UNIVERSITI PUTRA MALAYSIA

SECURITY AND PERFORMANCE ENHANCEMENT OF AUTHENTICATION PROTOCOLS IN HETEROGENEOUS WIRELESS NETWORKS

KAMAL ALI AHMED ALEZABI

SECURITY AND PERFORMANCE ENHANCEMENT OF AUTHENTICATION PROTOCOLS IN HETEROGENEOUS WIRELESS NETWORKS

By

KAMAL ALI AHMED ALEZABI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

September 2017

COPYRIGHT

DEDICATIONS

In the name of Allah, Most Gracious, Most Merciful

This thesis is dedicated to:

To the spirit of my beloved father. It was your wish, thus I insisted to make it come true.
To my beloved mother, who endured my absent. Her prayers for me have not stopped.
To my dear wife, who faithfully supported me and endured a lot for me.
To all of my family members for their unconditional love and support.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

SECURITY AND PERFORMANCE ENHANCEMENT OF AUTHENTICATION PROTOCOLS IN HETEROGENEOUS WIRELESS NETWORKS

By

KAMAL ALI AHMED ALEZABI

September 2017

Chair : Fazirulhisyam Hashim, PhD
Faculty: Engineering

For mobile users, interworking environment comprised of Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX) and Wireless Local Area Networks (WLAN) has become a practical consideration. As a prevalent technology, LTE and WiMAX have desirable features that support high data rate, mobile capabilities, good quality of service (QoS), and wide coverage area. On the other hand, WLAN provides higher bit rate but weaker mobility support. Additional features such as cost effectiveness in covering signal dead zones of LTE networks and its plentiful bandwidth for better QoS makes the WLAN a good complementary solution for LTE networks. Accordingly, integration between these wireless network technologies allows users to move from one to another wireless network to get better QoS in case of some applications that demand higher data rates or to connect to a network that has a stronger signal. However, interworking solutions between these different technologies increase the possibility of intrusion on such networks, consume their resources, affect the QoS and disclose its exchanged data. Thus, the security in such environment is considered as an urgent need. The authentication process is the basis of the security which should be performed appropriately whether in the homogeneous or heterogeneous networks. It is becoming an increasingly important factor during the handover (HO) process in the heterogeneous architecture, where authentication delay and signalling cost may contribute significantly to the handover delay and cost. On the other hand, the 3GPP standards have specified that, in interworking architectures between LTE and other wireless networks, each user should be authenticated by the home server in LTE network, which makes this server a subject of single point of failure. Therefore, designing authentication and re-authentication protocols that address the mentioned limitations and contribute to fast, seamless and secure roaming or HO at the same time is an open area that needs to be studied and improved. Several studies have modified the existing authentication protocols, but they are limited to 3G-WLAN interworking architecture. Besides, most of the existing authentication schemes are complex and vulnerable to network attacks such as User Identity Disclosure (UID) and Man In The Middle (MITM) attacks.

This thesis presents authentication protocols for homogeneous and heterogeneous wireless networks. In particular, a new method called Extensible Authentication Protocol-Tunnelled Transport Layer Security -Improved Secure Remote Password (EAP-TTLS-ISRP) is proposed for WiMAX networks. This method embeds the transmission of security messages in a secure tunnel. The proposed method outperforms other methods in terms of number of messages exchanged, where it is reduced by 16% compared to other WiMAX protocols, which leads to reducing the communication overhead. It also satisfies the EAP requirement for secure and efficient data exchange, as well as robust to MITM attack. In LTE networks, an Efficient Evolved Packet System (EEPS-AKA) protocol is proposed to overcome security and performance problems such as UID and MITM attacks; storage overhead and authentication delay. The proposed protocol is based on the Simple Password Exponential Key Exchange (SPEKE) protocol. Compared to the previous methods, our method is faster, since it uses a secret key method which is faster than certificate-based methods. In addition, the size of messages exchanged between the User Equipment (UE) and Home Subscriber Server (HSS) is reduced by 19%, this effectively reduces authentication delay and storage overhead. In LTE-WLAN interworking architecture, EAP with improved Authentication and Key Agreement (EAPAKA′) protocol is introduced to present new inter and intra re-authentication protocols. These protocols provide an efficient method to improve security against network attacks, protect the user identity and reduce the burden on HSS during the sequential handovers. Compared to the standard authentication protocols, the reduction of the authentication delay, signaling cost, handover delay, handover cost, and energy consumption reaches up to 23%, 30%, 34%, 21%, and 13%, respectively. In LTE-WiMAX-WLAN interworking architecture, authentication and re-authentication protocols are proposed, where they can be invoked if users perform vertical HO (between those networks) or horizontal HO (within the same network). These protocols provide an efficient method to protect user identity and reduce the burden on HSS. The results of analytical model show that the proposed protocols achieve better performance than standard and other protocols in terms of delay, cost, and energy consumption. Compared to the standard and other authentication protocols, the reduction of authentication delay, signaling cost, handover delay, handover cost, and energy consumption reaches up to 14%, 42%, 30%, 18%, and 17%, respectively. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used to provide a formal verification. Results show that the proposed protocols are efficient and secure against active and passive attacks.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENINGKATAN SEKURITI DAN PRESTASI UNTUK PROTOKOL PENGESAHAN DALAM RANGKAIAN WAYARLES HETEROGEN

Oleh

KAMAL ALI AHMED ALEZABI

September 2017

Pengerusi: Fazirulhisyam Hashim, PhD
Fakulti : Kejuruteraan

Untuk pengguna telefon mudah alih, persekitaran jalinan kerja yang terdiri daripada Evolusi Jangka Panjang (Long Term Evolution, LTE), Pengendalian Sedunia bagi Akses Gelombang Mikro (Worldwide Interoperability for Microwave Access, WiMAX) dan Rangkaian Kawasan Setempat Wayarles (Wireless Local Area Networks, WLAN) telah menjadi satu pertimbangan yang praktikal. Sebagai teknologi yang diguna secare meluas, LTE dan WiMAX mempunyai ciri-ciri yang baik seperti menyediakan kadar data tinggi, keupayaan mudah alih, kualiti perkhidmatan yang baik (quality of service, QoS) dan kawasan liputan yang luas. Berbanding dengan LTE dan WiMAX, WLAN pula menyediakan kadar bit yang lebih tinggi tetapi sokongan mobiliti lebih lemah. Ciri-ciri tambahan seperti keberkesanan kos dalam meliputi zon mati isyarat rangkaian LTE dan kelebaran jalurnya untuk QoS yang lebih baik juga menjadikan WLAN sebagai pelengkap bagi rangkaian LTE. Oleh itu, integrasi teknologi-teknologi rangkaian wayarles ini membolehkan pengguna bertukar-tukar di antara rangkaian wayarles bagi mendapatkan QoS yang lebih baik apabila menggunakan aplikasi yang memerlukan kadar data lebih tinggi atau sambungan ke rangkaian yang mempunyai isyarat yang lebih kuat. Namun begitu, pertukaran di antara rangkaian teknologi ini meningkatkan kebarangkalian sesuatu rangkaian itu diceroboh, menghabiskan sumbernya, mempengaruhi QoS dan mendedahkan data yang dihantar melaluinya. Oleh itu, sekuriti bagi persekitaran sebegini adalah sesuatu yang sangat diperlukan. Proses pengesahan adalah asas sekuriti, yang mana harus dibuat dengan betul sama ada dalam rangkaian homogen atau rangkaian heterogen. Faktor ini menjadi semakin penting dalam proses serahan (handover, HO) dalam seni bina heterogen, di mana kelewatan pengesahan dan overhed masing-masing boleh banyak menyumbang kepada kelewatan HO dan overhed komunikasi. Oleh yang demikian, perekaan protokol pengesahan dan pengesahan semula yang menyumbang kepada perayauan (roaming) atau HO yang lancar, selamat dan laju, merupakan bidang yang perlu dikaji dan diperbaiki. Beberapa kajian telah mengubah suai protokol pengesahan sedia ada tetapi hanya terhad kepada seni bina jalinan kerja 3G-WLAN. Lagipun, kebanyakan skema pengesahan sedia ada bersifat kompleks dan mudah terdedah kepada serangan rangkaian

seperti Pendedahan Identiti Pengguna (User Identity Disclosure, UID) dan serangan Orang Tengah (Man In The Middle, MITM). Tesis ini memperkenalkan protokol pengesahan untuk rangkaian wayarles heterogen. Secara khususnya, satu kaedah baru yang digelar Protokol Pengesahan Boleh Diperluas-Sekuriti Lapisan Pengangkutan Berterowong-Kata Laluan Jauh Selamat Diperbaiki (Extensible Authentication Protocol-Tunnelled Transport Layer Security-Improved Secure Remote Password, EAP-TTLS-ISRP) dicadangkan untuk rangkaian WiMAX. Kaedah ini membenamkan penghantaran mesej sekuriti dalam terowong yang selamat. Kaedah yang dicadangkan ini lebih bagus daripada kaedah lain, dari segi bilangan mesej yang dihantar sebanyak 16% berbanding dengan WiMAX protokol yang lain, dan seterusnya menyebabkan kos overhed yang kurang. Ia juga memenuhi keperluan EAP untuk pertukaran data yang selamat dan efisien, di samping teguh terhadap serangan MITM. Manakala dalam rangkaian LTE, sebuah protokol Sistem Paket Evolusi Efisien (Efficient Evolved Packet System, EEPS-AKA) dicadangkan bagi menangani masalah keselamatan dan prestasi seperti UID dan serangan MITM; simpanan overhed, dan kelewatan pengesahan. Protokol yang dicadangkan adalah berasaskan protokol Pertukaran Kunci Eksponen Kata Laluan Mudah (Simple Password Exponential Key Exchange, SPEKE). Jika dibandingkan dengan kaedah-kaedah yang lalu, kaedah kami lebih laju kerana ia menggunakan kaedah kunci rahsia yang lebih laju daripada kaedah berasaskan sijil. Tambahan pula, saiz mesej yang dihantar antara Peralatan Pengguna (User Equipment, UE) dan Pelayan Pelanggan Rumah (Home Subscriber Server, HSS) dapat dikurangkan dan ini mengurangkan kelewatan pengesahan dan simpanan overhed dengan efektif. Bagi seni bina jalinan kerja LTE-WLAN, protokol EAP yang dilengkapi Persetujuan Pengesahan dan Kunci yang dipertingkat (Authentication and Key Agreement, EAP-AKA′) diperkenalkan bagi menghasilkan protokol antara pengesahan semula dan protokol intrapengesahan semula yang baru. Protokol ini menyediakan kaedah efisien bagi meningkatkan sekuriti terhadap serangan rangkaian, melindungi identiti pengguna dan mengurangkan beban pada HSS semasa serahan berjujukan. Jika dibandingkan dengan protokol pengesahan standard, pengurangan kelewatan pengesahan, kos isyarat, kelewatan penyerahan, biaya penyerahan dan penggunaan tenaga mencapai sehingga 23%, 30%, 34%, 21%, dan 13%, masing-masing. Bagi seni bina jalinan kerja LTE-WiMAX-WLAN pula, protokol pengesahan dan protokol pengesahan semula dicadangkan, di mana ia boleh diaplikasi apabila pengguna melakukan HO vertikal (antara rangkaian berbeza) atau HO mendatar (dalam rangkaian sama). Protokol tersebut menyediakan kaedah efisien bagi melindungi identiti pengguna dan mengurangkan beban pada HSS. Keputusan model analisis menunjukkan bahawa semua protokol yang dicadangkan mencapai prestasi yang lebih baik berbanding protokol standard dan protokol lain dari segi kelewatan, kos dan penggunaan tenaga. Berbanding dengan protokol standard, pengurangan kelewatan pengesahan, kos isyarat, kelewatan penyerahan, biaya penyerahan dan penggunaan tenaga mencapai sehingga 14%, 42%, 30%, 18%, dan 17%. Alat Protokol dan Aplikasi Pengesahan Sekuriti Internet Automatik (Automated Validation of Internet Security Protocols and Applications, AVISPA) digunakan untuk pengesahan rasmi. Keputusan menunjukkan bahawa protokol-protokol yang dicadangkan adalah efisien dan selamat bagi mengatasi serangan aktif dan pasif.

ACKNOWLEDGEMENTS

First of all, I would like to thank the Almighty ALLAH, who helped me and gave me patience, perseverance and pleased me all difficulties. Praise and thanks to you, Ya ALLAH all the time. I thank my parents who taught me that the journey of a

thousand miles begins with one step. They were with me every step of the moral and financial support. I thank my brothers and sisters who have been supportive to me in all phases of the studies. I want to express my heartfelt gratitude and

sincere appreciation to my supervisor Dr. Fazirulhisyam Hashim, who has had great merit in completing this work in this way and always had a great supervisor example with loving, guidance and supportive of all students. I highly appreciate his fruitful guidance, invaluable advice and great effort which made the main impact in the completion of this work. I also express my heartfelt gratitude and thanks to

the Supervisory Committee, Prof. Dr. Borhanuddin Mohd Ali and Assoc. Prof. Dr. Shaiful Jahari Hashim for their continuous Support, encouragement and guidance until the end of this work. All thanks to my professors, lecturers, colleagues,

friends, and staff in the Faculty of Engineering and Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

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

Fazirulhisyam Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairperson)

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

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

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other 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 obtained from supervisor and the office of 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.: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

1G	1st Generation
2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
4G	4th Generation
AAA	Authentication Authorization Accounting
AERP	Intra LTE Re-authentication Protocol
AES	Advanced Encryption Standard
AK	Authorization key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
ANID	Access Network IDentity
ANRP	Intra WLAN Re-authentication Protocol
AP	Access Point
AS	Authentication Server
ASME	Access Security Management Entity
ASN	Access Service Network
ASN-GW	ASN Gateway
AUTN	AUthentication TokeN
AV	Authentication Vector
AVISPA	Automated Validation of Internet Security Protocols and Applications
AXRP	Intra ASN WiMAX Re-authentication Protocol
BAN	Burrows-Abadi-Needham formal method
BCID	Basic Connection ID
BS	Base Station
BSS	Basic Service Set
BWA	Broadband Wireless Access
CA	Certificate Authority
CDMA	Code Division Multiple Access
CL-AtSe	Constraint-Logic based Attack Searcher
CK	Ciphering Key
CSN	Connectivity Service Network
DH	Diffie Hellman
DHCP	Dynamic Host Control Protocol
DOS	Denial Of Service
DSL	Digital Subscriber Line
DSMIPv6	Dual-Stack Mobile IPv6
DSRK	Domain-Specific Root Key
DSSS	Direct-Sequence Spread Spectrum
DSUSRK	Domain-Specific Usage-Specific Root Key
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
ECC	Ellipse Curve Cryptosystem
ECDH	Elliptic Curve Diffie-Hellman
EMSK	Extended Master Session Key

eNB	Evolved Node B
EoIP	Everything over IP
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
eUTRAN	evolved UMTS Terrestrial Radio Access Network
FAKAP	Fast EAP-AKA′ re-authentication Protocol
FAST	Flexible Authentication via Secure Tunneling
FF	Fluid Flow
FHSS	Frequency Hopping Spread Spectrum
GTC	Generic Token Card
HetNets	Heterogeneous Networks
HLPSL	High-Level Protocol Specification Language
HLPSLIF	HLPSL Intermediate Format
HO	Handover
HSPDA	High Speed Downlink Packet Access
HSS	Home Subscriber System
HSUPA	High Speed Uplink Packet Access
IBSS	Independent Basic Service Set
IETF	Internet Engineering Task Force
IF	Intermediate Format
IK	Integrity Key
IKEv2	Internet Key Exchange
IMPI	IP Multimedia Private-user Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
INEA	Initial Network Entry Authentication
Inter FRP	Inter Fast Re-authentication Protocol
Intra FRP	Intra Fast Re-authentication Protocol
IP	Internet Protocol
ITU	International Telecommunication Union
K_{auth}	Authentication Key
K_{enc}	Encryption Key
KDF	Key Derivation Function
K_{ASME}	Key Set Identifier
LAN	Local Area Networks
LEAP	Light Extensible Authentication Protocol
LNAS	Lying Network Access Server
LTE-A	LTE-Advanced
LTE	Long Term Evolution
MAC	Message Authentication Code
MAKAP	Modified EAP-AKA′ Protocol
MAN	Metropolitan Area Networks
MCC	Mobile Country Code
MEPSP	Modified EPS Authentication Protocol
MIMO	Multiple-Input Multiple-Output
MITM	Man-In-The-Middle
MINEAP	Modified INEA Protocol
MK	Master Key

MME	Mobility Management Entity
MNC	Mobile Network Code
MS	Mobile Station
MSK	Master Session Key
MSIN	Mobile Subscriber Identification Number
NAI	Network Access Identifier
NAS	Non-Access Stratum layer
NNK	WLAN Network level Key
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OFMC	On-the-fly Model-Checker
OTP	One-Time Password
PAAA	Proxy AAA
PDF	Probability Distribution Function
PDN-GW	Packet Data Network Gateway
PEAP	Protected Extensible Authentication Protocol
PFS	Perfect Forward Secrecy
PIMSI	Protected IMSI
PHY	Physical Layer
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PPP	Point-to-Point Protocol
PRF	Pseudo-Random Function
EAP-PSK	EAP Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RAND	Random Value
RERP	Inter LTE Re-authentication Protocol
RNRP	Inter WLAN Re-authentication Protocol
RXRP	Inter WiMAX Re-authentication Protocol
SA-TEK	Security Association-Traffic Encryption Key method
SAE	System Architecture Evolution
SATMC	SAT-based Model-Checker
SC	Signalling Cost
SIM	Subscriber Identity Module
SK	Shared Key
S-GW	Serving Gateway
SN	Service Network
SPAN	Security Protocol Animator
SPEKE	Simple Password Exponential Key Exchange
SQN	Sequence Number
SS	Subscriber Station
TA4SP	Tree Automata based on Automatic Approximations for the Analysis of Security Protocols
TD-SCDMA	Time-Division Synchronous Code Division Multiple Access
TLS	Transport Layer Security
TPSK	Three Parties Shared Key
TSK	Transient Session Key

TTLS	Tunneled Transport Layer Security
UE	User Equipment
UEID	UE Identity
UID	User Identity Disclosure
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
WAAA	WLAN AAA
WAN	Wide Area Networks
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WISPs	Wireless Internet Service Providers
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPKI	Wireless Public Key Infrastructure
XMAC	expected MAC
XRES	Expected Response value

CHAPTER 1

INTRODUCTION

Unlike the past generations of mobile users, the new and future generations demand a seamless and secure connection to the wireless networks anytime, anywhere and regardless of the access network type or the service providers. Therefore, wireless networks are becoming more important and more widespread. With this deployment and multiplicity of technologies used such as the 4th Generation (4G) technology includes LTE and mobile WiMAX networks; and wireless networks such as WLAN networks, it has become necessary to provide appropriate solutions for communication between these technologies. An open and unsecured radio channel is used in the wireless network systems to send / receive data and signals between the network entities such as Base Stations (BSs) and Mobile Stations (MSs), therefore, the need arises for a reliable and non-penetrable security system to protect data traffic between those entities.

1.1 Overview

1.1.1 Broadband Wireless Networks

The wireless broadband refers to a wireless connection that provides data, voice, and video communication at high speed and capacity. It was not included in the early generations of wireless access technology such as the first generation (1G). The 1G has only provided mobile voice services. It was using the analog technology, which suffered from the absence of security features. In the early 1990s, the second generation (2G) that was represented by GSM systems has provided a digital technology. This has improved the capacity and coverage of mobile voice services. The security features have been added to GSM system by using authentication and cryptography technologies. The wireless broadband technology has been introduced in the third generation (3G), which is represented by the Universal Mobile Telephone System (UMTS). The 3G has provided the data communication at high speed. Whereas, the fourth generation (4G), which is represented by LTE and mobile WiMAX technologies has presented the wireless broadband networks with new radio technology at a higher data rate and capacity. It has also added many security features.

The UMTS has been defined in November 2004 by the Third Generation Partnership Project (3GPP). The 3GPP has many other projects such as High Speed Downlink Packet Access (HSPDA), High Speed Uplink Packet Access (HSUPA), Time-Division Synchronous Code Division Multiple Access (TD-SCDMA), System Architecture Evolution (SAE) and LTE release 8. The enhanced version of LTE is LTE release 10 or LTE-Advanced (LTE-A) where multiple carriers have been aggregated to provide wider bandwidth and improved antenna technologies have been used in both direction uplink and downlink. The widespread use of 4G networks leads to more needs of high bit rate, less delay in such networks.

WiMAX has been considered as one of the key technologies that is capable of addressing the increasing demand for high-speed data communication [1]. The main aim of

WiMAX (The standard IEEE 802.16) is to enable the delivery of last-mile wireless-broadband access and high-bandwidth connectivity to its users. This technology is considered as a practical alternative solution to conventional wired-broadband technologies, such as cable, digital subscriber line (DSL), and fiber optics. WiMAX provides many advantages, including fast and easy deployment, thus resulting in cost savings. This technology can be a beneficial choice in crowded, urban, or rural areas, where wired infrastructures are difficult to establish. Two main standards have been released to define functionalities of WiMAX in supporting wireless-broadband access. The IEEE 802.16-2004 standard addresses fixed and nomadic users [2], whereas the IEEE 802.16e-2005 standard provides the foundation of WiMAX mobility.

WLAN is considered complementary to broadband wireless networks because of its cost-effectiveness on covering signal dead areas of broadband wireless networks and its plentiful bandwidth for better quality of service.

1.1.2 Security in Wireless Networks

Interworking of different wireless network technologies allows users to choose an appropriate wireless network to attain a better QoS in case of some applications that demand higher data rates. Sometimes the roaming could be performed in order to connect to a network with stronger signals. However, interworking solutions between those different technologies increase the possibility of intrusion of such networks, consume its resources, affect the QoS and disclose its data exchanged, thus, security in such environment is considered as an urgent need.

The authentication is a very important process in both, homogeneous and heterogeneous wireless networks, since most of attackers target this process and then they try to be authenticated and treated as authorized users. After that, they utilize the network resources and prevent the legitimate users from utilizing the network services. Unfortunately, the authentication process becomes more burdensome in case of heterogeneous wireless networks, where the users should be authenticated and re-authenticated during different types of handover. The authentication process is playing a key role in the handover process, where authentication delay and overhead may contribute significantly to the handover delay and communication overhead respectively. Thus, designing authentication and re-authentication protocols that prevent attacks and contribute in fast, seamless and secure handover at the same time is a major challenge that faces the designers of authentication protocols.

In LTE networks, access security mechanism is used for authentication and key agreement between UE and the Evolved Nodes Base station (eNB). It also uses handover key management to refresh the session keys securely when UE moves from one to another eNB to mitigate the attacks caused by a malicious BS. These procedures are called AKA which was introduced in 3G networks and it is considered as an LTE security mechanism. AKA provides a mutual authentication between UE and eNB and it also provides key agreement. EPS-AKA protocol is the last version of UMTS-AKA, where the added improvements have raised the degree of security, but made the protocol more complex.

In the WiMAX networks, the Privacy Key Management protocol version 2 (PKMv2) is utilized to secure communication among its users, and PKMv2 utilizes the EAP protocol and methods as the framework. It is worth to highlight that IEEE 802.16 does not specifically dictate any EAP methods in its standard. In light of this, there is a wide-range of EAP authentication methods that have been developed by researchers and industry. In general, the EAP methods can be classified into three main categories [3]; the first type is password-based such as Message Digest 5 (EAP-MD5), Secure Remote Password protocol (EAP-SRP), Light Extensible Authentication Protocol (EAP-LEAP), Simple Password-Authenticated Exponential Key Exchange (EAP-SPEKE), and Flexible Authentication via Secure Tunnelling (EAP-FAST); the second type is certificate-based such as Transport Layer Security (EAP-TLS), Protected Extensible Authentication Protocol (EAP-PEAP), and Tunnelled Transport Layer Security (EAP-TTLS); and the third type is SIM card-based such as Subscriber Identity Module (EAP-SIM) and Authentication and Key Agreement (EAP-AKA). The password-based is simple and secure, but not as robust as the certificate-based. Meanwhile the SIM card-based is commonly used in cellular communications (i.e., installed in mobile phones). In IEEE 802.16e, the Initial Network Entry Authentication protocol (INEA) is a part of PKMv2that is performed by MS when connecting to WiMAX network.

In WLAN networks, the security was not specified completely in the earlier versions, where the Wired Equivalent Privacy (WEP) protocol was used to provide security. It was improved in the IEEE 802.11i amendment. In the standard IEEE 802.11i, the WiFi Protected Access (WPA) protocol has been specified, where the Advanced Encryption Standard (AES) block cipher is used. Improvements in key management, encryption and authentication are also included in this standard. As a part of WPA protocol, the Remote Authentication Dial in User Service (RADIUS) protocol is specified by the Internet Engineering Task Force (IETF) to provide security and authentication mechanism in the IP networks [4]. RADIUS protocol supports EAP authentication protocol, which works with different authentication methods such as TLS, TTLS, LEAP, PEAP and AKA.

1.2 Problem Statement

Four network architectures are addressed in this thesis: WiMAX network architecture, LTE network architecture, LTE-WLAN architecture and LTE-WiMAX-WLAN architecture. The problems in each architecture are presented and then the motivations to solve these problems are provided.

In WiMAX networks, the main advantage of using EAP is its capability to support both user and device authentication; it can be achieved by using either single or combined EAP methods. Nevertheless, using double EAP or combined methods may incur additional overheads, and due to this reason it is not completely specified in IEEE 802.16 standard. Therefore, it is considered not suitable to be implemented in most of the approaches defined by the IETF. Moreover, there is no state machine defined for combined methods in the IETF. In light of this, using a single EAP based method would be more appropriate.

For single EAP based authentication, there should be a suitable method for providing user and device authentication, while at the same time it should satisfy the security requirements. The most suitable solution for performing user/device authentication in the single EAP based is to use the tunnel based methods [3]. In such methods, a tunnel protocol such as TLS is executed between the MS and BS or Authentication Server (AS) to complete the device authentication followed by one or more authentication methods within the established tunnel. Although, the tunnel method with one of the authentication protocols provide an efficient solution, it may increase the communication overhead during user/device authentication. In this thesis, an effective and secure authentication method is proposed to provide user/device authentication in WiMAX networks. This method uses one of the tunnel methods to perform device authentication, and to protect the method (the control messages) that performs the user authentication, while at the same time satisfies the authentication requirements. This method is based on EAP-TTLS [5] as a tunnel method to complete the device authentication, and EAP-SRP to be executed within the TTLS tunnel to perform the user authentication [6], [7].

In LTE networks, the basics of Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA) are used in the LTE AKA protocol, which is called Evolved Packet System AKA (EPS-AKA) protocol to secure LTE network, however it still suffers from various vulnerabilities such as UID and MITM attacks; and significant storage overhead [8], [9]. To address these vulnerabilities, a new authentication protocol, called EEPS-AKA, is designed based on the SPEKE protocol.

In LTE-WLAN architecture, several studies have modified the existing authentication protocols, but they are limited to 3G-WLAN interworking architecture [10], [11]. Besides, most of the existing authentication schemes still inherit delay and cost during authentication and handover processes [12]. In addition, they still vulnerable to network attacks (e.g., UID attack) [13], [14]. For these reasons, the EAP is introduced with improved AKA (AKA′) protocol to present the new inter and intra re-authentication protocols specified for the LTE-WLAN interworking architecture.

In LTE-WLAN-WiMAX architecture, effective full EAP-AKA′, INEA and EPS-AKA authentication protocols or fast authentication protocols are performed during the handover process between these networks regardless of the type of handover (i.e., inter and intra). The inter handover is performed when UE moves across different network domains, whereas, the intra handover is performed when UE moves across different APs/BSs/eNBs within the same network domain. Thus, performing full authentication or fast re-authentication in each time the user connects to the wireless domain will increase the delay and cost of handover and authentication processes. In addition, authentication protocols that are used in this architecture still suffer from networks attacks such as user identity attack and other problems such as access networks key leakage. To address these limitations, the standard authentication protocols are modified and new inter/intra re-authentication protocols are proposed to provide secure and fast authentication during different handovers between these access networks.

In general, such heterogeneous networks that serve a huge number of users consume higher amounts of energy compared to homogeneous networks. On the other hand, depending on the home server to authenticate a huge number of wireless users makes it vulnerable to be a single point of failure.

1.3 Research Objectives

The aim of this thesis is to develop authentication and re-authentication protocols in homogeneous and heterogeneous wireless networks. The research objectives are as follows:

- To enhance the performance and security of authentication process in WiMAX networks by protecting the network against attacks such as MITM and replay attacks; and reducing the number of exchanged messages which reduces the communication overhead. These enhancements are achieved by designing a new tunnelled EAP based authentication method.
- To enhance the performance and security of authentication process in LTE networks by protecting the network against attacks such as MITM and UID attacks; and reducing the size of the exchanged messages that contributes in reducing the storage overhead. These enhancements are achieved by designing a new authentication and key agreement protocol.
- To improve the security and performance during the HO process in WLAN - LTE interworking architecture by protecting the networks against UID attack and reducing the authentication delay, signalling cost, handover delay, handover cost, and energy consumption. These improvements are achieved by improving the standard authentication protocols and designing new inter and intra re-authentication protocols.
- To provide fast and secure HO process in the LTE-WLAN-WiMAX interworking architecture by protecting the networks against UID attack and reducing the authentication delay, signalling cost, handover delay, handover cost, and energy consumption. These improvements are achieved by improving the standard authentication protocols of LTE, WLAN, and WiMAX networks. The improved protocols are used to present new inter and intra re-authentication protocols for each network.

1.4 Study Module

This work is dedicated to study the network access security, in particular the authentication and re-authentication protocols that play a key rule to provide secure and fast communication in both homogeneous and heterogeneous wireless networks. The other security aspects such as application, user and network domain security are out of the scope of this work.

The summary of approaches that have been chosen in this thesis is illustrated in Figure 1.1, where the solid lines along with the colored boxes denote the followed

direction to achieve determined objectives, and the dashed lines show the other research directions of the security aspects and authentication protocols which are not covered in this thesis.

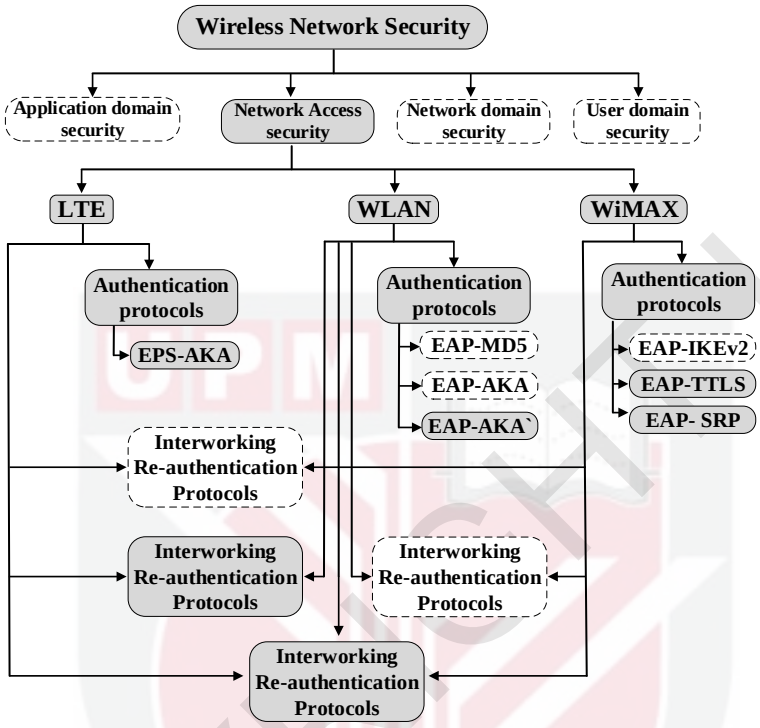

Figure 1.1: System module.

1.5 Main Contributions

The contributions in this thesis target the limitations and vulnerabilities of each wireless network separately and then address the limitation and vulnerabilities in the interworking architectures between these networks. The contributions are listed in the following:

- **Design of an authentication protocol for WiMAX networks**
  An authentication protocol has been proposed to provide mutual authentication, reduce the communication overhead, and protect the network against several types of attacks such as MITM and Replay attacks. For the single EAP based authentication, the proposed protocol provides both user and device authentication based on EAP-TTLS and EAP-SRP, respectively.

- **Design of an authentication protocol for LTE networks**
  The EEPS-AKA has been proposed for LTE network to overcome security and performance problems in EPS-AKA protocol such as UID and MITM attacks; and storage overhead. The proposed protocol is based on the SPEKE protocol.

- **Design of authentication and re-authentication protocols for LTE-WLAN interworking architecture**
  In the LTE-WLAN interworking architecture, the standard EAP-AKA′ is modified to provide mutual authentication between the UE and 3GPP Authentication, Authorization, and Accounting (3GPP AAA) server and the inter and intra handovers are considered by designing inter and intra re-authentication protocols. The proposed protocols with modified EAP-AKA′ protocol are aimed of reducing the delay and cost of both authentication and handover; and energy consumption. At the same time, the proposed protocols ensure the security aspects in authentication process. In addition, a new mechanism to renew the re-authentication identity is proposed.

- **Design of authentication and re-authentication protocols for LTE-WiMAX-WLAN interworking architecture**
  A new method to prevent the user identity attack and reduce cost and overhead on AS is proposed, which contributes significantly in reducing the delay, cost, and energy consumption during different handover types. Three standard protocols, EPS-AKA, INEA, and EAP-AKA′ protocols are modified and used to provide full authentication process between the user and LTE, WiMAX and WLAN networks, respectively, when the user connects to one of those networks for the first time. New re-authentication protocols are proposed to provide fast inter and intra re-authentication process in LTE-WiMAX-WLAN interworking architecture during horizontal and vertical handover. Moreover, a new unified key hierarchy is proposed to be suitable for the module of the networks involved in the designed protocols.

1.6 Organization of the Thesis

Each chapter in this thesis discusses the problems of authentication process in each network architecture and presents the proposed solutions to solve those problems. The remainder of the thesis is organized as follows:

Chapter 2 elaborates the architectures of WLAN, WiMAX, LTE networks, and interworking architecture between these networks. It also presents an overview of authentication and re-authentication protocols that are used in these architectures. In addition, it summarizes the related work in the field of security of wireless networks; and authentication / re-authentication protocols.

Chapter 3 presents the proposed protocols in homogeneous networks, it contains two main sections. The first section presents a new tunnelled EAP based authentication method for WiMAX networks to provide both user and device authentication and to protect the communications in WiMAX networks against MITM attacks. The second section presents an enhanced authentication and key agreement protocol for the LTE networks to improve the security of LTE network against user UID attack and to reduce the storage overhead.

Chapter 4 presents three authentication and re-authentication protocols for LTE-WLAN interworking architecture.

Chapter 5 presents the modified authentication protocols and the new inter/intra re-authentication protocols for LTE-WiMAX-WLAN interworking architecture. Chapter 6 concludes the thesis and future research.

BIBLIOGRAPHY

[1] S. Ahmadi. An overview of next -generation mobile WiMAX technology. *Communications Magazine, IEEE*, 47(6):84–98, June 2009.

[2] Jeffrey G. Andrews, Arunabha Ghosh, and Rias Muhamed. *Fundamentals of WiMAX: Understanding Broadband Wireless Networking (Prentice Hall Communications Engineering and Emerging Technologies Series)*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2007.

[3] Fan Yang and Ping Zhu. An EAP-TTLS-SPEKEY Method for Single EAP-Based Auth Mode of IEEE 802.16e PKMv2. In *International Conference on Computational Intelligence and Software Engineering (CiSE)*, pages 1–4, 2010.

[4] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), June 2000.

[5] P. Funk and S. Blake-Wilson. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0). IETF RFC 5281, Aug. 2008.

[6] T. Wu. The SRP Authentication and Key Exchange System. RFC 2945 (Proposed Standard), Sep 2000.

[7] Su Jung Yu and Joo Seok Song. An improved password authentication key exchange protocol for 802.11 environment. In *Computational Science and Its ApplicationsICCSA 2003*, pages 201–209. Springer, 2003.

[8] K. Kaur, A. S. Sharma, H. S. Sohal, and A. Kaur. Adaptive Random Key Scheme for Authentication and Key Agreement (ARKS-AKA) for efficient LTE security. In *2nd International Conference on Recent Advances in Engineering Computational Sciences (RAECS)*, pages 1–6, Dec 2015.

[9] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis. LTE Authentication Protocol (EPS-AKA) weaknesses solution. In *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, pages 434–441, Dec 2015.

[10] Younes El Hajjaji El Idrissi, Noureddine Zahid, and Mohamed Jedra. A New Authentication Method for Vertical and Horizontal Handover in 3G-WLAN Interworking Architecture. *Research Journal of Applied Sciences, Engineering and Technology*, 7(2):329–342, 2014.

[11] Sung-Shiou Shen, Shen-Ho Lin, and Jung-Hui Chiu. Fast Handover Pre-Authentication Protocol in 3GPP-WLAN Heterogeneous Mobile Networks. *Int'l J. of Communications, Network and System Sciences*, 2014(7):101–113, 2014.

[12] Ahmed H Hassanein, Abdel Hafez, A Ahmed, A Gaafar, and Abd El-hamid. New Authentication and Key Agreement Protocol for LTE-WLAN Interworking. *International Journal of Computer Applications*, 61(19):20–24, 2013.

[13] Shen-Ho Lin, Jung-Hu Chiu, and Sung-Shiou Shen. The performance evaluation of fast iterative localized re-authentication for 3G/UMTS-WLAN interworking networks. *Journal of Ambient Intelligence and Humanized Computing*, 4(2):209–221, 2013.

[14] Imen Elbouabidi, Faouzi Zarai, Mohammad S Obaidat, and Lotfi Kamoun. An efficient design and validation technique for secure handover between 3GPP LTE and WLANs systems. *Journal of Systems and Software*, 91:163–173, 2014.

[15] Karl Andersson. Interworking Techniques and Architectures for Heterogeneous Wireless Networks. *Journal of Internet Services and Information Security*, 2 (1/2):22–48, 2012.

[16] IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Standard 802.11i-2004*, pages c1–178, July 2004. doi: 10.1109/IEEESTD.2004.311922.

[17] IEEE 802 LAN/MAN Standards Committee et al. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Standard*, 802(11), 1999.

[18] S. More and D.K. Mishra. 4G Revolution: WiMAX technology. In *Third Asian Himalayas International Conference on Internet (AH-ICI)*, pages 1–4, 2012.

[19] Shantanu Pathak and Shagun Batra. Next generation 4G WiMAX networks - IEEE 802.16 standard. *Sundarapandian et al.(Eds): CoNeCo, WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT*, 7:507–518, 2012.

[20] IEEE. Draft IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. *IEEE Std P802.16e/D7*, pages –, May 2004.

[21] IEEE. Approved Draft IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems (Incorporated into IEEE Std 802.16e - 2005 and IEEE Std 802.16 -2004/Cor 1 -2005 E). *IEEE Std P802.16/Cor1/D5*, pages –, 2005.

[22] IEEE. IEEE Draft Amendment Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Advanced Air Interface. *IEEE P802.16m/D7 July 2010*, pages 1–932, Aug 2010.

[23] Mojtaba Seyedzadegan and Mohamed Othman. IEEE 802.16: WiMAX Overview, WiMAX Architecture. *International Journal of Computer Theory and Engineering*, 5(5):784–796, 2013.

[24] IEEE. IEEE Standard for Air Interface for Broadband Wireless Access Systems–Amendment 2: Higher Reliability Networks. *IEEE Std 802.16n - 2013 (Amendment to IEEE Std 802.16 -2012)*, pages 1–168, June 2013.

[25] IEEE. IEEE Standard for Air Interface for Broadband Wireless Access Systems– Amendment 3: Multi-tier Networks. *IEEE Std 802.16q -2015 (Amendment to IEEE Std 802.16 -2012)*, pages 1–117, March 2015.

[26] WiMAX Forum Network Working Group et al. WiMAX Forum Network Architecture Stage 3: Detailed Protocols and ProceduresRelease 1, Version 1.2. In *WiMAX Forum, January*, 2008.

[27] Iznan Husainy Hasbullah, Raja Kumar Murugesan, Sureswaran Ramadass, et al. Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods. *IETE Technical Review (Medknow Publications & Media Pvt. Ltd.)*, 30(1), 2013.

[28] D. Johnston and J. Walker. Overview of IEEE 802.16 security. *IEEE Security & Privacy*, 2(3):40–48, 2004.

[29] Syed A Ahson and Mohammad Ilyas. *WiMAX: standards and security*. CRC press, 2007.

[30] Noudjoud Kahya, Nacira Ghoualmi, and Pascal Lafourcade. Formal analysis of PKM using scyther tool. In *International Conference on Information Technology and e-Services (ICITeS)*, pages 1–6. IEEE, 2012.

[31] IEEE. IEEE Standard for Local and Metropolitan Area Networks –Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. *IEEE Std P802.16e/D7 (Amendment and Corrigendum to IEEE Std 802.16 -2004)*, pages –, 2005.

[32] Mohammad Zabihi, Ramin Shaghaghi, et al. Improving Security Levels of IEEE 802.16e Authentication By Diffie-Hellman Method. *International Journal of Computer Science Issues*, 8(3):163–168, 2012.

[33] Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, and Borislav Popovski. IEEE 802.16 security issues: a survey. In *16th Telecommunication forum (TELEFOR)*, pages 199–202, 2008.

[34] Stuart Jacobs. WiMAX subscriber and mobile station authentication challenges. *IEEE Communications Magazine*, 49(11):166–172, 2011.

[35] Elias Bou-Harb, Makan Pourzandi, Mourad Debbabi, and Chadi Assi. A secure, efficient, and cost-effective distributed architecture for spam mitigation on LTE 4G mobile networks. *Security and Communication Networks*, 6(12): 1478–1489, 2013.

[36] Nabil Seddigh, Biswajit Nandy, Rupinder Makkar, and Jean-Francois Beaumont. Security advances and challenges in 4G wireless networks. In *Eighth Annual International Conference on Privacy Security and Trust (PST)*, pages 62–71. IEEE, 2010.

[37] GSM 02.09 V6.1.0. Digital Cellular Telecommunications System (Phase 2+); Security aspects (GSM 02.09 Version 6.1.0 Release 1997). 1997.

[38] 3GPP. 3G security; Security architecture. TS 33.102 v8.2.0, 3GPP, Jun. 2009.

[39] 3GPP. 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401, 3GPP, 2011.

[40] Hyun-Ho Choi, Osok Song, and Dong-Ho Cho. Seamless Handoff Scheme based on pre-registration and pre-authentication for UMTS–WLAN interworking. *Wireless Personal Communications*, 41(3):345–364, 2007.

[41] Quoc-Thinh Nguyen-Vuong, Lionel Fiat, and Nazim Agoulmine. An architecture for UMTS-WIMAX interworking. *Broadband Convergence Networks*, pages 1–10, 2006.

[42] 3GPP. 3GPP system to Wireless Local Area Network (WLAN) interworking; System description. TS 23.234, 3rd Generation Partnership Project (3GPP), Dec. 2009.

[43] 3GPP. Architecture enhancements for non-3GPP accesses (Release 10). TS 23.402 V9.4.0, 3GPP, Sep. 2012.

[44] Chris G Guy and Myasar R Tabany. LTE and LTE-A Interworking and Interoperability with 3GPP and non-3GPP Wireless Networks. *Journal of Emerging Trends in Computing and Information Sciences*, 4(8), 2013.

[45] Ramon Ferrus, Oriol Sallent, and Ramon Agusti. Interworking in heterogeneous wireless networks: comprehensive framework and future trends. *Wireless Communications, IEEE*, 17(2):22–31, 2010.

[46] Tara A Yahiya and Hakima Chaouchi. On the integration of LTE and mobile WiMAX networks. In *19th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–5. IEEE, 2010.

[47] Fangmin Xu, Luyong Zhang, and Zheng Zhou. Interworking of Wimax and 3GPP networks based on IMS [IP Multimedia Systems (IMS) Infrastructure and Services]. *Communications Magazine, IEEE*, 45(3):144–150, 2007.

[48] Kumudu S Munasinghe and Abbas Jamalipour. Interworked WiMAX-3G cellular data networks: an architecture for mobility management and performance evaluation. *Wireless Communications, IEEE Transactions on*, 8(4):1847–1853, 2009.

[49] Mugen Peng and Wenbo Wang. A unified architecture and key techniques for interworking between WiMAX and Beyond 3G/4G Systems. *Wireless personal communications*, 45(1):67–90, 2008.

[50] R.A. Hamada, H.S. Ali, and M.I. Abdalla. Performance evaluation of a novel IMS-based architecture for LTE-WIMAX-WLAN interworking. In *International Conference on Engineering and Technology (ICET)*, pages 1–6, April 2014.

[51] Saeed Rashid A, Ahmed AM Hassan, Mukherjee Amitava, Falcone Francisco, Wong K Daniel, et al. WiMAX, LTE, and WiFi Interworking. *Journal of Computer Systems, Networks, and Communications*, 2010, 2010.

[52] IEEE. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 3: Advanced Air Interface. *IEEE Std 802.16m-2011(Amendment to IEEE Std 802.16-2009)*, pages 1–1112, May 2011.

[53] IEEE. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. *IEEE Std 802.16 -2004*, 802:16–2004, 2004.

[54] David Johnston and Jesse Walker. Mutual Authorization for PKMv2. *IEEE C802. 16e -04/229*, 2004.

[55] RM Hashmi, Arooj M Siddiqui, M Jabeen, and KS Alimgeer. Towards secure wirelessMAN: Revisiting and evaluating authentication in WiMAX. In *International Conference on Computer Networks and Information Technology (ICCNIT)*, pages 165–173. IEEE, 2011.

[56] Seok Yee Tang, Peter Muller, and Hamid Sharif. *WiMAX security and quality of service: an end -to -end perspective*. John Wiley & Sons, 2011.

[57] Ayesha Altaf, M Younus Javed, Sheraz Naseer, and Aisha Latif. Performance analysis of secured privacy and key management protocol in ieee 802.16e -2005. *International Journal of Digital Content Technology and its Applications*, 3(1): 103–109, 2009.

[58] AS Khan, N Fisal, ZA Bakar, N Salawu, W Maqbool, R Ullah, and H Safdar. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Indian Journal of Science and Technology*, 7(3):282–295, 2014.

[59] Naveen Chauhan and Rakesh Kumar Yadav. Security Analysis of Identity Based Cryptography and Certificate Based in Wimax Network Using Omnet++ Simulator. In *Second International Conference on Advanced Computing & Communication Technologies (ACCT)*, pages 509–512. IEEE, 2012.

[60] Yogesh Gedam and SD Chede. Design and Improvement in WiMAX 3G security using Multiple Keys. *International Journal of Engineering Science and Technology*, 3(7):5964–5973, 2011.

[61] 3GPP. 3GPP System Architecture Evolution (SAE); Technical Specification Group Services and System Aspects (Release 12). TS 33.402, 3GPP, Sep. 2013.

[62] L Blunk and PPP Extensible Authentication Protocol. PPP extensible authentication protocol (EAP), RFC 2284. *Network Working Group, IETF*, 1998.

[63] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). IETF RFC 3748, Jun. 2004.

[64] AK 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*, pages 881–885. ACM, 2011.

[65] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). RFC 4187 (Informational), Jan. 2006.

[66] J. Arkko, V. Lehtovirta, and P. Eronen. Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'). RFC 5448 (Informational), May 2009.

[67] 3GPP. Numbering, addressing and identification (Release 10). TS 23.003 V10.5.0, 3GPP, March 2012.

[68] 3GPP. Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks Stage 3 (Release 9). TS 24.302 V9.4.0, 3GPP, Sep. 2010.

[69] Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, and Valtteri Niemi. *LTE security*, volume 1. John Wiley & Sons, 2012.

[70] PUB FIPS. 180-3. Secure hash standard. *National Institute of Standards and Technology*, 1:27, 2008.

[71] PUB FIPS. 180-1. Secure hash standard. *National Institute of Standards and Technology*, 17:45, 1995.

[72] Stefania Sesia, Issam Toufik, and Matthew Baker. LTE: From theory to practice, 2009.

[73] David P Jablon. Strong password-only authenticated key exchange. *ACM SIGCOMM Computer Communication Review*, 26(5):5–26, 1996.

[74] Mohammed Awadh Ben-Mubarak, NK Noordin, A Ismail, CK Ng, et al. Review of handover mechanisms to support triple play in mobile WiMAX. *IETE Technical review*, 26(4):258, 2009.

[75] Ali Nawaz Khan, Waqas Anwer, Ehsan Ullah Munir, Uzair Farooqi, Ayesha Khaliq, Aqsa Malik, and Maryam Aizaz. Handover Techniques in Mobile WiMAX Networks: Analysis and Comparison. *Middle-East Journal of Scientific Research*, 15(11):1599–1605, 2013.

[76] Pedro J. Fernandez Ruiz, Fernando Bernal Hidalgo, Cristian A. Nieto Guerra, and Antonio F. Gomez Skarmeta. Mobility and security in a real VANET deployed in a heterogeneous networks. *Security and Communication Networks*, 9(3):208–219, 2016.

[77] Hamzah F Zmezm, SJ Hashim, A Sali, and Kamal Ali Alezabi. Pre-Authentication Design for Seamless and Secure Handover in Mobile WiMAX. *International Review on Computers and Software (IRECOS)*, 10(7):764–772, 2015.

[78] Yi-Fu Ciou, Fang-Yie Leu, Yi-Li Huang, and Kangbin Yim. A handover security mechanism employing the diffie-hellman key exchange approach for the ieee802. 16e wireless networks. *Mobile Information Systems*, 7(3):241–269, 2011.

[79] Shih-Feng Hsu and Yi-Bing Lin. A key caching mechanism for reducing WiMAX authentication cost in handoff. *Vehicular Technology, IEEE Transactions on*, 58(8):4507–4513, 2009.

[80] Anmin Fu, Yuqing Zhang, Zhenchao Zhu, Qi Jing, and Jingyu Feng. An efficient handover authentication scheme with privacy preservation for IEEE 802.16 m network. *Computers & Security*, 31(6):741–749, 2012.

[81] Thuy Ngoc Nguyen and Maode Ma. Enhanced EAP -based pre -authentication for fast and secure inter -ASN handovers in mobile WiMAX networks. *IEEE Transactions on Wireless Communications*, 11(6):2173–2181, 2012.

[82] Thuy Ngoc Nguyen and Maode Ma. An pre-authentication protocol with symmetric keys for secure handover in mobile WiMAX networks. In *IEEE International Conference on Communications (ICC)*, pages 863–867. IEEE, 2012.

[83] Hung-Min Sun, Shih-Ying Chang, Yue-Hsun Lin, and Shin-Yan Chiou. Efficient Authentication Schemes for Handover in Mobile WiMAX. In *Eighth International Conference on Intelligent Systems Design and Applications (ISDA '08)*, volume 3, pages 235–240, Nov. 2008.

[84] W.I. Khedr, M.I. Abdalla, and A.A. Elsheikh. Enhanced inter-access service network handover authentication scheme for IEEE 802.16m network. *Information Security, IET*, 9(6):334–343, 2015.

[85] Jin Cao, Hui Li, Maode Ma, Yueyu Zhang, and Chengzhe Lai. A simple and robust handover authentication between HeNB and eNB in {LTE} networks. *Computer Networks*, 56(8):2119 – 2131, 2012. ISSN 1389-1286.

[86] G.M. Koien. Mutual entity authentication for LTE. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pages 689–694, 2011.

[87] Lili Gu and Mark A Gregory. A green and secure authentication for the 4th generation mobile network. In *Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pages 1–7. IEEE, 2011.

[88] D. Caragata, S. El Assad, C. Shoniregun, and G. Akmayeva. UMTS security: Enhancement of identification, authentication and key agreement protocols. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pages 278–282, 2011.

[89] K. Hamandi, I. Sarji, A. Chehab, I.H. Elhajj, and A. Kayssi. Privacy Enhanced and Computationally Efficient HSK-AKA LTE Scheme. In *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 929–934, 2013.

[90] C. K. Huan. Security Analysis and Enhancements in LTE-Advanced Networks. *doctoral dissertation, Dept. of Mobile Systems Engineering,Sungkyunkwan University, South Korea*, 2011.

[91] Jacques Bou Bou Abdo, Hakima Chaouchi, and Mohammad Aoude. Ensured confidentiality authentication and key agreement protocol for EPS. In *Symposium on Broadband Networks and Fast Internet (RELABIRA 2012)*, pages 73–77. IEEE, 2012.

[92] Li Xiehua and Wang Yongjun. Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network. In *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pages 1–4, 2011.

[93] Chan-Kyu Han and Hyoung-Kee Choi. Security Analysis of Handover Key Management in 4G LTE/SAE Networks. *Mobile Computing, IEEE Transactions on*, 13(2):457–468, 2014.

[94] Fikadu B Degefa, Donghoon Lee, Jiye Kim, Younsung Choi, and Dongho Won. Performance and security enhanced authentication and key agreement protocol for SAE/LTE network. *Computer Networks*, 94:145–163, 2016.

[95] Naïm Qachri, Olivier Markowitch, and Jean-Michel Dricot. A Formally Verified Protocol for Secure Vertical Handovers in 4G Heterogeneous Networks. *International Journal of Security & Its Applications*, 7(6):309–326, 2013.

[96] Bruno Blanchet. Automatic verification of security protocols in the symbolic model: The verifier proverif. In *Foundations of Security Analysis and Design VII*, pages 54–87. Springer, 2014.

[97] Rajadurai Rajavelsamy and Sungho Choi. Security aspects of inter-access system mobility between 3GPP and non-3GPP networks. In *3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE)*, pages 209–213. IEEE, 2008.

[98] Xiaowei Li, Yuqing Zhang, Xuefeng Liu, Jin Cao, and Qianqian Zhao. A lightweight roaming authentication protocol for anonymous wireless communication. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 1029–1034. IEEE, 2012.

[99] N Christoforos and X Christos. One-Pass EAP-AKA Authentication in 3G-WLAN Integrated Networks [J]. *Wireless Personal Communications*, 48(4): 569–584, 2009.

[100] Christoforos Ntantogian, Ioannis Stavrakakis, and Christos Xenakis. Reducing the user authentication cost in next generation networks. In *Fifth Annual Conference on Wireless on Demand Network Systems and Services (WONS)*, pages 65–72. IEEE, 2008.

[101] Xinghua Li, Xiang Lu, Jianfeng Ma, Zhenfang Zhu, Li Xu, and YoungHo Park. Authentications and key management in 3G-WLAN interworking. *Mobile Networks and Applications*, 16(3):394–407, 2011.

[102] Hyeran Mun, Kyusuk Han, and Kwangjo Kim. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA. In *Wireless Telecommunications Symposium, 2009. WTS 2009*, pages 1–8, 2009.

[103] Y Deng, G Wang, and J Cao. Practical unified authentication for 3G-WLAN interworking. *Journal of Information & Computational Science*, 9(7):1991–2000, 2012.

[104] Younes El Hajjaji El Idrissi, Noureddine Zahid, and Mohamed Jedra. A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA. In *20th International Conference on Telecommunications (ICT)*, pages 1–5. IEEE, 2013.

[105] Shen-Ho Lin, Jung-Hui Chiu, and Sung-Shiou Shen. A fast iterative localized re-authentication protocol for UMTS-WLAN heterogeneous mobile communication networks. *EURASIP Journal on Wireless Communications and Networking*, 2011(1):1–16, 2011.

[106] Suresh Kumar, A Rajeswari, et al. Enhanced fast iterative localized re-authentication protocol for UMTS-WLAN interworking. In *International Conference on Electronics and Communication Systems (ICECS)*, pages 1–5. IEEE, 2014.

[107] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. A survey on security aspects for LTE and LTE-A networks. *Communications Surveys & Tutorials, IEEE*, 16(1):283–302, 2014.

[108] IEEE. IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004*, pages 01–175, 2004.

[109] IEEE. IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition. *IEEE Std 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008)*, pages 1–126, July 2008.

[110] YEHE Idrissi, Noureddine Zahid, and Mohamed Jedra. Security analysis of 3GPP (LTE)WLAN interworking and a new local authentication method based on EAP-AKA. In *International Conference on Future Generation Communication Technology (FGCT)*, pages 137–142. IEEE, 2012.

[111] Run hua Shi, Hong Zhong, and Liu sheng Huang. A novel anonymous authentication scheme without cryptography. *Transactions on Emerging Telecommunications Technologies*, 25(9):875–880, 2014.

[112] Olatunde Abiona, Adeniran Oluwaranti, Ayodeji Oluwatope, Surura Bello, Clement Onime, Mistura Sanni, and Lawrence Kehinde. Wireless Network Security: The Mobile Agent Approach. *International Journal of Communications, Network & System Sciences*, 6(10):443–450, 2013.

[113] Tao Feng, Hui Chen, and Jian-feng Ma. Secure Re-authentication Scheme for 3G-WLAN Integrating Network Based on Protocol Composition Logic. In *International Conference on Computer Science & Service System (CSSS)*, pages 800–805. IEEE, 2012.

[114] Chengzhe Lai, Hui Li, Xiaoqing Li, and Jin Cao. A novel group access authentication and key agreement protocol for machine-type communication. *Transactions on Emerging Telecommunications Technologies*, 26(3):414–431, 2013.

[115] IE Bouabidi, I Daly, and F Zarai. Secure handoff protocol in 3GPP LTE networks. In *Third International Conference on Communications and Networking (ComNet)*, pages 1–6. IEEE, 2012.

[116] Ikbel Daly, Faouzi Zarai, and Lotfi Kamoun. Re-authentication protocol for vertical handoff in heterogeneous wireless networks. In *Mobile Lightweight Wireless Systems*, pages 219–230. Springer, 2012.

[117] Imen El Bouabidi, Faouzi Zarai, Mohammad S Obaidat, and Lotfi Kamoun. Fast and Secure Handover into Visited WLAN Networks. In *Ubiquitous Information Technologies and Applications*, pages 649–657. Springer, 2013.

[118] Salwa Othmen, Faouzi Zarai, Mohammad S Obaidat, and Aymen Belghith. Re-authentication protocol from WLAN to LTE (ReP WLAN-LTE). In *IEEE Global Communications Conference (GLOBECOM)*, pages 1446–1451. IEEE, 2013.

[119] Ayesha Altaf, Faiza Iqbal, and M Younus Javed. S3H: A Secure Seamless and Soft Handover between WiMax and 3G Networks. In *International Conference on Convergence and Hybrid Information Technology (ICHIT'08)*, pages 530–534. IEEE, 2008.

[120] Li Wang, Mei Song, Ping Wang, Jie Li, and Junde Song. Performance modeling on dynamic authentication data management in heterogeneous interworking networks. In *Canadian Conference on Electrical and Computer Engineering (CCECE'09)*, pages 403–406. IEEE, 2009.

[121] Neila Krichene and Noureddine Boudriga. Securing roaming and vertical handover in fourth generation networks. In *Third International Conference on Network and System Security (NSS'09)*, pages 225–231. IEEE, 2009.

[122] Anmin Fu, Gongxuan Zhang, Zhenchao Zhu, and Yuqing Zhang. Fast and Secure Handover Authentication Scheme Based on Ticket for WiMAX and WiFi Heterogeneous Networks. *Wireless Personal Communications*, pages 1–23, 2014.

[123] Kuei-Li Huang, Kuang-Hui Chi, Jui-Tang Wang, and Chien-Chao Tseng. A Fast Authentication Scheme for WiMAX–WLAN Vertical Handover. *Wireless personal communications*, 71(1):555–575, 2013.

[124] Myoung Ju Yu, Seong Gon Choi, Hwa Suk Kim, and Kee Seong Cho. An improved scheme for reducing handover latency in heterogeneous networks. In *13th International Conference on Advanced Communication Technology (ICACT)*, pages 1534–1539. IEEE, 2011.

[125] Myoung Ju Yu and Seong Gon Choi. A new mechanism for fast handover between heterogeneous networks. In *13th International Conference on Advanced Communication Technology (ICACT)*, pages 954–959. IEEE, 2011.

[126] Li Wang, Mei Song, Junde Song, Yong Zhang, Ping Wang, and Jie Li. A Novel Dynamic Hierarchy AAA Scheme for Interworking Authentication in Heterogeneous Networks. In *IEEE International Conference on Communications Workshops. ICC Workshops*, pages 1–5. IEEE, 2009.

[127] Ali A Al Shidhani and Victor CM Leung. Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers. *IEEE Transactions on Dependable and Secure Computing*, 8(5):699–713, 2011.

[128] Elankayer Sithirasenan, Khosrow Ramezani, Saurabh Kumar, and Vallipuram Muthukkumarasamy. EAP-CRA for WiMAX, WLAN and 4G LTE Interoperability. *Selected Topics in WiMAX*, pages 978–953, 2013.

[129] Mei Song, Li Wang, Jianwen Huang, and Junde Song. An optimal interworking authentication scheme based on EAP-AKA for heterogeneous access networks. In *Canadian Conference on Electrical and Computer Engineering (CCECE'09)*, pages 794–797. IEEE, 2009.

[130] R. Housley and B. Aboba. Guidance for Authentication, Authorization, and Accounting (AAA) Key Management. RFC 4962 (Best Current Practice), Jul. 2007.

[131] Tingting Yang, Chengzhe Lai, Rongxing Lu, and Rong Jiang. EAPSG: Efficient authentication protocol for secure group communications in maritime wideband communication networks. *Peer-to-Peer Networking and Applications*, 8(2):216–228, 2015.

[132] T. Clancy, M. Nakhjiri, V. Narayanan, and L. Dondeti. Handover Key Management and Re-Authentication Problem Statement. RFC 5169 (Informational), Mar. 2008.

[133] LEE Song-Hee and PARK Nam-Sup. Secure Handover Protocol for Mobile WiMAX Networks. *IEICE transactions on information and systems*, 91(12): 2875–2879, 2008.

[134] Alessandro Armando, David Basin, Yohan Boichut, Yannick Chevalier, Luca Compagna, Jorge Cuéllar, P Hankes Drielsma, Pierre-Cyrille Héam, Olga Kouchnarenko, Jacopo Mantovani, et al. The AVISPA tool for the automated validation of internet security protocols and applications. In *Computer Aided Verification*, pages 281–285. Springer, 2005.

[135] AVISPA. The AVISPA User Manual. `http://www.avispa-project.org`.

[136] Yannick Chevalier, Luca Compagna, Jorge Cuellar, P Hankes Drielsma, Jacopo Mantovani, Sebastian Mödersheim, Laurent Vigneron, et al. *A high level protocol specification language for industrial security-sensitive protocols*. na, 2004.

[137] Yannick Chevalier and Laurent Vigneron. Rule-based programs describing Internet security protocols. *Electronic Notes in Theoretical Computer Science*, 124(1):113–132, 2005.

[138] Sidharth, Sreejesh and Sebastian, MP. A Revised Secure Authentication Protocol for IEEE 802.16 (e). In *International Conference on Advances in Computer Engineering (ACE)*, pages 34–38. IEEE, 2010.

[139] Ayesha Altaf, Rabia Sirhindi, and Attiq Ahmed. A novel approach against DoS attacks in WiMAX authentication using visual cryptography. In *Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'08)*, pages 238–242. IEEE, 2008.

[140] Siddharth Maru and Timothy X Brown. Denial of service vulnerabilities in the 802.16 protocol. In *Proceedings of the 4th Annual International Conference on Wireless Internet*, pages 1–9, 2008.

[141] Pranita K Gandhewar and Prasad P Lokulwar. Improving security in initial network entry process of IEEE 802.16. *International Journal on Computer Science and Engineering (IJCSE)*, 3(9):3327–3331, 2011.

[142] AKM Nazmus Sakib, Tanvir Mahmud, Samiur Mountain Munim, and Muhammad Mushfiqur Rahman Mountain Munim. Secure Authentication & Key Exchange Technique for IEEE 802.16 e by using Cryptographic Properties. *International Journal of Engineering Research and Applications (IJERA)*, 1 (3):490–496, 2011.

[143] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, and Yuanan Liu. Analysis of mobile WiMAX security: Vulnerabilities and solutions. In *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 828–833, Sept. 2008.

[144] Anjani Kumar Rai, Shivendu Mishra, and Pramod Narayan Tripathi. An Improved Secure Authentication Protocol for WiMAX with Formal Verification. In *Advances in Computing and Communications*, pages 407–416. Springer, 2011.

[145] Fan Yang and Ping Zhu. An EAP_TTLS_SPEKEY Method for Single EAP_Based Auth Mode of IEEE 802.16e PKMv2. In *2010 International Conference on Computational Intelligence and Software Engineering*, pages 1–4, 2010.

[146] Deepak Kumar Mehto and Rajesh Srivastava. An Enhanced Authentication Mechanism for IEEE 802.16 (e) Mobile WiMAX. *International Journal of Soft Computing and Engineering (IJSCE)*, 1(4):98–102, Sep. 2011.

[147] Anmin Fu, Yuqing Zhang, Zhenchao Zhu, and Jingyu Feng. EKMP: an enhanced key management protocol for IEEE 802.16m. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1137–1142. IEEE, 2011.

[148] Noudjoud Kahya, Nacira Ghoualmi, and Pascal Lafourcade. Key management protocol in WIMAX revisited. In *Advances in Computer Science, Engineering & Applications*, pages 853–862. Springer, 2012.

[149] Ayesha Altaf, M Younus Javed, and Attiq Ahmed. Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e -2005. In *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD)*, pages 335–339. IEEE, 2008.

[150] Raheel M Hashmi, Arooj M Siddiqui, M Jabeen, K Shehzad, A Zubair, and KS Alimgeer. Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16. In *International Conference on Information and Communication Technologies, ICICT'09*, pages 101–105. IEEE, 2009.

[151] Krishna Bakthavathsalu, Srinivas Sampalli, and Qiang Ye. Management frame attacks in WiMAX networks: Analysis and prevention. In *Seventh International Conference On Wireless And Optical Communications Networks (WOCN)*, pages 1–7. IEEE, 2010.

[152] Noudjoud Kahya, Nacira Ghoualmi, and Pascal Lafourcade. Secure key management protocol in WiMAX. *International Journal of Network Security & Its Applications*, 4(6):119–132, 2012.

[153] Yuh-Shyan Chen, Tong-Ying Juang, and Yao-Tsu Lin. A Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6 in 3GPP LTE Systems. *Wireless Personal Communications*, 61(4):629–656, 2011.

[154] Liu Wenju, Shang Yuzhen, Zhang Yan, and Wang Ze. An analysis of the improved EAP-AKA protocol. In *2nd International Conference on Computer Engineering and Technology*, volume 1, pages 10–13, 2010.

[155] J Vijay Franklin and K Paramasivam. Enhanced Authentication Protocol for Improving Security in 3GPP LTE Networks. In *International Conference on Information and Network Technology*, pages 28–33, 2011.

[156] P Prasithsangaree and P Krishnamurthy. A new authentication mechanism for loosely coupled 3G-WLAN integrated networks. In *IEEE 59th Vehicular Technology Conference, VTC 2004-Spring.*, volume 5, pages 2998–3003. IEEE, 2004.

[157] Christoforos Ntantogian, Christos Xenakis, and Ioannis Stavrakakis. Analysis and Modeling of False Synchronizations in 3G-WLAN Integrated Networks. In *Information Security and Privacy Research*, pages 475–488. Springer, 2012.

[158] JaeJong Baek, SungHoon Seo, Fei Shi, and JooSeok Song. A novel pre-authentication scheme based on fast channel switching in IEEE 802.11 WLANs. *EURASIP Journal on Wireless Communications and Networking*, 2012(1):1–15, 2012.

[159] Hyeyeon Kwon, Kwanghyun Ro, Aesoon Park, and Jaecheol Ryou. UMTS-WLAN interworking strategies for reducing handover delays. In *IEEE 64th Vehicular Technology Conference, VTC Fall. 2006*, pages 1–5. IEEE, 2006.

[160] Shen-Ho Lin, Jung-Hui Chiu, and Sung-Shiou Shen. The iterative distributed re-authentication scheme based on EAP-AKA in 3G/UMTS-WLAN heterogeneous mobile networks. In *International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, pages 429–434. IEEE, 2010.

[161] Ali Al Shidhani and Victor Leung. Pre-authentication schemes for UMTS-WLAN interworking. *EURASIP Journal on Wireless Communications and Networking*, 2009:1–16, 2009.

[162] Dorothey Stanley, Jesse Walker, and Bernard Aboba. Extensible authentication protocol (EAP) method requirements for wireless LANs. *Request for Comments*, 4017, 2005.

[163] Anjani K Rai, Vimal Kumar, and Shivendu Mishra. Strong Password Based EAP-TLS Authentication Protocol for WiMAX. *Anjani K. Rai et al./(IJCSE) International Journal on Computer Science and Engineering*, 2(02):2736–2741, 2010.

[164] Yu-Wen Chen, Jui-Tang Wang, Kuang-Hui Chi, and Chien-Chao Tseng. Group-based authentication and key agreement. *Wireless Personal Communications*, 62(4):965–979, 2012.

[165] Chengzhe Lai, Hui Li, Rongxing Lu, and Xuemin Sherman Shen. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. *Computer Networks*, 57(17):3492–3510, 2013.

[166] M. Prasad and R. Manoharan. Secure authentication scheme for Long Term Evolution-Advanced. In *International Conference on Information Communication and Embedded Systems (ICICES)*, pages 11–15, 2013.

[167] 3GPP. 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 14). TS 33.402, 3GPP, Jan. 2017.

[168] 3GPP. Mobility management based on Dual-Stack Mobile IPv6; Stage 3. TS 24.303, 3GPP, Jul. 2008.

[169] B. Aboba, D. Simon, and P. Eronen. Extensible Authentication Protocol (EAP) key management framework. IETF RFC 5247, Aug. 2008.

[170] J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri. Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK). IETF RFC 5295, Aug. 2008.

[171] Rafal Chrabaszcz and Piotr Pacyna. Fast re-authentication of mobile devices with EAP Re-authentication Protocol (ERP). In *15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS)*, pages 1–6, 2012.

[172] Feng Hao and Siamak F Shahandashti. *The SPEKE Protocol Revisited*. Springer, 2014.

[173] Masoumeh Purkhiabani and Ahmad Salahi. Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks. *International Journal of Information and Electronics Engineering*, 2(1):69–77, 2012.

[174] Jacques Bou Abdo, Jacques Demerjian, Kassem Ahmad, Hakima Chaouchi, and Guy Pujolle. EPS mutual authentication and Crypt-analyzing SPAKA. In *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, pages 303–308. IEEE, 2013.

[175] Jaeduck Choi and Souhwan Jung. A handover authentication using credentials based on chameleon hashing. *IEEE Communications Letters*, 14(1):54–56, 2010.

[176] Leonard Kleinrock. *Computer applications, volume 2, queueing systems*. Wiley, 1976.

[177] WiMAX Forum Network Working Group et al. WiMAX Forum Network Architecture: Detailed Protocols and Procedures- WiFi-WiMAX interworking Rel. 1.6. In *WiMAX Forum, Nov.*, 2010.

[178] Jong-Hyouk Lee and Tai-Myoung Chung. A traffic analysis of authentication methods for proxy Mobile IPv6. In *International Conference on Information Security and Assurance (ISA)*, pages 512–517. IEEE, 2008.

[179] Wenye Wang and Ian F Akyildiz. Intersystem location update and paging schemes for multitier wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 99–109. ACM, 2000.

[180] David W Carman, Peter S Kruus, and Brian J Matt. Constraints and approaches for distributed sensor network security (final). *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, 1(1):1–139, 2000.

[181] L.M. Feeney and M. Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1548–1557, 2001.

[182] G. Vijayalakshmy and G. Sivaradje. Interworking of WLAN-LTE for next generation wireless networks. In *International Conference on Information Communication and Embedded Systems (ICICES)*, pages 1–6, Feb. 2014.

[183] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar. Survey on Threats and Attacks on Mobile Networks. *IEEE Access*, 4:4543–4572, Sep. 2016.

[184] Mahdi Aiash, Glenford Mapp, Aboubaker Lasebae, and Raphael Phan. Providing security in 4G systems: unveiling the challenges. In *Sixth Advanced International Conference on Telecommunications (AICT)*, pages 439–444. IEEE, 2010.

[185] Yongsuk Park and Taejoon Park. A survey of security threats on 4G networks. In *Globecom Workshops, 2007 IEEE*, pages 1–6. IEEE, 2007.

[186] 3GPP. 3G security; Wireless Local Area Network (WLAN) interworking security. TS 33.234, 3rd Generation Partnership Project (3GPP), Mar. 2008.

[187] Frans Panken, Gerard Hoekstra, Delphin Barankanira, Charles Francis, Rico Schwendener, Ole Grondalen, and Martin G Jaatun. Extending 3G/WiMAX Networks and Services through Residential Access Capacity [Wireless Broadband Access]. *Communications Magazine, IEEE*, 45(12):62–69, 2007.

[188] Zhiwei Yan, Huachun Zhou, Hongke Zhang, Hongbin Luo, and Sidong Zhang. A dual threshold-based fast vertical handover scheme with authentication support. In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, pages 89–96. ACM, 2008.

[189] Junbeom Hur, Chanil Park, and Hyunsoo Yoon. An efficient preauthentication scheme for IEEE 802.11-based vehicular networks. In *Advances in Information and Computer Security*, pages 121–136. Springer, 2007.

[190] Minsoo Lee, Gwanyeon Kim, and Sehyun Park. Seamless and secure mobility management with location-aware service (LAS) broker for future mobile interworking networks. *Communications and Networks, Journal of*, 7(2):207–221, 2005.

[191] J. Linn. The Kerberos Version 5 GSS-API Mechanism. RFC 1964 (Proposed Standard), June 1996. Updated by RFCs 4121, 6649.

[192] Saber Zrelli, Nobuo Okabe, and Yoichi Shinoda. EAP-Kerberos: Leveraging the Kerberos Credential Caching Mechanism for Faster Re-authentications in Wireless Access Networks. In *UBICOMM 2010, The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pages 281–286, 2010.

[193] Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, and Seung-Jo Han. Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. *Computers & Mathematics with Applications*, 60(2):245–255, 2010.

[194] Saber Zrelli, Nobuo Okabe, and Yoichi Shinoda. EAP-Kerberos: A Low Latency EAP Authentication Method for Faster Handoffs in Wireless Access Networks. *IEICE TRANSACTIONS on Information and Systems*, 95(2):490–502, 2012.

[195] Ali Al Shidhani and Victor Leung. Local fast re-authentication for 3G-WLAN interworking. *Security and Communication Networks*, 1(4):309–323, 2008.

[196] WiMAX Forum Network Working Group et al. WiMAX Forum Network Architecture Stage 2 Architecture Tenets, Reference Model and Reference Points 3GPPWiMAX Interworking, Rel. 1, ver. 1.2. In *WiMAX Forum, January*, Jan. 2008.

[197] Kamisetty Ramamohan Rao, Zoran S Bojkovic, and Bojan M Bakmaz. *Wireless Multimedia Communication Systems: Design, Analysis, and Implementation*. CRC Press, 2014.

[198] Pejman Roshan and Jonathan Leary. *802.11 wireless LAN fundamentals*. Cisco press, 2004.

[199] Xinghua Li, Jianfeng Ma, YoungHo Park, and Li Xu. A USIM-based uniform access authentication framework in mobile communication. *EURASIP Journal on Wireless Communications and Networking*, 2011:1–12, 2011.

LIST OF PUBLICATIONS

Journals Papers

F. Hashim, S. J. Hashim, B.M. Ali, A. Jamalipour and **K. A. Alezabi**. On the authentication and re-authentication protocols in LTE-WLAN interworking architecture. Transactions on Emerging Telecommunications Technologies, 28 (4) April 2017, DOI: 10.1002/ett.3031.

F. Hashim, S. J. Hashim, B.M. Ali, A. Jamalipour and **K. A. Alezabi**. On the authentication and re-authentication protocols in LTE-WLAN interworking architecture. Transactions on Emerging Telecommunications Technologies, 28 (4) April 2017, DOI: 10.1002/ett.3031.

F. Hashim, S. J. Hashim, B.M. Ali, A. Jamalipour and **K. A. Alezabi**. Authentication Process Enhancements in WiMAX Networks. Security and Communication Networks, 9 (17):4703-4725 Aug. 2016.

F. Hashim, S. J. Hashim, B.M. Ali, M. S. Obaidat, A. Jamalipour and **K. A. Alezabi**. Security and Performance Enhancement for Authentication and Re-authentication Protocols in LTE-WLAN-WiMAX Interworking Architecture. Submitted to IEEE Access journal 2017.

Conferences Papers

K. A. Alezabi, F. Hashim, S. J. Hashim and B.M. Ali. 2013. A new tunnelled EAP based authentication method for WiMAX networks. Proceedings of the IEEE Malaysia International Conference on Communications (MICC). March 2013, Kuala Lumpur, Malaysia, pp: 412-417.

K. A. Alezabi, F. Hashim, S. J. Hashim and B.M. Ali. 2014. An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks. Proceedings of the IEEE Region 10 Technical Symposium (TENSYMP), March 2014, Kuala Lumpur, Malaysia, pp: 495-500.

K. A. Alezabi, F. Hashim, S. J. Hashim and B.M. Ali. 2014. Towards Efficient Inter Handover Reauthentication in LTE-WLAN Interworking. Proceedings of the International Conference on Defence and Security Technology. Sep. 2014, Kuala Lumpur, Malaysia, pp:32-36.