Vaasan yliopisto
UNIVERSITY OF VAASA

MOHAMMAD HOSSEIN AHMADZADEGAN

Security-Centric Analysis and Performance Investigation of IEEE 802.16 WiMAX

ACTA WASAENSIA 325

COMPUTER SCIENCE 12
TELECOMMUNICATION ENGINEERING

Reviewers

Ph.D Alexandru Mihnea Moucha
Department of Computer Systems,
Faculty of Information Technology
Czech Technical University in Prague
Thákurova 9, 16000 - Prague 6,
CZECH REPUBLIC

Ph.D Florin Codrut Nemtanu
Telematics and Electronics for Transport
Politehnica Universtiy of Bucharest
313, Splaiul Independentei, room JF201
Bucharest,
ROMANIA 060042

Julkaisija	**Julkaisupäivämäärä**	
Vaasan yliopisto	Toukokuu 2015	
Tekijä(t) Mohammad Hossein Ahmadzadegan	**Julkaisun tyyppi** Monografia	
	Julkaisusarjan nimi, osan numero Acta Wasaensia, 325	
Yhteystiedot Vaasan yliopisto Teknillinen tiedekunta Tietotekniikan laitos PL 700 FI-65101 Vaasa	**ISBN** 978-952-476-620-3 (print) 978-952-476-621-0 (online)	
	ISSN 0355-2667 (Acta Wasaensia 325, print) 2323-9123 (Acta Wasaensia 325, online) 1455-7339 (Acta Wasaensia. Computer Science 12, print) 2342-0693 (Acta Wasaensia. Computer Science 12, online)	
	Sivumäärä 203	**Kieli** Englanti

Julkaisun nimike
Security-Centric Analysis and Performance Investigation of IEEE 802.16 WiMAX

Tiivistelmä

WiMAX on langaton yhteystekniikka, joka tarjoaa nopeita laajakaistayhteyksiä ja esimerkiksi WLANia laajemman toiminta-alueen. Sen laitteet ovat suhteellisen edullisia ja helposti sijoitettavissa ja ennen kaikkea se mahdollistaa riittävän laadukkaan palvelun tason (QoS). Nykyään WiMAX on yksi yleisimmistä laajakaistatekniikoista ennen kaikkea kehittyvissä maissa. Tietotuvallisuus on langattomien laajakaistaverkkojen loppukäyttäjän näkökulmasta eräs merkittävimmistä tekijöistä, jotka periaatteessa voivat vaikuttaa WiMAX-verkon suorituskykyyn, sen puute tai heikkous saattaa paljastaa arkaluonteisia tietoja ja johtaa luvattomiin verkkoon kirjautumisiin. WiMAX, kuten muukin teknologiat, kärsii monista puutteista, tietoturvaongelmista ja haavoittuvuuksista. Tietoturvallisuuden säilyttäminen WiMAX-verkon puitteissa eri skenaarioissa ja sen suojaus lukuisia erilaisia tietoturvahyökkäyksiä vastaan ovat suuri haaste. Tämän lisäksi joitakin toimenpiteitä voidaan toteuttaa uhkien havaitsemiseksi ja lieventämiseksi heti alkuvaiheessa. WiMAX tekniikka voisi kehittyä jopa laajemmin käytetyksi, mikäli sen turvallisuus olisi paremmin taattu ja kaikista pikkutarkoista tietoturvatoimenpiteistä pidettäisiin aina huolta.

Tämä väitöskirja on kirjoitettu jotta voisimme puuttua tietoturvahuoliin ja lisätä ymmärrystä uhkien havaitsemiskeinoista aina niiden vähentämiseen ja jopa niitä vastaan taistelemiseen. Tutkimuksen lähestymistapa on turvallisuuskeskeinen nykyisten tietoturvaongelmien analysointi ja ratkaisumallien ehdottaminen. Työn keskeiset tulokset ovat tietoturvallisuuden perustekijöiden selvittäminen, selittäminen ja sen jälkeen ehdotetaan kahta uutta mallia uhkien luokitteluun. Ensimäisessä on kyse WiMAXiin kohdistuvista hyökkäyksistä ja uhkista, joiden vakavuutta arvioidaan hybridilähestymistavalla jossa mittareina käytetään uhan toteutumistodennäköisyyttä ja kyseisen uhan vaikutuksen vakavuutta järjestelmään. Toisessa suoritetaan luokitus sen skenaarion perusteella, jossa VoIP-palvelut tarjotaan WiMAX-verkon välityksellä. Eli näin tutkitaan sitä mitä turvallisuusuhat yhdessä hyökkäysten kanssa aiheuttavat järjestelmätasolla erityisesti juuri WiMAX systeemille. Väitöskirja tarjoaa lisäksi vertailevaa analyysia ja luettelee turvallisuuden perusasiat WiMAX, WiFi ja LTE verkoissa. Sen lisäksi se tarjoaa joitakin WiMAXin suorituskykymittauksia tietyissä tilanteissa esimerkiksi miten suuri samanaikaisten käyttäjien määrä vaikuttaa turvallisuuteen ja suorituskykyyn. Tämä suorituskyvyn hajaantuminen on kuvattu Kiyotaki-Moore mallilla. Lisäksi uhkien vastatoimenpiteenä esitellään ja ehdotetaan uutta vaihtoehtoista energiatehokasta tietomurtojen havaitsemisjärjestelmää WiMAX-verkoille, siinä tunkeilijan havaitsemisjärjestelmä IDS tarkkailee pakettien välitystä erityisesti DoS hyökkäysten aikana.

Asiasanat
WiMAX, Tietoturva, VoIP, Suorituskyky, LTE, WiFi, Luokittelu

Publisher
Vaasan yliopisto

Date of publication
May 2015

Author(s)
Mohammad Hossein Ahmadzadegan

Type of publication
Monograph

Name and number of series
Acta Wasaensia, 325

Contact information
University of Vaasa
Faculty of Technology
Department of Computer Science
P.O. Box 700
FI-65101 Vaasa
Finland

ISBN
978-952-476-620-3 (print)
978-952-476-621-0 (online)

ISSN
0355-2667 (Acta Wasaensia 325, print)
2323-9123 (Acta Wasaensia 325, online)
1455-7339 (Acta Wasaensia. Computer Science 12, print)
2342-0693 (Acta Wasaensia. Computer Science 12, online)

Number of pages
203

Language
English

Title of publication
Security-Centric Analysis and Performance Investigation of IEEE 802.16 WiMAX

Abstract
WiMAX is a wireless access technology which offers high speed broadband connections and provides a wider coverage area. It has inexpensive equipment's and more importantly it brings about an acceptable QoS. Moreover its ease of deployment further nominates it among other wireless access networks. Nowadays, WiMAX is considered as one of the most common broadband technologies mainly deployed in developing countries. When it comes to broadband wireless access, specifically from an end-user's perspective, security is counted as one of the chief factor's that basically affects the performance of the WiMAX network and its lack or weakness endangers sensitive information's by leading to unauthorized access. WiMAX, like other technologies does have many flaws, security breaches and vulnerabilities. The preservation of the security within the WiMAX framework in different scenarios and its protection under numerous attacks are the main problems. In addition to this some measures can be taken to detect and mitigate the threats in early stages. Therefore this technology can become even more widespread if its security would be warrantied and meticulous actions would be taken care of. In order to address the security concerns and pave the way for a better understanding of the means of detection, mitigation and even fighting back, this dissertation is aimed to employ a security-centric research approach to the existing problems. The key results obtained in this dissertation are targeting the security fundamentals, explaining and providing two models for the classification of threats. One is in the case of attacks and threats when it comes to WiMAX by taking a hybrid approach with the yardsticks of probability of happening and the impact on the system. The other carried-out classification is in the scenario when VoIP services are offered by WiMAX. Thus the security threats together with the attacks posed at the system have been investigated in a WiMAX specific manner. The dissertation further provides a comparative analysis and lists the security basics of WiMAX, WiFi and LTE. In addition to this it offers some performance investigation cases of WiMAX in specific scenarios like when the security and number of simultaneous users affects the performance of the WiMAX network. This performance devolution has been described by the Kiyotaki-Moore model. Moreover, as a countermeasure to the threats, an alternative power efficient WiMAX-based intrusion detection system has been proposed and especially DoS attack is scrutinized to observe how the IDS works on the packets.

Keywords
WiMAX, Security, VoIP, Performance, LTE, WiFi, Classification

ACKNOWLEDGMENT

First of all I express my deepest gratitude to the almighty God, creator of the universe to whom I owe my existence. Moreover, I have been granted the opportunity to pursue higher education and even for this reason, I am grateful to him.

I would like to express the highest level of appreciation to my supervisor and co-supervisor Professor Dr. Mohammed Salem Elmusrati and Dr. Mohammad Reza Keshavarzi, for accepting me as a PhD student and advising me throughout the process with kindness and patience. Without their continuous advises, it would have been difficult to fulfill all the expectations completely. The greatest thing that I did learn from them was being an independent researcher. I am also grateful to the official pre-examiners of this dissertation being Dr. Ing. Alex Moucha from Czech Technical University in Prague, Czech Republic together with, Dr. Ing. Florin Nemtanu from Technical University of Bucharest, Romania for taking time, reading and approving my dissertation by offering suggestions in view of the betterment of this work.

I should thank all my colleagues and friends who encouraged and supported me, particularly at times when things were going tough. I am also very grateful to the Finnish Government for providing me with the possibility of studying without tuition fees and granting me the study-right for pursuing higher education. In addition to this, I express my appreciation toward the University of Vaasa for its services and thank Vaasa University Foundation for their travel grant.

I am unlimitedly thankful to my kindest parents for their love, encouragement and care. They were not physically present but they facilitated the successful completion of my study in the University of Vaasa. I should thank my parents even more because of their financial support during my studies. I am also grateful to my brothers from whom I have learned many lessons in my life.

Finally, I would like to thank my loving wife “Azam” for her infinite care and warmness. She accompanied me in all hardships and difficulties and was a reason for me in order not to give up.

This work is dedicated to the dearest members of my family Jafar, Mina, M. Hessam, M. Sadegh, Azam, Hassan-Ali, Farah and of course my lovely newly born daughter “Noora”.

Vaasa, Finland, February 2015

M. Hossein Ahmadzadegan

Contents

Figures

Tables

Abbreviations

2G	Second Generation mobile networks
3G	Third Generation mobile networks
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
4G	Fourth Generation mobile networks
AAA	Authorization, Authentication and Accounting
AAS	Adaptive Antenna System
AAT	Advanced Antenna Technology
AC	Access Category
ACK	Acknowledge
ACM	Adaptive Coding and Modulation
ACs	Access Categories
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AIS	Artificial Immune System
AK	Authorization Key
AKA	Authentication and Key Agreement
AKID	Authentication Key Identifier
AMC	Adaptive Modulation and Coding
AMR	Adaptive Multi Rate
AP	Access Point
AR	Access Router
ARQ	Automatic Repeat Request
AS	Authentication Server
ASN	Access Service Network
ASN	Abstract Syntax Notation
ASN-GW	Access Service Network Gateway
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AUTN	Authentication Token
AV	Authentication Vector

AWGN	Additive White Gaussian Noise
BCID Basic	Connection Identity
BE	Best Effort
BER	Bit Error Rate
BLER	Block Error Rate
BPSK	Binary Phase Shift Keying
BR	Bandwidth Request
BRAS	Broadband Access Server
BS	Base Station
BSID	Base Station Identity
BW	Bandwidth
BWA	Broadband Wireless Access
CA	Certification Authority
CAC	Call Admission Control
CACBQ	Channel Aware Class Based Queue
CAPF	Cost Adjusted Proportional Fair
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CELP	Code Excited Linear Prediction
CID	Connection Identifier
CINR	Carrier to Interference plus Noise Ratio
CK	Cipher key
CMAC	Cipher Message Authentication Code
CMIP	Client-MIP
COA	Care-of-Address
COTS	Commercial Off-The-Shelf
CPE	Consumer Premises Equipment
CPS	Common Part Sublayer
CQI	Channel Quality Indicator
CQICH	Channel Quality Indicator Channel
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CS	Convergence Sublayer
CSC	Connectivity Service Controllers
CSCl	Convegence Sublayer Classifiers
CSMA CA	Carrier Sense Multiple Access with Collision Avoidance
CSN	Connectivity Service Network
CSP	Common Part Sub-layer
CSs	Service Classes

CW	Contention Window
CS	Circuit-Switched
CSCF	Call Service Control Function
CSG	Closed Subscriber Group
DAD	Duplicate Address Detection
DCD	Downlink Channel Descriptor
DCF	Distributed Coordination Function
DER	Distinguished Encoding Rule
DES	Data Encryption Standard
DFR	Decode and Forward Relay
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DHMM	Dynamical Hierarchical Mobility Management
DIAMETER	Protocol extending RADIUS
DiffServ	Differentiated Service
DL	Downlink
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense
DoS	Denial of Service
DSA-REQ	Dynamic Service Addition request
DSA-RSP	Dynamic Service Addition response
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication and Key Agreement
EAPOL	EAP over LAN
EAP-TTLS	EAP-Tunneled Transport Layer Security
EC	Encryption Control
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
EDF	Earliest Deadline First
EFR	Enhanced Full Rate
EIK	EAP Integrity Key
EKS	Encryption Key Sequence
ertPS	Extended Real Time Polling Service
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EAP-AKA	Extensible Authentication Protocol-Authentication and Key Agreement
ECC	Ellipse Curve Cipher
EDGE	Enhanced Data Rate for GSM Evolution

eNB	eNodeB
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS AKA	Evolved Packet System Authentication and Key Agreement
FA	Foreign Agent
FBack	Fast Binding Acknowledgment
FBSS	Fast Base Station Switching handover
FBU	Fast Binding Update
FCH	Frame Control Header
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIFO	First In First Out
FPC	Fast Power Control
FTP	File Transfer Protocol
FUSC	Full Usage of Subchannels
GKDA	Group-based Key Distribution Algorithm
GKEK	Group Key Encryption Key
GKMP	Group Key Management Protocol
GMH	Generic MAC Frame Header
GPC	Grant Per Connection
GPRS	General Packet Radio Service
GSA	Group Security Association
GSAID	Group SAID
GSM	FR GSM Full rate
GSM	Global System for Mobile Communications
GTEK	Group Traffic Encryption Key
GTK	Group Transient Key
GERAN	GSM EDGE Radio Access Network
GUTI	Globally Unique Temporary Identity
HA	Home Agent
HAck	Handover Acknowledgment
HAP	High Altitude Platform
HARQ	Hybrid Automatic Repeat Request
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HCS	Header Check Sequence
HDR	High Data Rate
HDTV	High-definition TV

HHO	Hard Handover
HI	Handover Initiation
HIPERMAN	High Performance Radio Metropolitan Area Network
HMAC	Hash Message Authentication Code
HNSP	Home Network Service Provider
HO	Handover
HOA	Home-of-Address
HOKEY	Handover Keying (Group)
HoL	Head of Line
HSPA	High-Speed Packet Access
HSPA+	Evolved HSPA
HT	Header Type
HUF	Highest Urgency First
HeNB	Home eNodeB
HN	Home Network
H2H	Human to Human
ICV	Integrity Checking Value
ID	Identifier
IE	Information Element
IEEE	Institute of Electrical & Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange (protocol)
ILBC	Internet Low Bit rate Codec
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISI	Intersymbol Interference
ISO	International Standard Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IV	Initialization Vector
IBC	Identity Based Cryptography
I-CSCF	Interrogating-CSCF
IMPI	IM Private Identity
IMS	IP multimedia subsystem
IK	Integrity Key
IKEv2	Internet Key Exchange Protocol Version 2
ISIM	IMS Subscriber Identity Module
KDF	Key Derivation Function
KGC	Key Generate Centre
KEK	Key Encryption Key

L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LDPC	Low Density Parity Check
Link ID	Link Identifier
LOS	Line of Sight
LRC	Low Runtime Complexity
LTE	Long Term Evolution
M3	Mesh Mobility Management
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MAP	Media Access Protocol
MAP	Mesh Access Point
MBRA	Multicast and Broadcast Rekeying Algorithm
MBS	Multicast and Broadcast Service
MCS	Modulation and Coding Scheme
MDHO	Macro Diversity Handover
MIB	Management Information Base
MIC	Message Integrity Code
MICS	Media-Independent Command Service
MIES	Media-Independent Event Service
MIH	Media-Independent Handover
MIHF	Media-Independent Handover Function
MIHU	Media-Independent Handover User
MIIS	Media-Independent Information Service
MIM	Man In the Middle
MIMO	Multiple Input Multiple Output
MIP	Mobile IP
MMR	Mobile Multi-hop Relay
MMS	Multimedia Messaging Service
MN	Mobile Node
MOS	Mean Opinion Score
MP	Mesh Point
MPDU	MAC Protocol Data Unit
MPEG	Moving Picture Expert Group
MPP	Mesh Portal Point
MRR	Minimum Reserved Rate
MS	Mobile Station
MS	Mobile Subscriber Station
MSB	Most Significant Bit

MSCHAPv2	Microsoft Challenge-Handshake Authentication Protocol
mSCTP	Mobile Stream Control Transmission Protocol
MSDU	MAC Service Data Unit
MSE	Mean Square Error
MSID	Mobile Station Identifier
MSK	Master Session Key
MSO	Multi-Services Operator
MSR	Maximum Sustained Rate
MSS	Mobile Subscriber Station
MTK	MBS Traffic Key
MVNO	Mobile Virtual Network Operator
ME	Mobile Equipment
MME	Mobility Management Entity
MTC	Machine Type Communication
M2M	Machine to Machine
NAP	Network Access Provider
NAP	Network Access Point
NAR	New Access Router
NBR	Neighbor
NCoA	New Care of Address
NGWS	Next Generation Wireless System
NLOS	Non Line-of-Sight
NMS	Network Management System
Node ID	Node Identifier
NRM	Network Reference Model
nrtPS	Non-Real-Time Polling Service
NSP	Network Service Provider
NSSK	Needham Schroeder Secret Key Protocol
NTSC	National television System Committee
NWG	Network Working Group
NAS	None Access Stratum
NCC	NH chaining counter
NDS	Network Domain Security
NGN	Next Generation Network
NH	Next Hop
OCSP	Online Certificate Status Protocol
O-DRR	Opportunistic- Deficit Round Robin
OFDM	Orthogonal Frequency Division Multiplex
OFDM2A	Orthogonal Frequency Division Multi-hop Multi-Access
OFDMA	Orthogonal Frequency Division Multiple Access
OSS	Operator Shared Secret

OTA	Over-The-Air
P2MP	Point to Multi-Point
PAR	Previous Access Router
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCoA	Previous Care of Address
PDAs	Personal Digital Assistants
PDU	Protocol Data Unit
PEAP	Protected EAP
PEAQ	Perceptual Evaluation of Audio Quality
PER	Packet Error Rate
PESQ	Perceptual Evaluation of Speech Quality
PF	Proportionate Fair
PFMR	Proportional Fair with Minimum/Maximum Rate Constraints
PHS	Packet Header Suppression
PHY	Physical Layer
PKC	Public Key Certificates
PKM	Privacy Key Management
PKM-REQ	PKM Request
PKM-RSP	PKM Response
PKMv1	Key Management Protocol version 1
PKM second edition	Key Management Protocol version 2
PM	Poll Me bit
PMIP	Proxy-MIP
PMK	Pairwise Master Key
PMM	Packet Mobility Management (protocol)
PMP	Point to Multipoint
PN	Packet Number
PoA	Point of Attachment
PPP	Point-to-Point
PPPoE	Point-to-Point Protocol over Ethernet
Pre-PAK	pre-Primary Authorization Key
PrRtAdv	Proxy Router Advertisement
PS	Privacy Sublayer
PSK	Pre-Shared Key
PSNR	Peak Signal to Noise Ratio
PSOR	PF Scheduling for OFDMA Relay Networks
PSTN	Public Switched Telephone Network
PTK	Pairwise Transient Key

PTP	Point To Point
PUSC	Partial Usage of Subchannels
P-CSCF	Proxies-CSCF
PDN GW	Packet Data Network Gateway
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QoS	Quality of Signal
OAM	Operation, Administration and Maintenance
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RAND	Random Number
RC	Resource Controller
REG-REQ	Registration Request
REG-RSP	Registration Response
REQ	Request
RES	Result
RF	Radio Frequency
RLC	Radio Link Control
RNG-REQ	Ranging Request
RNG-RSP	Ranging Response
RNM	Reference Network Model
ROC	Rollover Counter
RP	Reference Point
RR	Round Robin
RRA	Radio Resource Agent
RRC	Radio Resource Control
RRM	Radio Resource Management
RRP	Registration RePly
RRQ	Registration ReQuest
RS	Relay Station
RSA	Rivest, Shamir, and Adelman
RSP	Response
RSS	Received Signal Strength
RSSI	Received Signal Strength Indication
RTG	Receive/Transmit Transition Gap
rtPS	Real Time Polling service
RtSolPr	Router Solicitation for Proxy Advertisement
SA	Security Association
SAID	SA Identifier
SAP	Service Access Point
SBC-RSP	SS Basic Capabilitiy response

SC	Single Carrier
SCN	Service Class Name
SCTP	Stream Control Transmission Protocol
SDU	Segment Data Units
SeS	Security Sublayer
SFID	Service Flow IDentifier
SGKEK	Sub-Group Key Encryption Key
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SINR	Signal to Interference-plus-Noise Ratio
SIP	Session Initiation Protocol
SIR	Signal to Interference Ratio
SMS	Short Message Service
SNIR	Signal to Noise + Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SOFDMA	Scalable Orthogonal Frequency Division Multiple Access
SR	Superior Router
SS	Spectrum Sharing
SS	Subscriber Station
SSCS	Service Specific Convergence Sublayer
SSID	Service Set Identifier
STS	Sub-channels of a Time Slot
SVM	Support Vector Machine
S-CSCF	Serving-CSCF
SGW	Serving Gateway
SeGW	Security Gateway
SGSN	Service GPRS Supporting Node
SN	Serving Network
SN ID	Serving Network Identity
SQN	Sequence Number
TCP	Transmission Control Protocol
TrE	Trust Environment
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
THBA	Two-level Hierarchical Bandwidth Allocation scheme
TLS	Transport Layer Security
TLV	Type-Length-Value
TPP	Two-Phase Proportionating

TR	Transmit Receive
TTG	Transmit/Receive Transition Gap
TTLS	Tunneled Transport Layer Security
TTP	Trusted Third Party
TXOP	Transmission Opportunities
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UGS-AD	Unsolicited Grant Service-Activity Detection
UL	Uplink
UL-MAP	Uplink MAP
UMTS	Universal Mobile Telecommunications System
UNA	Unsolicited Neighbor Advertisement
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UMTS-AKA	UMTS-Authentication and Key Agreement
USIM	Universal Subscriber Identity Module
VBR	Variable Bit Rate
VCEG	Video Coding Experts Group
VHDA	Vertical Handoff Decision Algorithm
VHO	Vertical Handover
VNSP	Visited Network Service Provider
VoD	Video on Demand
VoIP	Voice over IP
W2-AP	WiMAX/WiFi Access Point
WBA	Wireless Broadband Access
WEIRD	WiMAX Extension to Isolated Research Data networks
WEP	Wired EquivalentPrivacy
WFPQ	Weighted Fair Priority Queuing
WFQ	Weighted Fair Queuing
Wibro	Wireless Broadband
WiFi	Wireless Fidelity
Wireless Man	Wireless Metropolitan Area Network
Wireless HUMAN	Wireless High Speed Unlicensed Metropolitan Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WiMESH	WiMAX Mesh
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WRI	WiMAX Roaming Interface
WRR	Weighted Round Robin

WRX	WiMAX Roaming Exchange
WWAN	Wireless Wide Area Network
XDSL	X Digital Subscriber Line
XML	Extensible Markup Language
XRES	Expected Response

1 INTRODUCTION

Interactive communication between people makes the nature of humanity. Telecommunication system is comprised of three parts being the transmitter, the channel and the receiver. The channel can be either wired with restricted mobility or wireless with more mobility freedom. Now the important objective here lies in the fact that, how one transmits the information so that the integrity would be preserved. The approach which one has to take for protecting the information that is being sent, is actually a set of policies and defined rules labeled and regarded as "security" measures. Several technologies and data communication networks have been developed up until now and some of them were targeted to provide high speed broadband access but they struggled more or less when it came to security issues.

Worldwide interoperability for microwave access or WiMAX is one of those emerging technologies that offers high speed transmission of information. The Wireless MAN or IEEE 802.16 that later was named by WiMAX forum as "WiMAX", operates ubiquitously in associated licensed or non-licensed spectrum between 2 and 66 GHz (Roger B. Marks 2006). The role of the WiMAX Forum (WiMAX Forum 2009) is to deal with the certification of implementations and designing more techniques for networking like mutual authentication and integration related issues with other wireless technologies.

In telecommunication field, WiMAX technology became prominent as a result of its wide coverage of applications. WiMAX is an access technology such as Gigabit Ethernet. On top of that and based on IP protocols one may use any applications like Internet Protocol Television (IPTV) and Voice over Internet Protocol (VoIP). Due to the fact that VoIP services can be provided under the WiMAX framework, the means for secure communication and VoIP threats together with vulnerabilities will be discussed and analyzed throughout the way.

WiMAX 802.16 has two layers of protocol stack being the medium access control layer together with the physical layer. The medium access control layer is in charge of security and connections. The physical layer manages error correction and connectivity of the signals together with ranging, bandwidth requests, and connection channels. The physical layer is comprised of a set of identical frames dispatched through the modulation of radio frequency signals. Moreover, 802.16 has the required flexibility to support various traffic types in the transport layer (C. Ecklund et al. 2002). When it comes to WiMAX, up until now the main emphasis was on security in medium access control layer, but the problem is that the

provided security is not enough to meet the existing demands of multi-hop cases (Kejie Lu et al. 2007).

The architecture of WiMAX, security of the standard, its security factors and the associated attacks and threats will be investigated thoroughly. Furthermore a new alternative classification and analysis of WiMAX security attacks would be provided. Moreover, a carried out comparison with LTE and WiFi has been performed and because of the fact that the security and number of simultaneous users naturally affect the performance, this degradation has been described by the Kiyotaki-Moore model. In addition to this, as a countermeasure to the threats, an alternative energy efficient WiMAX-based intrusion detection system has been proposed.

1.1 Motivations of This Research

The main motivations of conducting this research topic can be presented as follows:

1.1.1 Evolution of the Wireless Access Networks

Nowadays wireless access networks are very important and play an essential role in many aspects of our life. The common systems deployed for voice telephony on a global scale like GSM, CDMA2000 and UMTS voice-mode utilize connection-oriented switching and transmission technology. The newly appearing systems for video distribution deploy broadcast-specific transmission technology. The present generation of mobile Third Generation (3G) wireless access systems which provide Internet data services such as CDMA 1xEVDO and UMTS HSPA are mainly for applications of file transfer and browsing web (C. Smith 2000). The chief differences among these wireless access networks when it comes to technical issues are not tangible from consumer's perspective. In this era it can be observed that having access to multiple wireless networks is packed into a single integrated mobile customer device (W. H. Lehr et al. 2010).

The large scale popularity and utilization of IP-based wireless 3G networks may imply that wireless architectures are resulting in a convergence of wireless and wired network architectures. The reality is that this interpretation is wrong (D. Goodman 2011). There is no service provider to say that they intend to offer corporate video or voice broadcast services as an unnecessary application over its IP platform. It is not foreseen that usage of fourth generation networks will alter this basic dynamic. The fourth generation systems which are emerging and prevalent

are WiMAX together with LTE that are an IP-based networks having distinguished potentials together with a platform network architecture (Bogineni et al. 2009). Beside the fact that WiMAX and LTE provide remarkable enhancements in spectral efficiency compared to present 3G systems, they further enable increased capabilities per user that will lead to a remarkable growth of demand. A meticulous investigation of the balance among technology enhancements and user demand growth resulted in the fact that meeting user demand will need an extra 500 to 1000 MHz of commercial spectrum in the USA by 2020, all below 5 GHz (ITU 2006). Taking into account that governments seriously consider their need for spectrum increasing, and having observed the challenges of clearing the already dedicated spectrum, it is not realistic to think that this demand will be achieved by new allocations. Therefore one can draw a conclusion that 4G systems will have capacity limitations like present wireless access networks, thus the inefficiencies related to executing all the services over the top of a common platform will keep on not being feasible economically. This is the outcome which commercial providers speculate. For instance, there has been a considerable effort to integrate "voice fallback" capability into the WiMAX and LTE standard, making the service providers become able for coupling a dedicated voice network like a new design more efficient than GSM with their WiMAX or LTE network (S. Donegan et al. 2009; W. H. Lehr et al. 2010). In this dissertation WiMAX is the center of attention and investigations.

1.1.2 Security Concepts in Data Networks

When it comes to security in any type of data networks including wireless data access networks, three key issues are required to be addressed:

- Confidentiality: it is aimed to make sure that one message has not been seen by anyone other than the intended receiver. For example, the number of a credit card is confidential and its security must be preserved when it is transmitted via the Internet. An instance of how confidentiality works can be the data encryption: an encrypted message can just be seen in case a key is applied to the message that is known by the sender and the receiver like HTTPS-protocol between workstation and server when buying airline tickets from ebookers.com, where HTTPS creates secured tunnel end-to-end thus relaxing access networks from this burden.

- Authentication: when an identity is claimed, authentication is in charge of verifying it. For example, when it comes to utilizing a bank account, it is critical that just the real owner of the account

gain access to it. There are numerous sources which offer authentication. The simplest instance can be username/password-based system.

- Integrity: the completeness of the information should be maintained and it has to be free from any deliberate or accidental manipulations. Integrity is in charge of making sure that data is complete and that it is not changed while sending from sender to receiver takes place. For example data integrity is aimed to make sure that an electronic transference is carried out with the required amount of money. An instance of the mechanism for assuring about the data integrity can be the digital signature when it comes to an email that is an encryption method which ascertains us about the message's author and the fact that its content is intact (Security in WiMAX 802.16-2009 network Albentia Systems 2011).

1.1.3 Motivations for Research on WiMAX Security

Security is of great importance in data networks, but it is even more critical in wireless networks, and particularly when it comes to WiMAX technology. Some of the main reasons are mentioned as follows:

1- In case of wired networks, it can be difficult to illegally access the network as a result of the fact that a physical connection with cable is needed. WiMAX is counted among wireless technologies and thus data are sent by radio waves.

2- WiMAX is regarded as an outdoor technology capable of delivering services for covering large areas. Therefore these large areas are prone to an unauthorized access.

3- WiMAX was not primarily defined to be a Local Area Network (LAN) technology. Its initial intended usage was for MAN/WAN networks. WiMAX technology is for offering simultaneous services to multiple users. Thus, user's privacy and access privilege should not be violated and users must not be authorized to access other users' information.

4- Like in any other networks, if someone suspicious gets into our network, there are definitely several risks that can be threatening. For example, the Internet connection can be utilized without permission,

computers and files may be seen or e-mails, passwords, etc. may be sniffed. Therefore an absolute control over the network access is an essential issue.

5- It can be agreed that if a wireless unauthorized intrusion is regarded as rather dangerous in a private or personal network, it has even worst impact when it comes to a governmental, corporative or especially when it comes to military deployment that are usual WiMAX scenarios. Most essential environments and applications need high security alertness and WiMAX must be capable to offer that (Security in WiMAX 802.16-2009 network Albentia Systems 2011).

The above-mentioned five motivations are considered adequate from this dissertation's perspective to select this important topic and strive to carry out more research in the field and try to address these issues respectively.

1.2 Dissertation Research Problem

The main research problem of this dissertation can be defined as keeping the security in the WiMAX framework in various situations and its protection against numerous attacks. Other research problems maybe how the detection and mitigation can take place in order to protect the network in early stages. In order to deal with the above-mentioned problems one needs to have a clear classification and modeling of the existing threats and to achieve:

1- The first is to provide a well-investigated anthology of security issues and threats existing in WiMAX and by this contribute to a better understanding and comprehension of the subject.

2- The second aim is to study the behavior of this technology in different security scenarios.

3- The third goal was to determine the lacks and shortages when it comes to WiMAX and its associated security problems, so that suitable and relevant measures could be taken to act against them.

4- The fourth target of this dissertation has been taking alternative approaches and suggesting some ideas to apply in scenarios related with those cases.

1.3 Dissertation Research Methodologies

In this dissertation, a comprehensive theoretic security approach has been provided in such a way that security is at the center stage of each investigation and discussion. The theoretic notions are utilized in running comparative sort of analysis. The dissertation tries to verify the key findings by scientific judgment and interpretation, running attacks and validation tests. As a result of relying on this approach, the dissertation can be well comprehended and easy to read. Other aspect of the dissertation is the fact that notions and ideas which can be realized but are purely based on specific conditions to take place will not be taken into account. For instance there are some attacks and threats that can happen in huge networks having heavy loads with continental scales like Botnet army attacks which is beyond the scope of this dissertation and instead security issues that are based on real problems with which WiMAX technology encounters would be discussed.

1.4 Dissertation Contributions

Some of the results of this dissertation have been published in 4 IEEE conference papers and one journal paper in International Journal of Computer and Communication Engineering, IASCIT press (M. Hossein Ahmadzadegan et al. 2013). Furthermore, one paper has been submitted to IEEE Transaction journal. More papers could be submitted later. The contributions of this dissertation can be divided into the following three main areas:

- Proposing new classifications and modeling's of the security threats and attacks in two cases. One is the general attacks against WiMAX and the other is the security attacks and threats while offering VoIP services under the framework of the WiMAX network represented in Figure 18.

- Proposing a comparative analysis of the security basics, components and characteristics of next generation networks such as WiMAX, WiFi and LTE together with description of their deployment choice

- Proposing a new alternative WiMAX-specific intrusion detection system for the attack detection and prevention with structure explanations and functioning mechanism together with verifying its performance and running DoS attack for result validation and verification using NS2 simulator and Toshiba consumption analyzer. The proposed WiMAX-based intrusion detection system which has been presented is also power efficient. The carried out NS2/Toshiba simulations prove this claim. Moreo-

ver the amount of power savings and thus efficiency obtained are computed as well. The topic is covered in chapter 4 and chapter 6.

- The impact of the classification and modeling on security threat mitigation

One of the main contributions of this dissertation is its emphasis on the advanced classification of the security attacks and threats together with labeling them according to the risk they impose and the likelihood of their happening. In the technical literature, security analysis has mainly concentrated on the attacks which have been performed to challenge the system and therefore in some cases ignoring the possible impact of having an integrated comprehensive attack anthology for grouping the threats. Handling the security problems of a system requires great focus and attention. It is very important to analyze the threats and based on its characteristics choose the relevant countermeasure. Some attacks are similar in their essence and there is the possibility of taking similar actions to deal with them. As shown in this dissertation, it will be demonstrated how classification and modeling the security threats and attacks contributes to a better detection, protection and mitigation. This dissertation illustrates the importance of classifications in detection and mitigation by showing how significantly the security and thus the performance will decrease if the breaches and threats are not detected in early stages. Threat detection can be carried out utilizing some algorithms as shown in this dissertation thus drastically increasing the level of protection. Investigation of the security threats in some scenarios are included into this dissertation. Also, the behavior of the attacks are studied down the process after the classification and the risks are given attention.

- The role of comparative analysis in better protecting the next generation networks

This dissertation presents the extent of usefulness of comparative analysis when it comes to next generation networks. It is critical to understand that while going down the process there is a matter of options implying what technology to choose for better meeting the requirements of the end-user or the operator. Therefore by listing the security basics and properties of WiMAX, WiFi and LTE it is clarified which technology is superior having considered the background and goals of usage. The architectural aspects together with differences when it comes to dealing with security issues are discussed as well. It is foreseen that by summing up the most important characteristics of each technology a far better judgment can be deployed to deal with these 4G technologies

- Proposed IDS technique to detect and treat the threats

A new technique has been proposed according to the previous available literature (B. Zhou 2011) to detect and deal with the security threats in order to maintain a high level of security and performance. The technique and the know-how of its functioning is introduced and analyzed. In addition to this some analysis and simulations have been done by the aid of NS2 simulator and Toshiba consumption analyzer to asses and demonstrate its performance. One attack like DoS is also simulated to demonstrate how the proposed system functions.

1.5 Dissertation Outline

Chapter one contains the introductory descriptions and research motivations. Chapter two offers the details of the architecture of WiMAX together with WiMAX security elements and comparisons between other wireless access networks such as WiFi and LTE. Chapter three provides the literature review of the most recent available research findings. Chapter four describes the security of the WiMAX standard and at the end of this chapter LTE security problems together with their solutions are discussed as well. Chapter five and six both discuss the contributions and the details of published scientific papers. In these chapters the applied ideas of the author together with the papers will be demonstrated. Finally, chapter seven comprises dissertation results, their usage and conclusions followed by a proposed future works.

1.6 Original Publications

I. M. Hossein Ahmadzadegan, M. Elmusrati, R. Virrankoski, E. Antila “Security Centric Comparative Study of WiMAX and LTE” The IEEE Vehicular Technology Society, Asia Pacific Wireless Communications Symposium (APWCS), Seoul, South Korea, 2013

In this research work, the differences between emerging technologies being WiMAX and LTE are investigated from the security perspective. The security focus analyses various aspects of the technologies from structures to mechanisms and protocols together with discussions from technical viewpoints. Finally it concludes with an overall look over each one’s advantages and disadvantages. The content has been mainly included in 2.1.2 section page 15 and 4.7 in page 93.

II. M. Hossein Ahmadzadegan, M. Elmusrati “Hybrid Security Classification Approach to Attacks in WiMAX” IEEE International Conference on Signal Processing, Computing and Control (ISPCC), Shimla, India, 2013

In this research work, concentration has been on the detailed classification of the security attacks and threats together with labeling them based on an hybrid approach being the risk they impose and the likelihood of their happening. The classifications are integrated and reduced to four groups and each threat is investigated throughly. It is covered in chapter 4 page 52 and chapter 5 page 101.

III. M. Hossein Ahmadzadegan, M. Elmusrati "WiMAX-Based Energy Efficient Intrusion Detection System" IEEE International Conference on Robotics, Biomimetics, & Intelligent Computational Systems (ROBIONETICS), Yogiakarta, Indonesia, 2013

In this research work, a novel IDS technique has been proposed according to the previous literature to detect and deal with the security threats for maintaining a robust security level and performance within WiMAX. The technique and the know-how of its functioning is introduced and analyzed. Moreover some investigations and simulations have been performed through NS2 simulator and Toshiba consumption analyzer to test and approve its performance. It is explained in chapter 4 and 6.

IV. M. Hossein Ahmadzadegan, M. Elmusrati "Kiyotaki-Moore Approach to Performance Devolution in Mobile WiMAX" IEEE 5th International Congress on Ultra-Modern Telecommunications and Control Systems (ICUMT), Almaty, Kazakhstan, 2013

In this research work, it is proved that within 802.16, the security and number of simultaneous users affect the performance of the WiMAX network. This performance devolution and behavior of the system has been described by an economic theory the Kiyotaki-Moore model. The topic is covered in chapter 6, page 122.

V. M. Hossein Ahmadzadegan, M. Elmusrati, and H. Mohammadi, ("Secure Communication and VoIP Threats in Next Generation Networks"), *International Journal of Computer and Communication Engineering* vol. 2, no. 5, pp. 630-634, IASCIT Press, 2013

This research work discusses and classifies the attacks in case of VoIP services in wireless access and WiMAX-specific situation proposing a new model in Figure 18. It explains all the attacks and briefly describes them in each case. The topic has been covered in chapter 5, page 101.

2. ARCHITECTURE AND SECURITY COMPONENTS OF 802.16

2.1 Wireless Access Networks and WiMAX

When wireless data connections are utilized for connecting network nodes then that computer network can be regarded as a wireless access network. Nowadays wireless networking is an alternative way that telecommunications networks, business setups and homes deploy in order not to go through the process of cable installations in buildings that also requires spending a lot of money (Wireless overview 2008). Today radio communications are utilized to implement and manage wireless telecommunications networks. The physical layer of the OSI model is where the implementation occurs (Zimmerman 1980). Some instances of wireless networks among others are Wi-Fi local networks, cell phone and terrestrial microwave networks. In our era there are many ways for establishing a connection to the Internet. One way is the wireless Internet service which offers Internet access to customers without requiring any fiber, copper cables or any other network cabling. Wireless technology provides more mobility and convenience to computer networks if one compares it with cable internet and other wired services like DSL. Different common kinds of wireless Internet services available are described as follows:

Public WiFi Networks

Wi-Fi technology has been utilized in various municipalities for providing public wireless access services. Mesh networks are canonic points where several wireless access points (AP) come together to cover larger areas. In addition to this WiFi hotspots are offering public wireless Internet service in some locations too. Among providers of wireless Internet service WiFi is considered a low-cost option. Its related equipment is cheap and WiFi hotspots are free in some locations. Since availability is counted among key issues in WiFi as one cannot find public WiFi access in most rural and suburban areas. There is another form of wireless access regarded as Super WiFi which is different from WiFi. It is also famous as white spaces technology. Super WiFi performs over another part of the wireless spectrum and uses different radio spectrum than WiFi. White spaces technology has not been utilized widely and is expected not to become a popular choice of wireless.

Satellite Access

Satellite access came up for the first time in 1994 and became the first mainstream consumer wireless access service. Initially satellite access was taking place just for downloading information and thus it was a one-way operation. Users required to setup a dialup modem and utilize a telephone line associated with the satellite to get the system working and gain satellite access. Later on novel forms of satellite service came up and offered two-way connectivity as well. When it comes to wireless Internet service, satellite has the advantage of availability. By simply having a small dish antenna, a modem and subscription plan, this system of access performs acceptable even in rural zones where no other technologies are within reach. It should be also mentioned that satellite's setback is that it provides comparably low performing wireless Internet. This is because satellite is affected by high rate of latency in connections as result of the fact that far away distances should be traveled by signals among the orbiting stations and earth. Satellite also offers a nearly modest network bandwidth.

Fixed Wireless Broadband

WiFi hotspots or satellite access are different from fixed wireless broadband. Fixed wireless is a kind of broadband which deploys mounted antennas directed toward the towers of radio transmission.

Mobile Broadband

It is known that cell phones have been used for decades but it should be highlighted that just since the last 15 years the cellular networks have become able to offer wireless Internet service. Therefore by the aid of an already installed cellular network adapter, or plugging a cell phone to a laptop computer, one can keep on having Internet connectivity until when it resides within cell tower coverage. It should be mentioned that previous cellular communication protocols in the past years did permit networking but with a low speed. Third generation cell technologies such as UMTS and EV-DO bring about delivering network speeds much closer to DSL. Nowadays cellular providers and their access subscription plans are sold mainly separate from their voice related network contracts. WiMAX is considered being among new types of wireless access networks. It deploys base stations like in case of cellular networks, but the difference is that WiMAX is defined particularly to offer services and data access rather than voice phone communications. It is expected that as WiMAX becomes more widely used, it can provide roaming capability and offers a much better performance networking experience compared to satellite and it costs cheaper as well (B. Mitchell About Technology, 2012).

2.1.1 WiMAX versus WiFi

In addition to the mentioned issues, WiMAX has many advantages over WiFi which is another wireless access technology. Chief differences are listed as follows:

- Coverage: The WiMAX base station can offer coverage for as many as hundreds of users simultaneously together with administration of the transmission and reception of data at very high rates preserving network security whereas WiFi is restricted in terms of offering services and its coverage range is limited (O. Kharif 2003;Free WiMAX info 2012).

- High Speed: The quick connectivity speed over remote distances and offering high speed voice makes it more ideal in all areas including scattered populated and residential zones as well whereas WiFi cannot compete with WiMAX in this respect (T. Willson 2008).

- Multi-functionality: WiMAX carries out a wide range of applications simultaneously like offering quick speed internet, video streaming, telephone service and voice applications among others.

- Development and potentials: WiMAX has been a remarkable technology counted among the next generation networks because it has adequate potential for developing and ability to provide diverse services to users. One is able to establish a connection to Internet anywhere and browse any site and experience online conferencing with mobile Internet.

- Keep being in contact with the user: WiMAX network makes it possible to stay in contact with your friends deploying same WiMAX network as a result of the fact that it offers absolute communication service to the end users for seamless communications to be fulfilled.

- Infrastructure: The 802.16 infrastructure is very easy to work with and flexible at the same time thus it offers maximum reliability of network.

- Cheap network: Today WiMAX is a famous wireless network due to offering a low cost network replacement alternative for Internet services provided by local area network or ADSL.

- Rich features: WiMAX is indeed providing rich features that makes it even more demanding and practical. WiMAX comes up with dedicated voice and data channel for fun. Moreover it brings about fast connectively, freedom of movement and license spectrum among many others.

- Smart antenna and mesh topology: The smart antenna utilization in 802.16 network providing high quality widest array that enables one to make possible communication on far routes without any ciphering. It provides 2.3, 2.7, 3.3 and 3.8 GHz frequency ranges. The deployment of mesh topology in 802.16 network for the expansion is an extensive spectrum of antennas for residential and commercial users (Free WiMAX Info 2012).

- Ultra wide band: the unique infrastructure of WiMAX is providing Ultra-Wideband. Its design is offering range from 2 to 10 GHz and with an acceptable time response.

- Homeland security: when it comes to security, WiMAX also provides high security due to utilization of AES-based encryption systems. Thus one can transmit data throughout the network without having preoccupations (Free WiMAX Info 2012).

Here a brief analysis is carried out on WiMAX and WiFi to justify why WiMAX has been chosen from a security perspective:

1) Authentication: when it comes to authentication in WiMAX, it should be highlighted that due to using X.509 certificates and the digital signatures, it is indeed reliable. The authentication mechanism defines every user that is striving to enter the cell and also the dynamic keys that alter regularly together with the automatic re-authentication requests in the BS. These certificates cannot not be forged and provide protection against any unauthorized body from entering the WiMAX cell. Utilizing WEP encryption/authentication technology which deploys static keys has lead into an unfortunate security setback in WiFi, since it has become remarkably susceptible. Today any network deploying this system is prone to various kinds of cracking attacks. Even though WPA and WPA2 have addressed and settled the problems of the WEP mechanism, WiFi equipment should be rather modern to deploy them, thus older network equipment can just rely on WEP.

2) Encryption: it is to be highlighted that WiMAX utilizes basic block ciphers: AES and DES. It is the the way of selecting, transposition and association of the blocks in a message that determine the complexity of the algorithms. WiMAX deploys CBC (AES), CBC (DES), CCM (AES) and CTR (AES). For these methods, it is not the matter of being superior technologically compared with WiFi's, but that they are deployed correctly, for instance they utilize dynamic keys that expire after a time to live and are renewed automatically, without repeating initialization vectors, encrypting every SS's service flow independently, etc... . WEP

and WPA in WiFi have demonstrated to have security breaches when it comes to encryption, and just in case WPA2 is used then they can offer encryptions as strong as WiMAX.

3) Medium Access: the technology plays an important role and affects the security to a large extent. WiMAX offers a deterministic Medium Access that is permanently supervised by the base station. One can observe that when it comes to WiMAX, no station can send even a single bit if it has not been permitted before by the base station, thus the radio spectrum is supervised automatically and various types of attacks are prevented. Other wireless access technologies such as WiFi and its MAC layer that is CSMA/CA-based, utilize unsupervised and random Medium Access that results in a situation that any user floods the air with traffic, when it is not registered in the Access Point (AP). This causes these networks to be more susceptible to various Denial of Service intrusions.

4) Operator technology: WiMAX was not defined and intended to be used as a LAN technology, it has been invented to be an operator technology for WAN or MAN (Wide-Area, Metropolitan) networks. This means service to multiple independent users, wide coverage areas … and thus the WiMAX standard developers were alert regarding the security of this technology. WiFi differs a lot as a technology and has been designed for other usages: it is particularly designed for small local networks, so it was "born with lacks" when it comes to security aspects. WiFi is an affordable and cost-saving technology for the people around the globe. WiFi obviously has several advantages but it introduces some risks too, for instance when the number of users increase, it is normal to expect that more intruders and hackers will pop-up. If one searches the hacker communities, those who did focus on WiFi networks are a lot and even several programs are written to break into WiFi, whereas WiMAX has proved to be well-armed against existing threats.

5) Additional security not needed: security breaches and lacks when it comes to other technologies may be addressed by deploying extra equipment and servers or high level security protocols: Kerberos, Radius, EAP, PAP(LDAP), … It is clear that these "external" elements undoubtedly boost the security but cause additional costs and need extra equipments. If like WiMAX, many security mechanisms are already integrated into the technology, then it will be more feasabile to use a secure network without needing other methods (Security in WiMAX 802.16-2009 network Albentia Systems 2011).

2.1.2 WiMAX versus LTE

WiMAX or Worldwide Interoperability for Microwave Access is a wireless technology regarded as the IEEE 802.16 standard. The main aim for IEEE 802.16 standard is to offer broadband wireless access. WiMAX brings about some remarkable features like scalability, mobility, high data rates, quality of service and security.

Long-term evolution or LTE, is a rapid growing fourth generation standard for wireless communication, when it comes to mobile phones. In this dissertation we are going to come up with a comparative perspective to the security problem in both technologies and analyze their security architecture and features to determine their advantages and disadvantages. All the investigations are security-based. This research work can pave the way for a better understanding and having a more accurate picture of these two forth generation technologies and their differences. Such a comparative insight meticulously addresses the notion of technology application and usage.

This further clarifies the essential selection of the technology considering the requirements and existing infrastructure. It can be confirmed that by having a specialized look into the matter one can decide that for an intended network which technology is better to be deployed. Also the implementation itself does have complexities for each of the two technologies. This research addresses to make the selection easier by providing a comparative investigation of both LTE and WiMAX from a security point of view.

The security and architecture of the next generation networks have been the subject of many research projects and academic articles. WiMAX and LTE are among the most emergent wireless technologies belonging to the 4-G family. Due to this fact, indeed the investigation and comparative comparison of these two technologies from a security perspective becomes important. Therefore, the authors have addressed and carried out this comparative research and have highlighted the differences and similarities. So this would provide a precise insight which aids in a better understanding of the subject.

The WiMAX designs a multipurpose network that provides services within wide ranges. The Security of WiMAX is predefined in the Privacy Sublayer of the Reference Model. Below, some critical factors of the IEEE 802.16 Security Architecture are presented (S. Wattanachai 2006):

Authorization SAs comprises the following attributes:

• X.509 certificates. These digital certificates permit WiMAX communication factors to validate each other. The certificates are signed by the device manufacturer.

• Authorization key (AK). AKs are means for authenticating among BSs and MSs before the traffic encryption key (TEK). The authorization SA comprises an identifier and a key value for each and every AK.

• Key encryption key (KEK). The KEK is for encrypting the TEKs during the TEK exchange.

• Message authentication keys. It checks the authenticity of key messages while establishing the keys. These keys are deployed to sign management messages to validate message authenticity as well.

• Authorized data SA list. Given to the SS/MS by the BS, the authorized data SA list demonstrates that data encryption SAs the SS/MS is authorized to access. Data SAs establish the parameters deployed to protect unicast data messages among BSs and SSs/MSs. A data SA comprises the following security attributes:

• SA identifier (SAID). It is a unique 16-bit value that signifies the SA to recognize it from other

SAs.

• Traffic encryption key (TEK). TEKs are generated by the BS and are deployed to encrypt WiMAX data messages. For preventing the communications disruption during TEK rekeying procedure Two TEKs are generated.

• Data encryption SA type detector. This detector signifies the type of data SA. There are three types:

- Primary SA. This SA is defined as a unique connection for each and every SS upon initialization with the BS.

- Static SA: This SA secures the data messages and is generated for each service defined by the BS.

- Dynamic SA: This SA is created and eliminated in reflection to the initiation and termination of some service flows.

Group SAs includes the keying material for securing multicast traffic. Key material has restricted validity duration and is controlled by the BS. The BS informs the SS just after delivering key material. The SS's is in charge of requesting new key material within the validity duration. However, the entire authentication procedure has not to be performed.

Encapsulation Protocol

The Encapsulation Protocol provides the possibility for the data encryption among BS and SS. For this aim, it establishes the cryptographic packages that are cryptographic identifiers specifying authentication mechanism supported by the SS. A complete packet-like set of sequential cryptographic remedies are forwarded to the BS. The set comprises the encryption of data or the algorithm of authentication and encryption for the TEK (D. Johnson et al. 2004).

PKM Protocol

Privacy Key Management Protocol (PKM) is in charge of routine SS authorization, re-authorization and reception or renewal of key material. It is exactly similar to a typical client and server-model where the SS asks for key material from the BS that plays the role of a PKM server. By means of this mechanism, both client and SS just receive key material that is in line with their requirements. The architecture of LTE is categorized into five parts: 1- access security, 2- domain security, 3- user domain security, 4- application domain security, 5- discernibility of the security services. The LTE security architecture is presented in Figure 1. Compared with the security architecture of UMTS network, the differences are presented below: First of all, two-headed arrows are added between ME (Mobile Equipment) and SN (Service Network), which demonstrates that there are non-access-layer security between ME and SN too; Secondly, bi-directional arrow is added between AN and SN highlighting that security communication is desired between AN and SN; Thirdly, the notion of service network certification is injected, therefore one-way arrow has been replaced by a two-headed arrow among HE and SN;

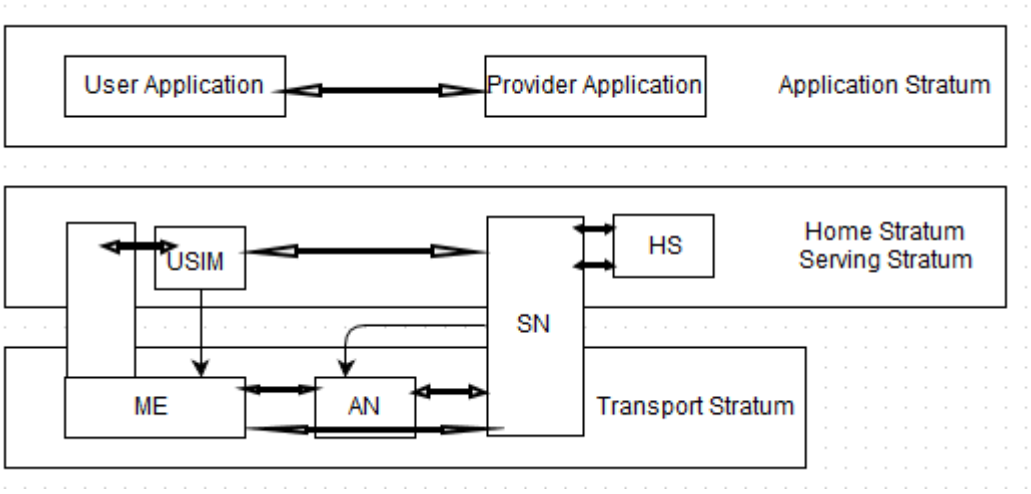


Figure 1. LTE Security Architecture (L. Zhu et al. 2012)

LTE determines a novel layering of security and the enforcement of a clearer separation of control plane security and user plane security offering strong security features. LTE has support for UMTS Encryption Algorithm 1 (UEA1), UMTS Integrity Algorithm 1 (UIA1) and their respective second versions UEA2 (SNOW algorithm supporting 256 bits keys) and UIA2. Signaling at User Plane Entity (UPE) and Mobility Management Entity (MME) relocation permits the transfer of algorithm information to the target UPE, MME and User Equipment (UE) (Ericsson, S3-060705 2006). WiMAX has a powerful encryption mechanism, deploying Advanced Encryption Standard. It also embodies key management protocol and support for privacy issues. The system has an authentication architecture that is in accordance with Extensible Authentication Protocol (EAP), which permits a variety of security issues, like username or password, smart cards and digital certificates (Tutorials Point, WiMAX Silent Features 2010).

When it comes to issues about security both LTE and WiMAX have similar functions but are not identical. LTE and WiMAX have mechanisms together with protocols for making sure that the connections are safe. One can draw a conclusion that LTE is better than the WiMAX when the main focus is technology due to being new and up-to-date. LTE appeared after WiMAX, thus some telecommunication firms already invested in WiMAX and offered commercial services. Therefore for some companies the process of transferring from WiMAX toward LTE does not seem financially feasible as a result of already focusing on WiMAX. As both WiMAX and LTE systems have similar technical profiles, the choice of the next generation technology hinges on the timeline benefit of the technology and the service provider's legacy platform.

2.2 The WiMAX protocol

The WiMAX broadband wireless access (BWA) standard can be explained according to the Open Systems Interconnection (OSI) model that is often regarded as the OSI seven layer model (Zimmerman et al. 1980). It starts from the Application Layer and finishes with the Physical Layer. Each protocol in line and in accordance with the role which plays, is assigned to various layers; it is so that the higher layers of this model benefit from services of their lower layers. As a defined and well-organized model the work is designed such that the lowest layers are concentrated on hardware aspects and the higher layers on software ones (M. Hossain 2008). It is important to mention that, as it can be seen in Figure 2:

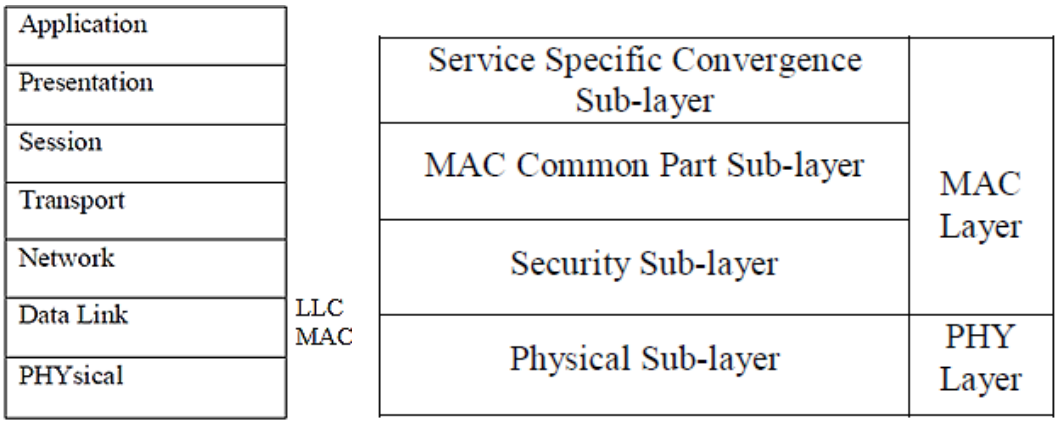


Figure 2. Seven layers of the OSI model (ITU-T X-Series Recommendations 1993) and WiMAX protocol layer architecture

For WiMAX just the Physical layer and Data Link layer are valid. Data link layer is comprised of Logical Link Control (LLC) and Medium Access Layer. Figure 3 demonstrates the critical functional factors of 802.16 network architecture, chiefly, the Mobile Station (MS)/Subscriber Station (SS), Connectivity Service Network (CSN) together with the Access Service Network (ASN) (WiMAX Forum 2006; J. G. Andrews et al. 2007). The first two belong to Network Access Provider (NAP) but the final one remaining is belonging to Network Service Provider. Due to the fact that the architecture has basically altered following the WiMAX standard's evolution, here the concentration is mainly on the model that corresponds to the eventual emerging standard being the mobile WiMAX. Basically MS refers to the device which the user utilizes to connect to the internet/network.

In fact, this maybe a mobile station capable of supporting several hosts. The user's 802.16 access network is actually represented by the ASN. Its role is offering a defined interface among the MS and the CSN. It is made of many Base Stations (BS) and a certain number of ASN gateways. The ASN actually manages the available radio resources. It performs several things like controlling the handover, establishing the layer-two connectivity, interactions with surrounding ASNs. They also perform the relaying among the MS and the CSN to make the connection possible for location controlling and paging within the IP layer. The BS device offers an interface among the MS and the corresponding WiMAX network.

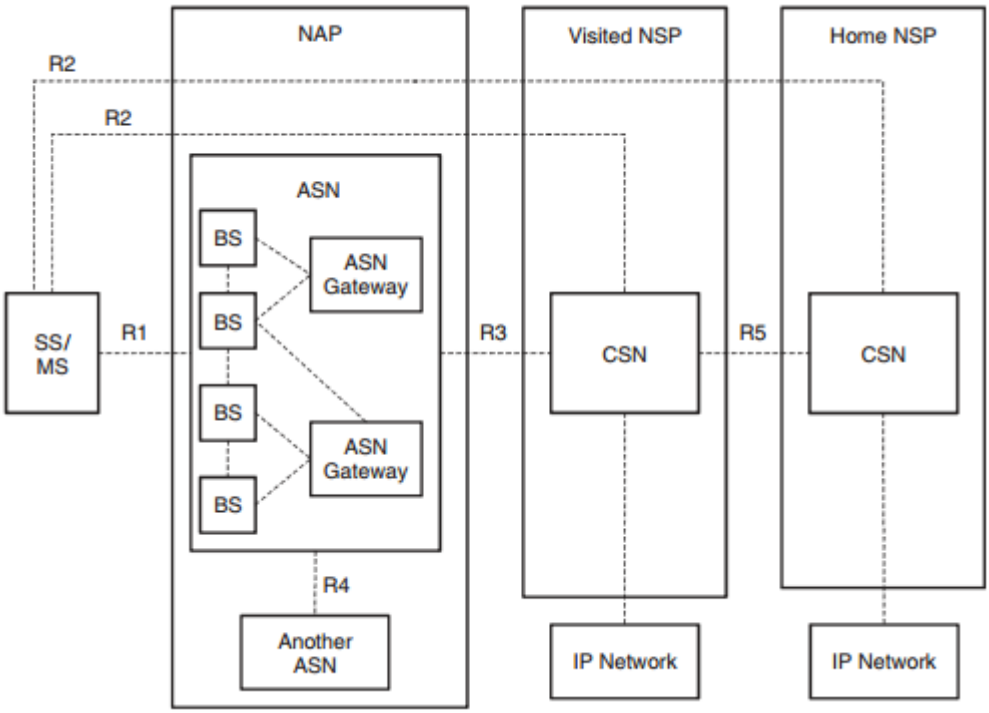


Figure 3. The WiMAX Network Architecture (S. Rekhis et al. 2010)

The ASN-GW is basically a canonic point where the corresponding LLC traffic sums up there within the ASN. It covers areas like mobility management and connections, DHCP relaying, authentication of clients to see whether they are authorized, the AAA mechanism, user associated issues, administration of service flow along many others. Sometimes the ASN-GW applies the notion of Foreign Agent (FA) within the internet protocol version 2 that offers the connection possibility to users which check the network together with saving the data regarding those (J. G. Andrews et al. 2007). The AAA user within ASN-GW gathers the data associated with the flow entitling the density of bits received /dispatched. The CSN plays the role of a heart in the network's body of WiMAX and is in charge of transporting, switching and authentication related complexities. It also

controls and balances the related admission procedure and prepares the billing. The CSN is the associated host to the AAA and DHCP servers, the home agent and also voice over IP gateways (J. G. Andrews et al. 2007). Two different functional entities are connected and associated by a group of references which define the links. The initial reference, denoted as R1, associates the mobile station with the base station. It basically demonstrates the defined radio interface within the medium access control sublayer and physical layer together with executing the standard. The R2 is regarded as the second reference that is an interface which is situated among CSN or ASN-GW and MS.

Further on R2 is related to the authentication/authorization. R2 is deployed for mobility/service administration or administration of IP host configuration. The R3 represents the interface among the CSN and ASN. It aids the processes of authentication/authorization, mobility administration together with policies among the CSN and ASN.

The R3 is also in charge of applying a tunnel among the CSN and ASN. The R4 interface locates among 2 ASNs to makes sure that by the time a MS displaces among them, the interworking of ASN remains seamless and functions as expected. The R5 indicates an interface among 2 CSNs which is deployed for internet access among a viewed network service provider and home. This interface also does activities like roaming.

2.3 The WiMAX Physical Layer

Physical Layer also settles and categorizes the type of deployed signals, the transmission power and modulations thoroughly. The WiMAX has set the frequency band of 2-66 GHz. The first part begins from 2 and stops at 11 GHz and is intended for NLOS transmissions. This was previously the 802.16a standard and the current sole range included in WiMAX. The second range is 11-66 GHz and was defined for LOS transmissions. This range is not deployed for WiMAX (Loutfi Nuaymi 2007; M. Hossain 2008).

The IEEE 802.16 standards came up with five PHY layers so that all of them can be deployed with the media access control (MAC) layer. The PHY layers defined in IEEE 802.16 are as follows:

• WirelessMAN SC: a single-carrier PHY layer. It is set for frequencies beyond 11GHz which need a LOS condition.

• WirelessMAN SCa: a single-carrier PHY for frequencies existing 2GHz-11GHz for point-to-multipoint operations.

• WirelessMAN OFDM: This PHY layer has been accepted by WiMAX for fixed operations and is regarded as fixed WiMAX. It is a 256-point FFT-based OFDM PHY layer for point-to-multipoint operations in non-LOS cases between frequencies 2GHz -11GHz.

• WirelessMAN OFDMA, a 2,048-point FFT-based OFDMA PHY for point-to-multipoint operations in NLOS cases between frequencies 2GHz - 11GHz.

• Wireless High-speed Unlicensed Metropolitan Area Network that is for license exempt band and for frequencies less than 11 GHz. WirelessHUMAN just uses TDD for duplexing (IEEE 802.16-2004, “IEEE Standard for Local and Metropolitan Area Networks).

It is important to notice that WiMAX just recognizes and works with OFDM and OFDMA PHYsical Layers of 802.16 standard (Loutfi Nuaymi 2007).

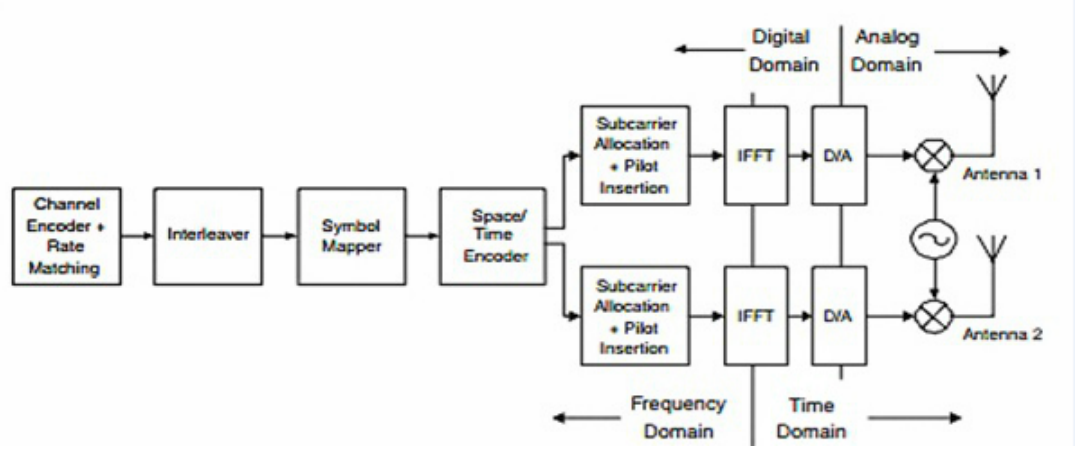


Figure 4. WiMAX PHY scheme (Jeffrey G. Andrews et al. 2007:273)

Figure 4 demonstrates the functional scheme of WiMAX PHY layer. One can first observe the functional units in charge of performing the forward error correction (FEC), channel encoding, interleaving, and symbol mapping. Furthermore, functional units are dealing with the construction of the OFDM symbol. The final functional units are working to convert the OFDM symbol from the frequency to the time domain to put it in the ideal analog form transmittable over the air.

2.4 The Media Access Control (MAC) Layer

The WiMAX MAC is intended to provide a bedrock for very speedy data rates and in the same time it is intended to offer a high level of quality of service. The WiMAX MAC deploys a variable-length MPDU and paves the way for more flexibility resulting to better transmissions.

The MAC layer has three sublayers, the CS (Convergence Sublayer), the CPS (Common Part Sublayer) and the Security Sublayer. Among the characteristics of MAC is being connection oriented and having 16-bit connection identifiers (CIDs). As a result of having associations together, several UL and DL channels are distinguished by a CID. The role of SSs is to verify the CIDs, and opt for those PDUs addressed to them. The MAC PDU can be described as a data unit being exchanged among the BS's and its SS's MAC layers. The MAC layer of WiMAX protocol is demonstrated in Figure 5.

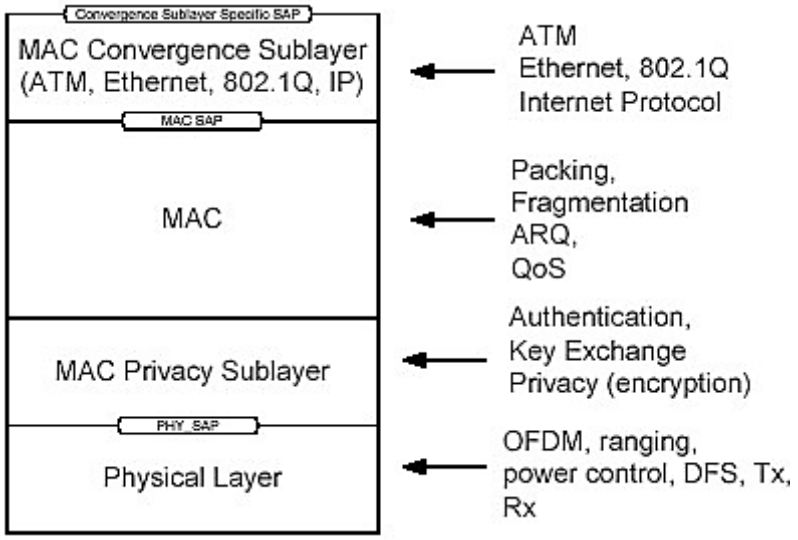


Figure 5. MAC Layer of 802.16 protocol (David Johnson et al. 2004)

2.4.1 Convergence Sublayer (CS)

The Convergence Sublayer (CS) is the top sublayer of the MAC Layer. The CS accepts higher-layer PDUs from upper layers and sends them to the MAC CPS. The CS is in charge of the optional Payload Header Suppression (PHS), which is

the process of suppressing repetitive payload parts of the headers at the sender and restoring them at receiver. In addition to this, the CS categorizes and maps the MAC service data units into relevant Connection Identifiers (CIDs).

2.4.2 MAC Common Part Sublayer (MAC CPS)

The Common Part Sublayer (CPS) is located in the middle of the MAC layer. It is in charge of the functions like bandwidth allocation and bilateral connection initialization and maintenance.

According to the 802.16-2004 version of the standard, during the connection initialization, management messages are being transferred between SSs and BSs. By the time the connection initialization takes places, the transfer messages can be sent to allow the data transmission. The CPS gets data from several CSs. When it comes to the PHY Layer, QoS is defined to evaluate the transmission. One of the main operations performed by the CPS are QoS management, radio resource management among many others (M. Hossain 2008).

2.4.3 Security Sublayer

The WiMAX security sublayer deals with authentication, encryption and integrity control. In case of WiMAX, the encryption is carried out by a protocol and it takes place at both sides. This protocol has a set of defined rules and algorithms for performing the encryption. Moreover, an encapsulation protocol is deployed for encryption of data packets. WiMAX security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. In this case, these services are provided for IP traffic only. Once the network endpoints are authenticated, IP traffic flowing among those endpoints is protected. Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

The Privacy Key Management (PKM) protocol is utilized to offer a secure data key distribution from the BS to the SS while they are often synchronized with

each other. The BS deploys PKM protocol to make sure not everyone gets access to the services. Further on, 802.16e came up with PKM second edition as an extension of the PKM first edition, with novel ciphering algorithms, reciprocal two-way authentication and some more features.

2.5 Packet Header Suppression

Packet header suppression (PHS) is the process of removal of the repetitive part of the SDU header. The procedure in which some identical repetitive parts in the packet header get deleted is called suppression. This action always takes place at the sender's side by the CS for diminishing the overhead. For instance, in the transmission of SDUs IP packets, the header of each IP packet comprises the source and destination IP addresses which remains the same for all the packets. This repetitive part is discarded at the transmitter prior to transmission and is then reinserted back into the SDU at the receiver. To achieve a successful PHS operation, the CS at the transmitter is synchronized with the receiver CS using PHS protocols. The application of PHS increases packet transmission efficiency such as VoIP though the implementation is optional in WiMAX but has problems if packets are lost (S. O. Ailen-Ubhi 2012).

The usage of PHS is performed by a well-defined PHS rule pack that creates the framework of the SDU header suppression, and the rule to be applied is distinguished by the CS hinging on the defined factors or the type of service, like HTTP or VoIP. The CS produces the needed connection identifier (CID), service flow ID (SFID) and PHS for the SDU action, instantly after a matching rule is established. (PHSV), the received PHS field (PHSF) bits are verified against the expected bits, utilizing the PHS rule. If the SDU PHSF and cache PHSF correspond, the SDU PHSF bytes are dismantled and a PHS index (PHSI) is attached on the SDU according to the matching rule. In addition to this, if the SDU PHSF and cache PHSF do not correspond, the suppression action is not performed on the SDU PHSF and a PHSI value of "null" is then appended. (Andrews et al. 2007: 309-310.)

2.6 Data/Control Plain

The data and control plain modules are distinguished by means of the application identifier on each and every connection. Each MS has a distinct MAC address of 48 bits, utilized for the establishment of the connection registration with a BS. The connection is identified by a 16 bit CID dedicated by the BS.

During the MS initial network entry, the BS makes two pairs of management CIDs. Moreover it makes an arbitrary third pair for MS that lets the network control action to take place. Two-way CIDs imply a CID pair for each and every connection. According to operational aspects, there exist three classification of management CIDs: basic management connection, primary and secondary management connection CIDs. The basic management connection CID is employed in the transfer of brief immediate MAC management messages between BS and MS, while primary management connection CID is used for lengthy and delay flexible MAC management messages. Secondary management connection CID is used in the exchange of standard-based messages for example DHCP (Ergen 2009: 312-313; S. O. Ailen-Ubhi 2012).

2.7 MAC PDU Format

In WiMAX network basically the data are transported in form of the MAC PDU. The MAC PDU structure shown in Figure 6 comprises a fixed length MAC header, a payload with flexible length and a Cyclic Redundancy Check (CRC). The 48 bits length MAC header is a host to information contents like the user ID and the instructions about the header's length. The arbitrary MAC PDU payload is comprised of a full or partial version of the MAC SDUs. Fragmented or partial version is the division of MAC SDU into further subparts fragments Sub-headers that are sent in various SDUs therefore improving the flexibility of the MAC PDU size. A Fragment Sub-header (FSH) has 16 bits factors appended to each and every MAC PDU which holds the SDU fragment. The FSH factors are as follows:

• Fragmentation Control (FC) that consists of 2 bits.

• Fragment Sequence Number (FSN) having dedicated 11 bits needed for non-ARQ connections.

• Block Sequence Number (BSN) consisting allotted 11 bits used for ARQ connections.

• Reserved 3 bits used for rounding purpose.

It is to be noted that the status of the payload fragmentation is represented by FC (00, 10, 01 and 11). Non-fragmentation is represented by 00, while first fragmentation is distinguished by 10, last fragmentation by 01 and continue fragmentation by 11. The FSN is in charge of providing the required SDU fragment sequence number. The length of the header is not always an integer number bytes, the standard uses the reserve bits to carry out an integer number of bytes length for all the headers (Can, Vannithamby, Lee & Koc 2008).

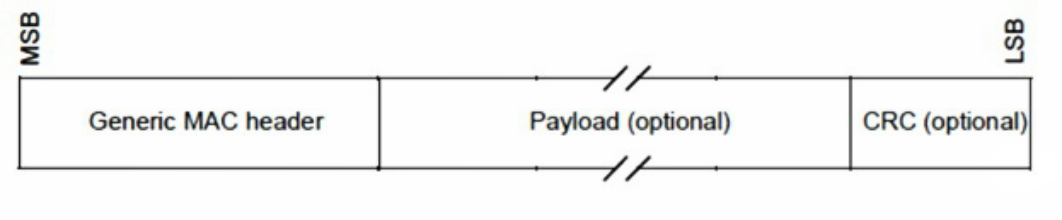


Figure 6. MAC PDU format (IEEE Std 802.16TM-2004 2004: 35)

2.8 MAC PDU Construction and Transmission

The structure and sending of MAC PDU procedure takes place by means of some three actions: fragmentation, concatenation, and packing that are carried out on management messages and data packets. Fragmentation action includes the splitting of each and every MAC SDU into several MAC PDUs and this paves the way for a better performance and enhances the QoS scheduling together with frame feedback. The sending of the fragments hinges on the status of the ARQ that is enabled or disabled. The enabled mode activates the retransmission of the fragments, while a single transmission in sequence is executed whenever the ARQ in disabled. The receiver utilizes the sequence number to recover the sent MAC PDU. In addition to this concatenation is an action where numerous MAC PDUs are mixed into a sole transmission.

Every MAC PDU holds a distinct CID and this provides a possibility so that the receiver become able to di-multiplex the received MAC PDU. Packing is a process which holds a sole MAC PDU consisting of the pack of numerous MAC SDUs. The MAC header length field can be employed to identify the packed SDU just in case when a fixed size of SDU is deployed. (Ergen 2009:320)

2.9. Network Entry and Initialization

A mobile station that is intending to get access to a WiMAX network should undergo network entry operations in order to establish communication with the network. At the onset of the entry operation, the MS checks for the availability of a DL channel of the intended WiMAX network. At the moment when the network presence is confirmed, the MS synchronizes itself with the DL channel of the selected network BS. On completion of synchronization, the MS procures transmission parameters from various control messages received from the BS and then carries out ranging. Further on, the MS negotiates basic capabilities to make sure that efficient network communication takes place, and subsequently undergo registration and authentication operations. Finally, the MS gets an IP address that accomplishes the network entry procedure and prepares the MS to start dynamic or provisioned service flows set up before transmission of data and management messages. (Ergen 2009: 325.)

2.10 Bandwidth Request and Request Mechanism

In 802.16, CIDs devoted ranging from just one to three are assigned to each and every mobile station to send and receive control messages during network entry and initialization. The target of the link pairs explains the usage of unique groups of QoS on MAC management traffic links. Bandwidth usage flexibility is imperative in all services besides incompressible UGS connections characterized with constant bit rate, whose demands for example channelized T1 may vary based on the traffic. Resources are allotted for Demand Assignment Multiple Access (DAMA) services based on demand and the time of need. BS is responsible for bandwidth allocation to MSs. MS requires bandwidth for successful transmission and the request message is communicated to BS through the following methods:

1- Requests

Requests are basically UL messages by which the mobile station announces the base station to allocate UL bandwidth. There are two types of requests: standalone bandwidth request header and the piggyback bandwidth request. As a result of the dynamic variability of the UL burst profile, the UL bandwidth requests consists the needed number of bytes for the transportation of the MAC header and payload.

The bandwidth request is cumulative or aggregate and is positioned in the bandwidth request header Type section. The base station replies to these two request types in two various manners. When it comes to cumulative bandwidth request, a

specific amount of bandwidth is added to the existing mobile station bandwidth of the link where in aggregate bandwidth request, the existing mobile station bandwidth is entirely substituted by the amount of the requested bandwidth.

2- Grants

Grants are messages by which the base station acknowledges the mobile station about the assignment of the requested bandwidth. These messages are sent to the mobile station basic CID since the base station is not aware of the connection CIDs that requires the assigned bandwidth. The distribution of the assigned bandwidth to the real CID connection is performed by the mobile station. In cases when the received assigned bandwidth is less than the needed bandwidth, the mobile station may withdraw momentarily and ask once again or specify the connection which will deploy the bandwidth, otherwise the MS deletes the SDU based on the received BS information.

3- Polling

Each and every connection needs bandwidth for sending. The mechanism of mobile station bandwidth requests also requires bandwidth assignment for operation. This mechanism by which a mobile station is specifically allocated bandwidth for bandwidth request purpose is known as polling. A single mobile station or sets of mobile stations may be recipients of these assignments. The assignments of a single mobile station is carried out by the fundamental CID and that of sets of mobile stations is by UL-MAP and special CID (IEEE Std 802.16TM-2004 2004: 141- 142).

2.11 Mobility Management

Mobility management was dealt with in the IEEE 802.16e standard following the amendment of IEEE 802.16d standard to support mobile applications. There are two points regarding the mobility in wireless networks. They are the power and handoff management. These issues are dealt with in mobile WiMAX (WiMAX Forum 2006: 22) by aspects like Sleep Mode and Idle Mode actions to smoothen a suitable deployment of power resources. Moreover, a consistent handoff scheme that makes sure a seamless and continuous communication of the mobile station

takes place when going from one base station to another at regular paces (S. O. Ailen-Ubhi 2012)

2.12 Encryption Mechanisms

In the IEEE 802.16 standard security sublayer, there exist a number of security mechanisms for encrypting the transport data. Therefore the most common mechanisms are briefly explained as follows:

2.12.1 DES (Data Encryption Standard), TDES (Triple Data Encryption Standard)

IBM came up with the Data Encryption Standard (DES) which was later pushed forward and became a standard in 1976. For enhancing DES, IBM made several efforts and eventually created the Triple Data Encryption Standard (TDES). The name is triple because the same approach is applied three times, moreover the existing 64 bit keys increases to 192 bits. Thus nowadays even with the latest advancements, TDES is considered very safe even for financial transactions (P. Hamalainen et al. 2001).

Both DES and TDES have a common secret key encryption mechanism. The DES mechanism can be deployed for data encryption while TDES algorithm maybe utilized for coding of the encryption keys.

In DES, a secret key is utilized along the way from plaintext to ciphertext. It is of great importance to notice that the data is encrypted with the first key, decrypted with the second key, and eventually coded again with the third one. Figure 7 demonstrates the just explained functional blocks. It is studied that for breaking the TDES with brute force attack $_2{}^{2112}$ tries are required. This actually indicates the robustness of TDES.

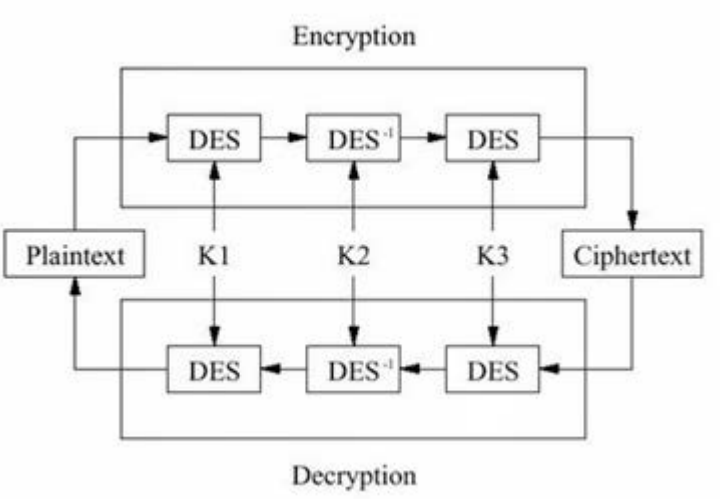


Figure 7. Triple DES (NIST Special Publication 800-67 Revision 1 2004)

2.12.2 AES (Advanced Encryption Standard).

In 2002, DES was gradually replaced with Advanced Encryption Standard (AES) that is regarded as "Rijndael". Rijndael has a block size of 128 bits and the key are variable from 128 bits to 256 bits (Chih-chung Lu et al. 2002). Rijndael deploys a substitution permutation network that is also handily implemented. The Rijndael is also regarded as being practically crack-proof (Chih-chung Lu et al. 2002). It is proven that the existing brute force attacks have not been successful against Rijndael. The AES mechanism is a shared-based encryption mechanism. When it comes to AES mechanism, the cipher key is of 128, 192 or even 256 bits length. This algorithm has a dual usage and can be deployed either for data encryption or encryption of keys.

2.12.3 RSA (Rivest Shamir Adleman)

In 1977, RSA was defined by Rivest, Shamir and Adleman and it is one of the common mechanisms for public-key encryption. It is utilized for coding the Authorisation Reply message by the SS public key. The Authorisation Reply message consists of the Authorisation Key (AK). RSA can be deployed for encryption of keys as well but just when the scenario is such that the keys are being sent from the BS to the SS.

2.13 HMAC (Hashed Message Authentication Code)

A keyed-hash message authentication code (HMAC) is deployed for computing a message authentication code (MAC) that consists of a hash function together with a secret key. It can be utilized to check the data integrity and message authentication. For computing the HMAC, hash functions like MD5 or SHA-1 can be deployed. Thus to what it leads, the mechanism is labeled as HMAC-MD5 or HMAC-SHA1 respectively. If the hash function is strong for instance with 160 bits output size the HMAC's degree of trust and reliability is higher. In other words if an attacker wishes to attack HMAC based authentication, he will need to find out the secret key of the HMAC. Take a HMAC with output size of 128 bits as the example, the attacker needs to acquired $_2{}^{64}$ correct plain messages with the corresponding HMAC value (with the same key) to figure out the right HMAC secret key. The attacker can only replace or generate fake massages and compute a good HMAC result if he knows about the secret key. One can refer to the RFC2104 to observe that this is considered an impossible task in any realistic scenario (for a message block length of 64 bytes, this would take 250,000 years in continuous 1Gbps link, provided without changing the secret key during all this time). If one replaces a strong HMAC with 160 bits output size as mentioned earlier then the number of original messages and HMAC code required should become 2^{80} which is even harder and impossible to attack.

2.14 Encryption Keys

Diverse set of encryption keys are deployed for the security of IEEE 802.16. All encryption keys belonged to the IEEE 802.16 standard are available below. Other details associated with it such as notation and the number of bits can be observed in Table 1.

Table 1. WiMAX Encryption Keys (Laurent Butti, 2007)

Encryption Keys	**Symbol**	**Number of Bits**	**Description**
Authorization Key	AK	160	SS gets authentication from its BSs It's a shared secret key and used for secure transactions. It is also used to generate encryption keys.
Key Encryption Key	KEK	128	Key Encryption Key used for the encryption of the TEK.
Traffic Encryption Key	TEK	128	Used to encrypt data by using different algorithms.
HMAC Key for the Downlink	HMAC_KEY_D	160	It authenticates messages in the downlink direction.
HMAC Key for the Uplink	HMAC_KEY_U	160	It authenticates messages in the uplink direction.
HMAC Key in the Mesh mode	HMAC_KEY_S	160	It authenticates messages in the Mesh mode.

2.15 Security Associations (SAs)

In WiMAX standard, the security association is comprised of a group of security data elements that the base station and its subscriber stations share for having a secure connection. In fact, base station is in charge of administrating the security associations. Therefore when it comes to an authentication scenario the base station transmits a group of Security Associations related to its connections to subscriber stations. Furthermore, the base station may come up with one or more SAs to the subscriber station. The SA's identity is regarded as "SAID" and is shared

between BS and the SS and is of 16 bit length. Moreover SA contains a cryptographic suite identifier (for selected algorithms), traffic encryption keys (TEKs) and initialization vectors (David Johnson et al. 2004)

2.16 X.509 Certificate

ISO/IEC and ITU introduced a standard called X.509 in 1988. The X509 is actually an electronic identity certificate (Hoyt L. Kesterson 1997). X.509 is an authentication mechanism which binds a name to a public key value. The role of the certificate is to associate a public key with the identity contained in the X.509 certificate. Thus when the BS is in the process of checking a client SS, due to the fact that SS holds a X.509 digital certificate, the identity would be verified with it. This digital certificate content is the so called SS's MAC address and public key. If an AK is desired, an SS presents its digital certificate to the base station. The base station checks the digital certificate and then codes the AK. Then the BS transmits and returns the AK to SS. Figure 8 demonstrates the X.509 authentication.

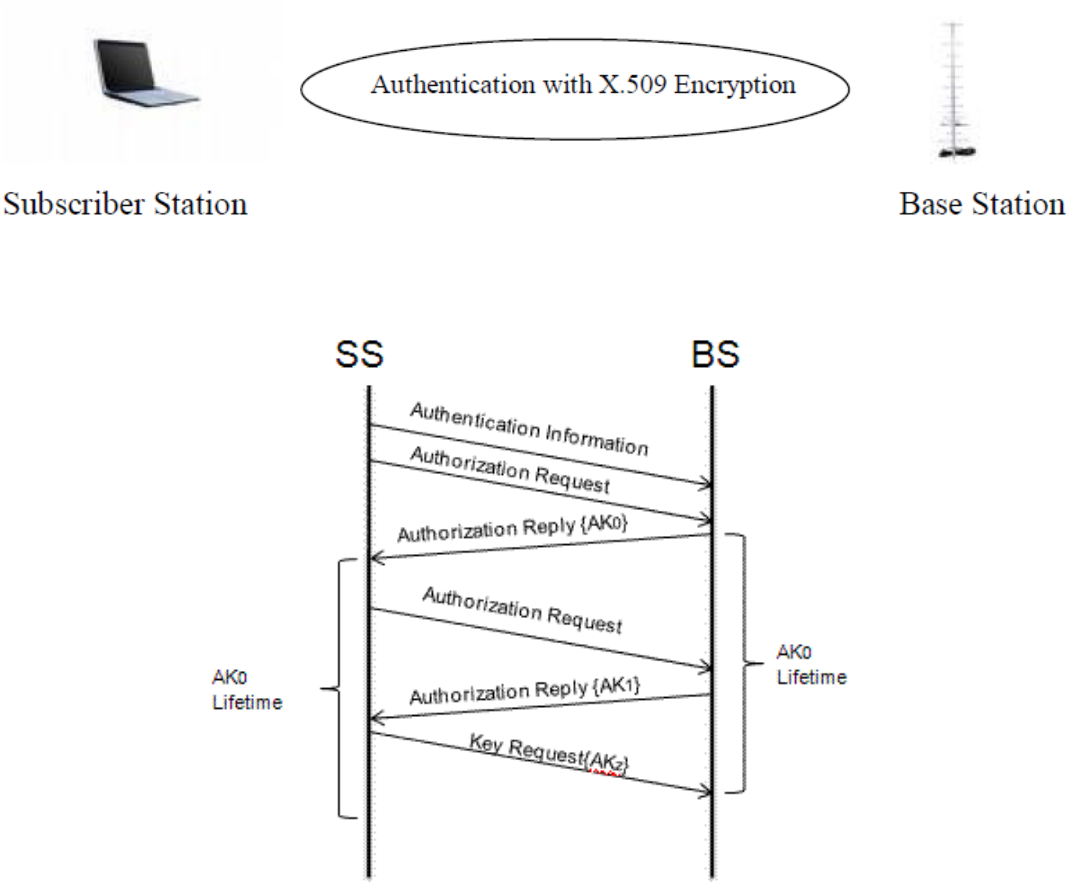


Figure 8. X.509 Authentication (Hoyt L. Kesterson 1997; M. Hossain 2008)

In fact, the BS proceeds with the authentication of the identity of a client SS and offering the services that the SS is permitted to access take place with the AK exchange. Therefore due to this BS-SS authentication process, base station can stay protected against a masquerading impersonation attack. Thus all SSs can hold factory-installed RSA public/private key pairs or have an internal algorithm to produce likewise key pairs dynamically. In case an SS requires to produce its RSA key pair by utilizing its internal algorithm, the SS produces the key pair prior to exchanging AK. Practically almost all SSs which count on internal algorithms to produce an RSA key pair basically support a mechanism for installing a manufacturer-issued X.509 certificate. The usage of a factory-installed RSA public/private key pair increases the intruder's chance of success. The initial uphill battle for an intruder is to have an SS from the same vendor as the aimed BS, and the second is cracking the X.509 encryption.

2.17 The PKM Protocol

For describing the functions of the PKM protocol one has to build a model in which the BS is the server who provides and transmits the secret key to client SS's. The PKM (Privacy Key Management) takes place while the process of authentication between BS and SS is going on. PKM protocol utilizes public key cryptography to determine a shared secret key among SS and the BS. The PKM protocol phases are shown below in Figure 9. It basically provides an in detailed picture of what actually takes place while the protocol phases follow their paths (S. Xu and C.-T. Huang 2006).

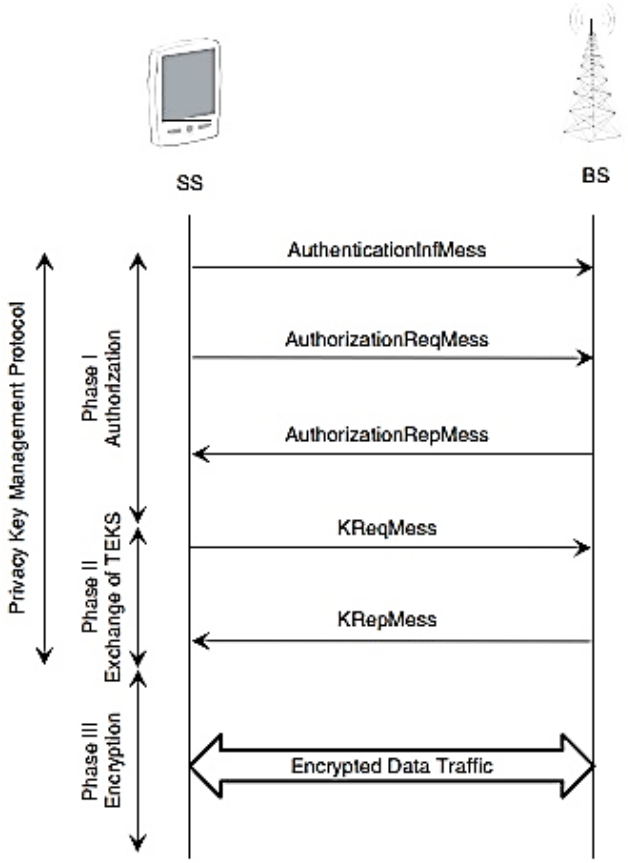


Figure 9. PKM protocol phases (S. Rekhis et al. 2010)

In WiMAX standard, the PKM protocol has two MAC management messages:

1- PKM Request: The PKM-REQ message includes one PKM message in the message payload. This message is transmitted from the SS to the BS.

2- PKM Response: The PKM-RSP message includes one PKM message in the message payload. It is transmitted from the BS to the SS.

So the BS checks the SS and offers key material to let the data coding take place. Each and every SS has the priority of beginning with RSA key pairs that are already set by its manufacturer. Therefore, the RSA key pairs are already set on the SS and it also holds a digital X.509 certificate. The X.509 certificate of the subscriber station is a public key certificate which combines the subscriber station's identifying data to its RSA public key. The operator receives the secret key AK. While asking for the AK, a subscriber station shows its digital certificate to the base station. The subscriber station's manufacturer signs the X.509 certificate digitally. As the base station is well-aware of the manufacturer's public key, it can check the signature. While asking for AK, the subscriber station gets the veri-

fication from the base station through presenting its X.509 digital certificate. It shows the supported cryptographic algorithm's description to the base station as well. This shared secret AK is in charge of further secure transactions (M. Hossain 2008). Prior to transmitting an authentication response to the subscriber station, the base station checks the digital certificate and specifies the ciphering mechanism which should be utilized. The RSA algorithm is deployed to cipher the AK with the checked public key. This RSA public key ciphered AK is then transmitted to the asking subscriber station from the base station. Initially, a PKM authorisation information message is transmitted by subscriber station. X.509 certificate is given with this message. This is actually an informative message that subscriber station transmits to the base station and the base station becomes aware of client subscriber station's certificate of manufacturer. Next to the authorization information message, the subscriber station transmits a PKM authorization request message to the base station. This message includes the X.509 certificate of the subscriber station, subscriber station's primary SAID and a description of its security ability. The digital certificate is checked again by the base station. The AK is ciphered by the public key. The base station returns a PKM authorization response message to the subscriber station containing this AK. Cloned subscriber stations are averted from passing incorrect credentials to a base station with this method. The PKM authorization stage is demonstrated below in Figure 10.

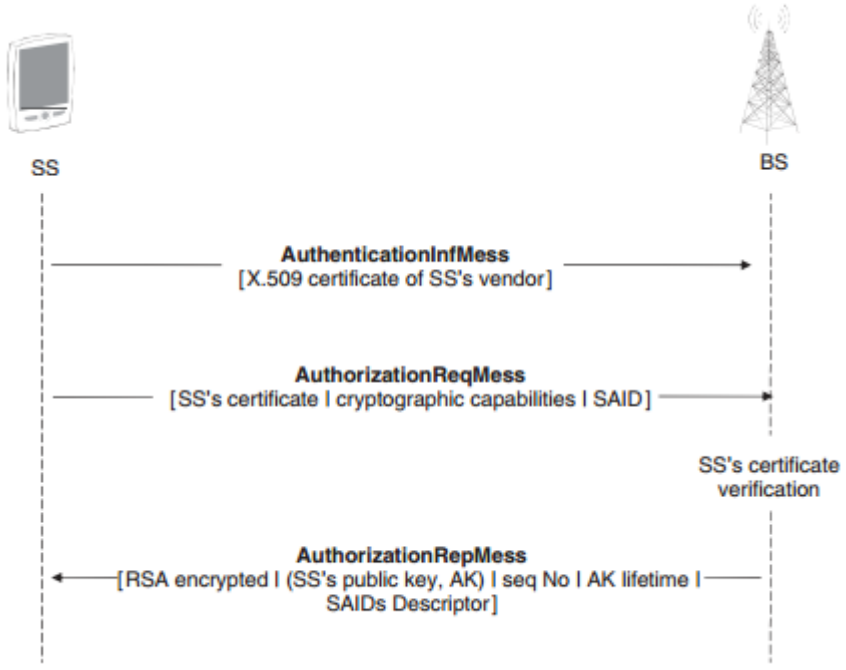


Figure 10. PKM authorization stages (S. Rekhis et al. 2010)

2.18 The Key Administration and Privacy

In the PKM protocol's second stage that is demonstrated in Figure 11, the target has been beginning the TEKs transfer together with fixing the SA. Mentioned TEKs will be further deployed for ciphering. As already mentioned, the authorization response message includes the characteristics of the SA together with the SAID. Thus, the subscriber station begins an individual state for every SAID specified in the authorization response message. Each state is in charge of administrating the keying material related to the associated SAIDs. For the TEK's renewal sake, each SS transmits a key request message to the base station regularly.

The message consists:

- The sequence number of AK that permits the base station to specify the HMAC Key of the uplink which the subscriber station utilizes to produce the HMAC digest
- The security association identifier associated to the SA
- The HMAC digest generated through the function of HMAC in case of the message payload via HMAC Key of the uplink

Following the assurance that at the SS, the captured SAID corresponds with the SA and checking the integrity and the authenticity of the KReqMess through verifying the HMAC, base station replies to the message. The base station transmits a key response message including the key material that the TEK state needs. It should be noted that for every SAID, the base station keeps 2 keying materials active that are represented with TEK-elements within the key response message. Therefore a keying material consists (S. Xu and C.-T. Huang 2006):

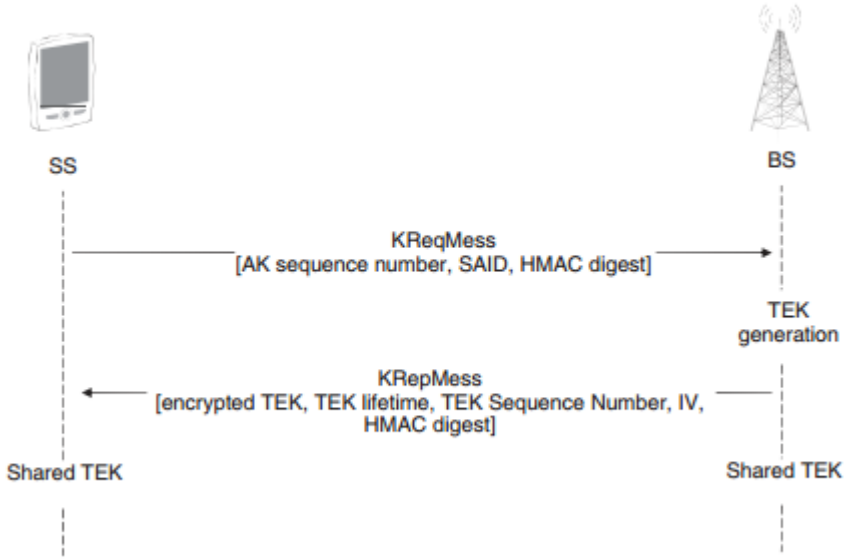


Figure 11. Privacy and key management phase (S. Rekhis et al. 2010)

- TEK ciphered by KEKs utilizing the AES in ECB mode with 128 bits, TDES in EDE mode with 128 bits or RSA PKCS#1
- The TEK's remaining lifetime
- The sequence number of TEK
- An initialization vector of 64-bits long

The key response message consists the security association identifier, the sequence number of AK, the new/old TEK associated parameters together with HMAC digest to assure the subscriber station that the base station has sent the message. It should be mentioned that the durations of validity belonged to both TEKs coincide. Actually, prior to expiration of the old TEK, the new TEK becomes activated. The subscriber station utilizes the mentioned TEK's lifetime to evaluate the timing of a previous TEK's invalidation or asking for a new TEK by the base station.

In case the KReqMess's security association identifier is invalid, the base station replies with a key message rejection consisting the sequence number of AK, the security association identifier, a HMAC digest and an error code together with the cause of rejection. Thus to obtain a new TEK the subscriber station can retransmit the KReqMess again.

It is essential to note that an optional message, represented as RkeyMess can be used as the starting point for describing the key administration and privacy stage of the PKM protocol. The base station transmits the RkeyMess for carrying out the rekeying prior to when the subscriber station asks for one. The message basically consists of the sequence number of AK, the security association identifier associated to SA whose keying materials are requested together with the message digest which the HMAC key of the downlink generates.

3. LITERATURE REVIEW

In the first place, by the aid of having a literature review of the problems and existing solutions when it comes to WiMAX security, a clearer picture can be obtained. This seems logic that being updated with the latest developments and advances offered by researchers and authors, paves the way for recognizing and understanding the existing open issues and further facilitates the mitigation. Moreover it helps making the contributions vividly distinguishable.

The IEEE 802.16 standard, specially the version brought up by Financial Times Information's Mobile Cloning in March 2005, defines the radar interface for fixed point-to-multipoint broadband wireless access networks. An outlook of the IEEE 802.16 can be reached in "Club de la securite des systemes d'information francais (CLUSIF)" Methods Commission. The IEEE 802.16e (LAN MAN Standards Committee of the IEEE Computer Society 2004) edition defines extra methods to support mobile subscribers at vehicular pace and also methods for data authentication. As it was mentioned before, when it comes to IEEE 802.16, security was taken into account as the chief issue while the design of the standard was taking place. Despite numerous considerations, security mechanisms of the IEEE 802.16 still have several open problems to be addressed. WiMAX is not yet utilized in a very large scale but theoretically it can be deployed in various scenarios and many security threats can pop-up as its usage grows.

An attacker having bad intentions like information theft may handily break into a weak WiMAX network by the aid of various techniques. In addition to this, in case the attacker has a strategic position with a RF receiver, it can block the messages transmitted wirelessly or simply do a jamming and thus a security mechanism revision would be required. From the literature review, one can draw a conclusion that present security mechanisms are not mitigating the entire issues to the full when it comes to IEEE 802.16a Mesh modes network. Therefore this results in emerging security threats. Thus it is essential to deal with the security aspects of the IEEE 802.16 standard and highlight the security faults, risks and threats connected to it.

Now the question is what motivates and why should an attacker thinks of intruding a system or network. The subject of what motivates a hacker to carry out attacks has been investigated in the literature for achieving the means for better countermeasures. In 1994, in an old study anthropologist R. Blake deployed the fundamental social stratification theory to claim that hackers are motivated chiefly by wealth, power and prestige. In his paper (R. Blake 1994) he believes that money is the main cause among other motivations. It can be observed that by sell-

ing private information or by eliminating a business rivals in the market both a remarkable financial gain and power in the market can be achieved. These reasons together with the prestige and attention which the hacker gets in the community are counted as powerful motives for intrusions.

In 1994, R. Schifreen suggested five probable motives for hackers.

In his paper (R. Schifreen 1994), he classified the motivations as follows:

-Opportunity: some systems have a poor security and this itself attracts the attentions

-Revenge: the intrusions can be launched by a disgruntled employee for taking revenge

-Greed: getting money for selling the information, blackmail or espionage

-Challenge: conquering a system having security measures itself can bring about a prestige

-Boredom: the hacker may have no other thing to do, thus when get bored can try to carry out intrusions

M. Barber, in his paper (M. Barber 2001) added the following motivations to the existing ones:

-Vandalism: the defacing of corporate or organization web sites

-Hacktivism: Intrusions carried out for scoring political, economic or ethical points

-Information Warfare: this is done by government to promote their own policies domestically or internationally

In order not to ignore the most updated security issues and motives together with the places where are challenged by them some professional problems like 1- military 2- corporates 3- Governments 4- Professional crime and 5- Fanciness should also be mentioned.

This dissertation provides an anthology of the attacks and countermeasures found in the literature contra IEEE 802.16 family of standards because this is the subject of investigation here in this dissertation. In addition to this the differences of WiMAX with other wireless standards will be briefly mentioned as well. The emphasis is on attacks contra physical and MAC layer up to the latest version of the

standard. Moreover, this dissertation tries to categorize and classify the attacks under realistic conditions (S. Karen et al. 2010).

For all of them primarily the susceptibility of the protocol that makes the attack realizable is demonstrated. Furthermore, the attack methodology is described and investigated according to two criteria's. A risk analysis of threats in WiMAX has been realized in the past (M. Barbeau 2005; M. Barbeau et al. 2007; K. Sansurooah 2009).

The DoS/Replay attacks and the authorization susceptibility of WiMAX were addressed and effectively solved (S. Xu, Manton Matthews, Chin-Tser Huang 2006). It needed a reasonable alternation to the standard, but it is intricate to foresee the precise impact on performance and scalability even though it is known that security solutions have practically always some impacts on performance and scalability. Therefore if it passes all those tests smoothly, one can regard it as an acceptable solution.

In 2007, a solution was proposed and settled down the authorization attack (Tian Haibo et al. 2007). It did need just a few alternations. In that paper it was expected that the performance would just slightly drop, but more research is required to attest this and to investigate the scalability of this solution.

The paper of Fuqiang Liu does not really solve a security problem. In this paper (Fuqiang Liu et al. 2006), what the solution provides is actually diminishing the key size for encryption, therefore reducing message size and boosting the performance. Therefore one can draw the conclusion that their modification to encryption and certificates passes the testing stage from performance and scalability perspective, but on the other hand if we look at it from the authentication and authorization enhancement, it simply fails because reducing the key size is always a bad idea. It is even a bad idea for boosting the performance.

In 2007, a theoretical framework was proposed that could offer numerous security advantages. In this paper (Kejie Lu et al. 2007) because an extra layer is required, the setback would be the fact that a major modification of the standard would be required thus it is yet to see whether this would be an efficient step to take or not. Moreover because no simulation results are presented, no conclusions on scalability and performance can be drawn.

As it can be confirmed technical difficulty is another notion which attackers deal with it. It refers to the technological challenges faced by an attacker in his efforts to pose a threat. It can be highlighted that similar difficulties are regarded as dynamic. The reality is that what sounds like an uphill in the path nowadays, may

not be so in the next few years. For instance, WiFi implementations in accordance with the IEEE 802.11 standard's original characteristics deploy the Wired Equivalent Privacy (WEP) approach to security (H. Haverinen et al 2004).

The standard's working team thought that WEP's security mechanisms causes firm technical hurdles to intruders. In 1999, the technical difficulty for attacks addressed to WEP was evaluated as being so strong, and attacks were not probable to happen. Nevertheless, it promptly became vivid that WEP had security faults and several weaknesses. WEP's security breaches were discovered by Fluhrer, Mantin, and Shamir and made public in 2001 (Technical Specification ETSI TS 102 165-1 V4 2003). The technical difficulty became solvable and the probability of attacks rose to the level of likely.

In 2002, Stubblefield, Ioannidis, and Rubin implemented an attack against WEP. Since that time, the attack has been known, and its relevant software has been out there available, diminishing the technical difficulty to “none” and upgrading the probability of the attack to likely. WiFi Protected Access (WPA), WEP's successor, is at present believed to cause strong technical difficulties to intruders but nobody knows if in future it would be as strong as now (M. Raya et al. 2004).

Scrambling is a kind of jamming that is performed for short intervals of time and aimed at particular frames. Scramblers can selectively scramble administration or control data for affecting the network’s normal functioning. The problem is of greater amplitude for time sensitive messages that are not delay tolerant, like the report requests/responses for measurement of the channel. Scrambling phenomenon and scramblers can be detected by monitoring anomalies in performance criteria. This issue has been studied for WiFi/802.11 systems (M. Raya et al. 2004). The situation for WiMAX/802.16 is much different, and further research is required for this case.

L. Maccari and his colleagues have investigated some security issues of the family of IEEE 802.16 standard which has not been addressed as far as we know. Thus the ideas in this paper (L. Maccari et al. 2007) were new and novel approaches were taken. Further on, they have highlighted the lack of message integrity code (MIC) for data and authentication packets. Lack of authentication at the base station (BS)’s side. In this paper authors have only proposed some modifications, such as the introduction of EAP (Extensible authentication protocol) protocol to strengthen the authentication stage. In contrary the authors have not suggested any solution and they just discussed regarding the problems. T. N. Nguyen and his fellow researchers improved EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. In this paper (T. N. Nguyen et al. 2012), it is discovered that there are three security vulnerabilities

that would result in DoS and replay attacks. For overcoming the vulnerability in the authentication process in handovers under the DoS and replay attacks together with enhancing the efficiency, the EEP scheme was proposed.

B. Sikkens has argued that even though IEEE 802.16e has a robust and promising security architecture, there are still some issues to be taken care of (B. Sikkens 2008). For example he has discussed about three problems being 1- DoS(Denial of Service) 2- Key Space Vulnerability and 3- Downgrade Attack. For DoS attack the author has suggested the timestamp approach together with signature of BS and SS for authentication. In addition to this, for "Key Space Vulnerability" the author has suggested to use more number of bits for Acknowledgment. To address the problem of Downgrade Attack, author has claimed to neglect the messages that are having security capabilities up to a limit. Having said all this, adding the timestamp and signature needs the modification of the Standard. Moreover, increased number of bits for acknowledgment needs alternation in encryption and decryption. Thus one can see that the suggested solution for downgrade attack would actually result in a DoS attack for SSs that do not have the required capabilities though because the way down grade attack works is such that the first message of the authorization process is an unsecured message from SS telling BS what security capabilities he has. An attacker could send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked SS to agree on an insecure encryption algorithm. The standard does not specify a concrete solution for the situation that two valid answers are received by a BS.

J. Brown designed a new and effective rekeying scheme for WiMAX networks. In this paper (J. Brown 2009), the author has mentioned that DoS attacks on the BS can take place during the PKM second edition. The author has said that Multicast and Broadcast Rekeying Algorithm (MBRA) do not actually scale up to the level of expectation. The author also suggests a Tree Base Rekeying Scheme for settling down and mitigating the DoS attack. The only setback can be the fact that Tree Base Rekeying Scheme would result in a possible storage overhead.

G. Kambourakis and his colleagues specifically zoomed on the Multicast and Broadcast Rekeying Algorithm (MBRA) of 802.16e. In this paper (G. Kambourakis et al. 2010), they have claimed that even though this algorithm has been created having considered the safety issues in mind, but it still has numerous security problems. In the paper the authors have recommended the utilization of several decryption key in asymmetric group key management protocol. The setback is that handling of multiple keys at decryption is another huge concern to be dealt with. Authors have also elaborated on attacks addressed to physical layer like jamming and scrambling and respectively at MAC layer DDoS attack (Dis-

tributed Denial of service), Traffic Encryption Key (TEK) and Authorization Key (AK) problems. In addition some protection methods against the attacks have been proposed. Many people in the scientific community have tried their best to classify and categorize the attacks and security issues of WiMAX. Some of these efforts and classifications are acceptable, however there are a number of reasons which explain why the classification proposed by this dissertation is superior to previous ones. The first point is that some of the attacks previously classified by other researchers are just according to pure theoretical definitions and some others cannot be traced for security mitigation and protection for instance when it comes to cyber army Botnet attacks. However the classification of WiMAX security attacks provided by this dissertation is meticulously inclusive implying that some special cases that cannot be traced and realized are not considered. The second point is that other classification versions look so scattered and one cannot find an integration between them. The third point which contributes to uniqueness of this dissertation's classification is that by removing some theoretical and not traceable attacks and having an integrated approach, our version will be more comprehendible and understandable even in a glance. The fourth point is that in the same time maximum efforts have been made in order not to neglect important posing threats and attacks. Finally the fifth point is that the attacks are only judged as being "Major" or "Minor" like black and white and there is no categorization in between like some others do. Further on Kambourakis and his fellow researchers recommend Intrusion Detection System (IDS), but the paper was just a review related to WiMAX and converged network. Moreover, in 2011 B. Zhou has proposed an intrusion detection system based on WiMAX. Also in 2011, Y. Zhang et al. proposed a new architecture for enhancing the cyber security of the smart grid by deploying a hierarchical and distributed intrusion detection system in the wireless mesh network while also achieving the ideal routing for smart grid communications. Security is enhanced by the categorization of intrusion data deploying the support vector machine (SVM) and artificial immune system (AIS) algorithms (Y. Zhang et al. 2011). All these evidences show the importance of deploying the IDS for wireless networks including WiMAX.

In 2010, M. Habib et al. have investigated the security issues for WiMAX and converged network. They have emphasized on the threats to both the technologies and security measures for these threats (M. Habib et al. 2010).

In 2011, F. Tshering et al. have described the security mechanisms currently existing in the WiMAX. The authors further elaborate on various security issues in PKM (Privacy and Key Management protocol) and the numerous solutions available in literature. They eventually conclude that more research is still needed for the security of IEEE 802.16e. The paper mostly addressed the Key Space Vulner-

ability and Downgrade Attack. Moreover, it also argued regarding the suitability of Cryptographic Algorithm-RSA (Rivest Shamir Adleman). Furthermore Tshering and his colleagues have pointed out already existing solutions like utilization of 8 bit sequence number rather than 4 bit for Key Space Vulnerability. Base station could neglect messages with security capabilities under known limit for Downgrade attack and rather than RSA, authors have recommended the utilization of ECC (Elliptic Curve Cryptography). That is because compared to RSA, the common public-key scheme of the internet today, ECC offers smaller key sizes, faster computation as well as memory, power and bandwidth savings. It can also be mentioned that while RSA and ECC can be both accelerated with dedicated cryptographic co-processors like in the case of smart cards, those co-processors need extra hardware adding to the size, complexity and cost of implementation.

The setback is the fact that the suggestion is not capable to implement 8 bit sequence number. Moreover the solution provided for Downgrade attack results in DoS (Denial of Service) for SS (Subscriber Station) and also there is this modification in standard that ECC needs.

M. Nasreldin and his fellow researchers have investigated on the security risks to wireless access networks and analyzed them based on their risk level (M. Nasreldin et al. 2008; M. Habib et al. 2010). The 802.16's physical and MAC layer threats are explained. Based on the author's investigations strong wireless protocols with robust ciphering methods together with deployment of Intrusion Prevention Systems (IPS) is practical for removing many wireless risks. The physical layer of WiMAX is susceptible to threats as compared to MAC layer. The jamming and scrambling are respective intrusions on physical layer. The authors described the points open to threats, and these threats were also categorized based on classes. Some of these risks are easy to deal with but issues are yet there due to several intrusions being intricate to mitigate; for example the DDoS attack which has a very hard detection procedure. The solutions which the authors propose are security association, spread spectrum mechanism, robust ciphering methods, reciprocal two-way authentication and authentication protocol (EAP). The setback of this paper is that the securing protocol has several susceptibilities like using the weak RC4 and key management.

As mentioned previously, M. Barbeau has investigated the intrusions on WiMAX as well. In this paper (M. Barbeau 2005) investigation of WiMAX/802.16 architecture has been carried out which demonstrates how the ATM cells together with the IP packets become frames. The main concentration in this paper is on the risk investigation of the 2 layers being the MAC layer and physical layer in details.

When it comes to physical layer, the bits flow is organized in a set of frames with identical length. Author points out 2 risks to the 802.16; “Jamming and Scrambling”. Jamming attack may be not intentional or malicious and also stated that jamming is handily detected and when detected then it is smooth for mitigation purposes. Scrambling attack is hard to carry out and also intricate to detect. While explaining the MAC layer the author highlights the MAC layer risks in terms of authentication and confidentiality. The majority of threats are regarding the authentication level. In this paper it is mentioned that there was no protection for the WiMAX’s data traffic integrity, but mobile WiMAX came up with this kind of protection methodology for protecting data. Traffic messages related authentication has been investigated as well. Authentication of traffic messages is a moderate motivation for an attacker because it is an attack originated from creating mischief. The modification of data traffic is very unlikely to happen if AES is utilized due to the strong technical difficulties encountered, and likely if AES is not deployed, given the lack of technical difficulty in carrying out an attack.

Such an attack has the potential to create short-term consequences for the user and system, resulting in a medium impact. If AES is not used, then this is a major threat, otherwise it is minor. It further adds that the message modification is probable when AES is not deployed, and then traffic modification becomes a serious risk. Author mentions that DDoS attack is a main issue on this point as well and that it is so intricate to mitigate it. The author recommended the IDS solution for handling some of the threats. The distinguished aspect of this paper is that it has discussed about almost all the previous research work carried out by the IEEE and the WiMAX forum up to the time when the paper was written. Another strong point of this paper is that the author has deployed a unique mechanism for the risk investigation. The major setback of this paper is that just 3 authentication choices are investigated being X.509 certificate based or EAP based and device-list based. However, actually all these three can be compromised by an intruder. If only device list-based authentication is deployed, identity theft by device address reprogramming can be launched, and the probability of a BS or MS masquerading attack is likely as a result of the fact that there are few technical difficulties to overcome. The effect on a user is considerable due to leading to loss of service for remarkable periods of time and also the user may be billed for some other user's fee. The effect when it come to a system is medium due to leading to limited financial loss or theft of resources. The risk is thus crucial for a user and major for a system, and there is the need for countermeasures. If X.509-based authentication is utilized, the probability for the MS to be the victim of BS masquerading is likely because of the asymmetry of the mechanism and the solvable technical difficulties. The strong technical difficulties in MS masquerading render it an unlikely threat to a system. The impact is the identical for the device list-based authenti-

cation. Therefore, in the case of a user, the risk is evaluated as major, and countermeasures are required. For a system, the risk is minor, and there is no need for countermeasures. If EAP-based authentication is deployed, the probability of a BS or MS masquerading attack is possible. Some of the EAP methods are still being defined, and security flaws are often uncovered in unproven mechanisms. The technical difficulties in launching an attack are thus best evaluated as solvable. The impact is identical as for the device list and X.509 certificate-based authentication, so the risk is labeled as major for both a user and a system.

J. Hasan published a review based paper. In this paper (J. Hasan 2006), what can be observed is that, the review has roots in other published materials, journals, literature and mostly from some relevant websites. In the paper it is elaborated that the WiMAX is still "on paper" and some of its mechanism are being developed. The WiMAX's MAC/physical layer have been investigated thoroughly. Primarily the MAC and physical layers are reviewed and then their security issues are analyzed. In addition to this susceptibilities and risks to the WiMAX are provided in an overview form. The chief flaws investigated were reciprocal two-way authentication, data privacy and key management. The author claims that the gates of WiMAX/802.16 are wide-open to threats that are the TEK and Authorization Key (AK) related problems. Actually they can be exposed and may cause problems. The subjects about user authentication, the issues associated to mobility are mentioned. The setback is that the author have not offered any novel ideas, just he has referenced to the other researcher's carried out achievements. The author has actually taken other's perspective and has sorted them out in a row in his paper. It is only a review, moreover the issues regarding mobility are only mentioned briefly and the sole suggestion is that more research is required in this field. Majority of the paper is about WiMAX's security in a converged network. It is a survey paper that elaborates on securing the data link layer, application layer and wireless access networks. The vulnerabilities list is provided and in addition, the infrastructure of security for these problems are taken care of in details. The security threats of WiMAX are identical to the threats in converged network. Finally the author explains that if one deploys secure devices by the WiMAX consequently the communication can be regarded as secure. This is always the case that the application level security is required to secure the communication and that the carrier should never be trusted. The strong point about this paper is that a detailed infrastructure for security purposes is offered on ways of securing the communication.

R. Mylavarapu described the method for the DoS intrusion detection. In this paper (R. Mylavarapu 2005), the session border controller (SBC) can be deployed to detect the DoS attack. It is a survey paper and the restrictions were not so tangi-

ble. The author's proposed infrastructure for security purposes is very safe but the major setback is that the cost will be remarkably high. Therefore the security and cost are affecting each other. In addition to this, the author elaborates on risks like server/client impersonation, tampering of the message, hijacking the session, signaling request leading to DoS intrusion and has suggested taking security measures like IDS, IPS, NAT traversal and firewalls, DoS and flood intrusion detection, hiding the topology, media and signaling security, session admission control together with granular access control.

In 2008, E. Eren et al. introduced the fundamental enhancements among the 802.16e and 802.16 together with the WiMAX security factors. The security methods like authorization, authentication, and ciphering are investigated in details for the BS and MS in various stages. The emphasis is on the 2 critical stages that have lacks being: "Authentication stage" and "Key Material Exchange stage".

According to the literature review which was discussed in details throughout this chapter and further investigations of this dissertation, one can conclude that major weaknesses, shortages and setbacks when it comes to mitigating and dealing with security issues of WiMAX can be seen as follows:

- Adding the timestamps and signatures needs many modifications to the standard.

- For Key Space Vulnerability using more number of bits for acknowledgment needs modification on the deployed encryption and decryption mechanism.

- Tree based Rekeying for prevention of Denial of Service attack scheme results in storage overhead.

- Neglecting the messages as a solution can end up in DoS.

- For Malicious Insiders attack utilization of several keys results in the issue of settling down the several keys at decryption or deciphering stage.

This dissertation proposes some useful algorithms, classifications and modellings together with interpretations and basic comparisons mainly in case of the proposed IDS design, WiMAX security and VoIP under WiMAX to fill the gap in the literature about the above weaknesses. In order to contribute and address the existing gap, this dissertation zooms on specific and existing attacks. Following this perspective in 2013, M. Hossein Ahmadzadegan et al. published a journal paper and launched a risk analysis of threats and vulnerabilities of VoIP that is a service which can be offered under the framework of IEEE 802.16.

In addition to this, deriving from the notion of bringing about innovative ideas, in 2013, M. Hossein Ahmadzadegan et al. published a paper and explained the degradation occurred in mobile WiMAX due to an instant increase in the number of simultaneous subscribers by an economic model regarded as Kiyotaki-Moore. Moreover, having mentioned the weaknesses and problems of existing security classifications, M. Hossein Ahmadzadegan et al. came up with a hybrid security classification approach which complies with the standards and in the same time fills the gaps.

Regarding the notion of IDS, having said about its necessity and importance, M. Hossein Ahmadzadegan et al. have proposed a more enhanced WiMAX-based intrusion detection system that is in the same time more efficient in terms of power consumption. Further on, the comparative analysis of fixed and mobile WiMAX and the encryption of data and keys in both the technologies has been provided. This is understandable because the similarities and differences offer a more professional perspective. Having this considered, in 2013 M. Hossein Ahmadzadegan et al. published a paper explaining the similarities and differences of WiMAX and LTE in terms of security basics with a comparative analysis approach.

An analysis of the security attacks on the WiMAX and architecture has been carried out as well. Main emphasis would be on the threats analysis of physical and MAC layer. Intrusion Detection System is recommended to be deployed for mitigating some of the threats. Jamming, scrambling, DDoS, rouge BS creation, compromising of X.509 digital certificates are just some of the common attacks on WiMAX technology. The offered techniques deployed contra these attacks are spread spectrum scheme, strong encryption techniques, communication keys security and reciprocal two-way authentication. In addition to this alternatives for authentication are elaborated. All the above mentioned issues are given attention with details in chapters.

4. SECURITY OF IEEE 802.16

4.1 IEEE 802.16 Main Security

There are several security methods defined in data over cable service interface specification (DOCSIS). The 802.16 methods are basically identical to those of DOCSIS (CableLabs® 2013). For encryption of the MPDUs payload, DES is deployed when it comes to WiMAX. The DES data encryption is shown in Figure 13. In addition to this, as previously mentioned PKM Protocol performs certificate-based authorization of the subscriber station. The PKM protocol utilization authentications and RSA public key systems to authenticate a SS to a BS. The SS gives its X.509 certificate to the BS, consequently revealing its identity together with public key to the BS. The BS replies with an authorization key to the SS, ensured by the SS's open key utilizing the RSA calculation.

The SS can decode the acknowledged key utilizing its private key. The authorization key is then deployed to determine key encryption keys (KEKs), the SS and BS, since they are both well aware that the authorization key can infer the same KEKs. To exchange a TEK (temporal encryption key) from the BS to the SS, the TEK is scrambled utilizing the Data Encryption Standard (DES) that is weak. In order to mitigate and encounter the threats, the 802.16e particularly incorporates security upgrades to utilize the AES-CCM coded mode and EAP-based validation (IEEE Std 802.16a, Amendment to IEEE Std 802.16 2001).

Michel Barbeau investigated on some vulnerabilities and security issues of the 802.16. In his paper (M. Barbeau 2005), vulnerabilities and problems related to the PHY and MAC layer were explored and all associated important aspects were investigated and compared with meticulous evaluation procedures set by ETSI. Dangers are grouped according to the level of criticality they have. The chief security problems are eavesdropping the admin management messages, admin management message alteration, BS or MS disguising, and DoS attacks. The WiMAX is said to have the potential to settle down the bandwidth bottleneck problem. Expanding the adventures and blemishes discovered in the 802.11, the WiMAX standard was precisely designed with security issues in mind, providing a more reliable protection.

The WiMAX system is such that a BS is playing the role of a cell phone tower and provides the signals all the time, thus those users who have a WiMAX modem can receive the signals and establish the connection. Therefore in this procedure the security becomes an essential topic to be taken care of. The WiMAX

MAC Protocol is in charge of the user's access to the physical layer. Having said all this, the WiMAX standard network topology outlook can be seen below in Figure 12.

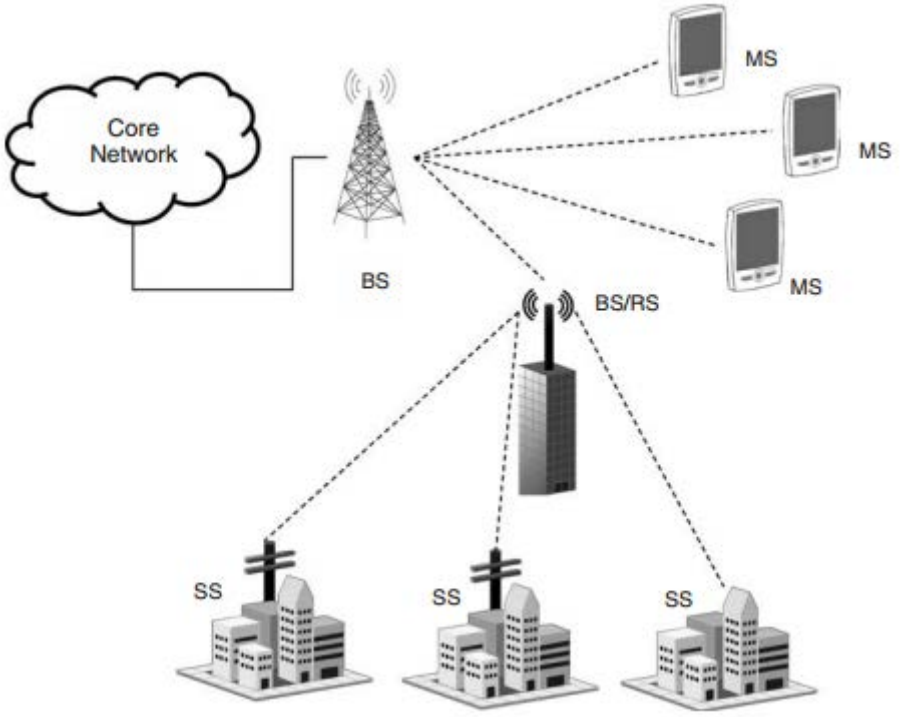


Figure 12. IEEE 802.16 standard's network topology (S. Rekhis et al. 2010)

When it comes to the 802.16 MAC, first-in first-out (FIFO) scheduling algorithm is deployed for the traffic and its associated issues. The 802.16 MAC protocol provides relatively ideal QoS by a fair bandwidth allocation.

4.2 Past IEEE 802.16 Security Concerns

Despite the fact that IEEE 802.16-2004 standard has all the elements of being secure because of the combination of security mechanisms within the MAC layer's security sublayer, numerous security shortcomings identified with this form were uncovered and are depicted by the previous carried out research works. Many of these shortcomings are identified with confirmation, protection, key administration and accessibility. This part portrays the fundamental security shortcoming identified the IEEE 802.16 standard, indicating potential security risks and the practical countermeasures to avert them.

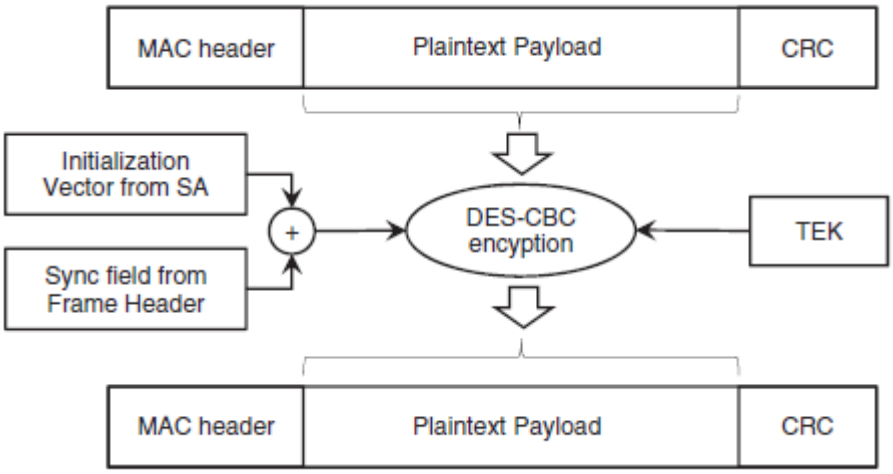


Figure 13. DES data encryption (IEEE 802.16 2004)

4.2.1 Physical Layer Attacks

The security issue is characterized on top of the physical layer when it comes to WiMAX standards, causing the network to inherit the susceptibilities of wireless medium. Therefore physical layer becomes susceptible to scrambling, jamming, flooding and forgery attacks. S. Xu and his colleagues suggested that jamming security risk comprises of creating a powerful Gaussian noise for diminishing and interfering the wireless channel's capacity (S. Xu et al. 2006). Such conduct may compromise administration accessibility, particularly if the attacker has shut the BS. If it is so then what WiMAX deploys like Scalable OFDM access (SOFDMA) and Orthogonal Frequency Division Multiple Access (OFDM) cannot fit for taking care of such sort of attack (S. Xu et al. 2006).

A jamming attack requires particular fittings. The danger connected with such a risk, which could be easily distinguished utilizing radio range analyzers and checking supplies, is critical. U. Tariq, and his colleagues highlighted that the area of the attack might be discovered utilizing radio scanning instruments (U. Tariq et al. 2007).

A scrambling attack implies to scramble administration or control data in a selective way, therefore disturbing the usual operation of the system, or even compromising the system and controlling it. Scrambling becomes very critical particularly when it addresses messages that are not delay tolerant, incorporating channel estimation report requests or reactions. A jamming attack could be distinguished hinging upon the dissection of disparities with respect to the framework's execution. Flooding is an alternative sort of attack belonged to the physical layer that

includes transmitting pointless frames keeping in mind the end goal to empty the SS's electric storage device or evaporate. In this setting, an alternative method for catching and tossing the fake outlines should be utilized. Therefore in brief the threats and their solutions can be as follows:

- Jamming attack

Jamming is described by M. Barbeau as an attack that can be launched by introducing a source of noise strong enough to significantly diminish the capacity of the channel (M. Barbeau 2005). Jamming can be either intentional or unintentional. It is not difficult to perform a jamming attack because necessary information and equipment's are easy to acquire.

Solution: According to M. Barbeau, one can protect against jamming attack by increasing the power of signals or by increasing the bandwidth of signals deploying methods of spreading like direct sequence spread spectrum (DSS) or frequency spread spectrum (FHSS). Furthermore as a result of the fact that, it is easy to detect jamming by deploying radio spectrum monitoring equipment and the sources of jamming are easy to be traced by deploying radio direction finding instruments, one can also ask help from law enforcement to stop the jammers.

- Scrambling attack

Also analyzed in (Barbeau 2005), scrambling can be considered as a kind of jamming but only provoked for small time intervals and targeted to particular WiMAX frames at the PHY layer. Attackers can selectively scramble administration or control data for affecting the normal network's functioning. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more intricate to perform a scrambling attack than to perform a jamming attack due to the need, by the attacker, to interpret control information and to send noise during specific intervals".

Solution: As a result of the fact that scrambling is occurring at irregular intervals, it is much more intricate to detect scrambling than jamming. Fortunately, one can utilize anomalies monitoring beyond performance norm to detect scrambling and scramblers.

- Flooding attack:

According to D. Johnson and J. Walker (D. Johnson et al. 2004), this is also a usual attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This type of attack is count-

ed as even more destructive than a typical Denial-of-Service (DoS) attack since the SS that is a normally a portable device is possible to have limited resources.

Solution: To prevent this kind of attack, a complex mechanism is essential to discard bogus frames, therefore avoiding running out of battery or computational resources.

- Forgery attack

In addition to threats jamming, scrambling and flooding attacks, 802.16 is also vulnerable to other attacks such as forgery attacks in which an attacker with a radio transmitter can write to a wirelesschannel (D. Johnson 2004) . In mesh mode, 802.16 is also vulnerable to replay attacks in which an attacker retransmits valid frames that the attacker has intercepted in the middle of relaying process.

4.2.2 Authentication Attacks

During the PKM protocol's authorization, mobile automatically dispatches its certificate for authenticating itself whereas the base station does not. An intruder can impersonate and pretend to be an authorized base station and in this way attract the mobile station. The attracted mobile station will strive to establish connection to the rouge base station. In case the CSMA mechanism is deployed, the intruder would normally be able to obtain the identity of the base station, and postpone the action until the medium allows the message transmission deploying the base station identity. The utilization of TDMA makes the attacks so intricate in 802.16 networks because the attacker should obtain the identity of the base station and wait for the authorized base station's time slot. It sends the message deploying a high power for forcing the subscriber station to block the signal transmitted by the authorized base station (Michael Barbeau 2005). Following the striving to attach itself to the fake base station, the subscriber station goes on with the PKM protocol's authorization through dispatching the primary two messages.

As soon as the Authorization- RepMess is received, the fake base station returns an authorization response message to the subscriber station. In it's content, the intruder puts an AK that is coded with the subscriber station's public key. As a result of the fact that, SS usually does not check the authenticity of the captured message because of impersonation and already establishing the connection, it approves the captured AK and goes on with KEK followed by generation of downlink/uplink HMAC keys therefore the intruder can get control over the communication of the subscriber station. Thus at the base station, by utilization of the credentials belonged to subscriber station, the intruder can register herself success-

fully, furthermore carrying out a MIM attack. The chief shortcomings associated to the explained attack are as a result of the lack of reciprocal two-way authentication (T. F. Elrahman 2005).

In order to make sure that subscriber station can authenticate the base station seamlessly, a probable way can be integration of the authorization response message, base station's certificate and the signature. For warrantying the activeness of the authorization response message together with replay attacks prevention, it is recommended to complement it with the relevant timestamp information that the subscriber station attached in the authorization request message. When it comes to the authorization request message, the point is to secure the base station against replay attacks and allow the subscriber station to check if the received message matches with the transmitted demand. One can notice the fact that the base station should take into account the attached timestamp throughout the signature of the authorization response message.

The principle impediment identified with the deployment of timestamps includes the requirement to adjust the subscriber station with the base station. It ought not to be challenging subsequent to the WiMAX standard, the subscriber station and base station adjust with one another throughout the first ranging prior to the PKM protocol's starting point. There the timestamps will be deployed. Some modifications were suggested for deploying timestamps as a countermeasure contra replay attacks (S. Xu, M. Matthews and C.-T. Huang 2006). The formal presentation of the messages can be observed as follows:

1. AuthenticationInfMess (SS → BS): Cert (Manufacturer(SS)).

2. AuthorizationReqMess (SS → BS): TSS | Cert(SS) | Capabilities | SAID | SigSS.

3. AuthorizationRepMess (BS → SS): TSS | TBS | [Pre-AK]pubSS | LifeTimeAK | SeqNo

| SAIDList | Cert(BS) | SigBS.

The subscriber station generates the timestamps that are denoted by TSS and injected in the authorization request message. In order to fight back against replay attacks, the base station puts the subscriber station's timestamp captured from the second message in the authorization response message, together with a newly issued TBS timestamp.

The message number two together with the message number three are signed by subscriber station and base station's private key. SigSS and SigBS represent the

two generated signatures. Through the aid of the timestamp and the signature of the base station, the subscriber station becomes able to check if the captured message is active and matches with its request.

Utilizing NonceSS rather than timestamps can be a practical result in authorization request/ response messages. It should be highlighted that deploying the public key of the subscriber station, the authorization response message's nonce may alternatively become ciphered. Other alternative can be utilizing pre-shared AK instead of AK and permit the base station and the subscriber station for deriving the AK (S. Rekhis et al. 2010).

Therefore there should be a promising method for pre-AK's integrity and authenticity transmitted among the base station and subscriber station. D. Johnston and J. Walker suggested that it is possible to change the PKM protocol's authorization as it can be oberved:

1. AuthenticationInfMess (SS → BS): Cert (Manufacturer(SS).

2. AuthorizationReqMess (SS → BS): NonceSS | Cert(SS) | Capabilities | SAID.

3. AuthorizationRepMess (BS→SS): NonceSS | NonceBS | [Pre-AK]pubSS | LifeTimeAK

| SeqNo | SAIDList | Cert(BS) | SigBS.

The subscriber station issues the NonceSS which is a random number, and further injects it in the authorization request message. Both the received NonceSS together with NonceBS are injected in the authorization response message by the base station.

The suggested measure just issues permission to the subscriber station to ascertain that the message number 3 is active and matches with its demand. When it comes to the authorization request message, for safeguarding the base station against the replay attacks, a set of already captured nonces from the same subscriber station must be deployed for detecting the replayed messages.

4.2.3 Key Administration Attacks

The PKM protocol's key administration stage is also susceptible when it comes to replay kind of attacks. Indeed, in certain cases, the subscriber station is not capable of distinguishing between a novel and an old reutilized data SA, particularly as the key response message does not contain enough data for checking the au-

thenticity of the replier's. The 802.16 key administration protocol is presented below:

Message 1. BS--->SS: SeqNo| SAID | HMAC (1)

Message 2. SS--->BS: SeqNo| SAID | HMAC (2)

Message 3. BS--->SS: SeqNo| SAID | OldTEK |

NewTEK | HMAC (3)

After authentication is carried out, subscriber station starts to ask for keying materials. The subscriber station transmits a key request message to the base station regularly, associated with one of its legitimate SAIDs. The base station replies with a Key-Reply message, including the BS's active keying material for the specific SAID. In this protocol, message 1 is arbitrary. BS transmits re-key message (message 1) to subscriber station just if base station considers it required to rekey prior to when subscriber station asks for it. The base station will select a SAID from the SAID list which the subscriber station is permitted to access. SeqNo is the sequence number of AK given by base station to this subscriber station in the authentication protocol.

This number permits the subscriber station (and base station in the next message) to determine which HMAC_KEY_D (HMAC_KEY_U in the next message) was actually deployed to authenticate the message. HMAC(1) is the digest of message 1 under HMAC_KEY_D. Both of the downlink HMAC key (HMAC_KEY_D) and the uplink HMAC key (HMAC_KEY_U) are originated from the AK. By calculating the value HMAC(1), it permits SS to identify message forgery or corruption. Once receiving message 1, SS will answer with the Key- Request message (message 2). In case SS does not get message 1 from BS prior to when the present key expires, SS will transmit the normal Key-Request message when the present key is near expiration, where the SAID is selected by SS itself from the SAID list, to ask for a refresh of keying material for this specific SAID. HMAC(2) is the digest of message 2 under HMAC_KEY_U, which ascertains BS about the authentication of the message. Further on the BS answers with the Key-Reply message (message 3) at once after receiving the SS's request that contains keying materials. Always BS keeps two active sets of keying material per SAID. The OldTEK is the keying materials for the presently used TEK, and the New-TEK is the keying materials for the new to be used after the current one expires TEK. The keying materials comprises the TEK ciphered by the KEK (Key Encryption Key) that is also originated from the AK. Moreover, the set of keying materials also contains the CBC initialization vector and the remaining lifetime of

each set of keying materials. HMAC(3) is the digest of message 3 under HMAC_KEY_D. As in message 1, HMAC(3) ascertains SS that message 3 is from BS and has not been changed. The key administration protocol is threatened by the message replay attack that is counted among the chief perils. The SS is not able to distinguish the reused data SAs, exactly similar to when it cannot distinguish reused authorization SA in authentication protocol. It should be mentioned that if the opponent resends message 3 to SS following when the SS has previously interchanged some keying materials with BS, the SS can express handily if message 3 matches with its request. This is due to the fact that each SAID keeps two set of keying materials, and that the relevant OldTEK received key reply message a little while ago should be the NewTEK in the past key reply message. Thus, for carrying out the replay attack, the opponent should mislead the SS from the starting point when initially the SS asks for keying materials. However by now the opponent will encounter another hurdle. The responsible utilization of the AK offers a manner for both BS and SS to verify the validity of the key administration protocol instance. In case the opponent wants to replay an old Key Reply message, the HAMC_KEY_D deployed in HMAC(3) should be originated from the AK that the SS utilizes presently. Therefore the sole opportunity for the success of this replay attack is that the opponent eavesdropped and saved a previous sequence of interchanged key request/reply messages, and the key administration protocol is reset that makes SS asking for a completely new keying materials. The countermeasure against this attack is forcing SS to ask for a new AK every time the present key administration protocol instance is reset or fails (S. Xu 2006).

The messages should be tied to a certain protocol for preventing replays from succeeding contra key administration. The method is to put the nonces interchanged in the past Authentication Protocol as the instance identifier but the responsible utilization of the AK already offers a manner to detect these instances. The SeqNo of AK offers some connections between the instance of related key administration protocol and the instance of authentication protocol. Nevertheless this number of 4-bits long is susceptible to be reused and thus makes the key administration protocol liable to replay attack, the digest of these messages interchanged while key administration takes place offers a path to ascertain both parties about the legitimate AK's validity. For the replay attack to be successful, the opponent must not just replay the SeqNo, but also replay the correct HMAC message whose ciphering key is originated from the presently deployed AK in the associated authentication protocol instance. The key administration protocol instance's binding failure to its associated authentication protocol instance will take place just in case when by chance another example of authentication protocol happened to have the same AK and the same SeqNo. As a result of the AK's random generation, this is labeled as rare.

Even though the subscriber station is free from the replay attacks when it comes to message 3, base station is yet susceptible to replay attacks on message 2. The reason behind is that the key request message does not have the keying material similar to the key reply message that permits the receiver to make comparison with its already received message. Therefore if an opponent replays the key request message to base station, the base station is not capable of distinguishing if it is subscriber station's fresh request or just an old one. Thus, base station then answers with message 3 that allocates new keying materials to subscriber station in case when subscriber station did not ask for at all. This can lead to regular interchange of keying materials which may cause the confusion in the utilization of TEK or an overflow of base station's capabilities. This case is relatively identical to the one base station encounters in the authentication protocol. Eventually, this attack leads to the fact that both the subscriber station and base station interchange keying material without intentions. The following method was suggested by S. Xu, M. Matthews and C.-T. Huang to stop this attack:

1. RkeyMess (BS → SS): TBS | SeqNo | SAID | HMAC(RkeyMess)

2. KReqMess (SS → BS): TBS | TSS | SeqNo | SAID | HMAC(KReqMess)

3. KRepMess (BS → SS): TSS | TBS | SeqNo | SAID | OldTEK | NewTEK | HMAC

(KRepMess)

Therefore basically the base station and subscriber station issue the TBS and TSS which are the 2 timestamps existing in messages they transmit. In case the base station transmits the alternative message RkeyMess, the subscriber station incorporates the TBS issued in that message in the KReqMess message. The base station can delete or neglect it in KRepMess by fixing its value to null. If the RkeyMess is not transmitted and the subscriber station begins the request, the timestamp TBS is set to null in KReqMess. The base station sets the TBS in KRepMess message associated to the KReqMess message's TSS value (S. Xu et al 2006).

For recognizing the TEKs, the standard deploys key identifiers of 2-bits long in a round buffer. Normally, within the largest value of AK lifetime, the key identifier space must support the deployment of several completely diverse key identifiers. Based on facts AK lifecycle can last up to 70 days, moreover the shortest TEK is 30 minutes long, therefore the key identifier section supports circa 3360 various TEKs. The latter ranges from three to null on each fourth rekeying action. An

intruder may then replay the utilized TEKs which will lead to a compromise of the TEK and the data.

4.2.4 Privacy Attacks

The WiMAX standard demonstrates the support for encryption by incorporating DES in CBC mode as an encryption algorithm. This algorithm has a mechanism which applies on data blocks of 64 bits to carry out the encryption or decryption action and utilizes 56-bit DES keys (TEK) and an Initialization Vector (IV). Basically, 56 bit key cannot be considered as secure enough as far as today's requirements are concerned, that handily permits one to check each and every probable key in a specific interval of time. In addition to this, the CBC-IV can be predicted because the SA IV is fixed and public for its TEK and the physical adjustment is typically repeated so many times. To deal with this issue and at the same time keeping the alternative of the utilization of DES, the only way would be producing each per-frame initialization vector in a random manner and injecting it in the payload, but this way definitely adds to the encryption overhead.

D. Johnston and J. Walker, claim that the CBC modes deploying block cipher can become untrustworthy after a certain amount of operation on $2^{n/2}$ blocks, where "n" denotes the block size. As a result of the fact that DES utilizes 64 bit blocks, it results in insecurity if deployed on more than 2^{12} 64-bit blocks. As already mentioned, the normal TEK life cycle is half of a day but lasts at most for up to seven days. If the pace permits one to generate the 2^{12} 64-bit blocks in an interval of time smaller than the TEK lifecycle, then the encryption scheme becomes very susceptible because if more tries would be performed and the security is only safeguarded up to a certain limit. Therefore if one takes a pace of 6 Mbps, the total of 2^{12} blocks will be generated in twelve hours.

Another essential point is that the data protection mechanism deploying DES not only fails to offer an acceptable confidentiality but also is not successful to protect contra replay attacks. According to the shortages and existing lacks regarding the deployment of DES, the standard permits for ciphering of the message utilizing the AES in CCM mode with 128 bit TEK key.

4.2.5 Attacks on Availability

Another method comprises of over harnessing and overusing the message replay in such a way that the authorized base station would be rejected (E. Eren and K.-O. Detken 2008). As a result of the fact that the authorization request message

does not include any section that makes sure if it is fresh and active, the PKM protocol becomes susceptible to replay attack.

Following when an authorized subscriber station transmits the authorization request message, the intruder intervenes and blocks this message and saves it. It would furthermore transmit the received message continuously to the base station. Considering the fact that this action does not permit the intruder to get the AK's value, it can overload the base station and cause it to reject the authentic and authorized subscriber station (E. Eren 2007).

To protect contra similar attacks, the authorization request message must include a nonce or time-stamp together with the signature of the subscriber station to make sure about the activeness and authenticity of the message.

When it comes to the second stage of the PKM protocol, considering the fact that the replay attack on the KRespMess message is not expected to be successful, the base station continues to be susceptible to an attack targeted at KReqMess message. Indeed, unlike the KRespMess message, the KReqMess message does not include keying materials that permit the receiver to make a comparison with the already captured message. As a result of the fact that the base station cannot check the activeness of the captured message, it would produce and allocate a novel keying material to the subscriber station, even if the latter did not ask for it. Further on, it answers with a KRespMess message to the subscriber station. It can be considered that if this procedure takes place regularly, it may end up the resources of the base station (E. Eren 2007).

Ranging Response messages (RNG-REP) that are interchanged while the node attachment takes place, are susceptible to numerous kinds of attacks. Indeed, these messages are not ciphered and thus they cannot be authenticated together with being stateless. As a result of the fact that a subscriber station takes into account instantly the novel parameters offered by the base station, RNG-REP messages could be utilized in a rogue and negative way by an intruder.

One of the arbitrary sections of this message, is the Ranging Status section that is deployed to state if uplink messages are captured within acceptable bounds by the base station. An intruder can distinguish the Channel ID (CID) that the target subscriber station is utilizing and produce a spoofed RNG-REP message by fixing the Ranging Status section to 2.

One should take care of the fact that the intruder can handily apply the brute force on the Channel ID by trying all the 65 536 expected values. Thus the target sub-

scriber station is blocked and not permitted to carry out regular ranging and is therefore excluded from the network.

According to the existing shortages and lacks in safeguarding the RNG-REP message, an intruder can utilize that message to disallow the downlink/uplink channel that the subscriber station utilizes. In case there is no base station functioning within that channel, the subscriber station will keep on to navigate and screen the frequencies by sniffing for a minimum of 2ms prior to moving to the next channel.

Hinging on the number of active channels, the latter action can last for a remarkable time interval. It is crucial to mention that after scanning the all the channels, the subscriber station will strive to reutilize the suitable channel. If the intrusion is happening again and again, the subscriber station would be incapable to get access to the network and deduces to a denial of service.

4.3 Present IEEE 802.16 Security Concerns

In WiMAX, the security sublayer was redesigned for manipulation of security faults existed in the past editions of this protocol and fulfill the security needs for mobile services.

In this framework, the security sublayer is improved, ciphering mechanisms are enhanced, reciprocal two-way authentication methods are suggested to safeguard contra numerous sorts of replay and MiM intrusions, pre-authentication among the base station and mobile station is put forward to diminish any possible services interruption while handover operations, a key hierarchy is designed to permit an mobile station authenticating itself with an AAA server once not dependent on the number of base station it authorizes with handover and then the PKM protocol is further expanded to version two.

It is of great importance to mention that in the expanded IEEE.16e security sublayer, both editions of the PKM protocol are covered. Version one is basically expanded to cover novel ciphering mechanisms entitling AES-ECB for confidentiality of the key material, TDES-EDE and AES-CCM for confidentiality of MPDU purposes (S. Rekhis et al. 2010).

From the other perspective, HMAC-SHA-1 is utilized for safeguarding the key administration message’s integrity. In this part, the security aspects of IEEE 802.16e would be clarified by explaining the improvement introduced associated

with the IEEE 802.16-2004 edition. Moreover characteristics and methods offered by the deployment of PKM second edition are concentrated in details.

4.3.1 Access Control, Authorization, Reciprocal Two-way Authentication

The PKM second edition protocol covers reciprocal two-way authorization and authentication providing the chance for the base station and subscriber station to identify each other's specifications. Various sorts of reciprocal two-way authentications are covered: EAP-based authentication (P. Urien and G. Pujolle 2008), RSA-based authentication together with EAP based authentication. RSA-based authentication includes the utilization of RSA encryption and X.509 certificates. EAP entitles the symmetric type of cryptography and is according to the utilization of EAP that is basically an authentication protocol for user authentication while accessing to local or remote networks.

The AAA architecture which is a reverse authentication infrastructure is deployed. The mobile authentication can be carried out utilizing a credential generated by the X.509 digital certificate or the operator. Numerous EAP authentication mechanisms (T. Otto 2006) are covered by the second edition of PKM, consisting EAP-AKA, EAP-TLS and EAP-CHAPv2. The feedback of EAP is 512-bit key, regarded as the Master Session Key (MSK) that is the origin of key hierarchy. By the aid of this key, the mobile station and the base station obtain a Pairwise Master Key (PMK) that is itself deployed to get to the AK.

Here a model based on the RSA authentication is suggested that is a key transport protocol deployed by the authorization stage of the PKM second edition protocol (A. Altaf, M.Y. Javed and A. Ahmed 2008). In this edition of the PKM protocol, a reciprocal two-way authentication method is deployed, and nonces are added to safeguard contra replay attacks. The authorization stage that is demonstrated below, is comprised of 4 stages, where the initial stage is optional:

1. Authorization initiation (MS → BS): MS.manufacturerCert.

2. Authorization Request (MS → BS): NMS | MSCert | Capabilities | BCID.

3. Authorization Reply (BS → MS): NMS | NBS | KUMS(pre-AK, MSID) | SeqNo |

Lifetime | SAIDs | BSCert | SIGBS (Authorization reply).

4. Authorization Acknowledgement (MS → BS): NBS | MSaddr | AK(NBS, MSAddr).

Indistinguishable to the PKM first edition, it is the mobile station that begins the authorization protocol. It would transmit an optional message consisting the mobile station manufacturer's certificate. The mobile station afterwards transmits an authorization request message containing its X.509 certificate, together with a nonce, represented by NMS, consisting 64-bit value which it issues.

The message as well entitles the mobile station's potentials together with the Basic Connection Identity (BCID) that is identical to the CID and allocated to the mobile station when it move into the network and asked for ranging. It is to be highlighted that, this message is not protected and can be a victim to rogue tries or alternations.

The base station replies with an Authorization Reply message after authorization request message's reception, including the mobile station's nonce, NBS that is a nonce issued by itself together with its certificate, pre-AK with mobile station's identifier (MSID) ciphered by the public key of the mobile station's and the characteristics of the Authorization key containing the sequence number, lifetime of the key and a single or several SAIDs (S. Rekhis et al. 2010).

The base station signs the authorization reply message. It is crucial to highlight that the SAIDs in this message are arbitrary if an RSA authorization interaction would proceed by an EAP authentication interaction. The AK would be originated from the pre-AK with the base station and mobile station addresses. As a result of the fact that an authorized subscriber station is capable of extracting the Pre-AK, the mobile station authorization may be verified in accordance with the condition of having the pre-AK.

For the base station to be able to approve the authorization request message and also an authorization acknowledgement message is transmitted by the subscriber station to the authorization reply message's reception through the base station to ascertain that the subscriber station has come up with a valid access request to the network services. This message comprises of the base station's transmitted nonce, the mobile station's MAC address ciphered with the pre-AK and the respective MAC address. In WiMAX networks, the mobility is covered in such a way that a mobile station can hand over from one visited base station to another. While the handover action takes place, a mobile station can utilize the pre-authentication with the new base station rather than performing the whole authorization process from the scratch.

In fact, as a result of the protocol of authentication being in accordance with the public key infrastructure's utilization, it might be recommended to avoid such steps and speedup getting into the network by initiating a new authorization key

in the targeted base station and mobile station in accordance with a pre-authentication mechanism. When it comes to migration of the voice call, for instance, the International Telecommunication Union proposes taking a certain time interval of fewer than thirty milliseconds from the first base station's leaving moment to establishing the context at another base station.

Normally, in case a Ranging message transmitted by a mobile station involves the novel serving BSID, and in case the base station to which the mobile station hands over has previously captured backbone's message including the data of mobile station, the PKM protocol's re-authorization procedure must be utilized by the mobile station and the novel base station to accomplish the network re-entrance when it comes to handover.

4.3.2 TEK 3-Way Handshake

The handshake protocol covers many actions involving activation of keys, negotiation on SA factors, acceptance of security negotiation and SA factors refresh (T. Haibo, P. Liaojun and W. Yumin 2007).Thus, the protocol is followed up to the first authorization or while handover takes place as below:

1. SA-TEK Challenge (BS → MS): NBS | SeqNo | AKID | LifeTime |H-C/MAC(-).

2. SA-TEK Request (MS → BS): NMS | NBS | SeqNo | AKID | Capabilities | SecNego-

Params | PKM Config | H-C/MAC(-).

3. SA-TEK Response (BS→MS): NMS | NBS | SeqNo | AKID | SA-TEKUpdate | Frame-

No | SA-Descriptors | SecNegoParams | H-C/MAC(-).

The AK can be originated from one of the three different ways hinging on the authentication scheme deployed. Prior to the beginning of the three-way handshake, the BS and SS derive a common shared KEK together with the HMAC/CMAC keys. The PKM second edition three-way handshake process takes place as follows. While the first network entry takes place, the BS transmits PKM second edition SA-TEK-Challenge to the SS after safeguarding it with the HMAC/CMAC. If the BS does not receive PKM second edition SA-TEK-Request from the SS within SAChallenge-Timer, it retransmits the past PKM second edition SA-TEK-Challenge up to SAChallengeMaxResends times. If the BS gets to

its maximum number of retransmissions, it starts another complete authentication or sometimes discards the SS (WiMAX Made Simple 2010).

If HO Process Optimization is fixed at Bit #1 , demonstrating that PKM authentication phase is ignored while network re-entry or handover, the BS starts the three-way handshake by attaching the SAChallenge tuple TLV to the RNG-RSP. If the BS does not receive PKM second edition SA-TEK-Request from the MS within SaChallengeTimer, it can drop the MS or start a complete re-authentication. In case the BS gets an initial RNG-REQ when PKM second edition SA-TEK-Request is expected, it will then transmit a new RNG-RSP with another SaChallenge TLV.

The SS transmits the PKM second edition SA-TEK-Request to the BS next to safeguarding it with the HMAC/CMAC. In case the SS does not get PKM second edition SA-TEK-Response from the BS during the expected time in SATEKTimer, then it has to retransmit the request. The SS may retransmit the PKM second edition SA-TEK-Request up to SATEKRequestMaxResends times. In case when the SS gets to its maximum number of retransmissions, it must start another complete authentication or strive to associate with another BS. The SS entitles the security capabilities that it included in the SBC-REQ message while the basic capabilities negotiation phase takes place.

As soon as when the PKM second edition SA-TEK-Request is received, the BS approves that the supplied AKID points to an AK that is existing and available. In case when the AKID cannot be recognized, the BS ignores the message. The BS also checks the HMAC/CMAC. If the HMAC/CMAC is not valid, the BS neglects the message. The BS must check that the BS_Random in the SA TEK Request corresponds with the value given by the BS in the SA Challenge message. In the scenario when the BS random value does not correspond, the BS will neglect the message. Moreover, the BS must check the SS's security capabilities encoded in the security negotiation parameters characterization contra the security capabilities offered by the SS through the SBC-REG message. In case when the security negotiation parameters do not corresponds, the BS will report the issue to upper layers. As successful validation of the PKM second edition SA-TEK-Request accomplishes, the BS transmits PKM second edition SATEK-Response back to the SS. The message contains a list of compound TLV each of which determines the static and primary SAs, their SAID’s, and other in detailed characteristics belonging to the SA which the SS is authorized to access. In the event when an HO takes place, the individual features of any dynamic SA that the asking MS was authorized in the past serving BS are available too. Moreover, the BS should entitle, via security negotiation parameters characterization, the security potentials

that it aims to highlight for the session with the SS. Moreover when it comes to HO, for every active SA in past serving BS, the matching GTEK, GKEK and TEK parameters are included as well. Therefore, SA_TEK_Update offers a shortcut mechanism for re-newing active SAs deployed by the MS in its past serving BS. It should be mentioned that TLVs determine SAID in the aimed BS that will substitute with active SAID utilized in the past serving BS together with "older" and "newer" TEK-parameters associated with the active SAIDs. The update can contain as well items like multicast/broadcast Group SAIDs (GSAIDs) and associated GTEK parameter pairs. When it comes to unicast SAs, the TEK-parameters characterization includes the whole associated keying material matching an specific generation of an SAID's TEK. This actually consists of the TEK, the TEK's left key life-time, its key sequence number, and the CBC IV. The TEKs are ciphered with the KEK. In the scenario of having group or multicast SAs, the TEK-parameters characterization includes the whole keying material matching to a certain generation of a GSAID's GTEK. This will be comprised of the GKEK, the GTEK, the GTEK's left key lifetime, the GTEK's key sequence number, and the CBC IV. The GTEK's type and length is equal to the ones of the TEK. The GKEK has to be shared similarly in the same multicast or broadcast group. The GTEKs and GKEKs are ciphered with KEK due to the fact that they are sent in form of a unicast. The HMAC/CMAC is regarded as the eventual attribute in the attribute list of the message. By the time when PKM second edition SA-TEK-Response is received, an SS checks the HMAC/CMAC. In case the HMAC/CMAC is not valid, the SS neglects the message. After successful validation of the PKM second edition SA-TEK-Response is accomplished, the SS set-ups the already received TEKs and related parameters correctly. The SS is also in charge of checking that the BS's security negotiation parameters of TLV encoded in the security negotiation parameters characterization against the security negotiation parameters of TLV offered by the BS via the SBC-RSP message. In case when the security potentials and capabilities are not corresponding, the SS has to report the issue to higher layers. The SS may opt to keep on the communication with the BS. In this scenario, the SS may adopt the security negotiation parameters encoded in SA-TEK-Response message (WiMAX Made Simple 2010).

4.3.3 Encryption and Key Hierarchy

When it comes to WiMAX standard, in order to encrypt the MAC PDU's payload, either the 128- bit keys of the Advanced Encryption Standard/ CCM mode or 56-bit keys of the Data Encryption Standard/CBC mode are deployed. In the initial mechanism, the data to be encrypted is separated into various blocks whereas just a single one is encrypted with the key.

Utilizing the second mechanism, the data is separated into various blocks of 128-bits long. Each and every ciphered MAC PDU includes a prefix of 4 bytes, denoting the packet number based on the SA. An Integrity Checking Value (ICV) of 8-bytes long is further attached to the payload's end. The packet number is not ciphered but involved when it comes to the ICV's authentication.

The payload of MAC PDU and the ICV are ciphered by the TEK deploying AES in CCM mode. By entitling a packet number, AES offers a method against replay attacks, in such a way that any packet number captured more than one time within a fix interval of time would be ignored. If one compares AES with DES or TDES, it has a better security but in the same time it is computationally more complex (IEEE Std 802.16TM-2004 2004: 35).

In mobile WiMAX data ciphering is done deploying AES in three more modes, chiefly 1- CBC mode having 128-bit keys 2- For broadcast/multicast services Counter mode (CTR) is used which has keys being 128-bits long 3- the Key-Wrap.

In the generic MAC header, the Encryption Control (EC) bit is deployed to judge if the MAC PDU is ciphered or not. It is to be highlighted that both the general MAC header and the general and initial MAC administration messages are not encrypted in mobile WiMAX. S.R. Bajgan, M. Pooyan, A. Khalilzadeh and R. Abdollahi in 2008 explained the utilization of AES in CTR mode with CBC authentication code (CCM). However for TEK ciphering with KEK, the mobile WiMAX standard covers four mechanisms, chiefly 1- TDES in EDE mode utilizing 128-bit keys, 2- RSA ciphering utilizing 1024-bit keys, 3- AES ciphering in ECB mode utilizing 128 bit keys and 4- AES Key Wrap utilizing 128-bit keys (S. Y. Tang et al. 2010).

It is clear that just the fourth mechanism is particular to mobile WiMAX, the rest were previously existing in past standards. Despite AES that utilizes the complete KEK's 128 bits to cipher the TEK, the TDES EDE mode utilizes the initial KEK's 64 bits for ciphering and the rest 64 bits for deciphering. The encryption procedure is done in three stages. Primarily, the TEK is ciphered by the first KEK's 64 bits, whereas in the second stage the first cycle's output is deciphered utilizing the second KEK's 64 bits. The third stage includes ciphering the second cycle's output utilizing the first KEK's 64 bits.

In the initial stage, the TEK is ciphered by the initial KEK's 64 bits whereas in the second stage the initial stage's outcome is deciphered deploying the second KEK's 64 bits. The third stage includes the ciphering of the outcome of the second stage utilizing the initial KEK's 64 bits. In addition to this, when it comes to

Mesh WiMAX structure, the TEK ciphering is carried out according to the deployment of the subscriber station's public key of the RSA.

4.3.4 Multicast and Broadcast Service (MBS)

The MBS of mobile WiMAX enables the distribution of data to multiple mobile stations with one single message therefore saving cost and bandwidth. As a result of the fact that base station should distribute the data securely, basically the whole nodes should have a shared group key. The key is regarded as GTEK and is deployed by the base station to cipher the broadcast or multicast traffic. The MBS of WiMAX utilizes an algorithm regarded as MBRA (Multicast and Broadcast Rekeying Algorithm) to issue, maintain and renew the GTEKs. Based on to the mentioned algorithm, a mobile station obtains the first GTEK by the aid of the Key Request/Reply messages. The mentioned messages are sent over the first management connection. Further on, for GTEK refreshment, the base station will send a PKM second edition Group Key Update Command message including an encrypted _ deploying the GKEK _ fresh GTEK to the members of the mobile station group. In fact, the WiMAX standard has 2 kinds of the PKM second edition Group Key Update Command message: the GKEK Update Mode and GTEK Update Mode. The first one is deployed for GKEK refreshment, whereas the other is for the GTEK refreshment of MBS. These two messages comprise a counter, namely Key Push Counter, for protection against replay attacks.

More specifically, the MBRA is executed as follows: the base station via its initial administration connection transmits a Key Update Command to every mobile station for the GKEK update. The message includes the new GKEK ciphered through the KEK. Each mobile station holds a specific key KEK that is originated from the Authorization Key (AK) established during authentication. Then, the base station sends a Key Update Command for the GTEK update via broadcast type of connection. The latter includes the new GTEK ciphered with the corresponding GKEK. In this context, broadcast messages are encrypted with a shared key (GTEK) known within the group. It is to be mentioned that, each member is able to decipher the traffic using the same known key. Message authentication is in accordance with the mentioned same key too. However, every group member is able to encrypt and authenticate messages as if they originate from the legitimate base station. The distribution of the GTEK when the MB RA is deployed is another critical issue. Specifically, GTEK is encrypted with the GKEK and broadcasted to all group members (G. Kambourakis et al. 2010). It is essential to observe that GKEK is also a shared key known to every group member. Thus, utilizing the GKEK, a malevolent insider is able to create fake encrypted and authenti-

cated GTEK Key Update Command messages and attempt to distribute this GTEK. In case this scenario goes as planned, members of the group cannot decipher MBS traffic coming from a real base station anymore.

An insider can force mobile stations to accept the forged key in diverse manners. If the system is not suitably implemented, the key contained in the last one of subsequently sent GTEK update command messages may substitute the original one. Therefore, all the adversary has to do is transmitting its GTEK update command message following when the base station broadcasts a Key Update. In case the implementation is according to the standard, the keys belonging to the two messages are accepted. Thus, the insider could falsify specific parts of the base station's GTEK update command message making the receiving mobile station to discard it. After that, the attacker can send its own GTEK update command message to the mobile stations. Considering the fact that MBS is one directional, the base station cannot distinguish that the mobile station has different GTEKs. In addition to this, the MBRA has another two chief lacks. Primarily when it comes to scalability: whenever the base station should refresh the GKEK, the new GKEK should be announced to all mobile station’s utilizing their respective key KEKs. Secondly, MBRA has several problems when it comes to the issue of forward/backward secrecy. By the time a new member gets into the group and captures the present GTEK, it can decipher the whole past multicast messages transmitted during the same GTEKs lifetime. Also, a mobile station that leaves the group can capture the following GKEK and decipher the following GTEK until the expiration of the present KEK. Moreover, GTEK lifetime has considerable impact on scalability and on forward/backward secrecy too. The standard does not mention any directions about the lifetime of the GTEK. Therefore one may suppose that the lifetime of GTEK is the same as that of Traffic Encryption Keys, given the fact that GTEK is a special kind of TEK. Therefore, according to the specifications one can infer that the lifetime of GTEK is set to be 12 hours and the interval for the minimum is 30 min and for maximum is 7 days. Taking into account that how many log-in and log-out’s happen, increased lifetime of GTEK results in much longer gaps when it comes to forward/backward secrecy, due to the fact that higher number of messages are ciphered via the given GTEK. MBRA is similar to the Group Key Management Protocol (GKMP), which does not provide a solution for keeping the forward secrecy except by creating a completely new group without the leaving member. Thus, one can easily infer that this scheme is not scalable to large dynamic groups (G. Kambourakis et al. 2010).

4.3.5 Handover Mechanism's Security

The mobile WiMAX standard has 3 handover scenarios, chiefly Fast Base Station Switching (FBSS), Macro Diversity Handover (MDHO) and the Hard Handover (HHO). Among these 3 scenarios the third one is obligatory but the others are regarded as soft handovers and are therefore optional. The mobile WiMAX standard covers 3 security configurations for each and every handover case. The Handover optimization bit#1 and bit#2 explain these security configurations when it comes to RNG-RSP message as below:

- Bit#1=0 & bit#2=0: Re-authentication and performing TEK 3-way handshake.

- Bit#1=1 & bit#2=0: No re-authentication process is performed. The TEKs for entire SAs are updated.

- Bit#1=1 & bit#2=1: No re-authentication or TEK 3-way handshake execution. The

MS continues utilizing the TEKs established with the serving BS

Utilizing an HHO, the mobile station just contacts with one base station at a time, implying that the mobile station is not able to fix a connection with the second base station prior to breaking its connection with the old base station. Every base station emits a Neighbor Advertisement Message (NBRADV) regularly that consists information regarding the neighbor base stations.

The mobile station re-executes procedures associated to registration authentication and ranging, following switching its link toward the aimed base station. Even though this handover mechanism is easy, it infers a considerable latency that can be much more than 100 ms. Especially, the execution of a full EAP authentication can take up to 1000 ms and causes the WiMAX network to become unfitting for transmission of data streaming or video conference.

When it comes to the MDHO scenario, a group of base stations can be included in the handover, and form a list regarded as a diversity set. The mobile station monitors the base stations in this list continuously, select one of them and register with that base station. In downlink case, several base stations can send data to the mobile station that would carry out diversity mixture. In uplink case, the data are transmitted by the mobile stations is captured by several base stations, which would carry out the diversity of selection. The base stations involved in a similar handover scenario should transfer or share data being MAC-context based like

ciphering keys/authentication utilized by established connections and the fixed ones.

As MDHO, the FBSS handover scenario permits the base station and mobile station to keep the diversity group and the MAC-context related information is also shared by all base stations involved in the handover. When it comes to uplink/downlink communication, the mobile station interchanges information just with the broadcaster base station (S. Y. Tang et al. 2010).

4.4 Investigation of Security Problems in WiMAX

In this part of the dissertation, the chief security shortcomings of the 802.16e are investigated. The previously discussed security issues were more focusing on authentication related problems and security of management communication messages together with key sharing when it comes to multicast/broadcast service. In this part, the chief solutions would be provided as far as the topic is concerned.

4.4.1 Authorization Attacks

During the authorization stage of the PKM second edition protocol, it can be observed that the request for authorization is not safeguarded against possible forgery/alternation attempts. This problem existed also in the PKM's first edition. It has been explained that in case an intruder receives such message, having been transmitted from an authorized mobile station, then if he/she transmits it repeatedly, it can overload and cause buffer overflow and thus force it to block the access to an authorized mobile station. In a scenario that even the request for authorization is signed, the protocol is yet susceptible. The point is that actually during the time when the nonces are transmitted back to each other in the replied messages, one can state that it is not required to verify the timestamps of the three interchanged messages and that the mechanism can introduce reciprocal two-way authentication and be deployed without needing adjusted clocks. It is observed that the protocol is susceptible to interleaving attack (S. Xu 2008) where the intruder can replay the initial message and answer the base station through mentioning the correct nonces, and utilizing the compromised mobile station as an oracle.

The intruder begins with transmitting to the base station, a replayed message which it received in the past from an authorized mobile station. Furthermore, next to capturing the base station response, the intruder recognizes that it is not capable to decipher the pre-AK that was ciphered by the authorized mobile station's public key. The intruder begins with transmitting a replayed message to the base sta-

tion which it received already from the authorized mobile station. Thus following the reception of the base station's reply, the intruder figures out that he is not capable to decipher the pre-AK that was ciphered by the authorized public key of the mobile station. Therefore the intruder will be unable to transmit the acknowledgement of authorization instantly due to not being able to cipher the base station's nonce together with its address with the correct AK. Hence, the intruder deploys the subscriber station as an oracle for issuing a correct acknowledgement message. It carries out an attack on the base station and invites the subscriber station to attach itself and execute the PKM protocol's second example. Followed by the transmission of the initial message by the authorized mobile station, the intruder answers to the mobile station by transmitting the base station, the nonce it captured in the initial session held with the authorized base station. Likewise, it consists the pre-AK and the MSID captured from the base station in the initial session and ciphered with the authorized mobile station's public key (A. Altaf et al. 2008; S. Y. Tang et al. 2010).

Nevertheless this message has a signature with the intruder's certificate. To make sure that the AK that would be produced by an authorized mobile station, and the AK produced by base station in the initial example of the protocol would be the same, the intruder requires to imitate the base station address. The explained threat presentation can be observed in Figure 14.

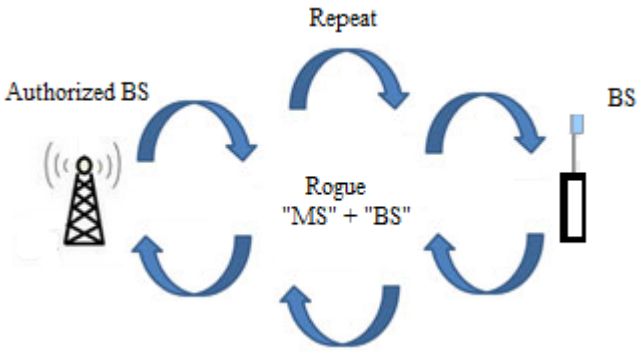


Figure 14. Threat presentation

The mobile station answers the intruder by transmitting its address and the authorized base station's nonce plus the AK ciphering of the two values. The intruder captures the message from the mentioned authorized subscriber station and replays it followed by transmitting it to the authorized base station for finishing the initial session where it imitated an authorized mobile station.

During the time when the PKM second edition deploys AAA to permit a security session, the intruder may replay and forge these messages to the mobile station as

well. To prevent this intrusion, a solution (S. Xu 2008) can be appending the base station identity (BSID) to the final message and cipher it altogether by the nonce of the base station and subscriber station's address. On the other hand, A. Altaf, M.Y. Javed, S. Naseer and A. Latif came up with the idea of introducing timestamps on the transferred messages, defining a twofold solution that deploys both nonces and timestamps (A. Altaf et al. 2008).

4.4.2 Investigation of SA-TEK 3-Way Handshake

S. Xu in 2008 demonstrated that the second edition of the PKM protocol's SA-TEK 3-way handshake is secure, even in case the initial message is prone to replay attack. Indeed, this protocol holds a familiar and likewise structure as the Needham Schroeder Secret Key protocol (NSSK) that was published in 1978 (S. Xu 2008).

The NSSK protocol was investigated thoroughly and it was found to be reliable and secure following some editions and revisions. To safeguard contra replay of the SA-TEK issue message, S. Xu proposed including timely information.

Interleaving attacks cannot endanger the SA-TEK 3-way handshake protocol due to utilizing secret keys rather than public keys.

E. Yuksel et al. indicated that the SA-TEK 3-way handshake is much more than secure because of the protocol's redundancy mechanism (E. Yuksel et al. 2007).

Due to the fact that the nonce is produced by the base station, it does assure nothing to the subscriber station. The nonce produced by the subscriber station is enough to make sure about the freshness and timeliness of the message.

4.4.3 Susceptibility to DoS Attacks

When it comes to WiMAX networks, the network entrance process, performed by a mobile station to attach itself to a base station is not protected. Intruders can sniff to the transferred traffic and deploy the obtained data to falsify requests for ranging or the response to ranging messages.

Due to the fact that message is not authenticated, the mobile station cannot specify its true origin. An intruder can block and falsify a RNG-REQ message by altering certain selected burst profile of the downlink. It can falsify a RNG-RSP message as well to fix mobile station's power to the minimum. This would carry out the first ranging process continuously because it can barely send to the base sta-

tion. Moreover, the communication administration among a mobile station and a base station includes the transmission of plaintext and the administration frame's origin, transmitted in broadcast and unicast that is unauthenticated (S. Rekhis et al. 2010). These messages consists of some critical unauthenticated messages (S. Naseer, M. Younus and A. Ahmed 2008): authorization invalid message, Mobile neighbor advertisement (MOB_NBR-ADV), Mobile Traffic indicator (MOB_TRF-IND), Multicast assignment request (MSCREQ), Fast Power Control (FPC), Mobile association Report (MOB_ASC-REP), Power control mode Change Request (PMC-REQ), Ranging Request (RNG-REQ), Downlink burst file change request (DBPC-REQ) and Ranging Response (RNG-RSP). These problems paves the way for appearance of several DoS attacks (A. Deininger et al. 2007).

The MOB_NBR-ADV message that is transmitted by the present serving base station to inform about the neighbour base station's characteristics, is unauthenticated. An intruder can falsify a similar message to announce the availability of rogue base station, therefore averting the mobile station from carrying out an efficient handover or blocking such an action.

The FPC messages that are transmitted by the base station to the mobile station asking it to balance the sending power can be falsified by an intruder to fix the mobile station's sending power at a very low level. This should balance its sending power in a regular manner to reach the base station once again, resulting in the transmission of aggregated power balancing messages.

The intrusion can aim at many mobile stations at the same time interval. When it comes to the uplink bandwidth request slots, as a result of the deployment of CSMA, such aggregated transmission can cause collisions. The attacked mobile station cause a long delay until achieving correct sending power gain. The intrusion can as well drain the mobile station's battery and be counted as a flooding attack (S. Rekhis et al. 2010).

The Auth-invalid message (Auth-Invalid) is transmitted from the base station to the mobile station if the AK shared among them expires or the HMAC/CMAC of some exchanged message in the Authorization phase indicates an unauthenticated message. Since the Auth-invalid does not include HMAC/CMAC digest and safety measure are therefore not respected, it results in a stateless rejection, and does not utilize the serial number of the PKM, it can be falsified by an intruder to block access to an authorized user. The base station normally transmits the Reset command (RES-CMD) for re-setting a malfunctioning mobile station or a non-answering one. The mobile station will reset its MAC state machine. The mobile station can authenticate RES-CMD messages contrary to previously mentioned

management messages. Nevertheless, the intruder can pressure a base station for transmitting this message to the aimed mobile station.

In order to carry out this, it adjusts with the network and for selecting a victim CID, captures the UL-MAP message. Further on the intruder sends a signal at the predefined moment for the victim. The signal would be deteriorated or becomes completely unintelligible hinging on the mobile stations signal power. If this action is repeated continuously, the base station would transmit to victim, a reset command to restart it from the scratch.

The base station transmits the DBPC-REQ or Downlink Burst Profile Change Request message to the mobile station to seek changing the burst profile for coping with the diversity of distance among the mobile station and base station together with the communication properties of the medium.

An intruder can falsify a similar message to alter the burst profile intentionally and block the communication among the base station and the attacked mobile station.

While the handover takes place, and during the time when an aimed base station together with a mobile station are association within the network, the aimed base station does not straightly transmit the ranging response message to the mobile station, but alternatively it pass it further through the serving base station's backbone.

The serving base station captures similar messages from all the surrounding target base stations, and sums up entire copies into a MOB_ASC-REP message which stands for Mobile Association report. The message would be transmitted to the mobile station utilizing the basic administration connection. Therefore similar messages that include data useful for the mobile station for opting an aimed base station are not authenticated and thus are not safe contra falsification attempts.

An intruder can falsify a MOB_ASC-REP message in such a way that it seems no service is provided from the aimed base stations. A likewise action avoids the mobile station from being connected with the best candidate base station and persuade it to keep on utilizing a deteriorated service.

4.4.4 Problems of Multicasting/Broadcasting

Utilizing the common shared symmetric GTEK, the information is given out among mobile stations in case the broadcast/multicast service is deployed. Within the same multicast group, a same key is shared among all the members. As a re-

sult of the fact that the key is symmetric, each mobile station can both cipher/decipher the multicast traffic deploying the same key.

An intruder can falsify the multicast traffic and transmit it to other mobile stations. The message holds a viable ciphering and HMAC/CMAC code of integrity. Within the multicast group, the users are not able to identify the origin of the traffic and almost always suppose that it comes from the base station.

Indeed, when it comes to mobile station joining the multicast group, it receives the current GTEK from the base station to be able to decipher all the multicast messages during the present lifecycle of GTEK. When it comes to the standard, it recommends a value ranging from half an hour to seven days, but the default is set to twelve hours. Due to the GTEK and update of the GKEK, a small value can diminish the overhead of the base station.

To make the GTEKs up-to-date, the Multicast Broadcast Rekeying calculation might be utilized. The base station transmits the encrypted GTEKs to all the multicast group members utilizing the shared GKEK. Each part that captures such message, deciphers it and upgrades the utilized GTEK.

Since every multicast's part has the GKEK, it can utilize the MBRA to disseminate a produced GTEK that has a good ciphering and validation code. Subsequently all the parts of the multicast would be compelled to upgrade their GTEK (IEEE C802.16-e05 2005). Further to such operation, none part can decipher the things that starts from the base station. This conduct is upheld until the following time the base station transmits the Group Key Update message to upgrade the present GTEK. In order to reduce the susceptibilities specified with broadcast/multicast service's key sharing, two proposed ideas were suggested (S. Naseer, M. Younus and A. Ahmed 2008). The solution comprises in safely dispersing the GTEK by the base station independently to each and every mobile station deploying the KEK imparted among the base station and mobile station. The second involves digitally marking the key upgrade message deployed to redistribute the GTEK, rather than annexing the HMAC.

H. Li together with his research group proposed a GKDA that is suggested to make use of an adaptable and secure answer for key appropriation in multicast cases (H. Li, G.B. Fan, J.G. Qiu and X.K. Lin 2006).

4.4.5 Handover Mechanism Weaknesses

While the ranging response message's handover bits could be utilized to diminish the latency, thus when the handover is carried out it likewise influences the system's security (J. Hur et al. 2008). The more the response time is diminished, the more the operation's security is diminished.

For example, by fixing the bit#1=1 and bit#2=1, constrains the system to continue utilizing identical secret keys prior and after the handover and avoid it from guaranteeing forward/backward secrecy.

Indeed in case a pernicious MS has taken over the serving base station's security, it could likewise trade off the security of every other previous one as well. In the situation when bit#1=1 and bit#2=0, throughout the handover operation, the TEKs will be upgraded yet the AK is kept. As a result of the fact that AK empowers inferring the KEK and therefore acquiring the TEKs, a serving base station can utilize the unaltered AK to verify the upgraded TEK of the accompanying aimed base stations. Therefore forward secrecy cannot be used. Considering the handover mechanism's shortcomings, both bit#1 and bit#2 ought to be fixed to null, with the intention that secret key would not be redeployed at all in an alternate base station following the handover operation (J. Hur et al. 2008).

4.5 IEEE 802.16 and IDS

In certain cases it is recommended to define and install an intrusion detection system (IDS) in a wireless-based system like WiMAX. This idea provides an opportunity for the administrator to detect and control the traffic for abnormalities, already defined security and attack signatures and many other threats.

It is a very meticulous measure to take when it comes to WiMAX system, particularly when the security of the mentioned network is of importance to that organization or institution. Moreover, for supervising and monitoring the intruders and hackers activities, the IDS system can be integrated with Honeypots to gather information about intrusions and track them respectively. M. Hossein Ahmadzadegan proposed a new approach to take for designing a WiMAX-based intrusion detection system that provides different features like being more efficient due to less processing cycles (M. H. Ahmadzadegan et al. 2013).

Even through many studies were carried out aiming for addressing the WiMAX security issues, there are still a large number of security faults, threats and vulnerabilities existing to be dealt with, for instance the BSs DoS rogue attacks, network

manipulation by spoofed frames and man-in-the-middle attacks. It is of great importance to recognize the fact that the precise capabilities of WiMAX for a possible confrontation with all security threats will be determined only after large-scale usage of the technology. It is correct that protocols can be proven to be secure even before systems are implemented and implementations can be tested before large scale launch but one should consider that new threats and attacks may popup any time and until the system is not fully operational in a large scale, it may not be discovered (M. Nasreldin 2008).

Therefore, for example in (C. Kolias et al. 2013) paper many attacks have been addressed and classified but some of them are not possible under real circumstances and require some special conditions to happen or be traced, additionally the attacks are divided into many categories and sub-parts which makes them so intricate to comprehend and at the same time the categorizations are not integrated and well-organized. Thus M. Hossein Ahmadzadegan proposed an alternative classification which has two criteria's for analysis and categorizes only the real attacks. In this paper (M. H. Ahmadzadegan et al. 2013), it is explained that by filtering based on that perspective there will not be a scattered number of groupings. Therefore following this unique approach the attacks are only divided into four classes.

The above-mentioned WiMAX-based intrusion detection system comprises of seven units: WiMAX Security Analysis unit, WiMAX Attack Database unit, Detection unit, Intrusion Detection unit, Backup & Storage unit, System Management unit and Response unit. The system design is presented below in Figure 15.

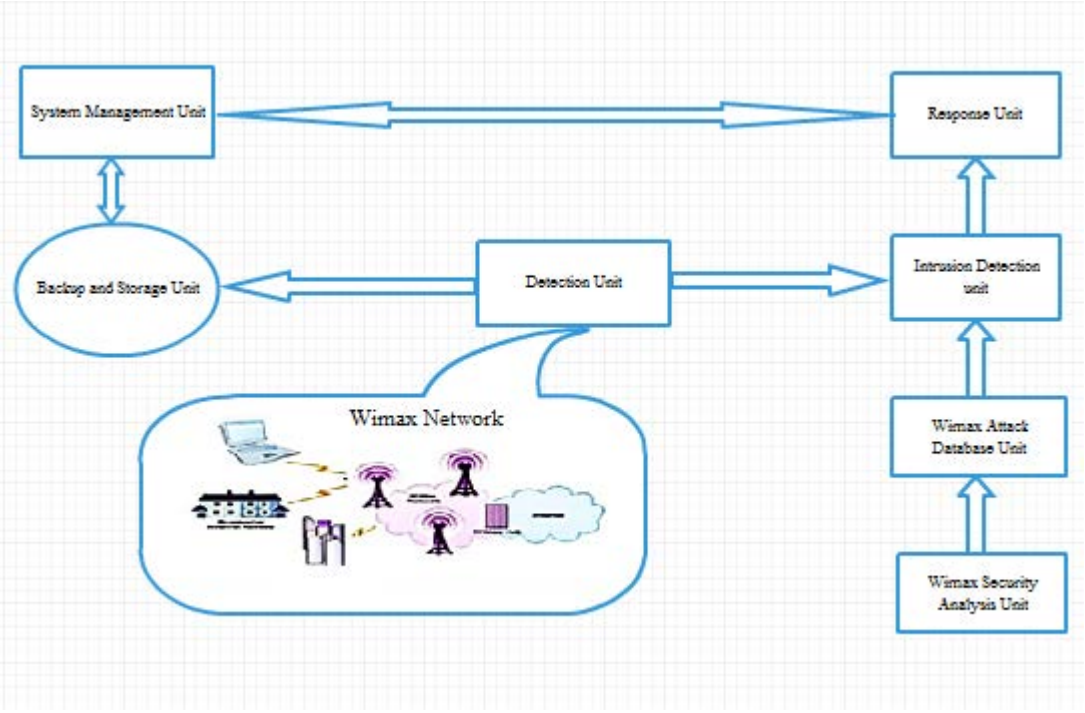


Figure 15. System design (M. H. Ahmadzadegan et al. 2013)

The system and functional mode is explained below as follows:

Primarily, the WiMAX Security Analysis unit system gets the attack characteristics of the WiMAX network and analyzes these characteristics by attack database unit, thus in this manner it facilitates the situation for the next stage being intrusion detection unit (T. Shon et al. 2010).

System should get data from the data link layer of WiMAX network, thus we set the wireless network cards to open mode. Furthermore the detector unit call open pcap function to open data packets captured by Lib pcap from WiMAX server, then pretreatment applies to packets and message goes to the detection unit and calls different IP layer analytical functions according to the protocol value that addresses the upper layer in the packets. Therefore after analyzing and decoding data, the packets will go to the intrusion detection unit.

As soon as the intrusion detection unit receives the data packets, it will judge to see if the system has been attacked by running a comparative sort of analysis that verifies if the information from WiMAX attack database unit with the captured message by matching algorithm rules to distinguish the attacks. If the packet corresponds to a rule, then this implies that there is definitely an attack suspicion that will be forwarded to response unit for the respective security measures, otherwise, the packet would be counted as normal and does not need any further action. Re-

sponse unit stores the intrusion packet that can be logged in the database (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011).

WiMAX security analysis unit:

This unit gets the intrusion attack features by the aid of the analysis of WiMAX vulnerabilities, and transmits these specifications to the WiMAX attack database unit. One can extract attack characteristics from the two kinds of WiMAX vulnerabilities being the security vulnerability of none authentication news and security vulnerability of sharing keys in multi-end radio service.

WiMAX attack database unit:

WiMAX attack database is the essential brain of an intrusion detection system that has a large number of defined attacks and signature databases. Moreover, it decides regarding the performance of the intrusion detection system. Basically when it comes to having more attack behavior and characteristics databases, this actually implies and leads to a better protection against the attacks due to already having them in the database the detection can be easier. This unit performs two important operations being the recording of a large number of known attacks, and in the same time storing the characteristics of new intrusion attacks by analyzing the WiMAX security faults (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011).

Detection unit:

Detection unit is situated in the bottom of the system, thus it is the so called “prime” unit of the system that processes the data at the initial entrance point. The system has to gather all network packets down from WiMAX network. The chief duty of the detection unit is to collect the data packets from WiMAX network and also process them partially. As the size of the network increases, the network packet flow also rises drastically.

As mentioned above the detection unit checks the received packets according to each layer and encapsulates protocol messages in the reverse order, by analyzing detailed protocol contents in each packet header. Then it transmits the investigation results to the intrusion detection unit. Also, the detection unit utilizes the plug-in technology that is handy for adding more features to the system (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011).

Intrusion detection unit:

The key function of Intrusion detection unit doing a comparison between the detection unit and attack database unit to determine if an intrusion takes place. In-

trusion detection unit is one of the core parts of the system, it will carry out a comparison between the data from the detection unit with intrusion rules along with the rule list, if it is found that the data corresponds with a rule existed in the feature database, it implies that an attack takes place, then sends the right warning to the response unit. If there isn't any rules match with the data, it implies that the data is following its expected path (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011). The intrusion detection unit and the process which it follows can be shown in Figure 16:

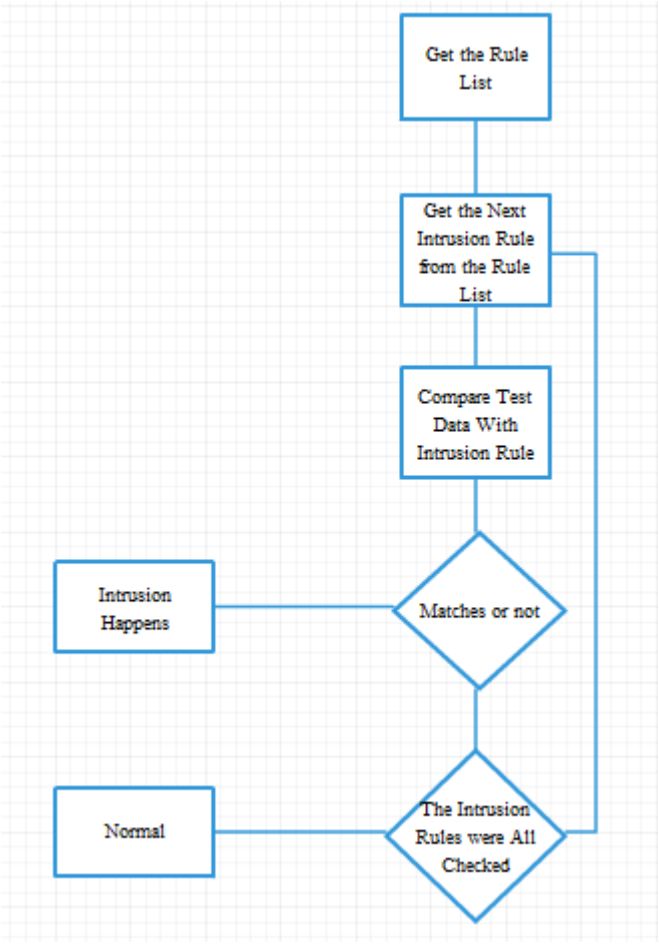


Figure 16. Intrusion detection unit

Backup and Storage unit:

The backup and storage unit is chiefly responsible about storing different important pieces of information in the system so that in this way it facilitates the system management, for example it captures network packet data of WiMAX network, strategies and information about attack database unit. The importance for the basic functionality of IDS is that it is connected both to the detection and

system management unit. Therefore some specific information's and suspicious traffic can be stored in this unit and further provided to the management unit to decide on the matter. For instance if the suspicious traffic and its pattern are of concern then that behavior and its characteristics can be introduced to the detection unit in view of updating the WiMAX attack data base unit so that next time that specific suspicious behavior could be blocked and detected at early stages.

System management unit:

This unit is in charge of the management operation of the proposed Intrusion Detection System (IDS). The key functions are to check the received data packets stored in storage unit, administration of system logs, upgrade the attack database unit together with disposing each and every unit of the system. User can manage the IDS by a set of different alternatives, like web or serial port (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011).

Response unit:

In case of no detected intrusions by the IDS, the response unit will not take any action, but, when IDS detects an intrusion action on WiMAX network, the response unit then takes corresponding measures after getting the confirmation and based on the user strategy (M. H. Ahmadzadegan et al. 2013). The actions are diverse but some are for instance are blocking the traffic in the WiMAX network and even stopping the entire service if the detected intrusion is of major threat category, in addition to this IDS can be set to cooperate with a firewall in a joint action so that after the detection the traffic would be blocked in the network bottleneck or add new rules to the firewall after a possible suspicious pattern is detected and labeled as a potential threat. Furthermore informing the administrator of IDS and setting alarms in the WiMAX network can be among other tasks of the response unit. The information saved on the response unit can facilitate the MS user's query and analysis, and is considered as a catalyzer for performing WiMAX network analysis. Indeed, the security of WiMAX is currently subject to several speculations (M. H. Ahmadzadegan et al. 2013; Bo Zhou 2011).

4.6 Real Attacks, Vulnerabilities and Classification

4.6.1 Ranging Attacks

As it can be confirmed, one of the most crucial stages of initial network entrance is ranging. During this operation both BS and MS should achieve an appropriate

timing offset and make precise power settings in order to set and fix their transmissions for the opted physical mechanism.

1) RSP DoS Intrusion: The intrusion could be either launched to just a single aimed mobile station or several ones. Its mechanism is easy to grasp but its execution is relatively intricate. Thus just in case there is a need and will it can done. In both scenarios the intruder should be aware of the network's radio channel targeted to be attacked and have a dedicated base station like device which permits him to send RSP messages. One should consider that RSP messages maybe sent in an unsolicited way that makes the intrusion likely. In the initial scenario, the intruder should be aware of the victim MS's CID. This piece of data may handily be listened from any unciphered administration message interchanged among certain base station and mobile station. Later on, the intruder generates a fake RSP message having "Ranging Status" section fixed as "abort" and transmits it for the victim (IEEE 802.16 Working Group 2005; W. Gu et al.).

In the second scenario, the intruder must go through the entire existing CIDs with a brute force approach, and transmit one fake RSP message for each and every CID. Following this the victim device will strive to re-associate to the network through running the first network entry. By repeating this loop-like procedure again and again, the intruder can transform it to a DoS with even higher user, numbers since each attack causes the mobile station to go through considerable signaling stages. The DoS effect will keep on just until the aimed mobile station remain affected by the intruder and she constantly sends bogus RSP messages. One should consider that this increases the intruder detection's risk. A serious intruder might opt to cooperate in a group or for preventing detection be on the move.

2) REQ Downgrading Intrusion: The REQ message can be utilized to announce the base station regarding the desired DL burst profile. Nevertheless, an intruder might misuse this and utilize this aspect in a negative way. For instance, by substitution of the burst profile optimum with a least efficient one, thus the intruder may become successful in downgrading the service (M. Habib et al. 2010; Bo Zhou 2011).

The intrusion's effectiveness hinges on the opted burst profile's level of manipulation. This bounds the intruder to thoroughly focus against a certain victim or a few aimed mobile stations. As a result of the fact that, a successful ranging request downgrading intrusion can only cause annoyance. Thus this intrusion is counted as minor.

3) REQ DDoS Intrusion: In this scenario a group of cooperating intruders can generate a huge number of forged and fake RNG messages and concurrently send them to the aimed-BS for finishing up its resources (T. Shon et al. 2010). In this attack the tiny amount of intrusive traffic make it extremely difficult for the Intrusion Detection Tools (IDS) to detect the attack so that the intrusion basically cannot be distinguished as abnormal and intrusive. Thus, this intrusion is labeled as major.

4) MOB ASC-REP DoS Intrusion: The MS during the ranging procedure rather than many RNGRSP messages can get a MOB ASC-REP message. This takes place when level 2 association is utilized.

In this scenario, the RSP data which is transmitted by every aimed base station is summed up into the serving base station over the network's backbone. The base station further gathers all the information's from the RSP messages to a single MOB ASC-REP that would be transmitted through Primary Management CID. As a result of the fact that the MOB ASC-REP messages are not protected, they can be falsified asserting that services are not available from the aimed base stations (T. Shon et al. 2010).

The intruder should also be aware in case the victim mobile station keeps level two associations that boosts the complication of the intrusion mechanism. Due to this cause also this type of intrusion is basically launched contra a few mobile stations or one mobile station. According to mentioned causes, an intruder which intends to have a definite success, will not deploy this strategy. Thus, this intrusion poses a minor threat (T. Shon et al. 2010; C. Kolias et al. 2012).

4.6.2 Power Conserving Attacks

The IEEE 802.16e features came up with support for mobile devices. As a result of the fact that majority of devices get their required power from a battery, the features included power-saving aspects for enhancing the mobile station's battery life. A connections set that have reciprocal requirement characteristics is a notion defined by the Power Saving Class (PSC).

There exist three types of PSCs: (a) The first type that is devoted to Best-Effort connections (BE), Non-Real Time Variable Rate (NRT-VR) type, (b) The second type that is suggested for Unsolicited Grant Service (UGS), Real-Time Variable Rate Service (RTVR) connections (c) The third type that is preferred for multicast connections and operations of management.

1) Signaling DoS Intrusion: As mentioned before power saving provides some advantages and benefits, the authors in (P. Trimintzios et al. 2010) came up and remarked an UMTS network's intrusion but highlighted that it can be technically launched in the WiMAX framework as well. Based on their investigation an intruder can simply infer issues by flowing a minimal traffic to the network. In other words, the intruder will create fake packets of TCP/IP, for instance having forty bytes of blank payload, and transmit them to many idle/sleep mobile stations instantly. Thus the intrusion traffic becomes as few as 64 bps. Therefore by deploying a cable modem having 1.5 Mbps bandwidth (uplink), affects circa 24000 mobile stations negatively. As soon as data availability is secured for a particular mobile station, the base station shall have to wake it up. Through this packet resending in intervals a little bigger than the mobile station's inactivity timeout, the intruder basically creates a repetitive loop of waking up-putting to sleep that could demonstrate a big burden of the signaling. One can observe that this intrusion mechanism is adequately easy and requires a low cost but there are many problems related to the mentioned mechanism. The primary problem is that the idle/sleep mode is an option for a mobile station. In addition to this the inactivity timeout counter differs to a large extent from one manufacturer to another because this factor's default value is not defined. The intruder would be bounded for sending in intervals as far as the inactivity timeout's maximum value. Moreover the intruder should have the IP's of aimed mobile stations and that which mobile stations are in idle/sleep mode. This implies that when network is dealing with a heavy load, the base station can select to delay the process of device waking ups. Due to observed causes this intrusion cannot be carried out in WiMAX framework (P. Trimintzios et al. 2010).

2) Sleep mode BR and UL DoS Intrusion: As logically described, it is foreseen for a mobile station to ask for sleep mode activation through transmitting a UL and BR sleep control header rather than the typical SLP-REQ message.

Moreover, it can be logic for an intruder to falsify an UL and BR control header with the identity of the victim and transmit for forcing that mobile station to switch into sleep mode. Consequently, the base station would not transmit messages to that MS anymore, even though MS needs to be paged and DoS will occur but this attack may rarely take place, therefore this attack should be labeled as a minor one (P. Trimintzios et al. 2010).

3) Location Update DDOS Intrusion: When a base station monitors the present location of a specific mobile station continuously, this process is called location update. The mentioned process can be started by the mobile station's request or in case one of these conditions are met: (a) a modification in paging group is detect-

ed by the mobile station, (b) the modification is detected before the idle mode timer expiration (c) The detection is detected as during the procedure of powering down, and (d) when the threshold of the mobile station's MAC hash counter exceeds. Secure location update or unsecure location update are the two supported modes. When it comes to secure location update, the mobile station should transmit a ranging request message to the base station consisting a HMAC/CMAC. Further on, the base station must check the value of the HMAC/CMAC. In case the security context is not shared among the present base station and the mobile station, it would ask for it through the location update request message from the backbone network. The backbone would issue and offer the keying material through a location update reply message. Trimintzios and his colleague's further state that this procedure may overload the network when it is carried out instantly by a huge number of devices. As a result of the fact that, for location update purposes, any mobile station may ask for bandwidth, the intruder would just have to create a valid ranging request but with invalid HMAC/CMAC. A rogue mobile station may issue a huge number of requests simply without any risks of being detected. Fundamentally, this intrusion is exactly like the ranging request DDoS except that it has some extra processes added by the backbone network and the base station which may lead to more harm because the outcome will be magnified. Having described the characteristics, this intrusion can be regarded as major.

4.6.3 Handover Attacks

Handover (HO) is the scenario in which a certain mobile station is handed over and moves from its present base station to another neighboring base station's air-interface. HO has several stages and consists of the following major steps (M. Nasreldin 2008):

- Base station re-option - A mobile station verifies neighboring base stations. For this purpose, the base station sends a MOB NBRADV message on regular bases that includes the appropriate information. This permits a mobile station that seeks for handover to identify all the base stations in the vicinity.

- HO Inception - An handover operation can start either by the mobile station or the active base station. In the first scenario, the intention is stated with a MOB MSHO-REQ where in the second case by a MOB BSHO-REQ one. Note that the handover command message consists of one or more target base stations.

- Synchronization to new base station - The mobile station will synchronize to the down link of the target base station and gets the parameters of its downlink and uplink.

- Ranging - the full initial or handover ranging can be performed among the mobile station and the target base station. Hinging on the amount of data which the target base station has about the mobile station it can take decisions if one or many stages of the ranging process may be skipped.

- Termination of mobile station context - The acting base station can put an end to all connections targeted at the mobile station or everything related to them

1) MOB NBR-ADV Downgrading Intrusion: As a result of the fact that, this kind of message is not integrity protected, the intruder is capable of altering them by deleting the information about the neighbor base station in the appropriate message fields.

This will block the handover and thus it will not take place because the mobile station would think there are no possibilities. Therefore as the mobile station leaves the acting base station, the mobile station would have no alternative but to stay attached to it and the QoS will diminish little by little until it becomes unavailable. The implementation mechanism is so intricate that it is expected to convince the intruders opt not to follow the case. One alternative solution is that the mobile station should scan the entire radar frequency to find new base stations. Thus, this downgrading intrusion can be counted as minor.

2) MOB NBR-ADV DoS Intrusion: The intruder can manipulate the MOB NBR-ADV such that the presence of a non-existing base station will be announced having better characteristics compared with the acting one. Therefore this would lead to DoS when it comes to authorized users because the mobile station disconnects from its present acting base station while striving to attach itself to the new base station which in fact is non-existing. Furthermore the intruder can entitle the rogue base station’s data which is compromised and therefore possibly link an authorized user with it. Based on it the connection termination with the acting base station takes place just as a final handover step and this just following when the mobile station has adjusted with the new base station. In case that would not take place, the mobile station would not leave its acting base station. The soft handover mode is better compared with the hard handover when it comes to this intrusion but it is not the default setting. The hard handover mode abandons the field open for this intrusion which leads to DoS in certain mobile stations. The chief peril is in fact an intruder with the possibility of linking with a rogue base

station and thus from there carry out more serious and harmful intrusions. This intrusion poses a minor threat. (IEEE 802.16 Working Group 2004).

As the mobile station disconnects from its presently acting base station while striving to attach to the new one which is non-existing, it is considered that, this will lead to DoS when it comes to authorized users. The true danger resides in granting the intruder the chance to relate with a rogue base station and from that point carry out harsher intrusions. Therefore, the intrusion causes just a minor threat.

4.6.4 Attacks Contra WiMAX Security Mechanisms

1) Interleaving Intrusion: This intrusion comprises of two rounds. Firstly the intruder imitates an authorized and valid mobile station and transmits an authentication information message next to an authorization request message that have been stopped and saved from a past mobile station's valid session.

Following the authorization reply message's reception the intruder should follow the protocol of authorization by offering a valid authorization acknowledgement response. The intruder cannot build this message due to the lack of having knowledge about the private key of the valid mobile station and cannot decipher the authorization reply message. Hence, the intruder in parallel with the first round may begin the second round targeting at deploying the valid mobile station as an oracle on his behalf for creating an authorization acknowledgement message. At this stage the intruder would play the base station's role. Through pressuring the mobile station to begin another instance of the protocol, the mobile station would deploy the first round's authorization reply. The valid mobile station would offer the correct authorization acknowledgement message that the intruder will pass on the valid base station and put an end to the first round. As it can be seen the intruder has taken a MiM entity approach to authenticate himself instead of the valid subscriber station which leads to registering the wrong user into the system. However, from service theft's point of view no rogue action or serious harm can be carried out. The intruder will not have access to the TEK, AK or other materials for keying and thus will not be capable of deciphering the traffic which the base station transmits or create messages having valid HMAC/CMAC. Form a best scenario's viewpoint, he may just keep on to play the role of a MiM and discard the valid conversation among the base station-mobile station through falsifying or even dropping the control messages which are unprotected. This intrusion can pose a minor threat to the WiMAX network.

2) Authentication Request Service Theft Intrusion: So it can be vividly indicated that Auth-Req's random number field, has not been successful for blocking the reply intrusion. The message could still be retransmitted by an intruder and the base station will not be aware of its timeliness and freshness.

The authentication request message's random number field is a method for relating every authentication reply message with one authentication request and therefore its goal has not been protecting against authentication request replay intrusions. The mobile station would be aware that the authentication reply is timely fresh, in case the mobile stations random number field corresponds with the one transmitted in the authentication request message. One can conclude that based on evaluations this intrusion does not harm but as it exists, it would be worth mentioning (P. Trimintzios et al. 2010).

3) Authentication Request Replay DoS Intrusion: Xu and Huang defined this intrusion against the PKM protocol first edition. In this intrusion, the attacker saves and replays the authentication request message instance belonged to an authorized subscriber station transmitted previously. It is probable that a base station has come up with a timer that pressures it to block duplicate authentication requests deriving from the same subscriber station within a certain period. This implies that the base station may drop authorized requests coming from victim subscriber station as well. Hinging upon the vendor this attack can be counted as feasible in the PKM protocol's second edition. Therefore in this scenario there exist 2 outcomes: (a) the intrusion will result in a DoS against a varied number of users, or (b) the base station would go on smoothly with the process of authorization paving the way for collaboration of intruders for DDoS attack. Concentrating on the second scenario, for every authentication request message the base station would have to check all messages signatures, issues keying material, create the authentication replay message and eventually send it to the mobile station. It is clear that this set of actions could be the base station's burden in case it is duplicated several times. This intrusion's issue that distinguishes it from other DDoS intrusions contra WiMAX, is that it has an upper limitation. This implies that there is a defined restriction on simultaneous request's number that cooperating intruders may generate. This is to a large extent because the authentication request message includes the SAID field that would be verified and deployed for the authentication reply creation. This basically bounds the intruder to replay authentication request messages of mobile stations whose CID is yet active. From a theoretic point of view, this intrusion's main challenge is to have N collaborating intruders generating simultaneously M requests where M is remarkably smaller than the number of simultaneous connections which a base station may cover.

4.7 LTE Main Security Issues

The security issues of the LTE can be divided in six branches being the security issues in LTE system architecture, LTE cellular security, LTE handover security, IMS security, HeNB security and MTC security. Here the problems and their present security measures are mentioned as follows:

- LTE system architecture

When it comes to the LTE system architecture, for addressing the security concerns regarding the handover, an acceptable and strong handover authentication scheme relying on enhanced proxy signature has been introduced in (J. Cao et al. 2012) that can be applied to all mobility cases consisting of the handovers among the Home eNodeBs (HeNBs), the handovers among the eNBs and the HeNBs, the handovers among the eNBs and the inter-Mobility Management Entity (MME) handovers. By utilization of this handover scheme, a User Equipment (UE) and the target eNB or HeNB can straightly carry out a reciprocal two-way authentication and set a session key with their old secret keys issued by the proxy signatures while the UE gets into the aimed eNB or HeNB's coverage area. Thus, it has an easy authentication process without a complicated key management and can have a good level of efficiency. Furthermore, a quick and secure handover authentication scheme has been suggested to obtain smooth handovers in the LTE networks among heterogeneous access systems. According to this scheme, the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), the trusted non-3GPP access networks and the Evolved Packet Data Gateway (ePDG) for untrusted non-3GPP access networks are regarded as Access Points (APs). As soon as the UE gets into the coverage of a new AP, the UE and the new AP can carry out an authenticated key agreement deploying their old keys generated by Key Generate Centre (KGC) to issue their shared session key just with 3-handshake. The mechanism in (J. Cao et al. 2012) can offer a strong security protection and remarkable efficiency and works on all mobility scenarios among the E-UTRAN and the non 3GPP access networks within LTE networks. Consequently, as a result of the fact that the utilization of the proxy signature method and Identity-based cryptography (IBC), the two mechanisms may cause a lot of extra computational expenses and depletion of battery that is not cost-efficient to the mobile devices having resource limitations.

- LTE Cellular Security

When it comes to the LTE cellular system, a hybrid type of authentication, key agreement and authorization mechanism in accordance with Trust Model Platform (TMP) and Public Key Infrastructure (PKI) for 4G mobile networks has

been brought up in (Y. Zheng et al. 2005). Due to the usage of the basics of trusted computing and PKI, it can offer a good level of security for mobile users when it comes to accessing sensitive data and services within 4G systems.

Moreover, passwords are linked with the fingerprint and public key to get reciprocal two-way authentication among UEs and the HN over the TMP. An authentication and key agreement mechanism according to self-certified public key (SPAKA) has been suggested for 4G wireless systems in (D. He et al. 2008). The mechanism issues a public key broadcast protocol according to a probabilistic method for a UE for determining the genuine base station, and therefore makes up for the lacks and gaps of 3G AKA scheme. Furthermore, 3 authentication protocols consisting register authentication, re-authentication and handover authentication have been demonstrated for diverse authentication cases. Further on, a Security Enhanced Authentication and Key Agreement (SE-EPS AKA) according to Wireless Public Key Infrastructure (WPKI) has been brought up in (X. Li et al. 2011). The proposed mechanism of Li and his colleagues ensures the security of user identity and the interchanged message with restricted power consumption by deploying Ellipse Curve Cipher (ECC) ciphering. The mechanism in (H. Mun et al. 2009) have investigated the vulnerabilities and intrusions in the 3G-WLAN interworking and have come up with a new EAP-AKA-based access authentication and key agreement protocols. The 2 mechanisms utilize the Elliptic Curve Diffie-Hellman (ECDH) having symmetric key type for cryptosystem to make up for the risks explained in the EAP-AKA protocol. It has been highlighted in (J. Abdo et al. 2012) that the SE-EPS AKA protocol is susceptible to brute force together with intelligent force attacks and therefore it cannot provide a certain promise for user identity's security. Further on, an ensured confidentiality authentication and key agreement (ECAKA) has been suggested to improve the user's confidentiality so that all the AKA messages are completely protected when it comes to the integrity via ciphering that can prevent the user identity disclosure.

All these mentioned mechanisms and schemes in previous paragraphs above (H. Mun et al. 2009; Y. Zheng et al. 2005; D. He et al. 2008; X. Li et al. 2011; J. Abdo et al. 2012) use the public-key based protection methods to deal with the gaps and lacks of the EPS AKA protocol, and therefore can get a reciprocal two-way authentication and make sure that the secure communication among the UE and HSS/AuC by the aid of UE and/or the HSS/AuC of public key certificates exists. Beside this it is necessary to consider that it will incur extra computational expenses and communication costs for mobile devices with resource restriction. Moreover, since LTE network has an open nature kind of environment, the public key infrastructure has to span around all operators with reciprocal two-way roaming agreements. Thus, the LTE network requires to take a huge number of de-

ployment overheads to set and organize the public key infrastructure. The 3GPP appears to be eager to mandate such a costly infrastructure (G. M. Kien 2009).

An EAPArchie technique (Z. Shi et al. 2009) has been proposed to address the access layer security within the LTE networks. By utilizing the AES ciphering, the mechanism in (Z. Shi et al. 2009) can get to a reciprocal two-way authentication and key agreement among the network access layer and the users. The point is that this mechanism encounters identical threats as the EPS AKA protocol does that is not capable of avoiding and protecting the LTE network contra user identity disclosure and spoofing attacks. A lightly altered version of the EPS-AKA protocol has been explained in (G. M. Koien 2011). The mechanism brings about a new subscriber module ESIM rather the USIM and offers a direct online reciprocal two-way authentication among the ESIM and the MME/HSS to make up for the gaps and lacks of the EPS-AKA protocol just with small changes of the access security architecture. The problem here will be the possibility of compatibility issues in the LTE networks as a result of the deployment of the new ESIM. Due to the fact that the HSS requires to take part in each authentication process for each UE, it may cause a huge number of communication delays and therefore incur congestion of signaling on the HSS. Moreover, it cannot address the problem of user identity disclosure. An improved EPS AKA protocol has been introduced in (M. Purkhiabani et al. 2011) to enhance the performance of the present authentication process by a little increase of SN' computation. During this introduced mechanism, the SN/MME issues and saves many authentication vectors (AVs) from the genuine AVs at the HN/HSS. The mechanism in (M. Purkhiabani et al. 2011) can remarkably diminish the authentication signaling interchange among the SN and the HN, and therefore stores the consumption of bandwidth at the HSS/HN. Another point about this mechanism is that it increases the MME's burden due to over generation of AVs at the MME. Hence, it can just improve the authentication procedure's efficiency, whereas existing security problems in the EPS-AKA process cannot be mitigated with it. In (C. Vintila et al. 2011), the utilization of the password authentication key exchange by Juggling Password Authenticated Key Exchange (J-PAKE) protocol in the authentication process rather than the EPS AKA protocol to offer a stronger security protection has been introduced. The J-PAKE (F. Hao et al. 2010) is a password authentication keying agreement protocol to offer a zero knowledge proof deploying a shared key that is never transmitted over the medium of transmission. This mechanism has just addressed the utilization of J-PAKE within the LTE networks without mentioning about the implementation know-how so that preserving the secure communication will not be violated.

- LTE Handover Security

When it comes to the LTE handovers, a hybrid type of authentication and key agreement mechanism has been suggested to support large-scale mobility and secure communications in 4G wireless systems (Y. Zheng et al. 2005). The mechanism in (Y. Zheng et al. 2005) relates a dynamic password with a public-key to offer a non-repudiation service together with a smooth authentication. Moreover, through making use of the public key broadcast protocol defined as a part of the mechanism, a reciprocal two-way authentication among the UE and foreign network (FN) can be established without any certificate utilization. This may cause many computational and storage costs because of public cryptography, and therefore brings about various difficulties for aiding and covering smooth handovers when it comes to 4G wireless systems. A security roaming alternative together with a vertical handover method among various access technologies in 4G wireless networks has been suggested in (N. Krichene et al. 2009). The mechanism in (N. Krichene et al. 2009) describes an authentication protocol to facilitate a vertical handover among heterogeneous access systems being UMTS, WiFi, GSM, and WiMAX without needing a pre- subscription of visited networks. The setback is that, this mechanism concentrates just on the handovers among GSM/ UMTS and WiMAX/ WiFi and entitles the existing security problems in the GSM systems. The handovers among the LTE systems and other access networks have not been covered, where the LTE systems are very different from the GSM and the UMTS when it comes to security threats and handover procedures. A novel reauthentication protocol for securing the roaming and interworking from the 3GPP LTE to the WLAN has been offered in (I. Bouabidi et al. 2012). The mechanism enhances the EAPAKA protocol and utilizes a hybrid unit to offer the secure 3GPP LTE-WLAN interworking. The setback is that through this mechanism, a new entity, Hybrid Interconnection Unit (HIU), requires to be used to act like a relay station among the the WLAN and the LTE network that may need huge deployment costs and alternations to the existing architecture and therefore result in system complexity. Moreover, handovers from WLAN to 3GPP LTE have not been demonstrated. An improved quick handover method has been provided in (R. Rajavelsamy et al. 2008) to take care of the handovers taking place among the 3GPP and the non-3GPP networks. In this method, it uses a security context transfer mechanism when it comes to the handovers among the 3GPP networks and the trusted non-3GPP networks and a pre-authentication mechanism for the handovers among the 3GPP and the untrusted non-3GPP networks to diminish the latency of the handover without endangering the security level. By taking the present approaches being pre-authentication mechanism and security context transfer, the mechanism in (R. Rajavelsamy et al. 2008) provides a bedrock for an acceptable mobility among the 3GPP networks and non-3GPP networks. The point

is that, there are yet many problems to be dealt like performance, security and compatibility issues among others. Five instances of secure and quick re-authentications protocols for the subscribers of LTE to carry out handovers among the WLANs and the WiMAX systems have been introduced in (A. A. Al. Shidhani et al. 2011) that protects against connecting authentication servers when it comes to the LTE networks while the handovers take place. By utilization of these mechanisms, the EAP-AKA protocol for the handovers from a WiMAX system to a WLAN and Initial Network Entry Authentication (INEA) protocol for the handovers from a WLAN to a WiMAX system can be enhanced by integrating additional security elements together with keys to accelerate the reauthentications in WiMAX-WLAN handovers. The altered edition of the INEA and EAP-AKA has identical messaging sequences like when it comes to the standard EAP-AKA and INEA that is capable of preventing interoperability issues with diverse services without a capability loss that can take place because of alternations. The mechanism in (A. A. Al. Shidhani et al. 2011) can get a fascinating performance when it comes to reauthentication delay and signaling traffic compared with the present 3GPP standards and can offer various security services consisting forward/backward secrecy. The setback will be the fact that this particular mechanism can just cover single-hop type of communications among the Base Station (BS) and the UE, therefore multi-hop type of wireless communications require further focus and concentration.

- IMS Security

When it comes to IMS security, several authentication mechanisms in the UMTS have been introduced for diminishing the authentication signaling expenses (Y. Lin et al. 2005; J. Fu et al. 2010; X. Long et al. 2010; G. Sharma et al. 2011; A. Golaup et al. 2009). An enhanced AKA practice when it comes to the next generation networks (NGNs) has been brought up in (C. Ntantogian et al. 2007). By this mechanism, the security key among the initial authentication and the second authentication may be applied in such a way that the user can be authenticated by the aid of the (IMPI, IMSI) pair at the IMS service layer authentication without the protection of security among the P-CSCF and the UE. Therefore it can diminish the authentication overhead remarkably compared with the process of multi-pass authentication. The setback is that this approach is very susceptible to the rogue utilization of IMS services like fake server attacks. An optimized AKA (I-AKA) authentication protocol has been dealt with in (L. Gu et al. 2011) when it comes to LTE networks to diminish power usage. By this mechanism, the IMS and network layer authentication can be carried out by the aid of the IMPI just without the user's IMSI. Following the successfulness of the network layer authentication, P-CSCF will be in charge of getting the AV from the MME to issue

the integrity keys and valid ciphering with the user when it comes to IMS layer authentication process. Thus, the mechanism can block the AKA protocol's double execution and therefore diminishes the overhead of signaling significantly. The setback will be that the mechanism may cause some issues in the deployment of normal network services as a result of the fact that the only IMPI has been utilized to get to the network layer authentication. A new IMS service authentication scheme has been suggested in (M. Abid et al. 2009) utilizing IBC to improve the security of the IMS authentication process. By using the implication of the IBC together with the Elliptic Curve Cryptography (ECC), the mechanism permits the IMS services personalization via user's authentication in a personal way while the services access takes place and offers an acceptable security level. The setback is that the mechanism may cause extra computational and storage costs because of the utilization of ECC and IBC that is not cost-efficient when it comes to mobile devices having restriction of resources. An enhanced IMS authentication method deploying an effective key re-use for a mobile user has been brought up in (M. J. Sharma et al. 2011). In this mechanism, the ciphering keys and authentication vectors achieved in the initial network authentication process will be re-utilized in the IMS authentication by transferring them from the Home AAA (HAAA) toward S-CSCF by the HSS. Thus, the mechanism is able to remarkably diminish the time needed to get authentication vectors and therefore prevent from devolution of QoS and additional overheads when the user displaces from one WLAN domain into another. The disadvantage is that, it cannot offer a reciprocal two-way authentication among the S-CSCF and UE in the suggested IMS authentication process.

- HeNB Security

When it comes to the HeNB systems, the problems of the authentication and access control of the HeNB users have been dealt with in (A. Golaup et al. 2009). A. Golaup and his colleagues offer a general picture of the works in progress when it comes to the HeNB standardization within 3GPP, particularly in case of access control strategy. Once a UE intends to connect the network through a HeNB, the CN becomes the entity in charge of carrying out the access control for the UE. For performing the access control, the CN is needed to preserve and update a list of CSG identities regarded as a permitted CSG list where the UE is subscribed. Every entry in the list relates the CSG identity to a PLMN identity. The data included in the UE permitted CSG list is saved as UE subscription data within the HSS and given to the MME for the sake of controlling the access. Prior to the reciprocal two-way authentication with the UE, the MME requires to verify if the UE is permitted to access the HeNB according to the permitted CSG list. A robust reciprocal two-way authentication and access control mechanism has been sug-

gested to safeguard secure communication for the HeNB by using a proxy-signature (C. K. Han et al. 2009). In this mechanism, the core network (CN) together with the OAM have a detailed agreement on the management, installation and operation of the HeNB through generating a proxy-signature to one another. Further on, the OAM re-selects its own proxy-signing ability to a HeNB. The CN also re-selects its proxy signing ability to the HeNB and generates its own signature to the UE. Eventually, the reciprocal two-way authentication among the HeNB and the UE can be obtained with the proxy signature on behalf of the CN and the OAM. The mechanism can block a diverse set of protocol attacks like pretending to be a valid HeNB, DoS and MiM attacks. The setback will be that, it causes a considerable amount of computational and storage costs and needs many modifications to the existing architecture because of the utilization of proxy signature that makes the system not efficient in real cases. Majority of the vulnerabilities and threats to the security and the privacy of the HeNB-enabled LTE networks have been investigated in (I. Bilogrevic et al. 2010) by new research approaches addressing some of these risks. I. Bilogrevic and his colleagues have proved a solution to the problem of location tracking and identity at the air interface via allocating and modifying identifiers according to the context. This solution offers a novel protection of identity regarded as user-based ID modification rather than network controlled strategy, where the mobile devices are able to take decisions on when to modify identifiers dynamically according to their own surrounding observations. Moreover, a secure protection method contra DoS attacks with a HeNB usage in the LTE architecture has been proposed as well. It has been highlighted that the solutions counted on the cooperation between various participating entities like Internet Service Provider (ISPs) can be an effective protection contra DoS attacks.

- MTC Security

When it comes to MTC, the security requirements, the threats and the respective solutions of the MTC security have been investigated in (M. Meyerstein et al. 2009). It has been recommended in (M. Meyerstein et al. 2009) that the Trust Environment (TrE) can be integrated within the MTC devices to safeguard the MTC device's security that can offer more strong secure functions for the authentication and cover many cryptographic potentials entitling the symmetric/asymmetric encryption/decryption compared with the present UICC. A key agreement and authentication mechanism for a set of UEs roaming from the same HN to a SN has been addressed in (Y. W. Chen et al. 2010). In this mechanism, several UEs that are devoted to the same HN, can shape as a group. By the time when the initial UE within a group goes toward the SN, the SN gets the authentication data for the UE from the respective HN by carrying out a complete authentication. There-

fore the SN can authenticate other members of the group when they visit the network locally without the HN involvement. This mechanism can diminish the communication expenses among the SN and the HN. The setback is that, there are yet several issues like network congestions in SN nodes when several devices go to the SN at the same time due to the fact that every device yet needs 4 signaling messages to perform an authentication. A novel mass-device access authentication mechanism according to a cumulative signature has been introduced in (J. Cao et al. 2012). Within this mechanism, a considerable number of MTCDs are initialized to shape as a MTC group to select a group leader. As soon as several MTCDs in the MTC group ask for accessing the network at the same time, the MME authorizes the MTC group by checking the cumulative signature issued by the group leader on behalf of all members of the group. Further on every MTCD relies on the MME by checking the Elliptic Curve Digital Signature Algorithm (ECDSA) signature from the MME through the leader of the group. Eventually, a separate session key among every MME and MTCD would be set based on the various key agreement elements transmitted from the asking MTCDs. The mechanism cannot just get to a reciprocal two-way authentication and a key agreement among every MTCD and MME simultaneously within a group, but can remarkably diminish the signaling traffic and therefore prevent from congestion of networks. The setback is that it may cause many extra computational expenses because of the utilization of cumulative and ECDSA signature, Moreover this mechanism needs the devices to cover both WiFi and LTE communications that is rare to take place that all MTCDs are needed to have both network interfaces. A M2M communication model according to 4G cellular systems has been proposed in (M. Saedy et al. 2011) where secure communication among two MTC devices can be obtained by fixing the ad hoc networks within the coverage area of the LTE systems. In this introduced model, the MTCDs can communicate in both ad hoc and cellular modes. In case a MTCD is located in the coverage area of the LTE network but distanced from other devices, it will then deploy LTE network resources. If not then it tries to contact the devices in the vicinity, where they shape as an ad hoc network. The problem will be when a device is in the range of both of other devices and the coverage of the LTE network has not been addressed in the suggested model. Moreover, the ad hoc network's introduction can cause many security problems that will affect the integration of the ad hoc architecture into the LTE networks. It needs more network optimizations and changes for integrating the M2M communications when it comes to the LTE networks (J. Cao et al. 2014).

5 SECURE COMMUNICATION AND VOIP THREATS IN WIMAX

5.1 Secure Communication and VoIP Threats in Next Generation Networks

5.1.1 Summary

VoIP is among the services and key issues that can be offered under the framework of the Next Generation Networks (NGN-4G) technologies like WiMAX. This technology consists of advantages and disadvantages similar to other emerging technologies. Today, the operators in telecommunication's field offer caller ID, call transfer/waiting, conference calling, together with other diverse services of VoIP in accordance with the NGN and the emerging solution of all IP. Therefore, the security of VoIP is among the important issues which are currently being investigated. In this dissertation it has been decided to focus on vulnerability classifications for the services of VoIP in NGN. It has been tried to demonstrate the shared and specific VoIP service's security threats and existing susceptibilities.

Determining the susceptibilities and their categorization, together with the system's risk scenarios clarify the know-how of system penetration and aids in the process of solving the problems. Only through being well-aware of the existing diverse specifications and security problems, the debate on VoIP matter would be taking the right course. Moreover, to send a message about the importance of identifying the VoIP security susceptibilities, the probability of the threats under the VoIP framework within 4-G technologies like WiMAX are classified. The fact is that VoIP is getting a lot more convenient and cost efficient when users are travelling. The VoIP industry is therefore continuously seeking for wireless platforms that could facilitate the voice traffic to and from mobile phones, laptops and etc. Up until now this has been the main challenge. Through utilization of 802.16, continuous connectivity of the users is assured. The point is that suburban users that cannot be provided VoIP service due to not living in a zone with a DSL line will eventually be covered with WiMAX.

5.1.2 Objectives and Approaches

Of course the attacks are not new and there exist many attacks which have been already discovered. Thus, the aim of this research work definitely was not finding

new threats or vulnerabilities, because attacks are mostly fixed in number but the main emphasis has been on looking from author's perspective and the special proposed classification. Therefore the approach is to classify and categorize the existing attacks in an alternative way such that they would not look scattered and provide a more focused and well-organized way of looking at them. Moreover, the classification is such that unlikely and purely theoretical threats and attacks are basically neglected. By defining this approach as the main objective, the attacks were investigated accordingly.

5.1.3 The VoIP Implementation over WiMAX

Voice over Internet Protocol (VoIP) offers a new type of telephone service provided by the old Public Switched Telephone Network (PSTN) through an IP network to transfer digitized voice. Nowadays VoIP applications are run over wireless technology as a result of the fact that packet switched air interfaces support flat IP architectures.

Compression | Decompression (CODEC) methods for VoIP conversion of audio signals to digital stream of bits. Speech samples are compressed even more to generate bit streams of 8–12 kbps that are transmitted over the IP network. As soon as the speech sample is compressed, it is further sent deploying the Real-time Transport Protocol (RTP) over the User Datagram Protocol (UDP) with the IP (R. Vannithamby et al. 2009).

It is very important to consider that the CODEC selection, packet loss, jitter and delay have a great impact on the VoIP over wireless networks. Unstable channel conditions normally incur latency increase and packet loss. For maintaining latencies to acceptable levels of 250–300 ms, the delay budget for sending over the air interface is 50–80 ms. The backbone, jitter buffer and CODEC infer the remaining delay. In order to control delays and maintain them within reasonable limits Hybrid Automatic Repeat Request (HARQ), dynamic link adaptation Channel aware scheduling with Quality of Service (QoS) are deployed. For compensating when it comes to delay jitter encountered by packets as a result of network congestion, timing drift or route changes, Jitter buffers are utilized.

- Elements for supporting VoIP over WiMAX

WiMAX offers several elements to support VoIP. The VoIP traffic prioritization is obtained by the categorization of the traffic into scheduling classes. It is essential to observe that detection of Voice activity together with Extended Real-Time Polling Service (ertPS), maintain and save the air link resources during silence

intervals of time. The channel scheduling and HARQ are deployed to diminish the sending latency on the top of the air link. The compression of protocol header is used to send the specific speech sample.

- ertPS for silence suppression

802.16 standard covers QoS requirements when it comes to data services and applications by transposing those requirements to one directional service flows that are transmitted over UL/DL connections.

In case of having no silence suppression, VoIP flows related service requirements are carried out by the UGS that is defined to support flows that produce fixed size packets of data on a regular basis. While the process of initialization of the voice session takes place, the grant size together with period are negotiated.

Service flows like VoIP having silence suppression produce larger packets of data while a voice flow is active, and respectively smaller packets during silence intervals. The rtPS is defined to cover real-time service flows that produce packets of data with variable sizes on a regular basis. Compared with UGS, rtPS needs more overhead of request, but also covers variable grant sizes. In a typical rtPS, a header asking for bandwidth is transmitted in a unicast request opportunity for permitting the subscriber station to determine the size of the required grant. The required grant is further on assigned in the following UL subframe.

The rtPS's mechanism of polling smoothens variable sized grants, deploying rtPS to switch among VoIP packet sizes when the SS swings among the talk and silent statuses infers access delay. Since the VoIP packet's size is very large for accommodating when it comes to the polling opportunity, the rtPS leads to MAC overhead as well, that can just accommodate a header asking for bandwidth. The delay among the subsequent bandwidth allocation with rtPS and the bandwidth request can infringe the delay limits of a VoIP flow. The rtPS also causes a considerable overhead from regular unicast polling which is not required while a talk spurt takes place.

The ertPS scheduling method enhances upon the rtPS scheduling method through increasing the allocation size deploying a bandwidth request header or diminishing the allocation size deploying a subheader in charge of grant management. The needed resource's size is indicated by the aid of the mobile station through modifying the Most Significant Bit (MSB) in the sent data.

- HARQ

Having aspects like the link adaptation and modulation together with coding, the HARQ is enabled in WiMAX deploying the protocol of "stop and wait", for offering a quick feedback to packet errors within the Physical (PHY) layer. Chase combining HARQ is applied to enhance the reliability of a resending when a Packet Data Unit (PDU) error is found. An Acknowledgment (ACK) channel is offered as well in the uplink for HARQ ACK/Negative Acknowledgment (NACK). Uplink NACK/ACK messages are basically piggybacked on downlink data. A HARQ operation with a few channels is used to enhance the error recovery efficiency. The 802.16 also offers signaling to permit asynchronous kind of HARQ operation for robust link adaptation.

The delay budget for VoIP on the down link or uplink is restricted within the 50-80 ms interval. This entitles the resending delay and queuing. Utilizing the HARQ resending for error recovery, remarkably enhances the system's potential to fulfill the outage criteria for VoIP and delay budget needs.

HARQ is a joint cooperation of error detection and forward error correction coding deploying the ARQ error control mechanism. When it comes to standard ARQ, the data is supplemented with some unnecessary bits to be sent deploying an error detecting code like cyclic redundancy check (CRC). When it comes to HARQ, Error Detection (ED) are supplemented with FEC bits to fix a subset of errors counting on ARQ to distinguish the unfixable errors. Thus HARQ functions better than normal ARQ when signal conditions are poor, whereas this causes having a tangibly lower rate in suitable signal conditions. There is normally a signal quality redline below which simple HARQ is superior, and above which basic ARQ has advantages.

Simple Hybrid ARQ

The HARQ's simplest edition, Type I HARQ, adds FEC and ED data to every message before sending. By the time the coded block of data is received, the receiver primarily decodes the error correction code. In case the quality of channel is fine, errors of sending should be all correctable, and the receiver can get the right data block. In case the quality of channel is bad, and sending errors cannot be all fixed, the receiver will recognize this situation deploying the error-detection code, further on the received coded block of data is rejected and a resending is asked by the receiver, like in the case of ARQ (J. G. Ramos et al. 2011).

Type II HARQ has a more complex form, the originator of message changes among message bits along with parity bits for error detection. As soon as the first sending is received without error, the FEC parity bits will not be transmitted. In

addition, 2 successive sendings should be mixed for error correction in case none is without error.

To comprehend the difference among the Type I and Type II Hybrid ARQ, consider the size of FEC and ED added data: error detection normally just adds a few bytes to a message that is an incremental in length increase. FEC can usually cause the message to become double or triple in length with error correction parities. In terms of speed, standard ARQ normally spends some parts of channel capacity for protection contra error, whereas the FEC spends half or almost majority of its channel capacity for channel enhancement.

When it comes to standard ARQ a sending should be received without error on any transmission for the error detection to pass. In type II HARQ, the first sending includes error detection and data. If received error free, then it is fine. In case data is received in error, the second sending will include FEC parities and error detection. The error correction can be tried by mixing the data received from both sendings.

The type I Hybrid ARQ has loss of capacity when it comes to robust signal conditions. Type II Hybrid ARQ is not so, due to the fact that FEC bits are just sent on subsequent resendings as required. In case of robust signal conditions, type II HARQ functions as good as standard ARQ when it comes to capacity. In case of poor signal conditions, type II HARQ functions having as good sensitivity as standard FEC.

HARQ with soft combining

Incorrectly received coded blocks of data are usually saved at the receiver instead of being blocked, and when the resent block is received, the 2 blocks are joined. This is regarded as HARQ with soft combining.

As it can be so that two transmissions cannot be separately decoded error free, it can take place that joining of the already erroneously received transmissions provides us with adequate data for decoding correctly. There are 2 chief soft combining mechanism when it comes to HARQ:

- Chase combining: every resending includes the same data and parity bits. The receiver deploys maximum-ratio combining to put together the received bits with the same bits from past transmissions. As a result of the fact that all transmissions are the same, chase combining can be regarded as an extra repetition coding. The reality is that each resending is like adding extra energy to the received transmission via an increased Eb/N0.

- Incremental redundancy: each resending includes various and different data than the past ones. Several sets of coded bits are issued, each demonstrating the same set of data bits. The resending normally deploys a different set of coded bits than the past sending, with various redundancy versions issued by the decoder output's puncturing. Therefore, at every resending the receiver gets additional knowledge.

HARQ can be deployed in stop-and-wait mode or in optional repeat mode. Stop-and-wait is less complex, but efficiency is diminished when one has to wait for the receiver's acknowledgment. Therefore several stop-and-wait HARQ processes are performed in parallel: when one HARQ process is waiting to get an acknowledgment, another process can deploy the channel to transmit some more data.

- Channel Aware Scheduling

One directional connections are set among the base station and the mobile station to control the ordering of transmission and scheduling on the 806.16's air interface. Each connection is known with a unique Connection Identification (CID) number. Each mobile station establishes a primary management connection, a secondary management connection and a basic connection for accessing the network. At the moment when all of the management connections are set, transport connections are fixed. On the downlink and the uplink, the traffic allocations are connection-oriented, and a specific mobile station may be related with several connections. The base station schedules resources in every Orthogonal Frequency Division Multiple Access (OFDMA) frame on the uplink and the downlink based on time-varying channel conditions and traffic dynamics. Link adaptation is utilized by HARQ, the feedback of channel quality and adaptive modulation/coding. On the downlink and uplink, the resource allocation is communicated in Mobile Application Part (MAP) messages at the start of each OFDMA frame. The Downlink-MAP is a message of MAC layer that is deployed to assign radio resources to mobile stations when it comes to down link traffic. Also the Uplink-MAP is a message of MAC layer deployed to assign radio resources to the mobile station for uplink traffic. The base station deploys data elements within the Downlink-MAP/Uplink-MAP to indicate the traffic allocations to the mobile station. The base station scheduler covers resource allocation in several sub-channelization mechanisms to balance speed needs and delay with channel conditions (J. G. Ramos et al. 2011).

- Main security issue in case of VoIP over WiMAX

Securing the voice communication is considered as being of great importance for VoIP over WiMAX to protect it against a possible interception or eavesdropping.

The double type of ciphering the X.509 for Authentication and 152-bit AES, TDES or 56-bit DES for data flow brings about the security of the transmission and makes the eavesdropping intricate to carry out. As soon as a subscriber station wants to connect to a base station, it transmits a request of authorization together with authentication data within a X.509 certificate frame as shown in Figure 17. The base station after checking the certificate replies by transmitting the message of authorization that has the authorization key ciphered with the public key of the subscriber for registering in the network. Thus an IP address is allocated to the subscriber station by the DHCP. The DHCP server is in charge of offering the address of the TFTP server, from where the subscriber station obtains the manufacturer's particular configuration data file as well. Further on, the base station accepts the subscriber. The data is further ciphered deploying 56-bit DES, TDES or 152-bit AES as demonstrated in Figure 17. This protects against the theft of service and eavesdropping possibility of the data as the connections among the base station and subscriber station are ciphered. Moreover 802.16 has integrated and built-in virtual LAN (VLAN) cover that offers protection for data sent by several users of the same base station.

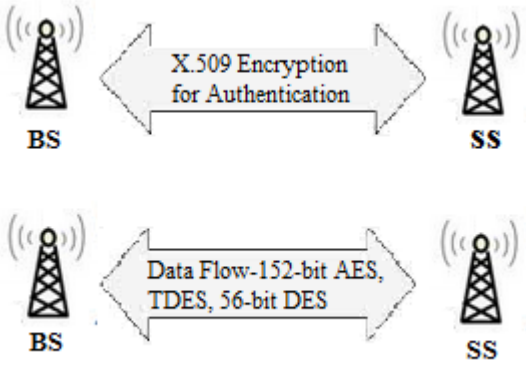


Figure 17. Main security issues representation in case of VoIP over WiMAX

5.1.4 Results

In this dissertation the susceptibilities of the VoIP have been given out into 2 classes, vulnerability source and vulnerable component, which are separately presented (A. D. Keromytis et al. 2009). It is important to categorize them in this manner so that the security of the system would be taken care of. Given the vulnerable component and its source it would be much handier to deal and mitigate the issue respectively. Furthermore, the VoIP vulnerabilities are classified in four groups being Threats against confidentiality, Threats against integrity, Threats against social context and Threats against availability. Therefore each of the

threats are fitting into one of these as sub branches. Moreover the threats are each one separately explained and the its relevant scheme is provided. Finally having explained and defined every aspect, a general vulnerability classification model is proposed and provided in Figure 18.

Source of Vulnerability

The vulnerabilities and risks contra VoIP system availability by exploiting implementation weaknesses are regularly seen (S. R. Chogan et al 2012). In this dissertation both issues regarding the implementation of VoIP in general and also in WiMAX specific case will be explained. First the general issues are discussed. One can consider the fact that several general VoIP implementations are proved to be vulnerable to hanging when given null, malformed, or big numbers of SIP INVITE messages. In order to investigate the vulnerability sources, here common cases are presented as follows:

• IP-Based Network Infrastructure: As a result of the fact that VoIP is a network infrastructure being IP-based, the threats and harms which endangers the internet protocol are inherited by the VoIP system. These consists of: Attacks on transmission control protocol, overload flooding, rogue fragmentation of IP and many other harms.

• Public Networks: Within the internet network that is public and open, an instance originated threat is SIP bomber attack that poses serious a threat.

• Standard Protocol: SIP and H.323 are among the protocols of VoIP that are standardizations being open to public for accessing purposes. Thus it is possible to produce a server/client from the base even in view of rogue purposes. Therefore, these open protocols due to can be exploited by the attacker.

• Compromised Interface: This possibility is offered to the attacker to generate traffic that is fake and/or nonsense because random port/IP scan can be performed.

• Live communication: As a result of the fact that the interruption must have no room when it comes to live communications any kind of negative impact from the attacker may diminish the quality of service.

• Mobility: VoIP allows its users to have virtual access to different locations. This characteristic leads to the complication of internet phone mobility and at the same time protection against the attackers will be more difficult. This is due to the fact that there will be no limits for tracing the packets as they can go anywhere but the point is that usually up to three-four servers or hops can be traced for identifying

the origin of the attack. Thus if the number of hops through which packets travel increase, it will be very hard to determine its exact launching point.

• Missing security devices, measures and features: One of the measures taken to stop the attacks against VoIP systems, is to utilize a firewall but due to system related complications and risks the described measure is not adequate.

• Integration of data and voice: Adding data to voice causes unexpected harms and if device performance does not fulfill the requirements, the quality of service will be reduced (A. D. Keromytis et al. 2009; Syed Ahson et al. 2009).

Vulnerable Component

• The components that are utilized by VoIP have some certain susceptibilities that influence it more or less. Therefore here some of the major components of VoIP together with their respective susceptibilities are highlighted in brief.

• VoIP application's operating system: Due to the fact that VoIP runs on UNIX, Linux, Windows operating systems, their susceptibilities are inherited by VoIP. It is necessary to take into account that the system security patches which are announced for operating systems from time to time demonstrate that there have been security breaches which could be passed on to affect the VoIP.

• The server/client of Web: is an application belonged to VoIP which offers services within web and thus inherits the susceptibilities of web client/server like worm threats and malicious traffic.

• Switch or Router Devices: In case the intruder can compromise the router and control the system it would be able to damage the systems seriously. For instance, an intruder can verify the media and signals of VoIP without affecting the working performance. As another instance, configuration errors in the 3rd layer of router can cause unnecessary broadcast and the attacker can achieve some information and through them will carry out the next attacks.

• Network: The susceptible component can be the network itself due to vast and unsupervised traffic, despite whether it is hurtful or not.

• Protocol Stack of the VoIP: Security parameters are not taken into account while VoIP protocols are initialized (Syed Ahson et al. 2009). A brief form of vulnerabilities can be modeled and proposed as in Figure 18.

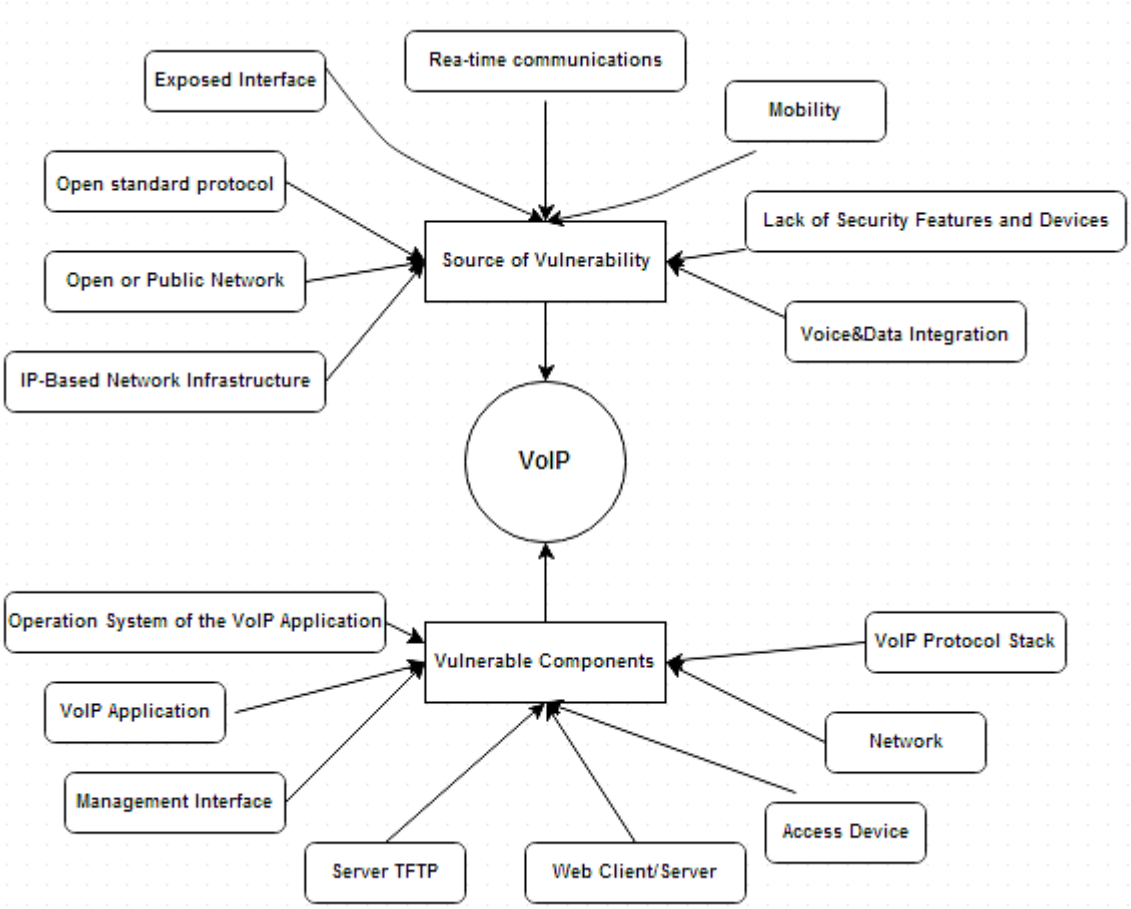


Figure 18. Proposed vulnerability classification model

After expressing vulnerabilities, we examine the classification of VoIP risks and threats.

The categorization of threats in VoIP

In this dissertation, we divided the VoIP threats to 4 categories:

1. Availability Threats

2. Confidentiality Threats

3. Integrity Threats

4. Social context Threats

Each of these categories includes some threat which we mention below.

- Availability Threats

Some risks are caused contra services provided 24 hours a day and thus result in failure of the system or disruption/interruption. A well-known example is the Denial of Service attack. When it comes to these threats we can point to the next instance:

Call Flooding

A DoS's well-known instance is the instant call flooding creation where the intruder causes a high amount of traffic due to valid/invalid calls and sends them to the aimed system, thereby significantly decreasing its efficiency or the system will break down (Patrik Park 2009).

Common methods are as follows, moreover call flooding is demonstrated in Figure 19 below:

•Valid or invalid registration flooding

•Valid or invalid request flooding

•Call control flooding after call setup

•Ping flooding

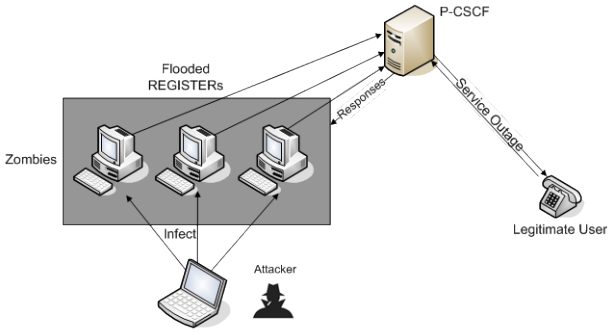


Figure 19. Call Flooding

It is to be highlighted that both the intentional flooding and unintentional flooding can result in the system failure called a "self-attack". Down this process the resources available on the servers become inaccessible duo to overflow of the requests and inability of responding to their demands. The following elements can be the cause of attack:

•Regional power outage and restoration

•Incorrect configuration of device

•Misbehaving endpoints

•Legitimate call flooding

Malformed Messages

An intruder may generate a malformed message and transmit it to a certain user for disrupting purposes. An instance of the malformed message can be found in Figure 20.This malformed message is similar to a protocol message but its text does not comply with the usual standard format, and it causes confusion in those devices (Dorgham Sisalem 2009). This threat takes place commonly as a result of the coming reasons mentioned:

- Protocol specification weakness

- Ease of generating malformed messages

- Implementation’s lack of handling exception

- Difficulty in verifying all cases of malformed messages

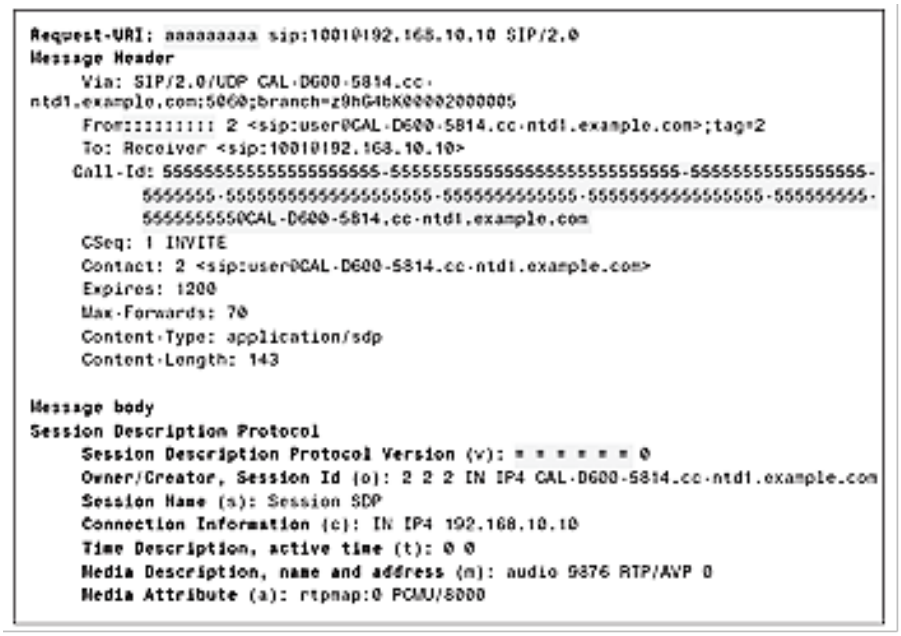


Figure 20. Malformed messages

Spoofed Messages

An intruder can insert a spoofed message to steal the session or discard the services. The "toll fraud" and "call teardown" are among the instances of spoofed messages.

Call Teardown

In this method the intruder controls a SIP conversation and gains the session data together with the “From”/“To” tags, and transmits a "SIP BYE" message to the communication device and thus simultaneously close the call session. An attack modeling can be seen in Figure 21 (Dorgham Sisalem 2009).

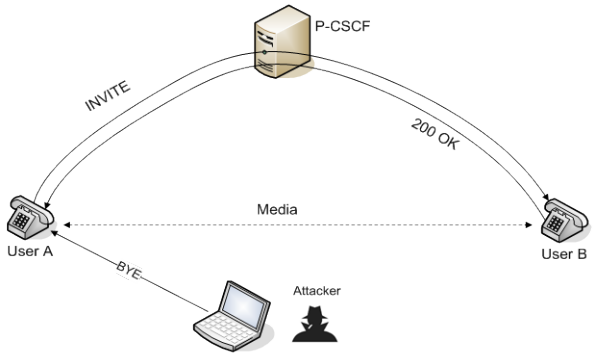


Figure 21. Call Teardown

Call Hijacking

Hijacking of the call occurs when the intruder compromises the transactions taking place among the network and a VoIP user. The common scenarios are hijacking registration, server impersonation together with hijacking of the media server (James F. Ransome 2005).

In this scenario, the attacker identifies himself as an authorized device, and steals the entire media/ contact sessions among the two parties. The transmitter supposes that, he is in contact with the aimed user, while the aimed user has no access to the messages sent by the transmitter. The call hijacking process described above can be observed in Figure 22.

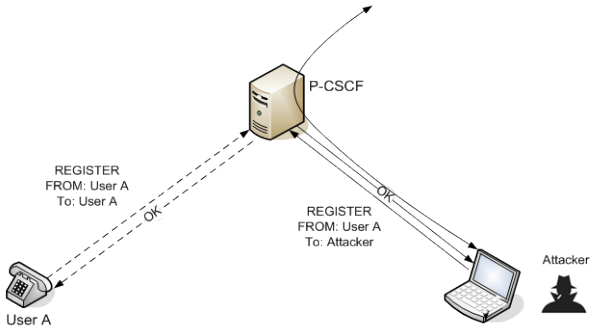


Figure 22. Call Hijacking

The Abuse of Quality of Service

In this mechanism, the intruder occupies a considerable portion of the bandwidth and thus the authorized user is capable of deploying services anymore or the QoS would be degraded.

- Confidentiality Threats

Contrary to the interruption of service described above, confidentiality threats do not affect present communications but through media theft and data storing, the intruder gets the information required for possible future threats. This is actually the most common kind of confidentiality threats.

Media eavesdropping

Media eavesdropping is carried out in 2 manners. One alternative can be listening to the packets of media within the same domain of broadcasting like the aimed user's. Secondly through an access device compromise (for example, a router or a layer2 switch) and forwarding together with repeating it to an intruder device (James F. Ransome 2005).

The media eavesdropping attack can be modeled as follows in Figure 23.

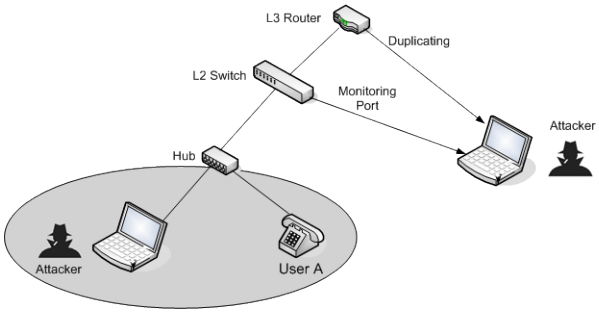


Figure 23. Media Eavesdropping

Trucking Call Patterns

In this mechanism, the intruder goes on in an unauthorized investigation of VoIP service and gains the required essential data. For instance, becoming aware that a company's CEO and CFO have been calling the CEO and CFO of another company can show that an acquisition is taking place.

Traffic Capture

Traffic capture is the process of storing the traffic in an unauthorized way and by any means which consists of storing packets together with packet snooping logging in view of unauthorized purposes. Traffic capture can be regarded as a fundamental mechanism for storing communication without all party's consent.

Data Mining

Gathering data such as phone number, user name, email address, URL address, or other kinds of data which the intruder deploys his rogue purposes: phishing, spam calls, toll fraud calls and service interruptions,.

Abuse of Service

Abuse of service is a considerable category in terms of service's improper utilization which consists of:

Abuse of call conference

Abuse of call conference is when the intruder hides his identity for fraud committing purposes.

Premium rate service fraud

Premium rate service fraud is a mechanism for increasing the traffic artificially without consent having goals other than maximizing the billings.

Improper bypass or adjustment to billing

Improper Bypass or Adjustments to Billing are methods of avoiding authorized service charges or for concealing other fraud by altering billing records (VoIP Security Alliance 2006).

- Integrity Threats

After the attacker has intercepted the message as a network interface, it tries to change. The alteration can consist of deleting, injection or replacing certain information in the VoIP message or media. This part is given out into 2 kinds:

• Message integrity threats (alteration of message)

• Media integrity threats (alteration of media)

The difference between the two lies on the content being alternated and the methods used to attack the integrity.

The message integrity threats (alteration of message) happen by the next 3 methods:

Rerouting the Call

The intruder access, through an unauthorized to call the routing data causes a call direction modification and rather than reaching the targeted user, the call is shifted elsewhere. Rerouting the call procedure can be shown as in Figure 24.

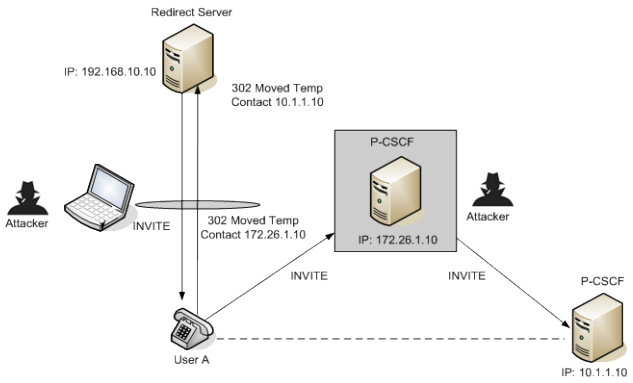


Figure 24. Rerouting the Call

Black Holing the Call

The process of refusing to forward or delete any protocol message's critical parameters through an unauthorized mechanism is regarded as black holing the call. The consequence is to delay call setup, refuse subsequent messages, make errors on application, drop call connections and so on.

False Caller Identification

Where there is a misrepresented identity/presence, it is an indicator of false caller identification

The media integrity threats (alteration of media) happen by the next 2 methods:

Media Injection

In this method the intruder either injects or replaces new media into an active channel of media. As a consequence the victim hears a noise or silence during the conversation. Media injection process can be demonstrated as follows in Figure 25.

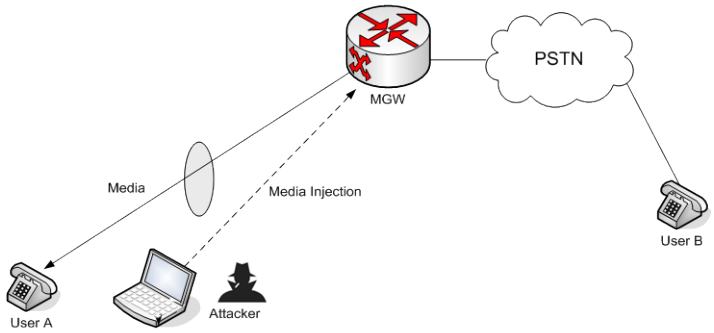


Figure 25. Media injection

Media Devolution

The intruder manipulates the packets belonging to the media control and infers reduction of quality of service when it comes to any communication.

- Social Context Threats

In this mechanism the intruder plays the role of a trust entity and transmits false data to the aimed victim for getting the required personal data and carry out the next threats (S. R. Chogan et al 2012).

Typical social context threats are as follows:

• Identity, rights, content and authority misrepresentation

• Voice Spam, IM, and presence

• Phishing

Identity, rights, content and authority misrepresentation

In case the intruder presents a false identity, the victim can be deceived and the intruder becomes aware of the key, password, and certificate.

Voice Spam, IM, and presence

A considerably huge amount of unsolicited requests to initiate a video/audio session, most utilized when it comes to internet related marketing (Tan Koon 2006). The spam presence message can be seen in Figure 26.

This part is given out into 3 kinds:

• Spam Call (SPIT)

• IM Spam (SPIM) or Instant Messaging Spam

• Spam Presence (SPPP)

Figure 26. Spam Presence

5.1.5 Contribution to the Research Area

There are diverse types of threats which affect the VoIP services within a networked/internet environment. The chief reason is that the majority of the intrusions are not traceable for finding their origins in view of mitigation and protection. Moreover, networks are known for possible types of sniffing and spoofing. Hence, in this dissertation, VoIP vulnerabilities and possible threats have been

categorized in a unique manner with a new approach explained above. The set of vulnerabilities and threats provided can be considered as a reference for future works and can be relied upon as a security anthology for interested scholars.

5.2 Hybrid Security Classification Approach to Attacks in WiMAX

5.2.1 Summary

WiMAX(World Wide Interoperability for Microwave Access) is a wireless communication technology that provides the possibility of last mile wireless broadband access in order to replace cable and DSL. The end users have the possibility of using WiMAX as the primary connection medium for benefiting from services like VoIP connections, on-demand video screening and mobile banking transactions. Overall most of the WiMAX-related research has been concentrated on physical and MAC layers; from the beginning there has been attention to security issues when it comes to WiMAX due to previous experiences like Wifi, but it requires to be further investigated. Numerous security problems should be mitigated in expected scenarios and for different types of users in the security standard of WiMAX. In this research work, a novel hybrid classification approach will be provided based on a new perspective. In this attempt vulnerabilities and threats are classified meticulously into two categories. In addition to this the criteria's of evaluation are also two that is explained later. Also attacks are classified in four classes together with their sub branches. The attacks are each explained shortly. The important point is that those attacks which cannot be realized under real conditions are omitted and not taken into account. This perspective has led into a less scattered and more concentrated investigation.

There are many attacks which pose threats to WiMAX. Most of them affect the MAC layer because this layer is in charge of security issues. The focus will be mostly on the attacks associated with this layer. Many people in scientific community have tried their best to classify and categorize the attacks and security issues of WiMAX and even some of them are so complete but the thing is that many of those attack are just according to pure theoretical grounds and some of them cannot happen under any circumstances. The second thing is that other classification versions look so scattered and one cannot find an integration between them. The third point of being distinguishable is that by removing the absurd theoretical attacks and having an integrated approach, our version will be more com-

prehendible and understandable even in a glance. In the same time maximum efforts have been made in order not to neglect important posing threats and attacks.

5.2.2 Objectives and Approaches

The attacks are categorized according to their kind into many classes. The attacks are categorized in 4 classes. As a result of the lack of some attack namings, respective names are coined with an arbitrary naming to boost the understandability of the dissertation. We classify the attacks based on the imposing risk to the system as: Major and Minor. This categorization is carried out by focusing on two criteria's:

1) Probability of happening - This criteria implies the attack occurrence possibility being carried out by utilizing the faults and system susceptibilities. The attack is counted as unlikely to happen if its costly, serious hurdles are on the way, or the risk of becoming known is high. An attack is foreseen in case its related costs/risks for the attacker are low and there are no impediments regarding the attack.

2) Effect on the system - This factor is a sign for the respective impact on the system, if the attack would be a successful one. The attack is counted as having low effect in case it influences a few users, for a short- limited time. An intrusion is counted as having a considerable impact if it influences a huge number of users for a remarkable time duration and leads to provider's financial or confidentiality loss for many users.

5.2.3 Results

The results of the classification and categorization of the author have been presented thoroughly, Based on author's studies, the attacks which fell into the realizable category were collected and sorted out in four different groups which are also integrated in their nature and provide a better and more precise understanding of the subject. In addition to this in scenarios when the attack was scarce, we have coined new labels. Finally the last point is that the attacks are only judged as being "Major" or "Minor" like black and white and there is no categorization in between. The criteria's of the classification are not something special or new and the author took these criteria's also in the VoIP paper.

5.2.4 Contribution to the Research Area

Nowadays, one can find research papers that have highlighted some of the security flaws and vulnerabilities of the IEEE 802.16. In this dissertation we have taken a hybrid classification approach so that the attacks are categorized in 4 classes together with their sub branches. In addition to this all of them are labeled in terms of severity and the risk which they impose, based on criteria's as probability of happening and the effect on the system. Furthermore, we evaluated briefly the characteristic of each attack. Finally our analysis made it clear that some attacks cannot be performed against the standard whereas majority of them can cause minor harm to the network.

6 PERFORMANCE MEASURE OF SECURITY IN MOBILE WIMAX

6.1 Kiyotaki-Moore Model Approach to Performance Devolution in Mobile WiMAX

Mobile WiMAX is developed to meet the demand for personal broadband services. Kiyotaki-Moore is an economic model that shows how small shocks to the economy might be amplified by certain factors, causing large output fluctuations. In this dissertation, we have taken a novel approach to the degradation of performance in mobile WiMAX by applying this model. We have produced a small shock by accidentally increasing the number of simultaneous users and then analyzed the output explaining the meaningfulness and applicability of this model. In this dissertation the performance of mobile WiMAX under special circumstances has been investigated. The performance degradation of mobile WiMAX is analyzed according to the system parameters which are the number of simultaneous users per each channel, the fixed height of antenna plus the fixed distances between the BS and the MSs. Four scenarios have been conducted for running the experiments. NCTUns 6.0 has been selected for simulating the scenarios. This simulation program provides the real world environment with a complete set of equipment's and application configurations. This simulation program has facilitated the process of setting up a network and running the analysis and experiments. In order to achieve the research target, four mobile WiMAX scenarios have been designed to simulate mobile WiMAX topology.

Objectives and Approaches

The objective was set to analyze and investigate the performance of mobile WiMAX under the condition of increasing the number of simultaneous users being increased at once. For this purpose and obtaining reliable results, an economic theory has been deployed to define and explain the occurred degradation which appears to the performance of the mobile WiMAX. A shock has been created and then analyzed the aftermath. Moreover it was observed that as the number of users increases the performance faces a logical decrease.

6.1.2 Results

NCTUns provides the possibility for configuring the network topologies and parameters, surveillance of traffic flows, and gathering statistics about a simulated network (Chin-Liang Wang 2010; R. B. Ramle et al. 2010).

Table 2. Simulation parameters

Parameters	Values
Frequency Bandwidth	5 MHz
Modulation Type	OFDM-QPSK
Length of the Frame	5ms
Simulation Time	100s
Routing Protocol	OSDV
Mean Length of Packet	1024 bytes
Number of Nodes	Scenario-based

Table 2 shows the simulation parameters. As one can see in Figure 27 the parameters are set to ensure a standard test condition. The frequency bandwidth is fixed at 5 MHz. The length of frame is of 5ms. The simulation duration is circa 100 seconds and the number of nodes is variable and based on scenarios defined through the process to make sure conditions do not interfere with the output.

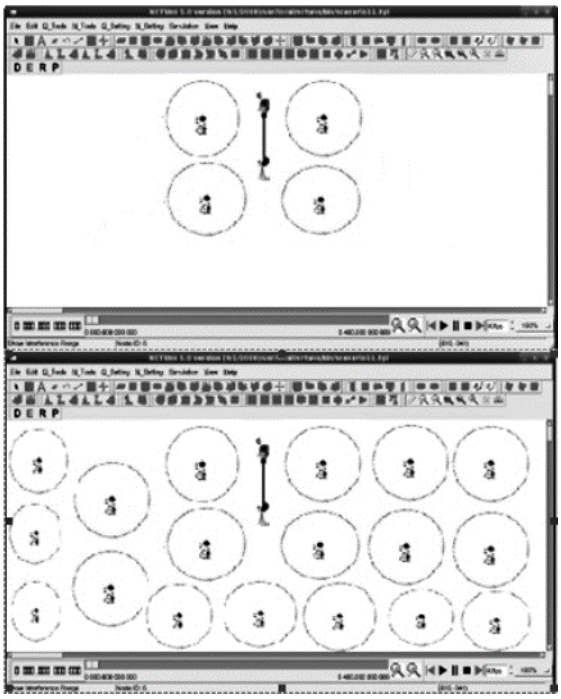


Figure 27. Creating the shock by an increase in the number of simultaneous users

In Figure 28, as one can observe, we have worked on the case where the number of simultaneous users have drastically increased. Therefore, by this way according to Kiyotaki-Moore model we have designed a small shock to the WiMAX network and as one can see the simulation results this small shock has led to a decrease of average data rate and finally resulted in a visible decline when it comes to the performance of the mobile WiMAX network. Therefore when the height of the base station and the distance between the BS and MS's are fixed at values of 25 meters and 1000 meters respectively, then if the number of simultaneous users is continuously increasing, the performance of the WiMAX network faces a decline.

The performance decline of Mobile WiMAX is analyzed according to the system parameters which are the number of simultaneous users per each channel, and the height of antenna. We have conducted 4 scenarios for running the experiments. NCTUns 6.0 has been selected for simulating the scenarios. This simulation program provides the real world environment with a complete set of equipment's and application configurations. This simulation program has facilitated the process of setting up a network and running the analysis and experiments. In order to achieve the research target, four mobile WiMAX scenarios have been designed to simulate mobile WiMAX topology. The scenarios can be seen listed in Table 3. There are four MSs used in this simulation and then the number has been in-

creased to forty MSs for creating the required small shock. It is to be mentioned that all the MSs are connected to one BS. The distance between the BS node and MS nodes is a fixed value of 1000 meters. In each of the scenarios, the number of the simultaneous users per channel has been increased by 20.

After running the test with the before mentioned parameters and values, we got the following results as shown in Figure 28:

Table 3. Simulation settings and outcomes

No Scenario	Base Station Height	Number of Simultaneous Users per Channel	Average Data Rate bits/second
Scenario 1	25	40	848
Scenario 2	25	60	842.78
Scenario 3	25	80	837.98
Scenario 4	25	100	832.78

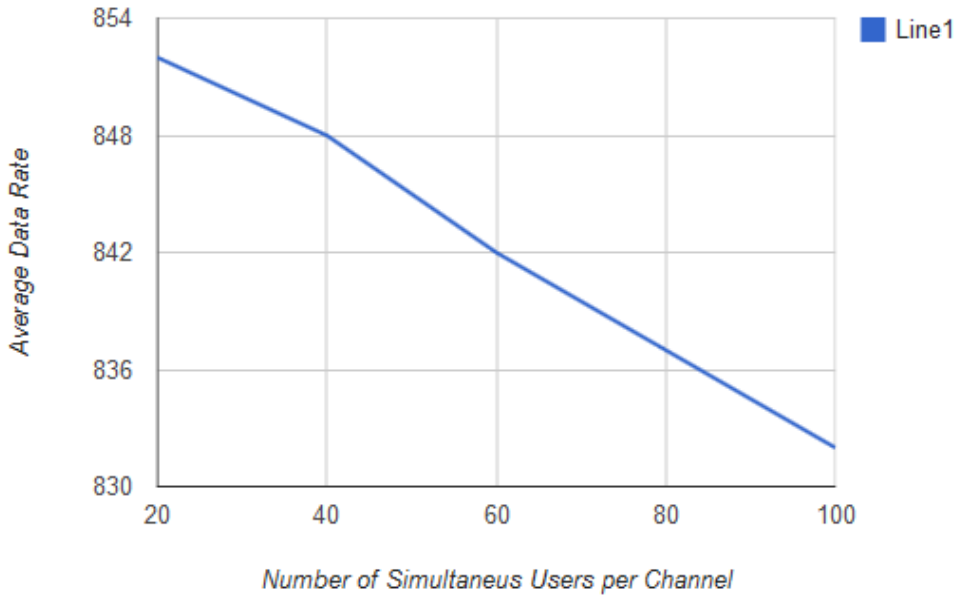


Figure 28. Performance decline of mobile WiMAX (x axis: number of simultaneous users per channel; y axis: average data rate)

In this economic model, by considering some factors a small shock to the economy can cause a large amount of fluctuations in the output of the system. The Kiyotaki-Moore model can be observed in Figure 29 as follows:

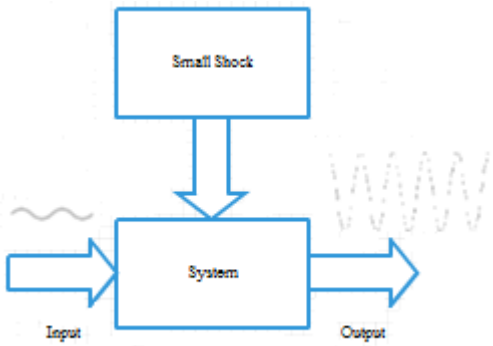


Figure 29. Kiyotaki-Moore Model (N. Kiyotaki et al. 1997)

WiMAX technology can be affected by various issues like the distance from the base station, environmental effects and many others (A.Vinel et al. 2011; Q. Ni et al. 2012; R.B. Ramle et al. 2010). In this dissertation we have analyzed the case when the numbers of simultaneous users have drastically increased. Hence, by this way based on Kiyotaki Moore model we have created a small shock to the WiMAX network and as one can see the simulation results this small shock has resulted in a sharp decrease of average data rate and eventually led to a visible decline when it comes to the performance of the mobile WiMAX network. This can be observed that when the height of the base station is fixed and the number of simultaneous users are constantly increasing, the performance of the WiMAX network faces a devolution.

6.1.2 Contribution to the Research Area

In this dissertation, we have presented the performance evaluation for mobile WiMAX utilizing the NCTUns 6.0 simulation program. The evaluation is determined based on the system parameters that are the height of BS and the number of simultaneous users. Eventually it can be observed that when the height of the base station is fixed and the numbers of simultaneous users are constantly increasing, the performance of the WiMAX network faces a decline. Hence, by this way based on Kiyotaki-Moore model we have created a small shock to the WiMAX network and as one can see the simulation results this small shock has resulted in a sharp decrease of average data rate and finally led to a visible decline when it

comes to the performance. This research is restricted to the number of the simultaneous users. It has been mentioned that other parameters like the height of the BS and the distances between the BS and MS's are fixed.

6.2 WiMAX-based Energy Efficient Intrusion Detection System

6.2.1 Summary

After careful consideration of security problems of WiMAX network and based on the specification of the WiMAX itself, in this dissertation we have taken a novel approach to these issues by designing a WiMAX-based power efficient intrusion detection system that has better performance and is more efficient. Our investigations indicate that this intrusion detection system can provide both an acceptable application value and in the same time offers a less power consumption alternative. An intrusion detection system (IDS) is usually a device or software application which monitors network for malicious activities and produces reports to an administration unit. By utilizing IDS various systems try to stop an intrusion but because the nature of it, is a monitoring system, further capabilities can be added by combining it with other security tools like firewalls. Intrusion detection system warns and replies to rogue operations prior to attacks against computer network and system. As a result of the fact that security is an indispensable part of a WiMAX network, a combination of the intrusion detection system and some policies can bring about a more reliable and efficient network. Therefore an efficient version of a WiMAX-based intrusion detection system has been introduced. The proposed IDS block diagram is represented in Figure 30.

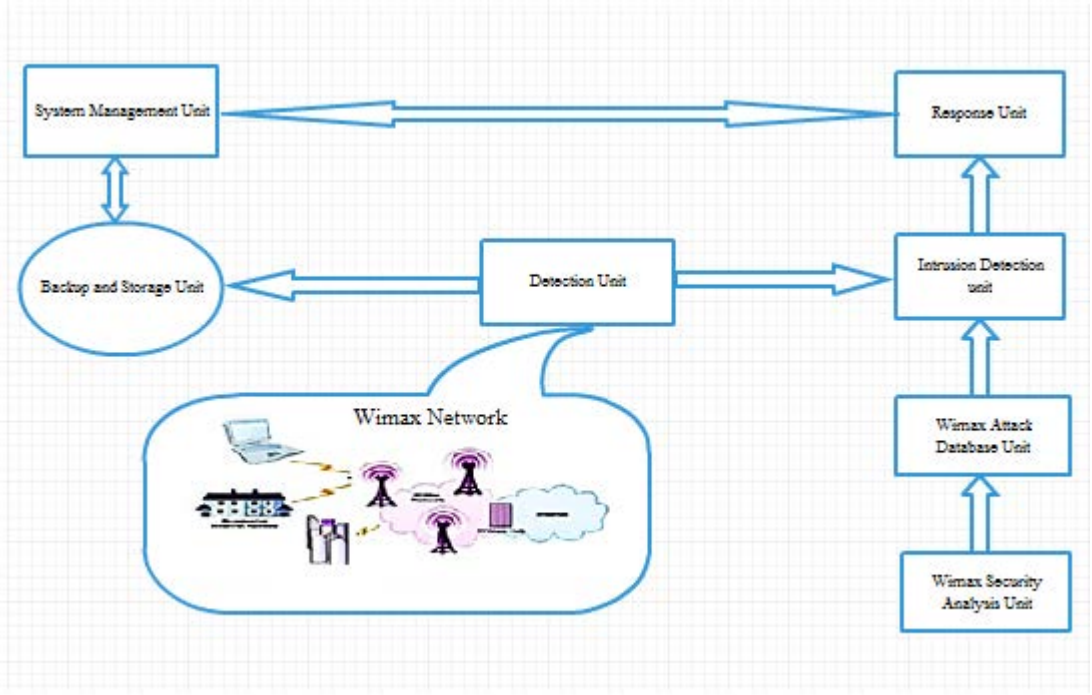


Figure 30. Proposed IDS Block Diagram

6.2.1 Objectives and Approaches

The initial objective has been nothing but a precise IDS capable of performing at high standards that is both efficient in terms of power and careful when it comes to processing and detection of any vulnerability based on a signature-based approach and SNORT-like (Snort 1998) deep packet inspection system. In detailed version of how everything works together with functional blocks have been described in section 4.5 starting from page 69. The related power calculations are done based on appendix reference computing procedures.

6.2.2 NS2 Technical simulation

There are two separate rounds of simulations carried out in this specific domain. One is the simulations performed in NS2 simulator and the second is the simulations completed in Toshiba consumption analyzer program. It is to be mentioned that primarily NS2 simulations will be investigated followed by the Toshiba consumption analyzer related simulations. The associated technical simulation is carried out by using the NS2 All-in-one 2.34 version. (Network Simulator) NS2 is a discrete event simulator for networking research. NS2 offers a considerable support for TCP simulation, routing, and multicast protocols over wired and wireless networks. NS2 does not offer WiMAX simulation by default. For the specific

targets and research goals of this dissertation the (Lightweight WiMAX Simulator) LWX is utilized. LWX module is a NS2 802.16 simulation module (IEEE 802.16 and IEEE 802.16j) designed for IEEE 802.16 researchers (Y. C. Lai et al. 2009). The ultimate aim of LWX is to provide a flexible and complexity-free software architecture with respect to IEEE 802.16 simulator for the scholars. Therefore if one intends to deploy LWX, the NS2 has to be installed primarily. LWX offers 802.16 MAC functionalities with QoS, various modulation coding rates, and traffic relay supports chiefly utilized for bandwidth allocation and relay link selection related scenarios. In addition to this LWX offers many bandwidth allocation algorithms for 802.16 and 802.16j networks including strict priority and round robin bandwidth algorithms for fundamental 802.16 network and round robin bandwidth algorithm for 802.16j relay network. The LWX should be pasted in the main directory of the NS2 all-in-one 2.34. During this carried out research the chief target is the simulation of WiMAX performance in the downlink and uplink when the proposed IDS is deployed compared with when the IDS is not used. The following Table 4 demonstrates the simulation configurations:

Table 4. NS2 simulation configuration

Configurations	Values
Max Packet Size	2048 bytes
Quality of Service	2 NS2 units
Rmin	130 k-bytes
Rmax	200 k-bytes
Jitter	30 ms
Lmax	60 ms
Simulation Time	300 s
Bandwidth Allocation	Round Robin
Radio Propagation Model	Two-Ray Ground
Network Interface Type	Wireless Phy
Routing Protocol	AODV

Topology Size	250 NS2 units
BS transmiter/receiver	5 Mbps

In order to support QoS, the IEEE 802.16 MAC layer defines five service classes including Unsolicited Grant Service (UGS), Real-Time Polling Serves (rtPS), Extended Real-Time Polling Services (ertPS), Non-Real-Time Polling Services (nrtPS), and Best Effort (BE) (Y. C. Lai et al. 2009). Each service class has its specific QoS parameters being comprised of Maximum Sustained Traffic Rate (*Rmax*), Minimum Reserved Traffic Rate (*Rmin*), Maximum Latency (*Lmax*), Tolerated Jitter, and Traffic Priority. *Rmax* defines the peak rate in k-bytes, *Rmin* implies the minimal sustainable rate also in k-bytes, *Lmax* specifies the maximum latency between the ingress time of a packet to the MAC layer and the forwarding time to its air interface represented in ms and the jitter in ms as well. The simulation time is set to be 300 seconds. BS transmitter and receiver has the throughput of 5 Mbps. NS2 has some default values which holds for normal WiMAX networks simulations especially in the case of jitter, latency and quality of service as shown above in Table 4. The bandwidth allocation has been selected to be round-robin. The radio propagation model is opted to be two-ray ground. The routing protocol is AODV and the network topology size has been fixed at 250 units of NS2 simulator. During this simulation we intend to run a DoS attack by running 50 FTP requests targeted at the base station which provides the services. Therefore as one can see in Figure 31 the attack is run as follows:

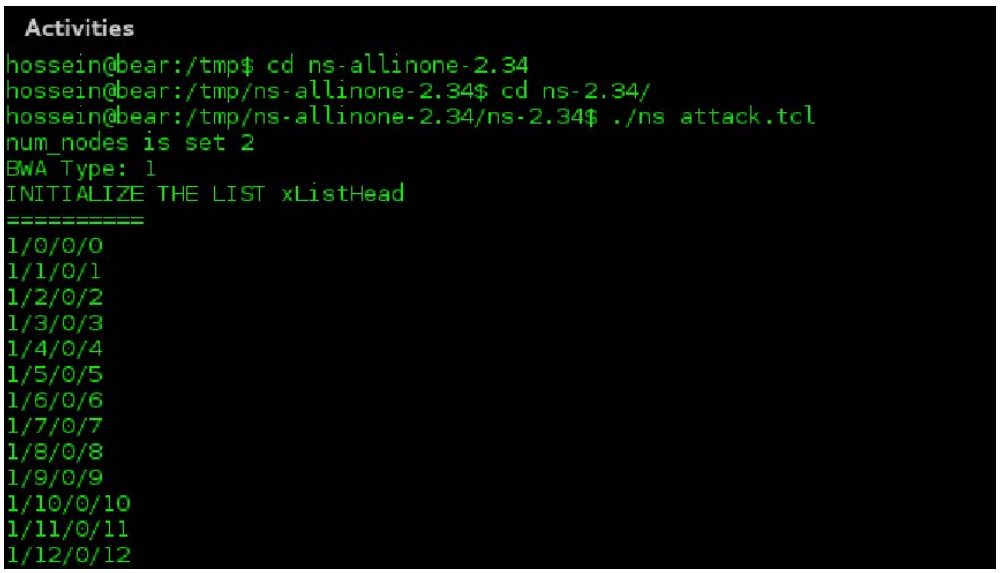


Figure 31. The screen shots represent all the fifty connection requests →

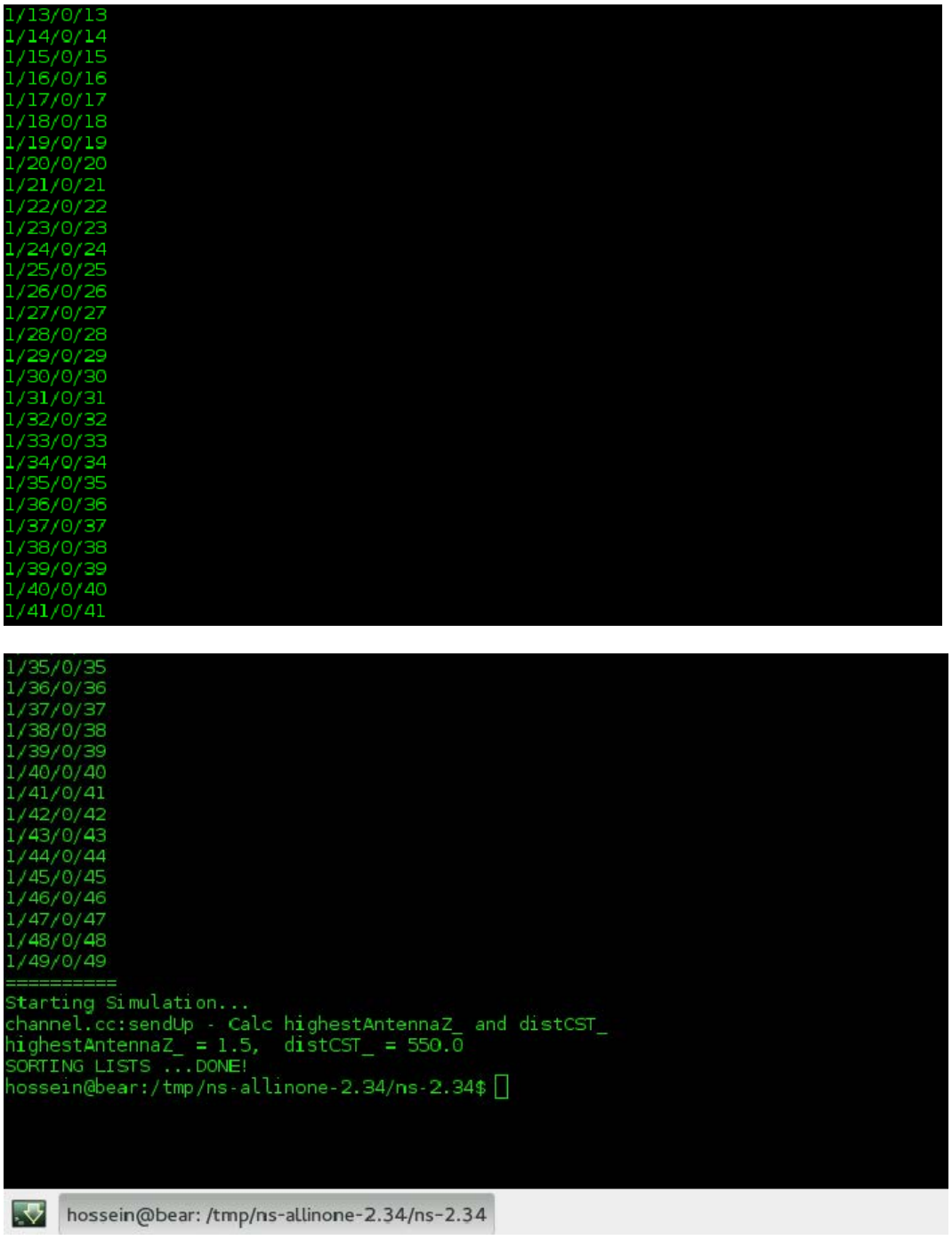
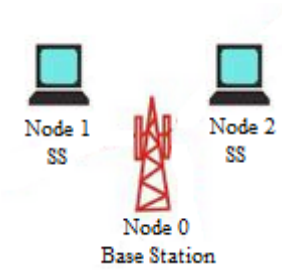


Figure 31. The screen shots represent all the fifty connection requests

As one can observe there is a list format having the structure of (x0/x1/ y0/y1). The first part that is comprised of x0 and x1 belongs to the source and y0 and y1 is dedicated to the destination. Further on, x0 and y0 are node numbers and x1 and y1 are the port numbers. It is to be mentioned that in NS2 usually node 0 is

the base station as it is also in our specific case. Furthermore node 1 and node 2 represent the subscriber stations as in Figure 32 below. In our case the base station is with x=15, y=15, z=0 NS2 unit coordinates and the subscriber stations are with x=17, y=17, z=0. The results of the simulations are stored in a file having the trace format regarded as “log.tr”. After running the simulation, result’s format can be observed in Figure 32:




```
Activities
  GNU nano 2.2.4                                                File: log.tr

s -t 1.370125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.370125009 -Hs 1 -Hd 1 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.370125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.370125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.370125009 -Hs 0 -Hd 0 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.370125009 -Hs 0 -Hd -2 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.375125009 -Hs 1 -Hd 1 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.375125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.375125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.375125009 -Hs 0 -Hd 0 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.375125009 -Hs 0 -Hd -2 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.375125009 -Hs 0 -Hd 0 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.375125009 -Hs 0 -Hd -2 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.380125009 -Hs 1 -Hd 1 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.380125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.380125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.380125009 -Hs 1 -Hd 1 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.380125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.380125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.380125009 -Hs 0 -Hd 0 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.380125009 -Hs 0 -Hd -2 -Ni 0 -Nx 15.00 -Ny 15.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
r -t 1.385125009 -Hs 1 -Hd 1 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
s -t 1.385125009 -Hs 1 -Hd -2 -Ni 1 -Nx 17.00 -Ny 17.00 -Nz 0.00 -Ne -1.000000 -Nl AGT -Nw --- -Ma 0
```

Figure 32. The setup and screenshots of the simulation outcome in NS2 interpretation format

Due to the horizontal length of the results, they cannot fit the A4 page format and thus the continuance of the results are located after the first screenshot. The results continue much more until 300 seconds but as a result of the page limitations two screenshots are presented. In order to understand what specific NS2 acronyms which are of interest to us represent, a small table is provided to facilitate a better interpretation of the outcomes as in Table 5.

Table 5. Specific NS2 acronym interpretations

NS2 Result Acronyms	Interpretation
r	receiver
s	sender
-t	time
-Hs	source
-Hd	destination
-Ne	energy level
-Il	packet size
-Ii	sequence number

Now that the results of the simulation are completed and they are stored in a trace file, we intend to draw the graphs for demonstrating how the packets are flowing. In addition to this we target to show how the proposed IDS works and what is its specific impact on WiMAX network's performance. In order to process and sketch the obtained results an analyzer programming code has been written in Perl language to facilitate the investigation and analysis respectively. What the code actually does is the fact that from the result list it takes the time and the amount of bytes being transmitted. Then it sums up all the Il's which are all the packet sizes and further on divides the outcome of the summation by the covered time interval. The final result will be undoubtedly the speed. The written piece of code can be observed as follows:

```
open(LOG,$ARGV[0]);
@logs = <LOG>;
close(LOG);
$total_data = 0;
$last_speed = 0;
%data_per_second;
foreach(@logs){
        ($time,$packet) = $_ =~ m,\-t\s(\d*\.\d*).*\-Il\s(\d*),;
        if(exists($data_per_second{$time})){
                $data_per_second{$time} += $packet;
}else{
                $data_per_second{$time} = $packet;
}
}
$last_time = 0;
foreach(sort(keys(%data_per_second))){
        print $_.";".($data_per_second{$_}/(1024*($_-$last_time))."\n"
        $last_time = $_;
}
```

Therefore after processing the results with this Perl program we get this in Figure 33:

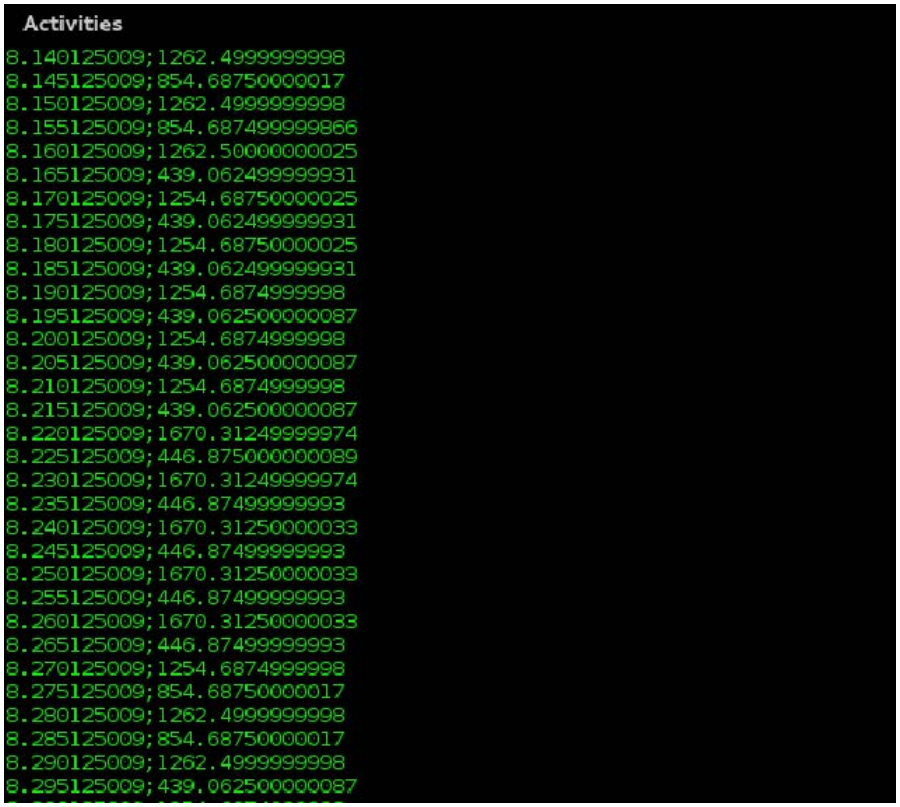


Figure 33. The screenshots from processed results formatted for CSV transfer →

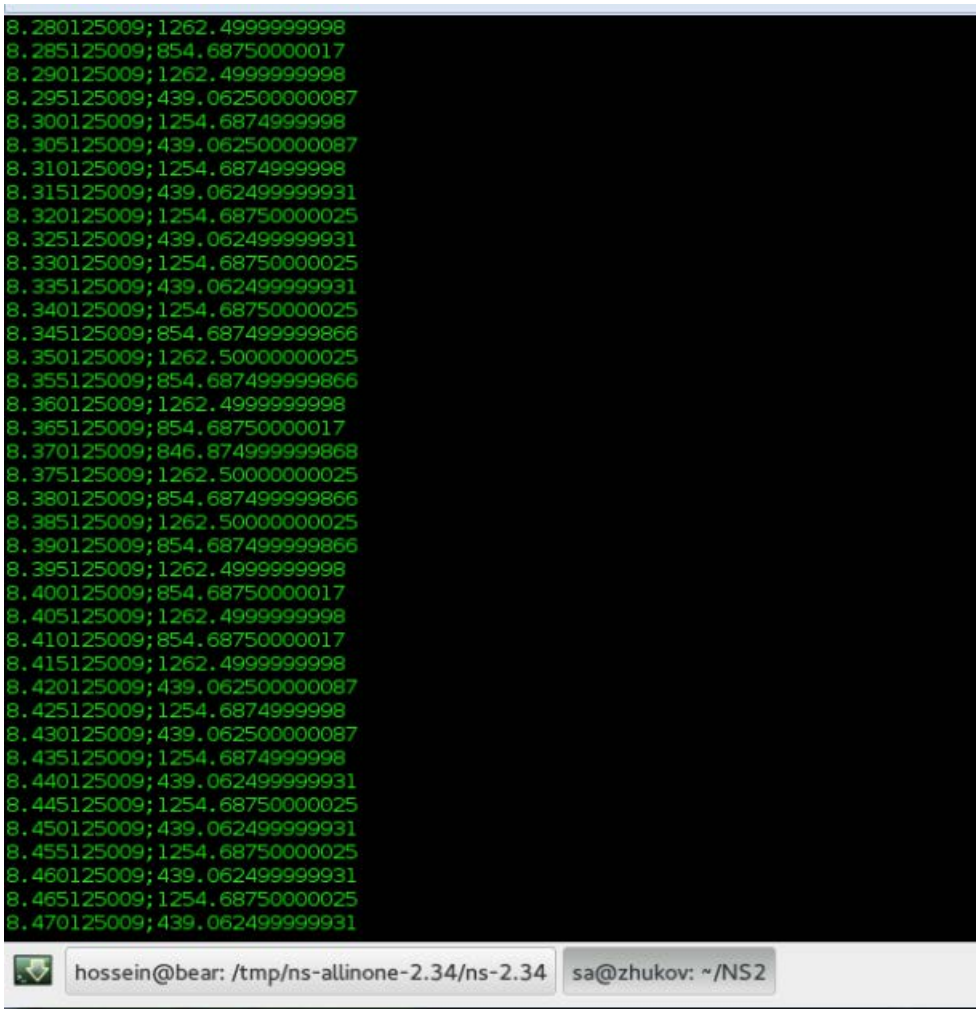


Figure 33. The screenshots from processed results formatted for CSV transfer

The CSV file format is structured like (x0; x1). As it can be observed the obtained results are put in CSV format to be able to transfer the resulted values there and then sketch the graphs for further evaluations and investigations. There will be totally six graphs. The first two graphs represent the WiMAX downlink having speed and time in their y and x axis respectively. There are two graphs because one represents the transmission speed having the proposed IDS and the other represents the downlink without having the IDS. Followed by these simulations there comes two graphs for the WiMAX uplink with the same specifications as just mentioned above. The final two graphs are dedicated to the simulation of the bandwidth so that the amount of packets replaced per time interval will be evaluated.

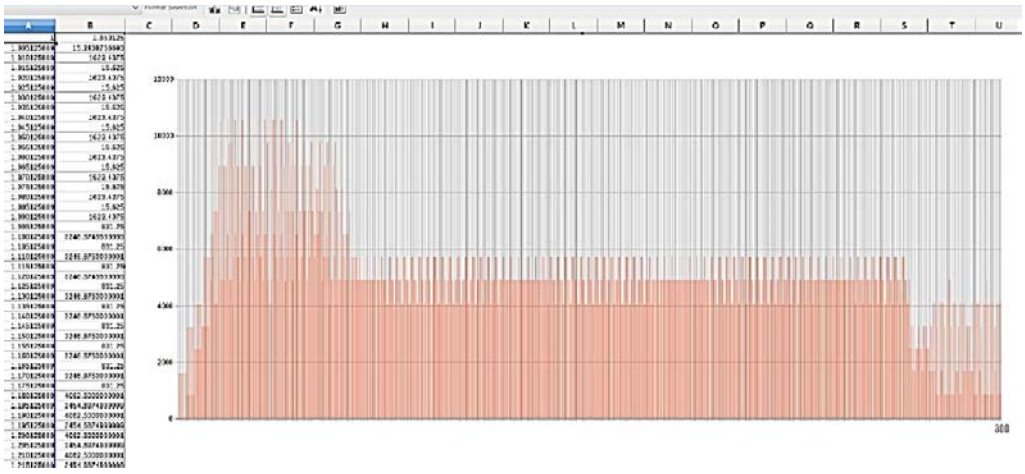


Figure 34. The simulation result in case of WiMAX downlink without IDS having programming bar calculations-part 1

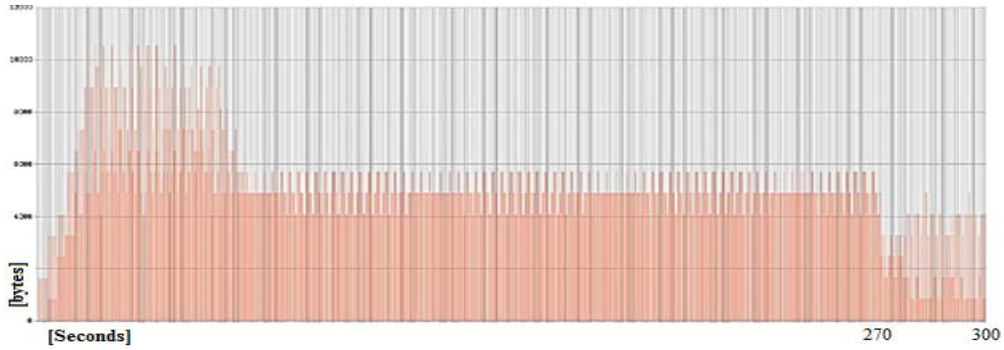


Figure 34. The simulation result in case of WiMAX downlink without IDS-part 2

In Figure 34 as it can be seen WiMAX downlink has been simulated in the IDS absence scenario. One can observe that the simulation starts with a visible transmission speed increase (normal for network simulations) and scores some peaks and following that the network becomes stable with relatively constant fluctuations until the simulation time ends. It is important to note that from 270th second because the simulation time is going to end the 50 connections, they start to close one by one and thus it is visible that there is a time interval until all connections stop completely.

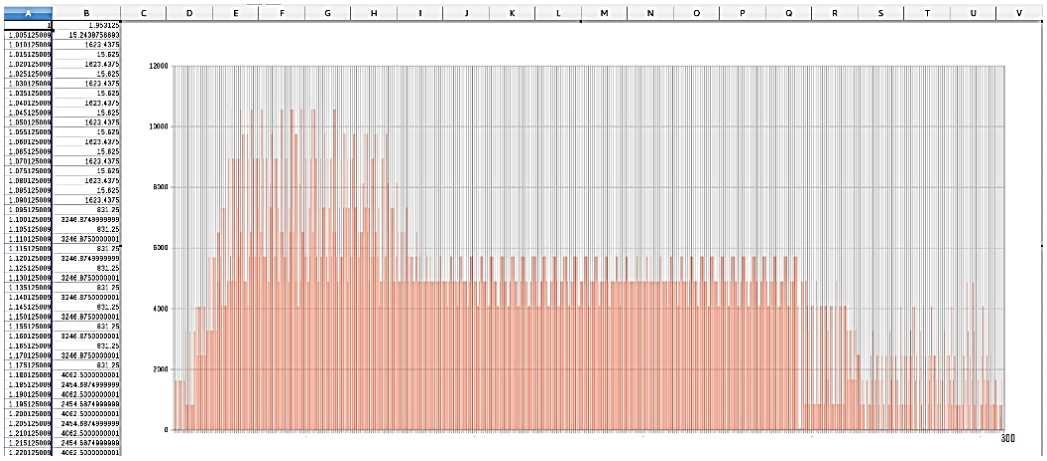


Figure 35. The simulation result in case of WiMAX downlink with IDS having programming bar calculations-part 1

Figure 35. The simulation result in case of WiMAX downlink with IDS-part 2

In Figure 35 as it can be agreed WiMAX downlink has been the subject for simulation but this time our proposed IDS has been utilized. One can see that the simulation begins with a tangible transmission speed increase (normal for network simulations) and then records several peaks and following that the network becomes stable with nearly constant fluctuations until the proposed IDS detects the threat and abnormality of sending 50 FTP requests and blocks them. The red arrow indicates the moment when the attack is stopped. It is critical to highlight that at 237th second the IDS blocks the DoS attack and thus it does not let the WiMAX resources get wasted by the SS's abnormal requests. It can be also mentioned that the proposed IDS in the case of WiMAX downlink blocks the attack 33 seconds earlier (compared with the downlink case without IDS) before the simulation time begins to end by closing the 50 connections one by one and thus it is visible that a specific amount of power has been saved here which will be calculated later on.

Figure 36. The simulation result in case of WiMAX uplink without IDS having programming bar calculations-part 1

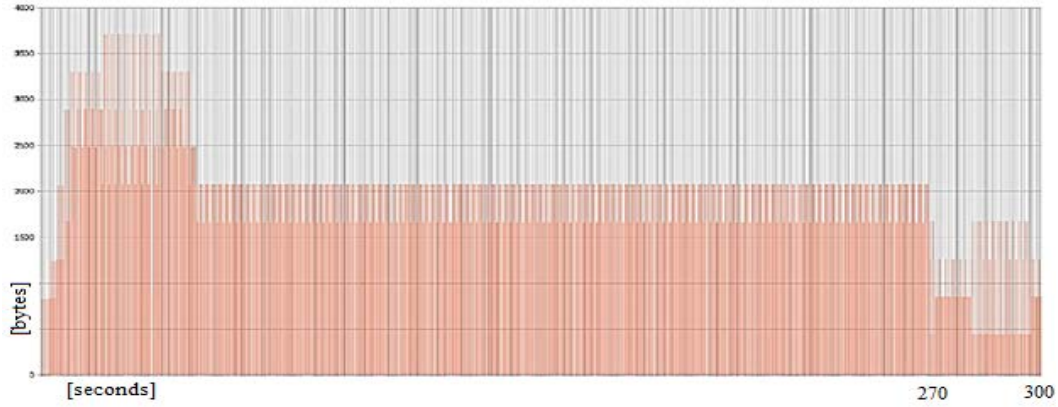


Figure 36. The simulation result in case of WiMAX uplink without IDS-part 2

In Figure 36 one can take a look at the WiMAX uplink that has been the subject for simulation in case when the IDS is not deployed. One can agree that the simulation begins with a considerable rate increase (normal for network simulations) and experiences numerous peaks and following that the network goes stable with constant fluctuations until the simulation time ends. It is essential to mention that from 270th second because the simulation time is going to end the 50 connections, they start to close one by one and thus it is visible that there is a time interval until all connections stop entirely.

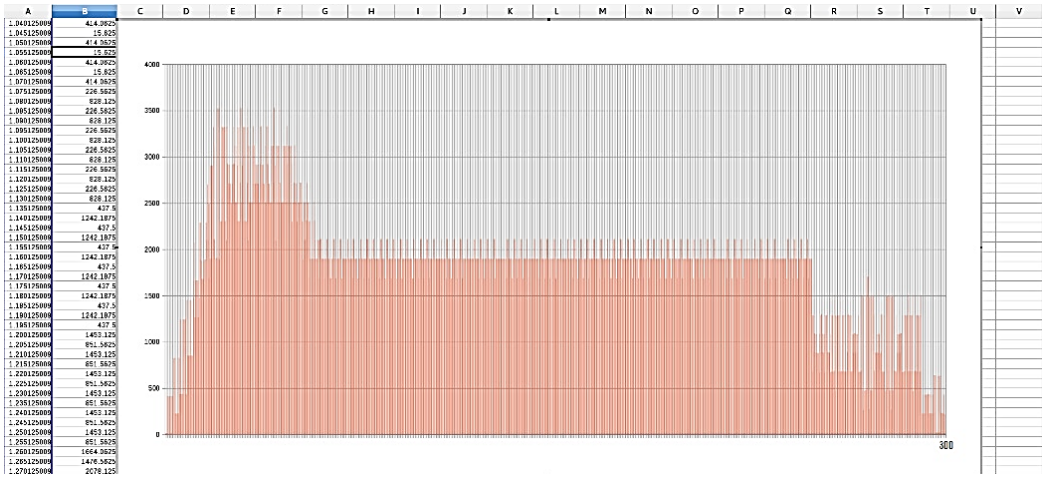


Figure 37. The simulation result in case of WiMAX uplink with IDS having programming bar calculations-part 1

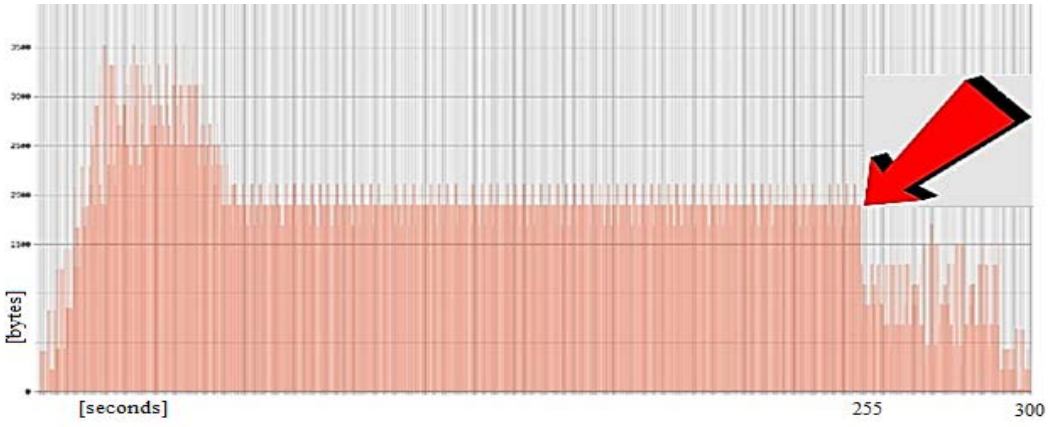


Figure 37. The simulation result in case of WiMAX uplink with IDS-part 2

In Figure 37 as it can be observed WiMAX uplink has been simulated by NS2 but this time our proposed IDS has been used. It is clear that the simulation starts with a considerable pace increase (normal for network simulations) and then has many peaks and following that the network becomes stable with relatively constant fluctuations until the proposed IDS detects the attack of 50 FTP requests and blocks it. The red arrow indicates the moment when the attack is stopped. It is critical to point out that at 255th second the IDS blocks the DoS attack and therefore it does not let the WiMAX resources get wasted by the SS's abnormal requests. It can be also explained that the proposed IDS in the case of WiMAX uplink blocks the attack 15 seconds earlier (compared with the uplink scenario without IDS) before the simulation time goes to end by closing the 50 connections one by one and thus it is clear that a specific amount of power has been saved here which will be calculated later on.

Now we try to measure the efficiency level and finalize the evaluation. According to the (K. Gomez et al. 2012), a reference power consumption model has been proved accountable for specific wireless access networks including WiMAX. Each one is separately discussed and investigated. Therefore if traffic is generated using the Iperf traffic generator and then inserted into the WiMAX network through the BS and power consumption amount is measured by the "Watts Up?" power meter, then one can refer to this graph and chart for meticulous calculations.

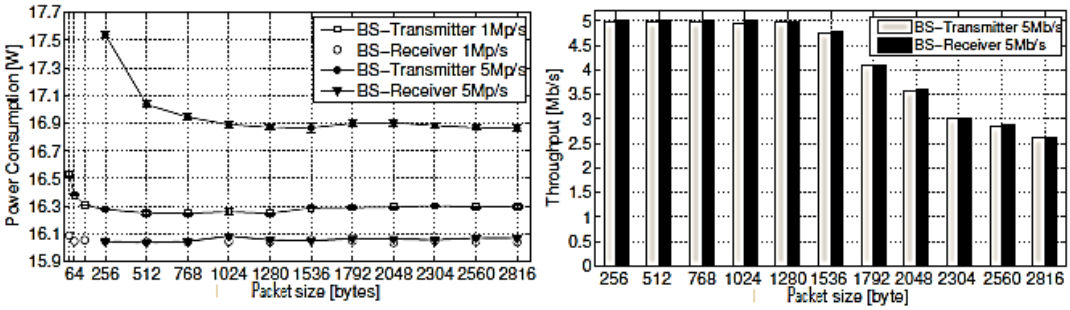


Figure 38. WiMAX power consumption and throughput per packet size (K. Gomez et al. 2012)

"Watts Up?" is a "plug load" meter that measures the amount of electricity used by whatever electrical appliance is plugged into it. The meter incorporates digital electronics to perform accurate power consumption measurements. Such measurements are then logged into the device's internal memory with a granularity of 0.1 W and a sampling period of 1 second. The "Watts Up?" meter is interconnected via its USB interface to the BS where a custom data logging software is deployed for extracting the power consumption samples. Here we start to explain and calculate the amount of the power saved and therefore the efficiency obtained.

If one looks at the power consumption graph in Figure 38, it can be read that each packet with the associated size of 2816 from a WiMAX receiver that has 5 Mbps, consumes 16 W to be received. The data related to the BS transmitter of 5 Mbps in WiMAX power consumption graph is exactly the WiMAX downlink. The above graph together with the chart tells us that each packet with its specific size takes specific power in Watts to be transmitted successfully. What we do is that we calculate the average size of packets in case of with IDS and without IDS and further on multiply it by the amount of Watts they need to be transmitted. After this step in order to compute the amount of saved power (power efficiency), we

subtract the total power consumption in case of without IDS from the total power consumption in case of IDS presence.

Therefore for WiMAX downlink we have:

For the case without IDS the total number of packets are 21892. Further on the average packet size is 2104.83 and one can observe that based on the graph, each packet has consumed 16.9 W thus in total 369974.8 W has been consumed.

For the case with IDS the total number of packets are 17721. Further on the average packet size is 1826.75 and one can observe that based on the graph, each packet has consumed 16.9 W thus in total 299484.9 W has been consumed.

369974.8 - 299484.9 = 70489.9 W Amount of saved power

Thus one can demonstrate that by doing a subtraction when it comes to the total consumption of without IDS and with IDS the amount of saved power and therefore efficiency obtained is calculated respectively.

Here we come to the WiMAX uplink so we have:

For the case without IDS the total number of packets are 18192. Further on the average packet size is 1039.08 and one can observe that based on the graph, each packet has consumed 16 W thus in total 291072 W has been consumed.

For the case with IDS the total number of packets are 14492. Further on the average packet size is 1049.86 and one can observe that based on the graph, each packet has consumed 16 W thus in total 231872 W has been consumed.

291072 - 231872= 59200 W Amount of saved power

Therefore one can show that by doing a subtraction when it comes to the total consumption of without IDS and with IDS the amount of saved power and therefore efficiency obtained is calculated relatively. One can draw a conclusion that the proposed IDS can bring about some power savings and thus it can make the WiMAX network more efficient especially when the network should deal with threats, attacks and abnormalities.

For sketching the bandwidth graphs with and without IDS we have to write another analyzer program in Perl because in this case we want to deal with the bandwidth and the amount of data that is being transferred. For this target the fol-

lowing bandwidth analyzer program has been written in Perl language which can be observed as follows:

```
open(LOG,$ARGV[0]);
@logs = <LOG>;
close(LOG);
$total_data = 0;
$last_speed = 0;
%data_per_second;
foreach(@logs){
        ($time,$packet) = $_ =~ m,\-t\s(\d*\.\d*).*\-Il\s(\d*),;
        if(exists($data_per_second{$time})){
                $data_per_second{$time} += $packet;
}else{
                $data_per_second{$time} = $packet;
}
}
foreach(sort(keys(%data_per_second))){
        print $_.";".$data_per_second{$_}."\n";
}
```

After processing the results and sketching the CSV file we get the following from the bandwidth graph in case of not having the proposed IDS as follows:

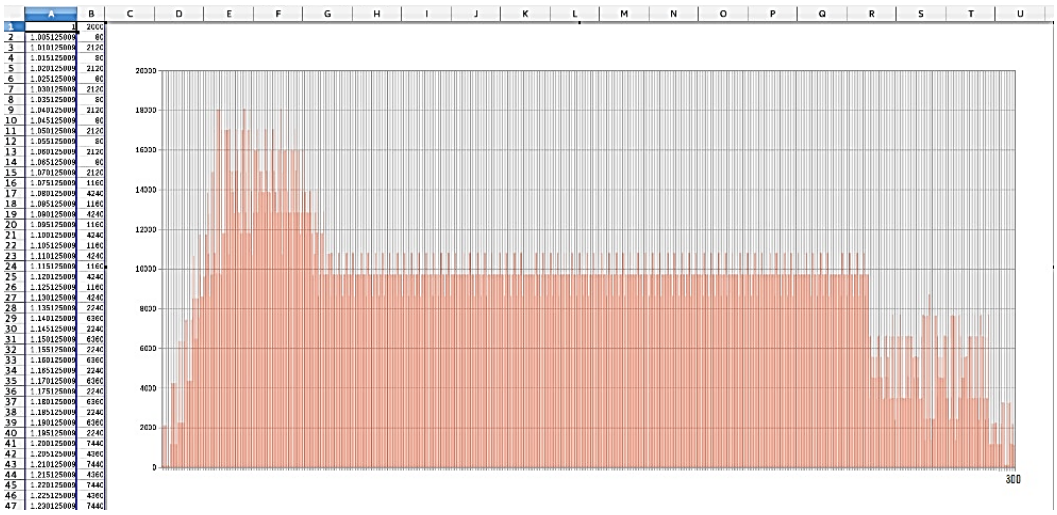


Figure 39. The simulation result in case of WiMAX bandwidth without IDS having programming bar calculations-part 1

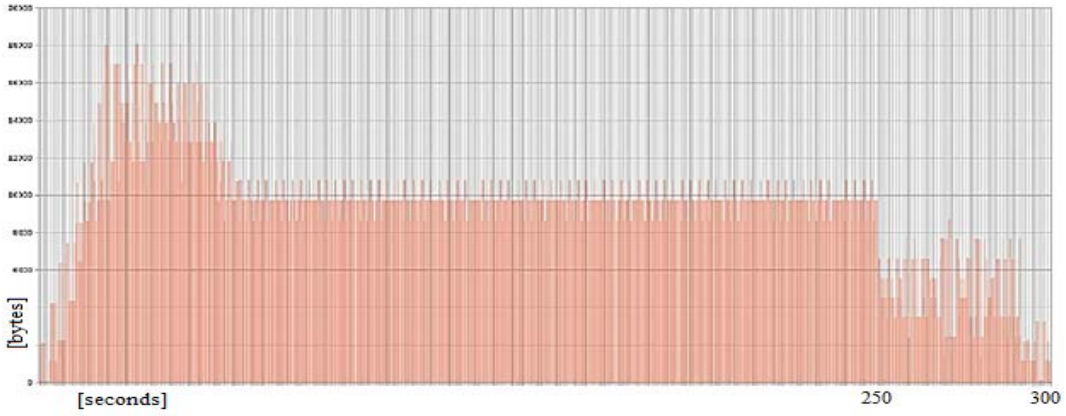


Figure 39. The simulation result in case of WiMAX bandwidth without IDS-part 2

In Figure 39 one can see that the WiMAX bandwidth has been the subject for simulation in case when the IDS is not deployed. One can interpret that the simulation begins with a considerable speed increase (normal for network simulations) and records several peaks and following that the network becomes stable with constant fluctuations until the simulation time ends. It is important to state that from 250th second because the simulation time is going to end the 50 connections, they start to close one by one and thus it can be viewed that there is a specific time interval until all connections stop altogether.

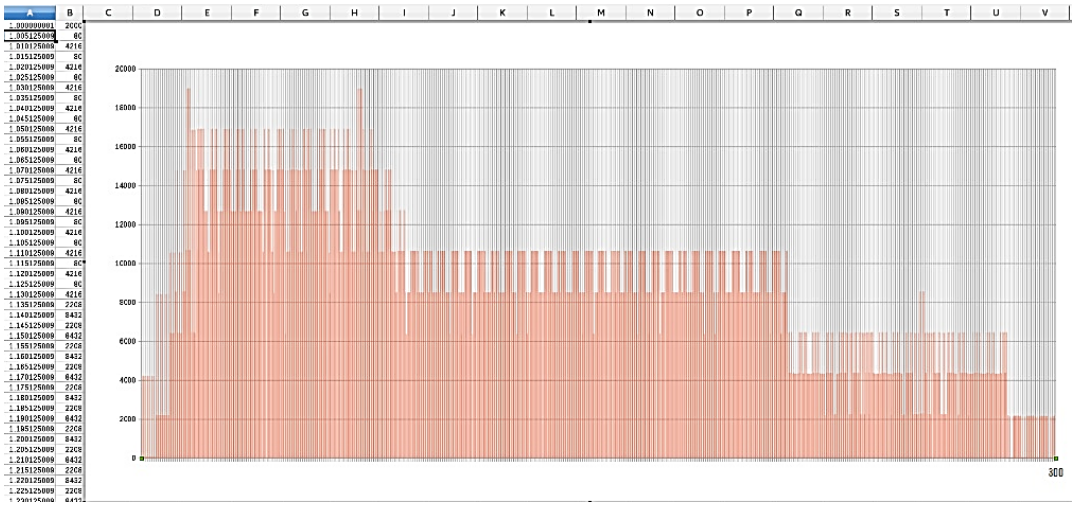


Figure 40. The simulation result in case of WiMAX bandwidth with IDS having programming bar calculations-part 1

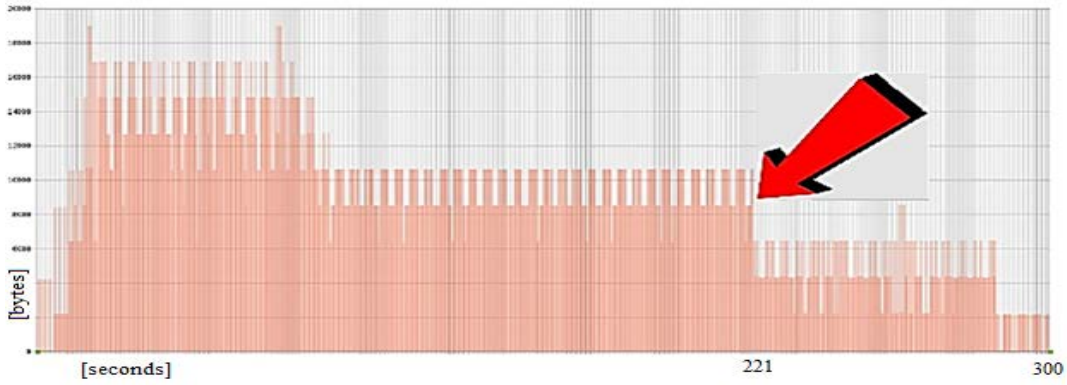


Figure 41. The simulation result in case of WiMAX bandwidth with IDS-part 2

In Figure 40 as it can be viewed WiMAX bandwidth has been simulated by NS2 but this time our proposed IDS has been utilized. It is understandable that the simulation starts with a considerable rate increase (normal for network simulations) and then has many peaks and following that the network goes stable with nearly constant fluctuations until the proposed IDS detects the attack of 50 FTP requests and blocks it. The red arrow indicates the moment when the attack is stopped. It is important to declare that at 221th second the IDS blocks the DoS attack and thus it does not permit the WiMAX resources get wasted by the SS's abnormal requests. It can be also explained that the proposed IDS in the case of WiMAX bandwidth blocks the attack 29 seconds earlier (compared with the bandwidth scenario without IDS) prior to when the simulation time goes to end by closing the 50 connections one by one and thus it is clear that a specific amount of power has been saved here.

6.2.4 Toshiba Consumption Analyzer Technical Simulations

WiMAX technology provides high-speed connection for internet and data transmission within a cell radius of as far as 50 km (P. Trimintzios et al. 2010). This itself describes the importance of power for transmission to remote distances. Even though IDS makes the WiMAX network become more secure, but considering the realities of WiMAX, in case our IDS would diminish the overall performance of the WiMAX network, then IDS would not be valuable from an evaluation perspective. The test conditions were two computers, one simulates the WiMAX network, the other executes IDS, and two computers have identical settings as follows: 3 GHz dual-core Intel Pentium CPU, 4 GB memory, hard drive speed is 7200 rls, operating system is Windows 2003. As it can be observed the reading and writing time with and without IDS are presented in Figure 41.

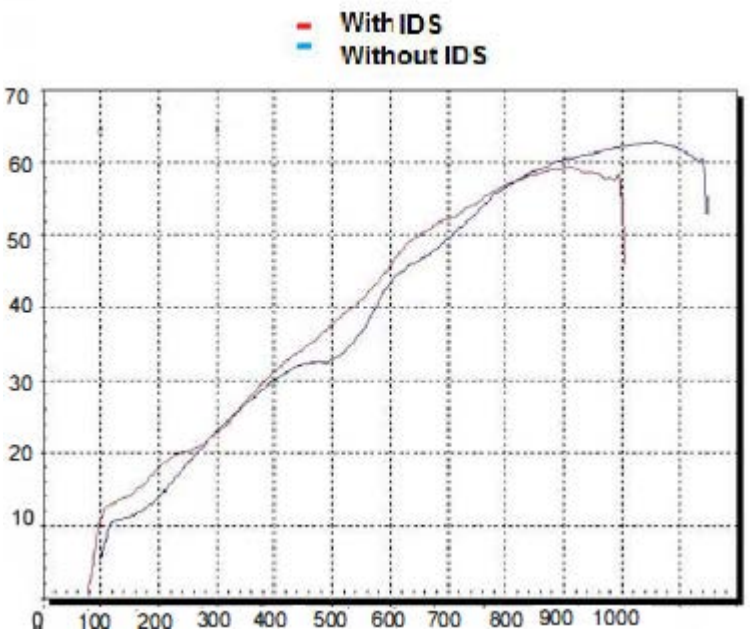


Figure 42. Reading and writing time with and without IDS

In Figure 41, the x-coordinate shows the data size, the unit is MB. On the other hand y-coordinate denotes the reading and writing time, and the unit is second. Figure 40 implies that the reading and writing time with IDS is only a little more than without IDS, the more size is fundamentally stable. The experimental result indicate that, in the case of improving the security of WiMAX network, a small decrease of disk reading and writing capability is negligible.

During the test procedures and once the power consumption of the system by Toshiba consumption analyzer were seen with the proposed IDS and without it, it has been interestingly found that the power consumption is slightly lower with IDS in comparison with the case without it. This result comes in normal network load. In addition to this, the VMware software has been utilized for the simulation of the two systems. It should be mentioned that by an investigation of fluctuations of the consumption one can observe that when it comes to normal circumstances in the network, the power consumption under the IDS mode is slightly better. This is the result of the application of numerous integrations performed during the design process which would lead to less utilization of power and more efficiency. Unlike Matlab, the Toshiba consumption analyzer does not provide the possibility to put both results in one plot. For the sake of having a better picture and a more accurate understanding the two results are put into one plot for analysis using the mapping technique. Thus if one draws a virtual line in between the two obtained

results and locate markers and points in peak and lowest values, then it can be clearly identified even with open eyes that the average value of the highest and lowest values are slightly upper in case of having no IDS in the network whereas in case of having the IDS this represents a lower values and therefore it implies having a lower consumption. Figure 42 represents the power consumption without and with the proposed IDS.

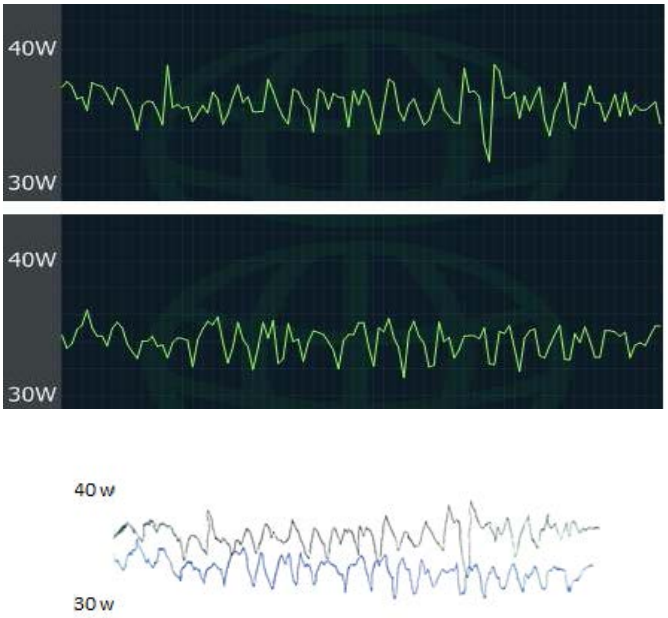


Figure 43. Power consumption of simulating system without and with IDS

6.2.5 Contribution to the Research Area

With the increasing demand for application of WiMAX, the related research on the security aspects of the new generation of mobile wireless networks will rise. As a result of the existing security problems of WiMAX network, intrusion detection system can be counted as an effective security countermeasure. It provides many advantages and plays an important role. This dissertation designs and proposes a WiMAX-based intrusion detection system by defining technical operations in seven units being: WiMAX security analysis unit, WiMAX attack database unit, detection unit, intrusion detection unit, backup and storage unit, system management unit and response unit. Besides bringing about more security to the WiMAX network, the final result leads to a less power consumption alternative as the outcome of the simulations carried out by NS2 and Toshiba Consumption Analyzer demonstrated and thus this proves the effectiveness and efficiency of the proposed IDS. For simulation model conformance verification of WiMAX designs and characteristics in this dissertation some two algorithms are utilized based on (S. I. Al-Akhras et al. 2013). Due to the fact that it is beyond the scope to explain the verification details, the algorithms are available in the appendix and for details of how it was carried out, the above research work should be referred.

7 CONCLUSIONS

7.1 General outcomes

Even the primary versions of WiMAX, were more secure than (Wireless Fidelity) WiFi. The most recent version of WiMAX, IEEE 802.16e came up and settled down the issues (J. G. Andrews et al. 2007). For fixing the security problems data integrity mechanisms, reciprocal two-way authentication, and AES-CCM were added to address the issues as efficient solutions.

Based on all security issues which were investigated in their relevant chapters, if one wants to provide an outline of the security issues, attacks and vulnerabilities including physical ones, they can be briefly explained as follows:

Physical layer attacks:

As mentioned previously, the security of 802.16 is designed at the layer 2 of the stack model, therefore the physical layer may be subject to the harms. As a result of the fact that there is always a threat to the radio networks, 802.16 is vulnerable when it comes to DoS and jamming. An intruder can utilize a well-configured radio station for launching jamming attacks.

This also existed in WiFi but the vulnerability and harm is much higher in Wi-MAX because of a larger scale coverage and thus affecting more users at a time. Through adding to the power of signals by using high gain transmission antennas or increasing the bandwidth utilizing spreading techniques one can fight against the jamming attack. What can be visibly sensed is that even the designers are not paying much attention to the physical threats and these threats are just on the paper.

MAC Layer attacks:

As discussed even though physical layer attacks are existing, they are not considered as important as attacks on the MAC layer of WiMAX. On the other hand, MAC layer attacks should be taken seriously because they can cause serious harms to clients and ISP’s. Thus some of these attacks can be mentioned as follows:

Replay attacks – as noted above, once WiMAX was having an authentication in one direction where base station authenticates the subscriber stations. This is why replay attacks happen because the subscriber station would be subject to harms. In

WiMAX, a well-situated intruder can locate between a base station and a number of subscriber station's and by setting a fake base station to impersonate as being the real base station.

Authentication Key (AK) - The AK suffers from many security flaws, First of all the generated keys are not random, therefore this itself questions the credibility of it. Now if the random number generator has bias problems the outcome would be a reduced key space for AKs that leads to compromised TEKs for subscriber station's connected to base stations.

In addition to this, the protocol defines a bilateral relation among a SS's MAC address and the key pair certified to deploy by that subscriber station. This will result to confusions and problems. Therefore in case an intruder can get the private key for a public machine, they can obtain the AK for future unauthorized access from that specific machine because knowing the private key, they can proceed with a successful authentication and thus gain access without being authorized. Traffic Encryption Keys (TEK) - TEKs are re-keyable. The space for rekeying is 2-bits wide, causing the TEKs to wrap every forth rekeying. This limited keying space and the use of sequence number instead of RNG make the protocol more vulnerable to replay attacks. The TEK also suffers from the lack of clear definition of 'randomness' that the AK suffers from (Mohammed El-Gammal, 2010). Data packets encryption - TEK has 56 bit DES keys which makes it less secure than AES protected packets. Moreover, MAC header of the packets are not encrypted for routing to happen smoother. When it comes to TEK encryption, data packets remain without protection. Finally X.509 does not provide any solution for handling the revocation of certificate if private key falls in wrong hands.

This dissertation has worked on past and present security problems of IEEE 802.16 and listed and explained all of them in a classified way. Efforts have been made to explain the security threat primarily and then separately provide the solution afterwards. Further on several investigations and analysis of the threats and security weaknesses have been carried out respectively and the detailed descriptions can be followed in chapter four. In addition to this security issues of the LTE have been addressed and up-to-dated countermeasures and respective mitigation techniques have been provided. Some comparisons between WiMAX and other alternative wireless access networks such as LTE and WiFi have been performed as well. The dissertation has provided an alternative IDS based on WiMAX for detection and prevention against security vulnerabilities within WiMAX that can be referred to in Figure 15 and Figure 16. It has been tried to demonstrate via NS2/Toshiba simulations, how it works and what advantages it can offer like being more power efficient than the previous available alternative.

Moreover, this dissertation worked on the general security threats when it comes to VoIP together with WiMAX specific security issues while VoIP services are being offered under the WiMAX framework. The classification and modeling provided can be observed in Figure 18.

7.2 Results of This Dissertation

To be brief, WiMAX, like other technologies does have many flaws, security breaches and vulnerabilities. This technology can become even more widespread if its security would be warrantied and meticulous measures would be taken care of. This dissertation carried out a security centric analysis listing the security basics of WiMAX and LTE together with a scientific comparison with other wireless access technologies like WiFi. In this process the architecture of WiMAX, security of the standard, its security elements together with the respective attacks and threats were covered, modeled and classified. This dissertation proposed an alternative classification model and analysis of WiMAX security attacks and as WiMAX is counted among next generation networks (4G) and many services are provided under its framework, VoIP service general threats and WiMAX specific security issues together with means of secure communication are modeled and classified respectively. As a result of the fact that maintaining the security and increasing the number of users affects the performance of a wireless access network such as WiMAX, this degradation was described by the Kiyotaki-Moore model. In addition to this, as a countermeasure to the threats, a power efficient WiMAX-based intrusion detection system was proposed. The NS2 simulations together with Toshiba Consumption Analyzer simulations were carried out in scenarios including WiMAX downlink, WiMAX uplink and WiMAX bandwidth. In each specific case the outcomes were compared when IDS were deployed and when it were not. Indeed some power savings were obtained. Then the efficiency related calculations were performed to demonstrate that this proposed IDS can make a difference.

7.3 The usage of the Results of this Dissertation

The results of this dissertation can be deployed for obtaining more secure systems that will fulfill the criteria’s set for a wireless access network including WiMAX. This has been done by classifying and modeling the security attacks and threats caused by bugs and breaches in the wireless access systems. Therefore two modellings and classifications have been carried out in case of attacks in WiMAX and security threats while VoIP services are provided under the WiMAX framework.

The required security countermeasures and ways of mitigation are mentioned where possible. This dissertation will also increase the awareness of the impact of the security to the performance and trust of the users and hopefully results in more reliable systems in the future. With the proposed IDS, it is possible to check the packets with respect to format and essential criteria's to detect and mitigate the attacks in early stages. Therefore, it is possible to investigate some likely scenarios when security attacks escalate. In this case, one can test the proposed IDS system to stop the intrusion.

This dissertation has also a significant impact on research methodology in particular implying that especially security has been the factor which has been under scrutiny. The proposed IDS can be implemented and even go further for industrialization. The IDS can detect early signs of security threats. Analyze it and take decisions. Also the attack behaviors can be stored so that it would be prevented in case it happens again. This provides a mechanism to protect the system against intruders having bad intentions and motivations.

7.4 Future Work

As it was observed throughout the dissertation, the major concentration was devoted to security in WiMAX framework. Having considered all the technical points mentioned earlier, Mobile WiMAX, the ultimate standard for WiMAX already provides remarkable security enhancements over IEEE 802.16. It basically deploys more reliable encryption techniques and holds an extra secure key management protocol. In addition to this, it has a novel authentication technique that is according to Extensible Authentication protocol (EAP). However there are still several security breaches to be addressed. A serious attention should be paid to authentication and authorization because they are the bedrock of security when it comes to wireless technology.

Therefore future work should deal with authentication and authorization of IEEE 802.16e more than other factors. The following research questions can be ideally addressed in future studies:

1) What are the major authentication and authorization features in Mobile WiMAX?

2) Which are the existing security breaches threatening the authentication and authorization in Mobile WiMAX?

3) What are the comprehensive security solutions to address the issues in such a way that the efficiency would also be preserved?

4) What measures should be taken to enhance the level of security and in the same time maintain the integrity and reliability?

References

Abdo J., Chaouchi H., Aoude M., ”Ensured Confidentiality Authentication and Key Agreement Pro-tocol for EPS,” Proc. Broadband Networks and Fast Internet (RELABIRA 2012), May 2012, pp.73-77.

Abid M., Song S., Moustafa H., Afifi H., ”Efficient Identity-based Authentication for IMS based Services Access,” Proc. 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM ’09), 2009, pp. 260-266.

Ahmadzadegan M. Hossein, Elmusrati M. “Dual Security Categorization of Threats in WiMAX” IEEE Latin America Transaction Journal, 2013 (Submitted, Paper ID 1850).

Ahmadzadegan M. Hossein, Elmusrati M. “Hybrid Security Classification Approach to Attacks in WiMAX” IEEE International Conference on Signal Processing, Computing and Control (ISPCC), Shimla, India, 2013.

Ahmadzadegan M. Hossein, Elmusrati M. “Kiyotaki-Moore Approach to Performance Devolution in Mobile WiMAX” IEEE 5th International Congress on Ultra-Modern Telecommunications and Con-trol Systems (ICUMT), Almaty, Kazakhstan, 2013.

Ahmadzadegan M. Hossein, Elmusrati M. “WiMAX-Based Energy Efficient Intrusion Detection System” IEEE International Conference on Robotics, Biomimetics, & Intelligent Computational Systems (ROBIONETICS), Yogiakarta, Indonesia, 2013.

Ahmadzadegan M. Hossein, Elmusrati M., Mohammadi H., ("Secure Communication and VoIP Threats in Next Generation Networks") International Journal of Computer and Communication Engi-neering vol. 2, no. 5, pp. 630-634, 2013.

Ahmadzadegan M. Hossein, Elmusrati M., Virrankoski R., Antila E. “Security Centric Comparative Study of WiMAX and LTE” The IEEE Vehicular Technology Society, Asia Pacific Wireless Com-munications Symposium (APWCS), Seoul, South Korea, 2013.

Ahson S. A. , Ilyase M., “Security Issues of VoIP, VoIP Handbook”, CRC Press Taylor & Francis Group, 2009.

Ailen-Ubhi S. O., “WiMAX Link Performance Analysis for Wireless Automation Applications” Uni-versity of Vaasa Press, 2012.

Al- Shidhani A. A., Leung V.C.M., ”Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers,” IEEE Trans. Dependable Secure Comput., Vol.8, No.5, Septmber-Octomber 2011, pp.699-713.

Al-Akhras S. I., Tahar S., Nicolescu G., Langevin M., Paulin P.,"On the Verification of a WiMAX Design using Symbolic Simulations", Concordia University Research Project, 2013.

Altaf A., Javed M.Y. and Ahmed A. ,'Security Enhancements for Privacy and Key Management Pro-tocol in IEEE 802.16e-2005', in Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. 2008. Phuket, Thailand.

Andrews J. G., Ghosh A., Muhamed R., "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", 2007.

Bajgan S. R., Pooyan M., Khalilzadeh A., Abdollahi R., "Security in link layer of WiMAX net-works", in World Congress on Science, Engineering and Technology. 2008. Bangkok, Thailand.

Barbeau M., "WiMax/802.16 Threat Analysis", in 1st ACM international workshop on Quality of service & security in wireless and mobile networks 2005: Montreal, Quebec, Canada

Barbeau M., "WiMax/802.16 Threat Analysis", Q2SWinet'05, October 13, Montreal, Quebec, Cana-da, 2005.

Barber R., "Hackers Profiled - Who Are They and What Their Motivations Are". Computer Fraud & Security, 2001(2):14{17, February 2001}.

Basak C., Vannithamby R., H. L. Hyunjeong, Koc A. T. "MAC-PDU Size Optimization for OFDMA Modulated Wireless Relay Networks". Proceedings of the IEEE Global Telecommunications Confer-ence, ISBN: 978-1-4244-2324-8, December 2008, Pages 1-6.

Blake R. "Hackers in the Mist". www.e®.org/Net culture/Hackers/hackers in the mist.article, 1994.

Bogineni, K., Ludwig R., Mogensen P., Nandlall V., Vucetic V., Ecklund B. C., Marks R.B., Stan-wood K.L., Wang S., IEEE Standard 802.16: "A technical overview of the wireless MAN air inter-face for broadband wireless access", IEEE Communications Magazine, Vol. 40, No. 6, pp. 98–107, June 2002.

Bouabidi I., Daly I., Zarai F., "Secure Handoff Protocol in 3GPP LTE Networks," Proc. Third Inter-national Conference on Communications and Networking (ComNet), March 2012, pp.1-6.

Butti L., "Wimax: Security Analysis and Experience Return", Network Security Senior Expert, Or-ange Division R&D, France Telecom, 2007.

CableLabs®, "Advanced Modem Technology Proposals". Retrieved 16 December 2013

Cao J., Li H., Ma M., Zhang Y., Lai C., ”A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks”, Computer Networks, Vol. 56, No. 8, May 2012, pp. 2119-2131.

Cao J., Ma M., Li H., ”A Group-based Authentication and Key Agreement for MTC in LTE Net-works”, Proc. IEEE GLOBECOM 2012, Dec. 2012, accepted for publication.

Cao J., Ma M., Li H., ”An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks”, IEEE Trans. Wireless Commun., Vol. 11, No. 10, Oct. 2012, pp 3644-3650.

Cao J., Ma M., Li H., Zhang Y., Luo Z., “A Survey on Security Aspects for LTE Networks”, IEEE Communications Surveys & Tutorials, Vol. 16, No. 1, First Quarter, 2014.

Chogan S. R., Heidarzadeh M., Yeganeh H., Mohammadi H., “Survey of Vulnerability and VoIP Threats” International Review on Computers and Software, 2012.

Club de la securite des systemes d'information francais (CLUSIF) Methods Commission. Mehari V3 Concepts and Mechanisms. www.clusif.asso.fr/en/clusif/present, 2002.

El-Gammal M.,”Overview of the WiMAX Security”, Washington, 2010.

El-rahman T. F., “Security Technologies in Wireless Networks”. 2005; available from: www.aims.ac.za/ resources/archive/2004/tayseer.ps.

Eren E., ‘WiMAX Security Architecture – Analysis and Assessment’, in 4th IEEE Workshop on In-telligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 2007. Dortmund, Germany.

Ergen M. “Mobile Broadband: Including WiMAX and LTE. Springer Science & Business Media, LLC, 2009. ISBN: 978-0-387-68189-4.

Ericsson, S3-060705, “On security algorithm selection for LTE”, 3GPP TSG SAWG3 Security, SA3#45, Ashburn, USA, 31 October - 3 November, 2006.

Financial Times Information. Mobile cloning, March 2005.

Franklin J.V. ,Paramasivam K., ”Enhanced Authentication Protocol for Improving Security in 3GPP LTE Networks,” Proc. International Conference on Information and Network Technology (ICINT 2011), 2011.

Fu J., Wu C., Chen J., Fan R., and Ping L., ”Lightweight Efficient and Feasible IP Multimedia Sub-system Authentication,” Proc. Networking and Information Technology (ICNIT), June 2010, pp.139-144.

Golaup A., Mustapha M., and Patanapongpibul L. B. , ”Femtocell Access Control Strategy in UMTS and LTE,” IEEE Commun. Mag., Vol.47, No.9, Septmber 2009, pp.117-123.

Gomez K., Boru D., Riggio R., Rashid T., Miorandi D., Granelli F., “Measurement-based Modelling of Power Consumption of Wireless Access Network Gateways”, Proceedings of IEEE Greencom 2011 and IEEE computer Networks Journal, 2012.

Goodman D. J.,"3G Cellular Standards and Patents". IEEE Wireless com. Polytechnic Institute of New York University, 2011.

Gu W., Kartalopoulos S., Verma P., "Wen Gu, Stamatios V. Kartalopoulos, Pramode K. Verma," WSEAS Transactions on Communications,9(2): lIS-126

Habib M., Ahmad M., "A Review of Some Security Aspects of WiMAX and Converged Network," Proceedings of the 2010 Second International Conference on Communication Software and Net-works, 2010, pp. 372-376.

Haibo T., Liaojun P., Yumin W., “Key management protocol of the IEEE 802.16e’ Wuhan University Journal of Natural Sciences”, 2007. 12(1): 59–62.

Hamalainen P., Hannikainen M., “Configurable Hardware Implementation Of Triple DES Encryption Algorithm For Wireless Local Area Network”, Tampere University of Technology, Finland, 2001.

Hao F., Ryan P.,”J-PAKE: Authenticated Key Exchange without PKI,” Trans. Computational Sci-ence XI, LNCS, Vol. 6480, 2010, pp.192-206.

Hardjono T., Dondeti L.R., “Security in Wireless LANs and MANs”. 2005: Artech House Publishers.

Hossain M., “Analysis and assessment of the security issues of IEEE 802.16”, Belkinge Institute of Technology Press, Sweden, 2008.

Huang C.-T., Chang J.M., “Responding to Security Issues in WiMAX Networks”, IT Professional, 2008. 10(5): 15–21.

Hur J., Shim H., Kim P., Yoon H. and Song N.-O. ,“Security Considerations for Handover Schemes in Mobile WiMAX Networks”, in IEEE Wireless Communications and Networking Conference. 2008.

Husso M. J., ‘Performance Analysis of a WiMAX System under Jamming’, in Department of Electri-cal and Communications Engineering. 2006, Helsinki university of technology.

IEEE 802.16 Working Group, Amendment to IEEE Standard for Local and Metropolitan Area Net-works, “Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layer for Combined

Fixed and Mobile Operation in Licensed Bands", IEEE Std. 802.16e- 2005, December 2005.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", 1 October, 2004.

IEEE C802.16-e05/278, "Clarification of GKEK-related Parameters for the MBRA", Broadband Wireless Access Working Group, http://ieee802.org/16; Jun. 8, 2005, 9 pages.

IEEE Std 802.16a (Amendment to IEEE Std 802.162001), "IEEE Standard for Local and metropoli-tan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 211 GHz", January 2003

Iperf Network Traffic Generator: http://iperf.sourceforge.net/

ITU, "Estimated spectrum bandwidth requirements for the future development of IMT-2000 and IMT-Advanced," International Telecommunications Union (ITU) ITU-R Working Party 8F Report M.2078, May 2006 (available at: http://www.itu.int/publ/R-REP-M.2078/en).

Johnston D. and Walker J., "Overview of IEEE 802.16 Security", IEEE Computer Society, 2004.

Karen S., Tibbs C., Sexton M.,"Guide to Securing WiMAX Wireless Communications Recommenda-tions of the National Institute of Standards and Technology", NIST Special Publication 800- 127, Gaithersburg, MD, 2010, NIST.

Keromytis A. D., "Voice over IP: Risks, Threat and Vulnerabilities." In Proceeding of Cyber Infra-structure Protection (CIP) conference, June 2009.

Kesterson H. L., "Digital Signature-Whom do you trust?" Bull HN Worldwide Information Systems Inc, Phoenix, Arizona 85029, 1997.

Kharif O.,"Paving the Airwaves for Wi-Fi". Bloomberg Business week, 2003.

Kien G. M., "Entity Authentication and Personal Privacy in Future Cellular Systems," River Publish-er, Oct. 2009.

Kiyotaki N., Moore J. "Credit Cycles", Journal of Political Economy, 1997, vol. 105, no. 2.

Kolias C., Kambourakis G., Gritzalis S., "IEEE Communications Surveys & Tutorials", 2013.

Koon T., "Phishing and Spamming via IM (SPIM)". Internet Storm Center. http://isc.sans.org/diary.php?storyid=1905. Retrieved December 5, 2006.

Krichene N., Boudriga N., ”Securing Roaming and Vertical Handover in Fourth Generation Net-works,” Proc. Network and System Security (NSS ’09), October 2009, pp.225-231.

Lai Y. C., Chen Y. H., “Designing and Implementing an IEEE 802.16 Network Simulator for Per-formance Evaluation of Bandwidth Allocation Algorithms”, In proceedings of 11th IEEE International Conference on High Performance Computing and Communications, Taiwan, 2009.

LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. Local and metropolitan area networks – Part 16: Air interface for fixed broadband wireless access systems. IEEE Standard 802.16-2004, 2004. (Revision of IEEE Std 802.16-2001).

Lehr W. H., Chapin J. M., “On the Convergence of Wired and Wireless Access Network Architec-tures”, Massachusetts Institute of Technology Press, 2009-2010.

Li H., Fan G.B., Qiu J.G., Lin X.K., “GKDA: A Group-Based Key Distribution Algorithm for Wi-MAX MBS Security”, Lecture Notes in Computer Science, 2006. 4261: 310–18.

Li X., Wang Y., ”Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network,” Proc. Wireless Communications, Networking and Mobile Computing (WiCOM), Septmber 2011, pp.1-4.

Lin Y., Chang M., Hsu M., Wu L., ”One-pass GPRS and IMS Authentication Procedure for UMTS,” IEEE J. Sel. Areas Commun., Vol.23, No.6, June 2005, pp. 1233- 1239.

Liu F., Lu L., “A WPKI-based Security Mechanism for IEEE 802.16e”, IEEE Communications Soci-ety, Wuhan University, China 2006

Long X., Joshi J., ”Enhanced One-Pass IP Multimedia Subsystem Authentication Protocol for UMTS,” Proc. Communications (ICC), May 2010, pp.1-6.

Lu C-C., “Integrated design of AES (Advanced Encryption Standard) Encrypter and Decrypter”, IEEE International Conference on Application-Specific Systems, Architectures and Processors, Tai-wan, 2002.

Lu K., Qian Y., University of Puerto Rico, Hsiao-Hwa Chen, National Sun Yat-Sen University. “A Secure and Service-Oriented Network Control Framework for WiMax Networks”, May 2007.

Lu K.; Qian Y., Chen H-H., “Wireless Broadband Access: WiMAX and Beyond - A Secure and Ser-vice-Oriented Network Control Framework for WiMAX Networks”, IEEE Communications Maga-zine, May 2007

Marks R. B., “IEEE Standard 802.16 for Global Broadband Wireless Access,” ITU Telecom World 2003, Session: “The future of wireless” Geneva, Switzerland. mber=4482831 978-0-7695-3096-3/08 $25.00 © 2008 IEEE DOI 10.1109/WAINA.2008.190

Meyerstein M., Cha I., Shah Y., ”Security Aspects of Smart Cards vs. Embedded Security in Ma-chine-to-Machine (M2M) Advanced Mobile Network Applications”, Security and Privacy in Mobile Information and Communication Systems, Vol. 17, 2009, pp. 214-225.

Michelle D., "New Specs Deepen LTE Voice Dilemma," Unstrung News Analysis, July 7, 2009. Available online at http://www.unstrung.com/document.asp?doc_id=178915).

Nasreldin M., Asian H., El-Hennawy M., El-Hennawy A., “WiMAX Security”, IEEE 22nd Interna-tional Conference on Advanced Information Networking and Applications - Workshops, 2008. AINAW, Okinawa, 2008.

Ni Q., Hu L., Vinel A., Xiao Y. M., “Performance analysis of contention based bandwidth request mechanisms in WiMAX networks”, Hadjinicolaou Systems Journal, IEEE 4 (4), 477-486, 2012.

NS2 Network Simulator: http://www.isi.edu/nsnam/ns/

Ntantogian C., Xenakis C.,Stavrakakis I., ”Efficient Authentication for Users Autonomy in Next Generation All-IP Networks,” Proc. Bio- Inspired Models of Network, Information and Computing Systems, December 2007, pp.295-300.

Nuaymi L., “WiMAX Technology for Broadband Wireless Access”, John Wiley & Son Ltd, 2007.

Otto T., “Extensible Network Access Authentication”. 2006, University of Lubeck.

Overview of Wireless Communications. Cambridge.org. Retrieved 8 February 2008.

Pang D., Tian L., Hu J.L., Zhou J.H., Shi J.L., “Overview and Analysis of IEEE 802.16e Security”, 2007;

Park P., “Voice over IP security”, Cisco Press, 2009.

Poisel R. A., Modern Communications Jamming Principles and Techniques. 2003: Artech House Publishers

Power Measurements and Power Calculations of 802.16 WiMAX, Application Note, 1EF60, Rhode&Schwarz.

Rajavelsamy R., Choi S., ”Security Aspects of Inter-access System Mobility between 3GPP and Non-3GPP networks,” Proc. Communication Systems Software and Middleware and Workshops (COMSWARE), January 2008, pp.209-213.

Ramle R. B., Ekhsan H. B. M., Hamid J.N.B., ”Investigating the Distance Effect on Performance Degradation of Mobile WiMAX”, International Conference on Science and Social Research (CSSR), 2010.

Ramos J. F., Serrano A. S., “VoIP over WiMAX”, Sapienza Universita Di Roma, 2011.

Ransome J. F., CISM, CISSP, “VoIP security”, Elsevier Digital Press, 2005.

Rekhis S., Boudriga N., “WiMAX Security and Quality of Service”, John Wiley & Sons Ltd, 2010.

Saedy M., Mojtahed V., ”Ad Hoc M2M Communications and Security based on 4G Cellular Sys-tem,” Proc. Wireless Telecommunications Symposium (WTS), April 2011, pp.1-5.

Saedy M., Mojtahed, V. ”Machine-to-Machine Communication and Security Solution in Cellular Systems,” International Journal of Interdisciplinary Telecommunications and Networking (IJITN), Vol. 3, No. 2, 2011, pp. 66-75.

Sansurooah K., “An Assessment of Threats of the Physical and MAC Address Layers in Wi-MAX/802.16”

Schifreen R., “What Motivates a Hacker?” Network Security, 1994(8):17{19, August 1994.

Sharma G., Vidhate A., and Devane S., ”Improved One-pass IMS Authentication in UMTS,” Proc. Communication Software and Networks (ICCSN), May 2011, pp.244-248.

Sharma M.J., Leung V.C.M., ”Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks,” Proc. Computer Communications Workshops (INFOCOM WKSHPS), April 2011, pp.1000-1005. Magazine, vol. 47, no. 2, February 2009.

Shi Z., Ji Z., Gao Z., Huang L., ”Layered Security Approach in LTE and Simulation,” Proc. (ASID 2009), August 2009, pp.171-173.

Shon T., Koo B., Park J., Chang H., "Novel approaches to enhance mobile WiMAX security," EUR-ASIP Journal on Wireless Communications and Networking, 2010,12(2): 1-13.

Sisalem D.,“SIP Security”, John Wiley and Sons Ltd, 2009.

Smith C., Collins D.. "3G Wireless Networks", page 136. 2000.

SNORT. Network intrusion detection system. http://www.snort.org/.

Stubblefield A., Ioannidis I., and Rubin A., “Using the Fluhrer, Mantin and Shamir Attack to Break WEP”, Proceedings of the 2002 Network and Distributed Systems Security Symposium, 17{22, 2002}.

Tariq U., Jilani U.N., Siddiqui T.A., “Analysis on Fixed and Mobile WiMAX”. 2007, Blekinge Insti-tute of Technology.

Tracy W., "How Municipal WiFi Works". computer.howstuffworks.com, 2008.

Trimintzios P., Georgiou G., "WiFi and WiMAX secure deployments," Journal of Computer Systems, Networks, and Communications, 2010, 9(1): 1-28.

Tutorials Point, “WiMAX - Salient Features”, Robust security, 2009.

Urien P., Pujolle G., “Security and Privacy for the Next Wireless Generation’ International Journal of Network Management”, 2008. 8(2): 129–45.

Vannithamby R., Srinivasan R. “WiMAX Evolution: Emerging Technologies and Applications”, Wiley Online Library, Chapter 13, 2009.

Vinel A., Staehle Ni, D., Turlikov A., “Capacity analysis of reservation-based random access for broadband wireless access networks”, Selected Areas in Communications, IEEE Journal on 27 (2), 172-181, 2011.

Vintila C., Patriciu V., Bica I., ”Security Analysis of LTE Access Network”, Proc. The Tenth Interna-tional Conference on Networks (ICN 2011), January 2011, pp. 29-34.

VoIP Security Alliance, “VoIP Security and Privacy Threat Taxonomy, version 1.0,”2006.

Wang C-L,”NCTUns Simulation Tool for WiMAX IEEE 71st Vehicular Technology Conferenc, Taipei, Taiwan. May 2010.

Wang D. H, J., Zheng Y., ”User Authentication Scheme based on Self-certified Public-key for Next Generation Wireless Network,” Proc. Biometrics and Security Technologies (ISBAST 2008), April 2008, pp.1-8.

Wattanachai S., “Security Architecture of the IEEE 802.16 Standard for Mesh Networks,” Depart-ment of Computer and Systems Sciences Stockholm University/Royal Institute of Technology, 2006.

Wattsup Power Consumption Meter: http://www.wattsupmeters.com/

WiMAX End-to-End Network Systems Architecture - 3GPP/ WiMAX Interworking, Release 1; Wi-MAX Forum, 2006

WiMAX Forum. WiMAX Forum® Network Architecture – Architecture Tenets, Reference Model and Reference Points Part 1 - Release 1.5, September 2009

Xu S., 'Security Protocols in WirelessMAN', in College of Engineering and Computing. 2008, Uni-versity of South Carolina.

Xu S., Huang C.-T.. 'Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions' in 3rd Inter-national Symposium on Wireless Communication Systems. 2006. Valencia Spain.

Xu S., Matthews M., Huang C.-T., 'Security Issues in Privacy and Key Management Protocols of IEEE 802.16', in 44th annual South-East regional conference. 2006: Melbourne, Florida

Xu S., Matthews M., Huang C-T, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", ACM SE'06, March 10- 12, 2006, and Melbourne, Florida, USA

Yi and Zoran Zvonar (eds) (2009a), "LTE Part 1: Core Network," IEEE Communications

Yuksel E., Nielson H.R., Nielsen C.R., Orencik M.B.. "A Secure Simplification of the PKM second edition Protocol in IEEE 802.16e-2005", in Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis. 2007. Wroclaw, Poland.

Zhang Y., Wang L., Sun W., Green R., Alam M., "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE Transactions on Smart Grid, Vol. 2, No. 4, De-cember 2011

Zheng Y., He D., Tang X., Wang H., "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform," Proc. Fifth International Conference on Information, Communi-cations and Signal Processing, 2005, pp.976-980.

Zheng Y., He D., Xu L., Tang X., "Security Scheme for 4G Wireless Systems," Proc. Communica-tions, Circuits and Systems, May 2005, pp.397- 401.

Zhou B., "An intrusion detection system based on WiMAX" International Conference on Computer Science and Network Technology (ICCSNT), 2011, Page(s): 2448 – 2451

Zhu L., Mao H., Hu Z., "Research on 3GPP LTE Security Architecture" 8th Intl Conference on Wire-less Communications, Networking and Mobile Computing (WiCOM)", Shanghai, 2012.

Zimmermann H., "OSI Reference Model — The ISO Model of Architecture for Open Systems Inter-connection". IEEE Transactions on Communications 28 (4): 425–432, 1980.

Appendices

Appendix 1. Power Measurements and Power Calculations of 802.16 WiMAX OFDMA

A typical TDD WiMAX signal is not continuous, but has a burst structure. The follo-wing figure shows the power versus time graph of a WiMAX signal.

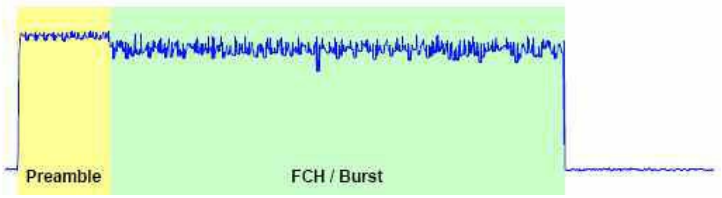


Figure 1: Power vs. time graph of a WiMAX signal [1]

The start of every downlink frame is the preamble followed by the frame control header (FCH) / burst. The preamble, used for synchronisation, contains BPSK-modulated carriers and is one OFDMA symbol long. It is power boosted and the level is a few dB higher than the level of the following data burst [2].

As an example the **following signal parameters** are assumed for all the measure-ments described and all figures in this application note:

- WiBro DL signal (OFDMA)
- 1 PUSC zone with 30 symbol and all subchannels used
- 16 QAM1/2 modulation
- 1 segment, #0 used
- Total frame length 5 ms
- FFT size, NFFT = 1024 carriers

Within the WiMAX application firmware R FSx-K93 there are two tables which show all important parameters at a glance and thus help you to optimize your system. Beside EVM, RSSI, CINR, IQ constellation,… different power pa-rameters of WiMAX signals are calculated. The first table ‘List 1’ shows the re-sults of power measurement in time domain (TD) (see section 2). On the second

table ‘List 2’ you can see the results of power measurement in frequency domain (FD) (see section 3).

Result Summary of Analyzed Subframes						
	Min	Mean	Limit	Max	Limit	Unit
TD Power DL Preamble	-8.74	-8.74		-8.74		dBm
TD Power Subframe	-12.38	-12.38		-12.38		dBm
TD Power Zone	-12.56	-12.56		-12.56		dBm

Figure 2: This list shows the power of certain parts of the signal measured in time domain: TD power DL preamble, TD power subframe and TD power zone.

Result Summary of Analyzed Zone/Segment						
	Min	Mean	Limit	Max	Limit	Unit
Power DL Preamble	-3.16	-3.16		-3.16		dBm
Power Data and Pilots	-11.71	-11.71		-11.71		dBm
Power Data	-12.17	-12.17		-12.17		dBm
Power Pilots	-9.68	-9.68		-9.68		dBm

Figure 3: This list displays power values measured in frequency domain: power DL preamble, power data and pilots, power data and power pilots.

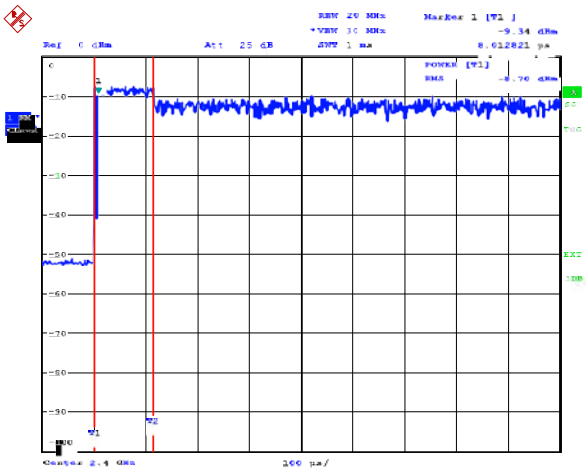
WiMAX – Time Domain Power Measurement

This section describes typical time domain measurements on a WiMAX OFDMA signal in spectrum analyzer mode.

Settings

The time domain power parameters of a WiMAX signal as displayed in ‘List 1’ (figure 2) can be easily measured with a spectrum analyzer using the time domain power function. This function is a stan-dard measurement function of R&S spectrum analyzers (‘Meas’ softkey M ‘Time Domain Power Function’). To make a correct measurement the resolution bandwidth (RBW) of the spectrum analyzer has to be wider than the bandwidth of the RF signal [1]. For an optimum measurement result you have to switch on the RMS detector. Then you can use the limit lines to evaluate the power in certain areas of the burst (e.g. in the preamble and the data part).

Measurement using a Spectrum Analyzer



The figure below shows the measurement of the TD Power DL Preamble. The measured value correla-tes with the one in ‘List 1’ (figure 2).

Figure 4: Time Domain measurement – TD Power DL Preamble

Between the other two TD Power parameters, measured in figure 5, and the values of ‘List 1’ there is also a good correlation:

‘List 1’ (figure 2) TD power measurement TD Power DL Preamble - 8.74 dBm - 8.70 dBm (figure 4)

TD Power Subframe -12.38 dBm -12.38 dBm (figure 5, left) TD Power Zone -12.56 dBm -12.54 dBm (figure 5, right)

The inconvenience of this measurement method is that the limits for the burst power measurement need to be set manually. For the determination of TD Power DL Preamble only the preamble part of the WiMAX frame (see figure 1 preamble part) is measured. The measurement range of TD Power Subframe includes the preamble and FCH/burst part of figure 1, the measurement range of TD Power Zone includes only the FCH/burst part.

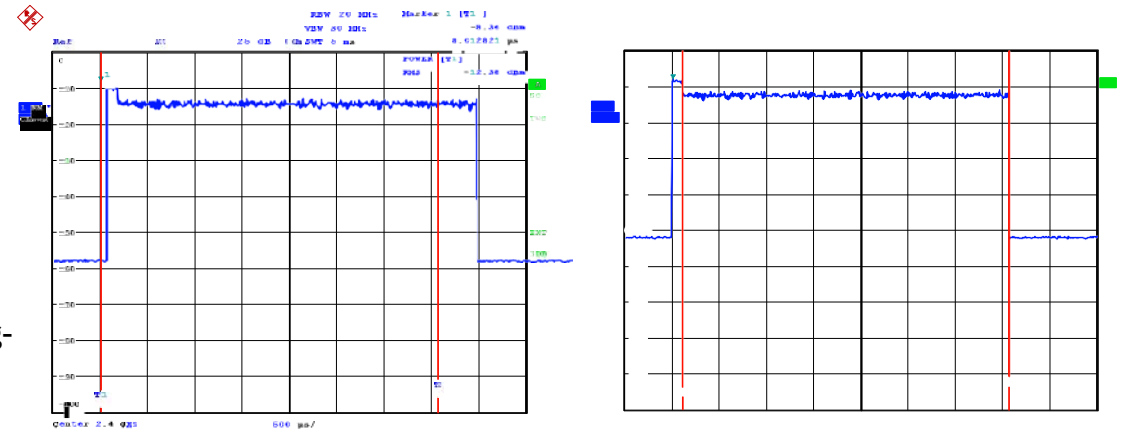


Figure 5: Time Domain measurement – left: TD Power Subframe, right: TD Power Zone

WiMAX – Frequency Domain Power Measurement

This section describes the calculation of the boosting factors and the mathematical relations of the power parameters in frequency domain and in time domain.

Boosting Factor

All constellations (BPSK, QPSK, 16QAM, 64QAM) in the diagram are normalized to achieve equal average power, e.g. QPSK data is normalized by multiplying the constellation point with c = 1/O2. According to standard [16-2004] the subcarriers are boosted by the factor 2(1/2-wk) compliant with the subcarrier index k and with wk = {0,1}. For QPSK modulated data you obtain (figure 6):

Re{data,QPSK} = 1/rad2 * 2(1/2-wk) = rad2 * (1/2-wk) Im{data,QPSK} = 1/rad2 * 2(1/2-wk) = rad2 * (1/2-wk).

The pilot carriers within the symbol and the preamble are BPSK modulated. Thus the imaginary part is not necessary and only the real part in the IQ domain is boosted. The pilot carriers within the symbol are boosted according to [16-2004] equation 135:

Re{pilot} = 8/3*(1/2-wk) = 4/3 * 2(1/2-wk) Im{pilot} = 0.

The power of the pilots (with wk = {0,1}) is Re{pilot}max = 4/3 and in log scale 20 * log (4/3) = **2.5 dB**

above the data subcarrier power level i.e. the pilots are power boosted by

2.5 dB. This is a fixed value for all permutations except UL PUSC (partial usage of subchannels), UL Ranging and DL FUSC (full usage of subchannels). For those permutations the boosting factor for the pilots is 0 dB (figure 6).

The **carriers in the downlink preamble** are boosted according to [16- 2004] equation 136:

Re{preamble} = 4*rad2 *(1/2-wk) = 2*rad2 * 2(1/2-wk) Im{preamble} = 0.

Consequently the boosting factor of the preamble amounts to Re{preamble}max = 2*rad2 and in log scale

20 * log (2*rad2) = 9.0 dB.

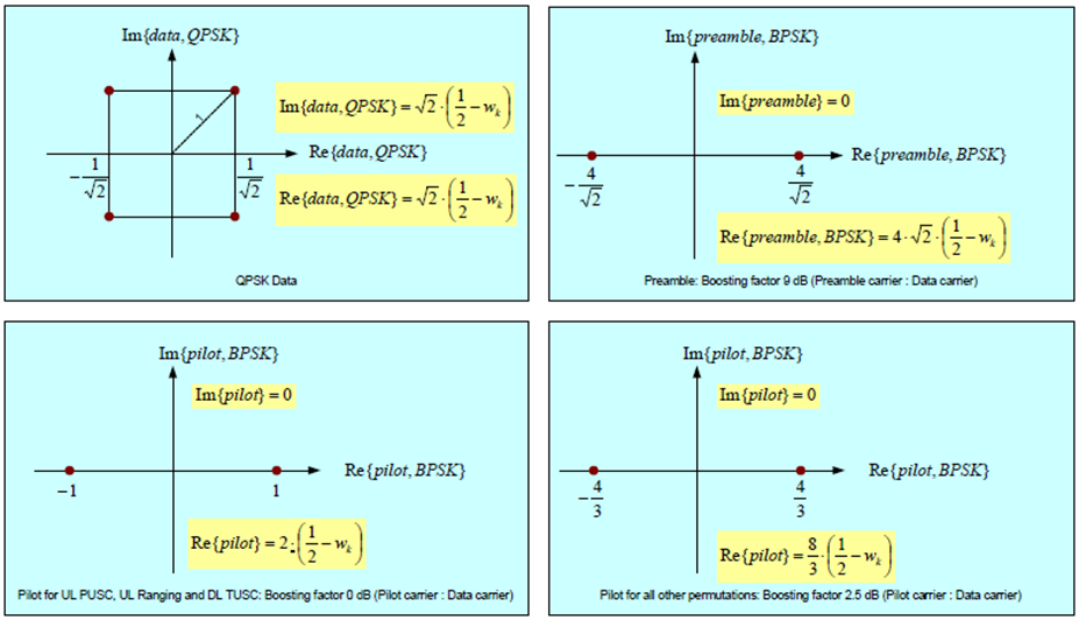


Figure 6: Modulation Symbol Power – Modulation and boosting factor of QPSK data, preamble and pilots

When not all subchannels are used within the first DL PUSC zone, zone boosting is applied (acccording to [16e-2005] section '8.4.9.6 Zone boosting') and thus the data and pilot subcarriers in the corresponding zone are boosted. The subcarrier level of the zone is increased as follows:

10 * log(Nuseful / Nallowed)

Nuseful – all useful subcarriers (of all subchannels) depending on permutation scheme (according to [16e-2005] Table 310x) and excluding DC subcarrier

Nallowed – subcarriers of the selected subchannels (that are allowed to be used in the zone)

The following equations summarize the relations for the boosting factors in frequency domain:

Boosting:		
$P_{FD,Preamble}$ $P_{FD,Preamble}$	= 9 dB + $P_{FD,Data}$	(all subchannels used) (1)
	= 9 dB + $P_{FD,Data}$	+ 10 * log(N_{useful} / $N_{allowed}$)
$P_{FD,Pilot}$		(limited usage of subchannels) (2)
	= 2.5 dB + $P_{FD,Data}$	-3

where $P_{FD,Preamble}$ is the power level of the preamble in frequency domain, $P_{FD,Data}$ of the data, and $P_{FD,Pilot}$ of the pilots.

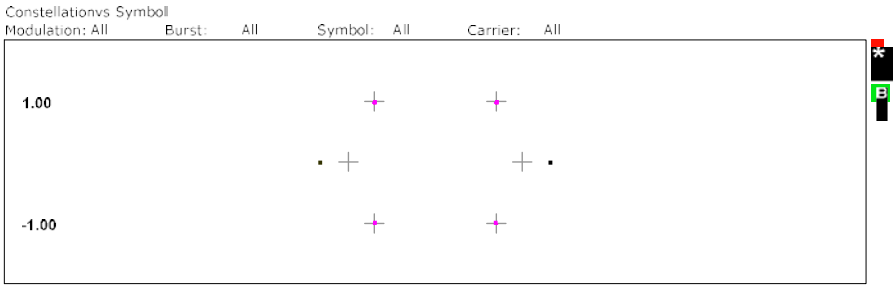


Figure 7: Constellation diagram of a WiMAX OFDMA signal with a QPSK modulated data burst. The pilots are BPSK modulated. As they are power boosted they do not correspond with the indicated BPSK constel-lation points.

There is only one parameter of ‘List 2’ (figure 3) that has not been explained yet: the power value for data and pilots in frequency domain $P_{FD,Data/Pilots}$. It can be calculated from $P_{FD,Data}$ and $P_{FD,Pilot}$ as follows:

$$P_{FD,Data/Pilots[mW]} = (N_{Data} * P_{FD,Data[mW]} + N_{Pilot} * P_{FD,Pilot[mW]}) / (N_{Data} + N_{Pilot}) \quad (4)$$

For this calculation the power must be noted in mW. The number of data carriers NData and pilot carriers N_{Pilot} depends on the FFT size and the permutation scheme and is defined in the standard [16e-2005] Table 310. For an example please refer to section 5 in this application note.

Mathematical Relations Time Domain / Frequency Domain

Beside measuring the preamble power in time domain $P_{TD,Preamble}$ you can also calculate this value from the preamble power in frequency domain $P_{FD,Preamble}$:

$$P_{TD,Preamble} = 10 * \log(N_{used,Preamble}/N_{FFT}) + P_{FD,Preamble} \quad (5)$$

The number of preamble carriers used $N_{used,Preamble}$ depends on the number of used segments. The DL supports up to three segments. A segment is a subdivision of the available OFDMA subchannels (one segment may include all sub-channels). As previously mentioned the transmission begins with a preamble. Further to synchronisation the preamble indicates which of the three segments of the zone are used. Therefore the preamble subcarriers are divided into three carrier-sets. Carriers 0,3,6… indicate that seg-ment 0 is to be used, carriers 1,4,7,.. indicate that segment 1 is to be used, and carriers 2,5,8,… indicate that segment 3 is to be used. For every active segment a third of the carriers is used:

$$N_{used,Preamble} = N_{avail\_p} * N_{segments} /3$$

The number of subcarriers available for the preamble symbol Navail_p depends on the FFT size NFFT and the number of guard carriers Nguard_p:

$$N_{avail\_p} = N_{FFT} - N_{guard\_p}$$

The number of guard carriers N_{guard_p} can be found in the standard [16e- 2005] section ‘8.4.6.1.1 Pream-ble’.

A similar equation is valid for the zone power $P_{TD,Zone}$ of a WiMAX signal:

$$P_{TD,Zone} = 10 * \log((N_{useful} + 1) /N_{FFT}) + P_{FD,Data/Pilots} \quad (6)$$

Figure 8 illustrates the relation of both lists displayed in the application firmware FSx-K93 in brief. The numbers signify the associated equation:

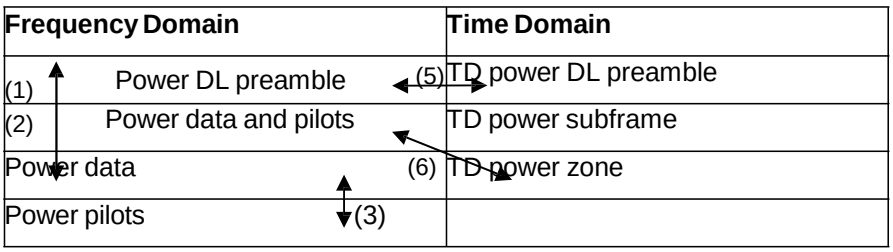


Figure 8: Relation of the parameters displayed in ‘List 1’ and ‘List 2’

OFMDA Calculation Example

The following example shows how to calculate the main power parameter of an OFDMA system signal. As mentioned in the first section we have a 1024-FFT OFDMA downlink PUSC signal with one segment and all sub-channels used.

Values according to standard

Based on the defined signal there are some fix parameters specified in the standard [16e-2005]. The num-ber of pilots, data, and guard subcarriers varies for different sub-channelization schemes. The values below are valid for a WiMAX 1024-FFT OFDMA DL PUSC signal (according to standard [16e-2005] Ta-ble 310a, page 528):

N_{used} = 841 (incl. DC subcarrier) N_{Data} = 720

N_{Pilot} = 120

For the preamble symbol there will be 86 guard band subcarriers on both sides of the spectrum (accord-ing to standard [16e-2005] section '8.4.6.1.1 Preamble'):

$N_{avail\_p} = N_{FFT} - N_{guard\_p} = 1024 - 86*2 = 852$

In our example only one segment is used and thus only a third of all preamble carriers:

$N_{used,Preamble} = N_{avail\_p} * N_{segments} /3 = 852 * 1/3 = 284$

Frequency Domain Power Calculation

The power of the data carriers in frequency domain PFD,Data is given in 'List 2' and necessary to calculate the other power parameters:

$\mathbf{P_{FD,Data}}$ = -12.17 dBm ('List 2': Power Data)

The WiMAX signal uses **all subchannels**. Thus zone boosting is not applied and the power of the pream-ble (according to formula (1)) and the power of the pilots (according to formula (3)) result in:

$\mathbf{P_{FD,Preamble}}$ = 9.03 dB – 12.17 dBm = **-3.14 dBm** ('List 2': Power DL Preamble = -3.16 dBm)

$P_{FD,Pilot}$ = 2.49 dB – 12.17 dBm = **-9.68 dBm** (‘List 2’: Power Pilots = -9.68 dBm)

The power of data and pilots PFD,Data/Pilots is calculated as follows (according to formula (4)):

$P_{FD,Data}$ = -12.17 dBm ^= 0.061 mW

$P_{FD,Pilot}$ = -9.68 dBm ^= 0.108 mW

$P_{FD,Data/Pilots}$ = 0.067 mW ^= **-11.71 dBm** (’List 2’: Power Data and Pilots = -

11.71 dBm)

Additional example:

If you have a signal with limited usage of subchannels (e.g. only 20 of 30 sub-chan-nels used) zone boosting is applied. In this case 560 subcarriers are useful (Nuseful = (841–1)*20/30 = 560) and 840 are allowed (Nallowed = 841–1). Thus the difference between PFD,Preamble and PFD,Data is 7.27 dB (9.03 dB + 10 * log(560/ 840)) instead of 9 dB.

Time Domain Power Calculation

According to formula (5) the power of the DL preamble is:

$P_{TD,Preamble}$ = -3.16 dBm + 10 * log(284/1024) = **-8.73 dBm** (‘List 1’: TD Power DL Preamble = -8.74 dBm)

and the time domain power of the zone (according to formula (6)):

$P_{TD,Zone}$ = -11.71 dBm + 10 * log(841/1024) = **-12.56 dBm** (’List 1’: TD

Power Zone = -12.56 dBm)

Appendix 2. List of Standards

WiMAX (Stage 2)	Forum, WiMAX Forum Network Architecture. Stage 2: Architecture, Tenets, Reference Model and Reference Points. V. 1.2, WiMAX Forum Std., 2009.
WiMAX (Stage 3)	Forum Network Architecture. Stage 3: Detailed Protocols and Procedures, WiMAX Forum Std., 2009.
802.1X	IEEE Std 802.1X-2004, "802.1X IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control", Revision of IEEE Std 802.1X-2001, IEEE, 2004.
802.11	IEEE 802.11-2007 "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", IEEE, 2007.
802.11e	IEEE 802.11-2005 "IEEE Standard for Information Technology – Telecommunications and Information Exchange between Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.
802.11i	IEEE Std 802.11i-2004, "Amendment to IEEE Std. 802.11, 1999 Edition, Amendment 6: Medium Access Control (MAC) Security Enhancements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE, 2004.

802.11n	IEEE 802.11n-2009 "IEEE Draft Standard for Information Technology – Telecommunications and Information Exchange between Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" Amendment: Enhancements for Higher Throughput.
802.16 Conformance01-2003	IEEE Standard for Conformance to IEEE 802.16, Part 1: Protocol Implementation Conformance Statement (PICS) Proforma for 10–66 GHz WirelessMan-SC air interface.
802.16 Conformance02-2003	IEEE Standard for Conformance to IEEE 802.16, Part 2: Test Suite Structure and Test Purpose for 10–66 GHz WirelessMan-SC air interface.
802.16 Conformance03-2004	IEEE Standard for Conformance to IEEE 802.16, Part 3: Radio Conformance Tests (RCT) for 10–66 GHz WirelessMAN-SC Air interface.
802.16 Conformance04-2006	IEEE Standard for Conformance to IEEE 802.16, Part 4: Protocol Implementation Conformance Statement (PICS) Proforma for Frequencies below 11 GHz.
IEEE 802.16.2-2004	IEEE Recommended Practice for Local and metropolitan area networks, Coexistence of fixed broadband wireless access systems.
802.16-2001	IEEE 802.16-2001, "IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", Approved 6 December 2001, IEEE Press, 2002.
802.16-2004	IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.
802.16-2004/Cor1-2005	IEEE 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.

802.16c-2002	IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems-Amendment 1: Detailed System Profiles for 10–66 GHz.
802.16d	IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004.
802.16e	IEEE 802.16e-2005 "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, 2006.
802.16f	IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems- Amendment 1: Management Information Base.
802.16g	IEEE Standards for Local and metropolitan area networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 3: Management Plane Procedure and Services.
802.16j	IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 1: Multiple Relay Specification.
802.16k	IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Bridges Amendment 5: Bridging of IEEE 802.16.
802.16m	IEEE 802.16m-2009 "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems" Amendment: Advanced Air Interface.
802.21	IEEE 802.21-2008 "IEEE Standard for Local and metropolitan area networks Part 21: Media Independent Handover", IEEE, Jan. 2008.
RFC1213	The Internet Engineering Task Force (IETF); Management Information Base for Network Management of TCP/IP-based internets: MIB-II.

RFC2459	The Internet Engineering Task Force (IETF); Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
RFC2560	The Internet Engineering Task Force (IETF); X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
RFC2865	The Internet Engineering Task Force (IETF); Remote Authentication Dial In User Service (RADIUS), Network Working Group Std., 2000.
RFC 3344	The Internet Engineering Task Force (IETF); IP Mobility Support for IPv4 (Mobile IP), Network Working Group Std., 2002.
RFC3588	Internet Engineering Task Force (IETF); Diameter Base Protocol, Network Working Group Std., 2003.
RFC3748	Internet Engineering Task Force (IETF); Extensible Authentication Protocol (EAP), Network Working Group Std., 2004.
RFC 4187	Internet Engineering Task Force (IETF); Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), Network Working Group Std., 2006.
RFC5246	Internet Engineering Task Force (IETF); The Transport Layer Security (TLS) Protocol Version 1.2, Network Working Group Std., 2008.
RFC5281	Internet Engineering Task Force (IETF); Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), Network Working Group Std., 2008.

AES	FIPS 197, "Announcing the Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, Nov. 2001.
DES	FIPS PUB 46-3, "Data Encryption Standard (DES)", Federal Information Processing Standards Publication, Reaffirmed 1999 October 25, U.S. Department of Commerce / National Institute of Standards and Technology, 1999.
RSA	"PKCS #1 v2.1: RSA Cryptography Standard", RSA Laboratories, June 2002.

Appendix 3. Checking Algorithms

Computational Equivalence Checking Algorithm

Algorithm presents our Computational Equivalence checking algorithm, which we explain in the sequel.

Algorithm Computational Equivalence Checking

1: t = t_0;
2: $\phi(t_0) = \{Spec_j(t_0)\}\ 0 < j \leq m$;
3: **while** $t \leq K_{Spec}$ **do**
4: $\phi(t) = SymSim\_Step(\phi)$
5: If NoDeltaCycle then t = t+1
6: **end while**
7: SPEC = $\phi(t_0 + K_{Spec})$
8: t = t_0;
9: $\varphi(t_0) = \{Imp_i(t_0)\}\ 0 < i \leq m$;
10: **while** $t \leq K_{Imp}$ **do**
11: $\varphi(t) = SymSim\_Step(\varphi)$
12: If NoDeltaCycle then t = t+1
13: **end while**
14: IMPL = ReplaceRepeated ($\varphi(t_0 + K_{Imp}), R_{Abst}$)
15: MatchQ ($\varphi(T), \phi(T)$); // T = t_0 + k

Property Checking Algorithm

Algorithm presents our proposed property checking Algorithm, which we describe in the following.

Algorithm Property Checking

1: PROP = { Prop(IMPL) };
2: t = t_0;
3: $\varphi(t_0) = \{Imp_i(t_0)\}\ 0 < i \leq m$;
4: **while** $t \leq K_{Imp}$ **do**
5: $\varphi(t) = SymSim\_Step(\varphi)$
6: If NoDeltaCycle then t = t+1
7: **end while**
8: IMPL = ReplaceRepeated ($\varphi(t_0 + K_{Imp}), R_{Abst}$)
9: MatchQ (IMPL, PROP) // T = t_0 + k

Appendix 3. Checking Algorithms

Computational Equivalence Checking Algorithm

Algorithm presents our Computational Equivalence checking algorithm, which we explain in the sequel.

Algorithm Computational Equivalence Checking

1: t = t_0;
2: $\phi(t_0) = \{Spec_j(t_0)\}\ 0 < j \leq m$;
3: **while** $t \leq K_{Spec}$ **do**
4: $\phi(t) = SymSim\_Step(\phi)$
5: If NoDeltaCycle then t = t+1
6: **end while**
7: SPEC = $\phi(t_0 + K_{Spec})$
8: t = t_0;
9: $\varphi(t_0) = \{Imp_i(t_0)\}\ 0 < i \leq m$;
10: **while** $t \leq K_{Imp}$ **do**
11: $\varphi(t) = SymSim\_Step(\varphi)$
12: If NoDeltaCycle then t = t+1
13: **end while**
14: IMPL = ReplaceRepeated ($\varphi(t_0 + K_{Imp}), R_{Abst}$)
15: MatchQ ($\varphi(T), \phi(T)$); // T = t_0 + k

Property Checking Algorithm

Algorithm presents our proposed property checking Algorithm, which we describe in the following.

Algorithm Property Checking

1: PROP = { Prop(IMPL) };
2: t = t_0;
3: $\varphi(t_0) = \{Imp_i(t_0)\}\ 0 < i \leq m$;
4: **while** $t \leq K_{Imp}$ **do**
5: $\varphi(t) = SymSim\_Step(\varphi)$
6: If NoDeltaCycle then t = t+1
7: **end while**
8: IMPL = ReplaceRepeated ($\varphi(t_0 + K_{Imp}), R_{Abst}$)
9: MatchQ (IMPL, PROP) // T = t_0 + k