster handovers in mobile WiMAX networks." Wireless Personal Communications 65.1 (2012): 165-187.

[73] Fu, Anmin, et al. "A fast handover authentication mechanism based on ticket for IEEE 802.16 m." Communications Letters, IEEE 14.12 (2010): 1134-1136.

[74] Shih, Chen-Hua, Wei-Yun Chang, and Yaw-Chung Chen. "A Pre-authentication Scheme on WiMAX for QoS Improvement of Mobile Services." High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on. IEEE, 2011.

[75] Nguyen, Thuy Ngoc, and Maode Ma. "An pre-authentication protocol with symmetric keys for secure handover in mobile WiMAX networks."Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012.

[76] Sridevi, B., T. S. Supriya, and S. Rajaram. "Fast and secure handover of intra-ASN IEEE802. 16 network by proposed certificate based pre-authentication." International Conference on Communication and Electronics System Design. International Society for Optics and Photonics, 2013.

[77] Leu, Fang-Yie, Yi-Fu Ciou, and Yi-Li Huang. A handover security mechanism employing diffie-Hellman PKDS for IEEE802. 16e wireless networks. Springer Berlin Heidelberg, 2011.

[78] Chuang, Ming-Chin, and Jeng-Farn Lee. "A lightweight mutual authentication mechanism for network mobility in IEEE 802.16 e wireless networks."Computer Networks 55.16 (2011): 3796-3809.

[79] Banerjee, Subharthi, and Hamid Sharif. "A Survey of Wireless Communication Technologies & Their Performance for High Speed Railways." Journal of Transportation Technologies 6.01 (2016): 15.

[80] Zhou, Yuzhe, and Bo Ai. "Handover schemes and algorithms of high-speed mobile environment: A survey." Computer Communications 47 (2014): 1-15.

[81] Ahmed, Ejaz, Bob Askwith, and Madjid Merabti. "Pre-authentication and selection of suitable target Base Station during Handover procedure in Mobile WiMAX Network." Whitepapers Mob. Wirel. Tech Republ (2011).

[82] Stevan Hilarius; maximum distance of a fiber optic link by Rsearchgate,june 2013,https://www.researchgate.net/post/What_is_the_maximum _distance_of a_fiber_optic_link_that_can_be_achieved_without_using_any_optical_ampli fier_or_repeater (accessed 10 April. 2016).

© COPYRIGHT UPM