SECURITY ALGORITHMS FOR WIMAX

M Alzaabi[1], K D Ranjeeth[2], Professor T Alukaidey[3] and Dr K Salman[4]

[1]School of Engineering & Technology, University of Hertfordshire, Hatfield, UK
Alzaabi@adpolice.gov.ae
[2]School of Engineering & Technology, University of Hertfordshire, Hatfield, UK
kdavidranjeeth@yahoo.com
[3]School of Engineering & Technology, University of Hertfordshire, Hatfield, UK
T.Alukaidey@herts.ac.uk
[4]Department of Engineering Technology, Middle Tennessee State University,
Murfreesboro, Tennessee, USA
Karim.Salman@mtsu.edu

ABSTRACT

Security is always important in data networks, but it is particularly critical in wireless networks such as WiMAX. Authentication is the first element in wireless security that, if not well safeguarded, all following security measures will be vulnerable. Denial of Service is one of the attacks that could target a WiMAX network to make its operation inefficient. This paper is an investigation into a) the weakness and threats on WiMAX security algorithms and b) the best method that could prevent DoS attacks prior to the authentication algorithm.

The paper is presenting the architecture of WiMAX and identifying the main layers and sub layers that these security algorithms are performing their functions from within. The paper incorporates the new method with the authentication algorithm to improve the efficiency of the security of WiMAX.

KEYWORDS

DoS, WiMAX, Media Access Control, Physical Layer, DLL. LLC

1. INTRODUCTION

The aim of this paper is to highlight some of the security threats that face today's wireless networks such as WiMAX and try to address one of these threats which is the Denial of Service (DoS) attack.

WiMAX is an evolving wireless technology based on IEEE 802.16 standard. IEEE 802.16e standard defines the security mechanisms in WiMAX. The security sub-layer in WiMAX Network is where authentication, authorization and encryption take place.

This paper starts with a look at WiMAX architecture and its components. Then, it addresses IEEE 802.16 protocol layer that is associated with security issues. Next, it tackles some of the WiMAX vulnerabilities that could cause DoS attacks. After that, it examines some of the up today encryption protocols. Finally, it suggests a way forward to tackle some of the possible causes of DoS attacks.

DOI : 10.5121/ijnsa.2013.5304

2. WIMAX ARCHITECTURE

WiMAX Architecture is designed and developed on all-IP platform with all packet technology and without any legacy circuit telephony. Figure 2.1 presents WiMAX architecture. This IP-based WiMAX network architecture consists of three main sections, namely User Terminals, Access Service Network (ASN) and Connectivity Service Network (CNS) [4].

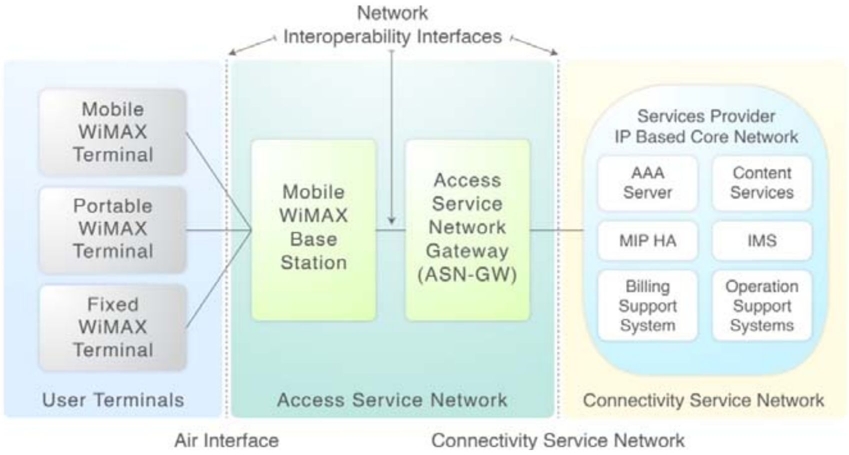

Network
Interoperability Interfaces
Mobile WiMAX Terminal
Portable WiMAX Terminal
Fixed WiMAX Terminal
User Terminals
Mobile WiMAX Base Station
Access Service Network Gateway (ASN-GW)
Access Service Network
Services Provider IP Based Core Network
AAA Server
Content Services
MIP HA
IMS
Billing Support System
Operation Support Systems
Connectivity Service Network
Air Interface
Connectivity Service Network

Figure 2.1: WiMAX network IP-based Architecture

These three sections are explained briefly in section 2.1.

2.1. WiMAX main Three Sections

WiMAX consists of three main sections, User Terminals, Access Service Network and Connectivity Service Network.

2.1.1. User Terminals

They are the terminals that work with the Base Station (BS) to provide wireless access functions and support mobility such as Mobile Station (MS) and Subscriber Station (SS). The MS and SS enable connection to a variety of servers through the ASN [7].

2.1.2. Access Service Network (ASN)

ASN functions are as follows:

- The Access Service Network (ASN) sets and defines the network functions for providing WiMAX MS and SS with wireless access [7]. The ASN consists of network elements (such as one or more BS and ASN Gateways) and provides the following functions:
- Layer 2 connectivity with MS and SS
- Transfers AAA messages (Authentication, Authorization and, Accounting) to WiMAX subscribers.
- Relay functions for building MS and SS and Layer 3 connectivity
- Wireless resource management
- ASN and CSN secured mobility
- Paging

2.1.3. Connectivity Service Network (CSN)

CSN consists of various network elements, including AAA, home agents, routers, gateways and user databases. CSN provides WiMAX subscribers connectivity with the following functions:

- Allocates MS and SS IP addresses and endpoint parameters for user sessions.
- Internet access.
- AAA proxy/server.
- Policy and authorization control based on user subscription profiles.
- ASN-CSN tunnelling support.
- Accounting among WiMAX subscribers and settlement among operators.
- Tunnelling between CSNs for roaming.
- Mobility between ASNs.
- Services based on positional information, connectivity with peer-to-peer services, provisioning, etc. [7].

The end to end WiMAX network architecture significantly supports mobility and handover which includes:

- Vertical or inter-technology handovers under multi-mode operation.
- IPv4 and IPv6 based mobility management.
- Roaming between Network Service Providers (NSPs).
- Seamless handover up to vehicular speed satisfying bounds of service disruptions.

WiMAX network architecture supports QoS via differentiated levels of QoS, admission control, bandwidth management, and other appropriate policies [4].

2.2. Vulnerable parts of WiMAX to breach security

WiMAX is based on the IEEE 802.16 standard, which is realized to have security flaws including, vulnerabilities in authentication and key management protocols. Message replay is one of the most well-known attacks on authentication and authenticated key establishment protocols. The idea behind replay based attacks is to flood a network with false management frames, which cause a denial of service (DoS) [5].

In IEEE the 802.16 standard, Privacy Sub-layer sits on the top of Physical layer. Therefore, 802.16 networks are vulnerable to physical layer attacks such as jamming and scrambling. Jamming is done by initiating a source of strong noise to significantly decrease the capacity of the channel, thus denying services (DoS) to all parties. Scrambling is another type of jamming, but it takes place for a short interval of time targeting specific frames. Control or management messages can be scrambled, but it is not possible with delay sensitive message i.e., scrambling Uplink slots are quite difficult, because the attacker has to interpret control information and to send noise during a particular interval.

The main purpose of the Privacy Sub-layer is to protect service providers against theft of service, rather than guarding network users. It is obvious that the privacy layer only guards data at the OSI layer two (data link), whereas it does not guarantee end to end encryption of user data. Likewise, it does not protect the physical layer from being intercepted.

Identity theft is another threat, which is reprogramming a device with the hardware address of another device. The address can be stolen over the air by interrupting management messages.

3. IEEE 802.16 protocol layer associated with Security issues

IEEE 802.16 standard uses the Open Systems Interconnection (OSI) network reference seven-layer model. The OSI model divides the functions of different protocols into a series of layers. The two lowest layers are called the Physical (PHY) Layer and the Data Link Layer. Data Link layer consists of Logical Link Control (LLC) and Media Access Control (MAC).

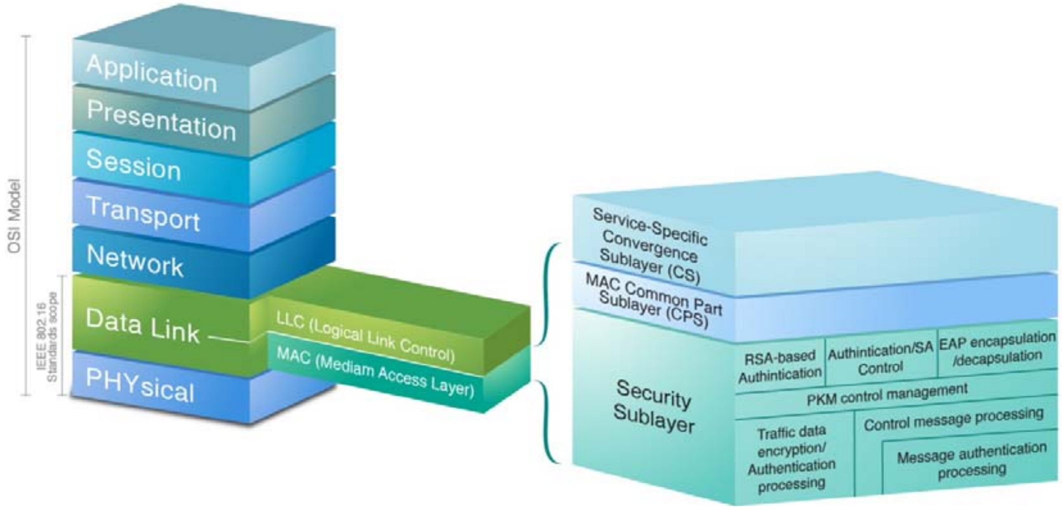

OSI Model
IEEE 802.16 Standards scope
Application
Presentation
Session
Transport
Network
Data Link
PHYsical
LLC (Logical Link Control)
MAC (Mediam Access Layer)
Service-Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (CPS)
Security Sublayer
RSA-based Authintication
Authintication/SA Control
EAP encapsulation /decapsulation
PKM control management
Traffic data encryption/ Authentication processing
Control message processing
Message authentication processing

Figure 3.1: IEEE 802.16 – 2004 Standards Scope Protocol Layers in OSI Model

The physical connection between the communicated parties is created by the PHY layer while the establishment and maintenance of this connection is the responsibility of the MAC layer. The 802.16 standard defines only these two lowest layers [6]. Moreover, it divides the MAC layer into three sub-layers, Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer [6]. These three MAC Sub-layers are explained briefly within sections 3.1, 3.2 and 3.3.

3.1 Convergence Sub-layer (CS)

The CS is right above the MAC CPS sub-layer. The CS performs the following functions:

- Receiving higher-layer Protocol Data Unit (PDU) from the upper layers.
- Classifying and mapping the MAC Service Data Unit (MSDU) into appropriate Connection IDentifier (CID) which is a basic function of the Quality of Service (QoS) management mechanism of 802.16.
- Processing based on the classification, the higher-layer PDUs (if required).
- Payload Header Suppression (PHS) which is the process of suppressing repetitive parts of payload headers at the sender and restoring these headers at the receiver (optional function).
- Delivering CS PDUs to the appropriate MAC Service Access Point (SAP) and receiving CS PDUs from the peer entity [6].

Figure 3.1.1 shows Physical protocol Data Unit. The message within MSDU follows the encryption services that are defined as a set of capabilities within the MAC Security Sub-layer.

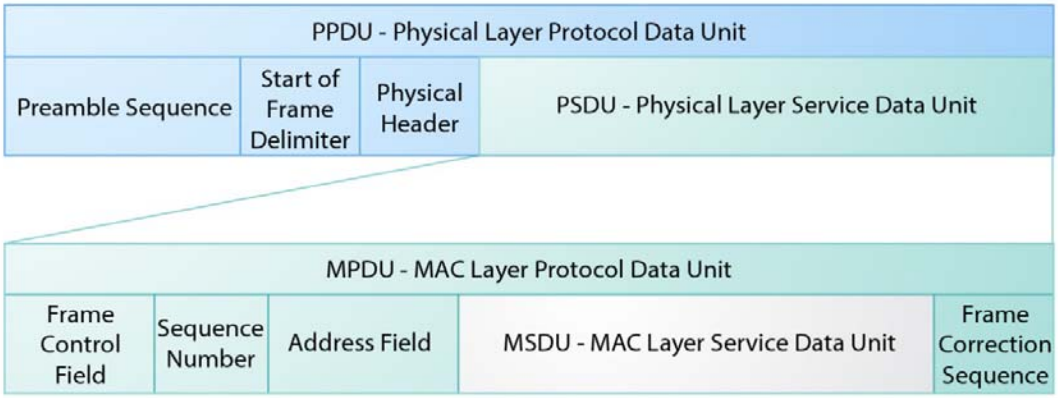

PPDU - Physical Layer Protocol Data Unit
Preamble Sequence
Start of Frame Delimiter
Physical Header
PSDU - Physical Layer Service Data Unit
MPDU - MAC Layer Protocol Data Unit
Frame Control Field
Sequence Number
Address Field
MSDU - MAC Layer Service Data Unit
Frame Correction Sequence

Figure 3.1.1: The Preload is scrambled in MSDU

3.2. Medium Access Control Common Part Sub-layer (MAC CPS)

The CPS sits in the middle of the MAC layer and is responsible for:

- Bandwidth allocation.
- Connection establishment.

Maintenance of the connection between the two sides [6].

3.3. Security Sub-layer

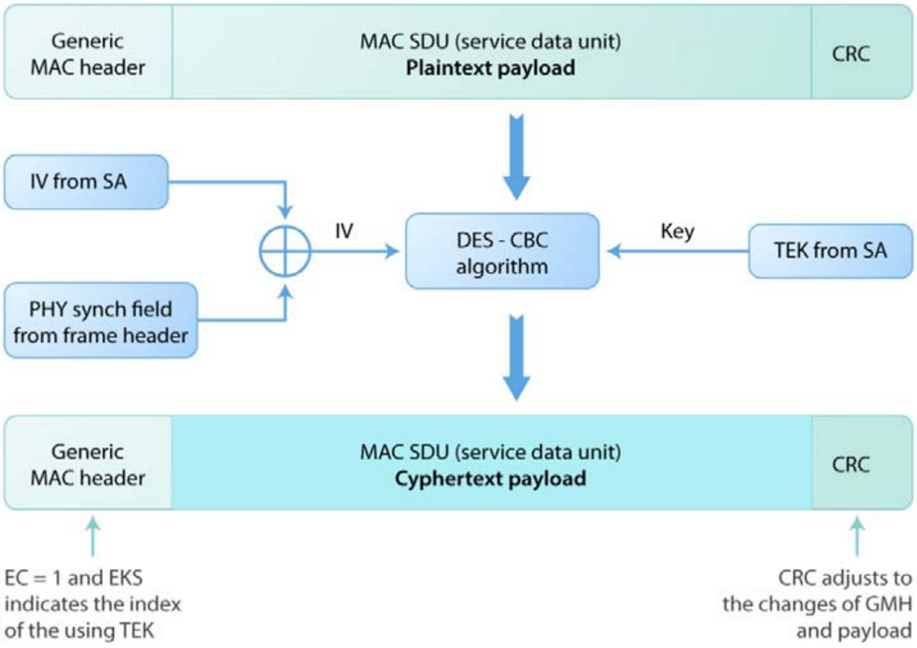
The Security Sub-layer sits between the MAC CPS and the PHY. It provides authentication, secure key exchange, encryption and integrity control across the system.

In the 802.16 standard, encrypting connections between the Subscriber Station (SS) and the Base Station (BS) are generated with a data encryption protocol applied both ways. This protocol defines a set of supported cryptographic suites. An encapsulation protocol is used for encrypting data packets across the network [6].

The Privacy Key Management (PKM) protocol, which is an authentication protocol, is used to provide the secure distribution of keying data from BS to the SS. Through this secure key exchange, due to the key management protocol, the SS and the BS synchronize keying data. The basic privacy mechanisms are strengthened by adding digital certificate based SS authentication to the key management protocol. Furthermore, the BS uses the PKM protocol to ensure conditional access to network services [6].

3.4. WiMAX MAC Protocol Data Unit (MPDU) Encryption Process

After the completion of authentication and initial key exchange, data starts to flow between the BS and the SS by using the Traffic Encryption Keys (TEK) for encryption. Figure 3.4 shows this process. The Data Encryption Standard with Cipher Block Changing (DES-CBC) enciphers the MPDU payload field only leaving the header and the Cyclic Redundancy Check (CRC) without encryption in order to support diverse services. Once the security sub-layer generates an MPDU, it checks the Security Association (SA) associated with the current connection and obtains the Initialization Vector (IV). The MPDU IV is generated by XORing the SA IV with the synchronization field in the PHY frame header. The DES-CBC algorithm then encrypts the MPDU plaintext payload by using the generated MPDU IV and the authenticated TEK. To indicate that the payload in the MPDU is encrypted, the Encryption Control (EC) field of the MAC header is set to 1. The 2-bit Encryption Key Sequence (EKS) indicates which TEK is used. The CRC field is updated in accordance with the changes in both the payload and MAC header



.

Figure 3.4: WiMAX encryption Process

4. WiMAX Vulnerabilities

There are various vulnerabilities and possible attacks to WiMAX network. One of the obvious attacks is the Denial of Service (DoS) attack. DoS attacks in WiMAX may include the following:

4.1. DoS attacks based on Ranging Request/Response (RNG- REQ/RNG-RSP) messages

The RNG-REQ message is the first message sent by a SS to BS requesting transmission time, power, and frequency and burst profile information before joining the network. This initial message is not encrypted nor verified for authentication which makes it vulnerable to interception and modification to the least effective settings for the SS leading to degrading or denying the service to the SS. The RNG-RSP message is the message that the BS responds with to the RNG-REQ message from the SS. The BS uses this message to change the up and downlink channels of the SS, transmission power level, fine-tune the settings of the transmission link and terminating the communications with the SS. Like the RNG-REQ, this message is neither encrypted nor authenticated and is exposed to alteration. For example, the SS transmitting power can be set to its maximum to quickly drain its battery [8].

4.2. DoS attacks based on Mobile Neighbour Advertisement (MOB_NBR-ADV) message

TheMOB_NBR-ADV message is sent from the BS to announce properties of neighbouring BSs to its SSs that are about to perform a handover. Similarly, this message is neither encrypted nor authenticated and could, if forged, lead to inefficient or incorrect handovers [8].

4.3 Dos Attacks based on Fast Power Control (FPC) message

The FPC message is used by the BS to the make the SS quickly adjust its transmission power. Also, without an authentication mechanism, the FPC message is exposed to torture DoS attack [8].

4.4 DoS attacks based on Authorization-invalid (Auth-Invalid) message

The Auth-Invalid message is sent from the BS to the SS when the Authorization Key (AK) expires or the BS cannot verify the Hash-based Message Authentication Code/Cipher-based Message Authentication Code (HMAC/CMAC) properly. Since it is not protected by HMAC, it can be altered to invalidate a legitimate SS [8].

4.5 DoS attacks based on Reset Command (RES-CMD) message

The RES-CMD message in sent from the BS to the SS to reinitialize its MAC state machine when it is not responding properly or is malfunctioning .It is protected by HMAC; however, it is still vulnerable to DoS attacks [8].

5. Up to today Encryption Protocols

People have always looked for ways to protect their valuable information from others. In older times, they would either make a simple pattern change to an alphabet or substitute other letters or numbers into written messages to protect private information. Thus, began the age of cryptography. Encryption components may be different in each encryption algorithm but they are all meant to protect private information and provide access to those only for which the information was intended.

5.1 Overview:

A security protocol represents an abstract protocol which performs functions related to security and implements cryptographic methods. When data is encoded through encryption, then only computers having the appropriate decoder can read it and also use it. Encryption can be used by anyone who wants to safeguard files and electronic mails sent to friends and colleagues. The encryption key can tell the computer about what kind of computations are required for encrypting something or to decrypt something.

5.2 Comparison of existing encryption protocols:

IBM developed the Data Encryption Standard (DES) cipher which was approved as a federal standard in 1976. The Data Encryption Standard Algorithm (DEA), a simple Fiestel network block cipher, uses a 56 bit key length and 64 bit block size. DES cipher remained a standard among the U.S. Government and other governments around the world until it became possible to crack in less than twenty four hours using simple brute force attacks. Thus, DES is now considered outdated and less secure [10].

In order to improve on DES, IBM developed the Triple Data Encryption Standard (TDES) in the late 1970's. The Triple Data Encryption Algorithm (TDEA), which could be considered as three-times the DEA, replaces 64 bit keys used in DES with 192 bits. This longer key length provides an effective defence against a brute force attack and despite being theoretically crackable, it is not practical to crack TDES using modern technology [10]. Thus, a reputation of being fairly secure has made it a popular choice to process financial transactions.

Ron Rivest developed the "Rivest Cipher" or RC2 encryption algorithm in 1987 which uses a 64 bit block size and variable key length. RC2 was originally created for Lotus to be used in their Lotus Notes messaging software. RC2 was suited to its time and remained secret before becoming publicly available over the internet. RC2 can be cracked with 234 chosen plaintexts, thus, its status as a fairly easily cracked cipher makes it unsuitable for modern encryption needs [9].

Ron Rivest improved on RC2 with RC4, also known as ARC4 or ARCFOUR, where "A" stands for "alleged". RC4, a software stream cipher, is currently the standard encryption in many network protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [11]. Even though, it is considered "secure enough", it is vulnerable to crack due to not being consistently random for encryption purposes. Despite being better than RC2, RC4 is not suited to new applications which require higher levels of security.

Bruce Schneier developed the Blowfish cipher in 1993 which is a symmetric key block cipher that uses a 64 bit block size and variable key length. With key lengths between 32 bits and 448 bits, Blowfish is a very secure cipher but it is being replaced by Twofish and Rijndael due to its small 64 bit block size. Blowfish is one of the fastest block ciphers to date but does slow considerably when changing "keys" which is why it is not used in some applications. Created with the intention of unrestricted and unlimited use by anyone, Blowfish continues to remain in the public domain [2].

Bruce Schneier improved upon Blowfish with another encryption tool Twofish which is also a symmetric key block cipher but uses larger block size of 128 bits and variable key sizes up to 256 bits [2]. Though faster than Blowfish, Twofish is still slightly slower than Rijndael for 128 bit keys. But Twofish does have a speed advantage over Rijndael when it comes to 256 bit keys.

Though considered a very strong encryption algorithm, Twofish remains vulnerable to a truncated differential cryptanalysis attack despite not being broken yet.

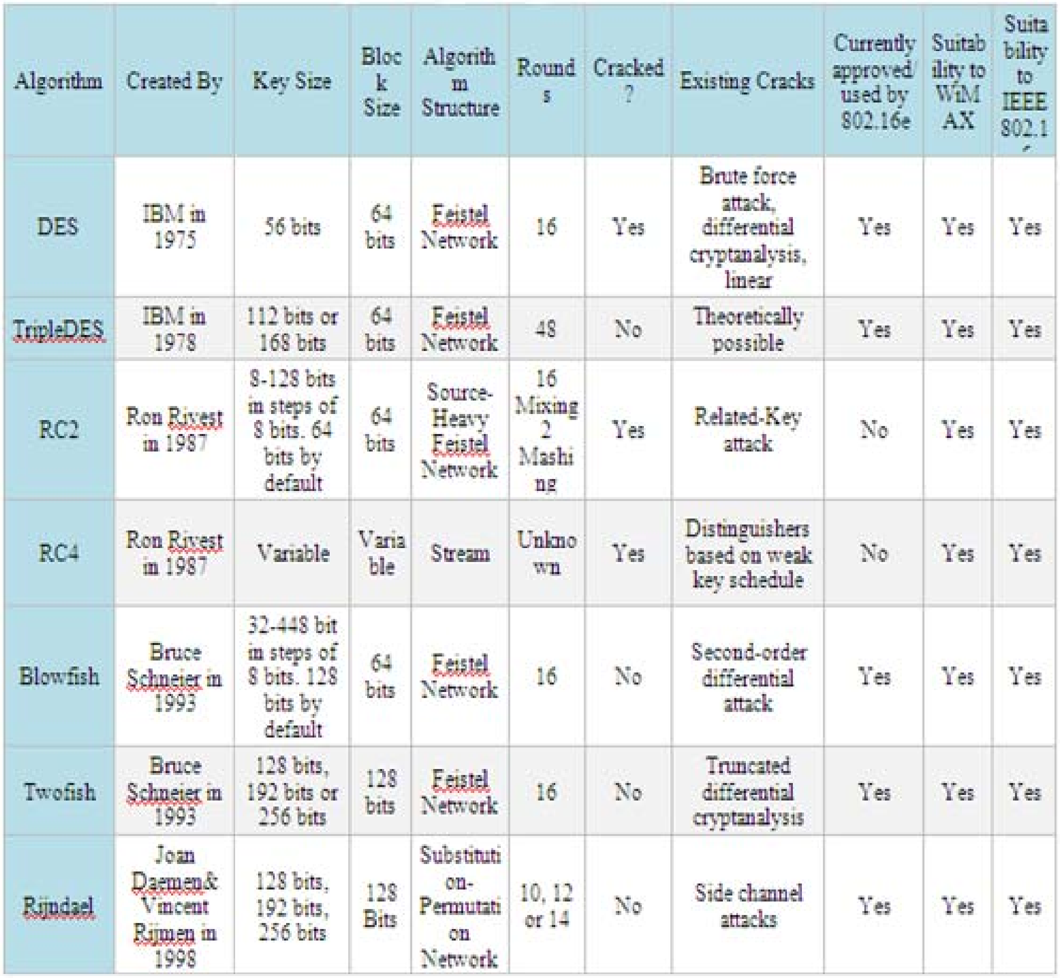
In 2002, the United States Government replaced outdated standard DES with Advanced Encryption Standard (AES) which is also known as Rijndael, named after Rijndael symmetric block cipher developed by two Belgian cryptographers Vincent Rijmen and Joan Daemen. Rijndael uses a block size of 128 bits with a variable key length of 128 bits to 256 bits [12]. Instead of Feistel Network which is used by DES and other ciphers, Rijndael uses a substitution-permutation network [3]. The substitution-permutation network not only makes Rijndael fast in both hardware and software applications and increases its appeal but Rijndael is also popular due to being easy to implement and requiring little memory.

The government uses Rijndael for both classified and non-classified information due to its reputation for being practically crack-proof. Though a crack is theoretically possible, the state of technology has not reached there yet. Brute force attacks have been ineffective against Rijndael so far. Side channel attacks, which target implementations of cipher rather than the cipher itself, indicate that a crack can only be effective if it runs on the same server where encryption is taking place.

Table 5.1 compares those popular encryption algorithms in term of their key size, block size, algorithm structure, rounds, whether they have been cracked or not, their existing cracks if any, whether they are approved by 802.16e, their suitability to be used in WiMAX, and their suitability to the IEEE 802.16 MAC and Physical Layers. It can be seen that the best ones in key size were the Blowfish, Twofish, and Rijndael algorithms. When it comes to bock size, the Twofish and Rijndael algorithms were the worst. It is obvious that most algorithms use the Feistel Network structure. The fastest algorithms were DES, RC2, Blowfish, Twofish, and Rijndael. It is noticeable that algorithms TripleDES, Blowfish, Twofish, and Rijndael are more secure as it has never been proven that they are able to be cracked. All algorithms are suitable to be used by IEEE 802.16e and its MAC & Physical Layers; however, the RC2 and RC4 algorithms are not yet approved/ used by IEEE 802.16e.

Hence, the need for various and proven secure algorithms are sought from authentication to Web browsing and emailing. The hopeful two methods that would offer an optimum overall solution to WiMAX security systems are the initial entry key protocol and firewall.

Table 5.1 Comparison of Popular Encryption Algorithms



Algorithm	Created By	Key Size	Block Size	Algorithm Structure	Rounds	Cracked ?	Existing Cracks	Currently approved/ used by 802.16e	Suitability to WiMAX	Suitability to IEEE 802.1
DES	IBM in 1975	56 bits	64 bits	Feistel Network	16	Yes	Brute force attack, differential cryptanalysis, linear	Yes	Yes	Yes
TripleDES	IBM in 1978	112 bits or 168 bits	64 bits	Feistel Network	48	No	Theoretically possible	Yes	Yes	Yes
RC2	Ron Rivest in 1987	8-128 bits in steps of 8 bits. 64 bits by default	64 bits	Source-Heavy Feistel Network	16 Mixing 2 Mashing	Yes	Related-Key attack	No	Yes	Yes
RC4	Ron Rivest in 1987	Variable	Variable	Stream	Unknown	Yes	Distinguishers based on weak key schedule	No	Yes	Yes
Blowfish	Bruce Schneier in 1993	32-448 bit in steps of 8 bits. 128 bits by default	64 bits	Feistel Network	16	No	Second-order differential attack	Yes	Yes	Yes
Twofish	Bruce Schneier in 1993	128 bits, 192 bits or 256 bits	128 bits	Feistel Network	16	No	Truncated differential cryptanalysis	Yes	Yes	Yes
Rijndael	Joan Daemen& Vincent Rijmen in 1998	128 bits, 192 bits, 256 bits	128 Bits	Substitution-Permutation Network	10, 12 or 14	No	Side channel attacks	Yes	Yes	Yes

Firewalls are used to block unwanted programs and websites. Firewalls behave as both firewalls and routers depending on the initial installation configuration. A firewall stops viruses and worms by blocking block ports used by them. A firewall can be configured with different policies which enable them to filter access to websites and firewall resources for different users within the network. Based on their router capabilities firewall can be used to configure virtual private networks (VPNs) which can be used to create a secure channel between networks thereby guaranteeing confidentiality of information exchanged these networks. Firewalls normally operate in the Network layer and Application layer; hence the connection has to be established before the firewall can come into the picture.

Assumption taken is that the Rogue base station is broadcasting bogus downlink map messages at a higher RSSi than the legitimate base station. During the initial setup of customer premises equipment of outdoor unit which is the antenna and the indoor unit which provides RJ45 ports for users to have access to the fixed and nomadic users, a firewall is installed with rules configured for allowing only legitimate base stations based on their IP addresses. The network diagram will be typically as shown in figure 5.1 below.

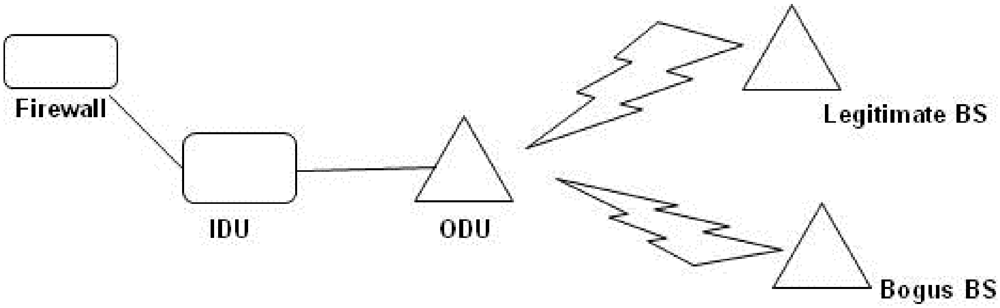


Figure 5.1: Firewall at Client's Premises

The rogue base station will flood the client with multiple bogus messages, transmitting at a higher RSSi than the legitimate base station once these packets get to the firewall the source will be identified based on the stored list of legitimate BS IP addresses and will be identified as invalid and a new scan is started for legitimate BS. This is an idea for basic DoS attacks, for more complex attacks it might be impossible for the firewall to detect the attack due to the layer in which they operate but they still provide good protection for any attacks that are made from behind the firewall. The installation of firewall at all clients' premises will mean more cost and hence the service will be more expensive for the client.This scenario is applicable to fixed and nomadic users but not for mobile users.

5.3 Securing Management Messages &Authentication in 802.16 WiMAX (SeMMAN)

This section looks at novel ways to secure the management messages. The certificate authority method of securing the management messages does not entail much extra financial investment except making sure the BS certificate is pre-installed in the MS device. The shared key alternative might involve additional database server for shared key verification involving slight extra cost which might be a factor for determining the cost of the service. The following two subsections briefly discuss the ranging with X.509 Certificate and ranging messages exchange with shared key protocol.

5.3.1SeMMAN Version A

The X.509 certificate for the required BS in the region can be installed in the MS on commissioning. The MS can send the selected ranging codes and its X.509 certificate based on the public key of the communicating BS retrieved from the BS's X.509 certificate. The BS can send subsequent messages encrypted with the MS's public key retrieved from the X.509 certificate it receives. The protocol is shown in Figure 5.2.

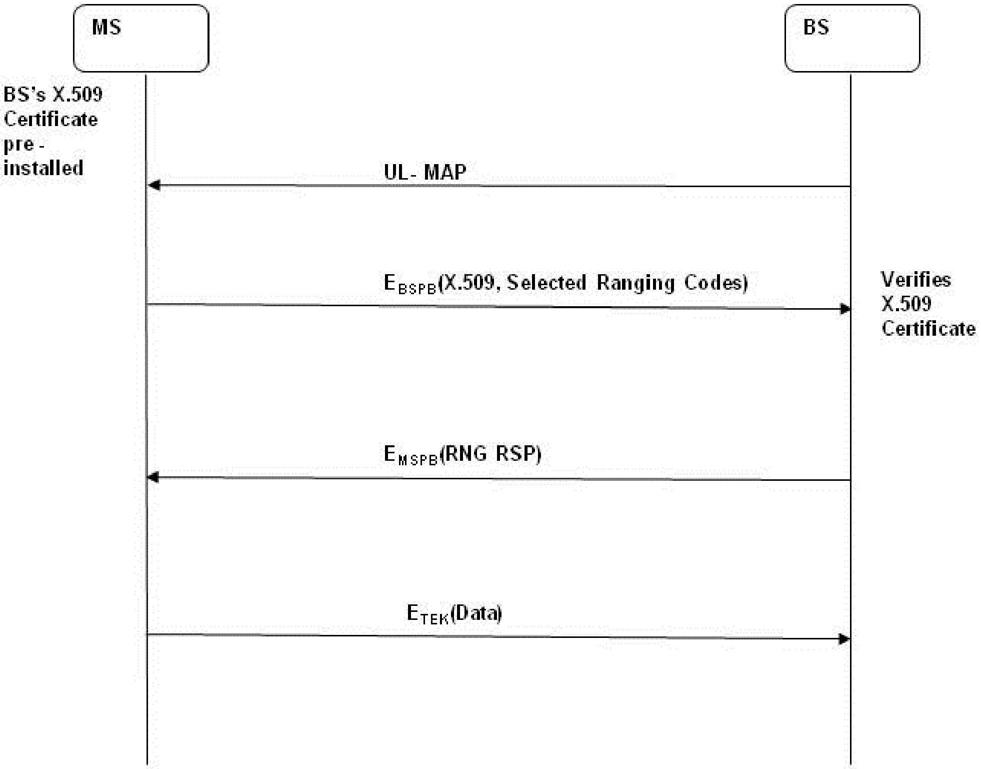

MS
BS
BS's X.509 Certificate pre - installed
UL- MAP
E_{BSPB}(X.509, Selected Ranging Codes)
Verifies X.509 Certificate
E_{MSPB}(RNG RSP)
E_{TEK}(Data)

Figure 5.2 Ranging with X.509 Certificate

Considering the mobility of the MS the X.509 certificate can be updated since automatically if it moves from one region to another by means of soft handover and identifying the base station via GPS since the communication is happening through a secured channel. The above protocol can be adopted with Authorization key and Key Generation Key, and Traffic Encryption Key being incorporated right from the management messages.

5.3.2 SeMMAN Version B

The initial encryption key could be generated by a function using the unique Mac address of the device and encrypt subsequent ranging messages with the key generated, the MS sends a RGN-REQ message a MAC function output and a nonce can be included to provide integrity and freshness. The BS can decrypt the message from a database of matching key which is identified by a function which gives identical encryption as the one received by an alleged valid device and is activated on a sever before commissioning of the client end device, the BS responds with a RNG-RSP message which includes a MAC and a nonce after verifying the integrity and freshness of the message sent by the MS. The protocol is as described in the Figure 5.3.

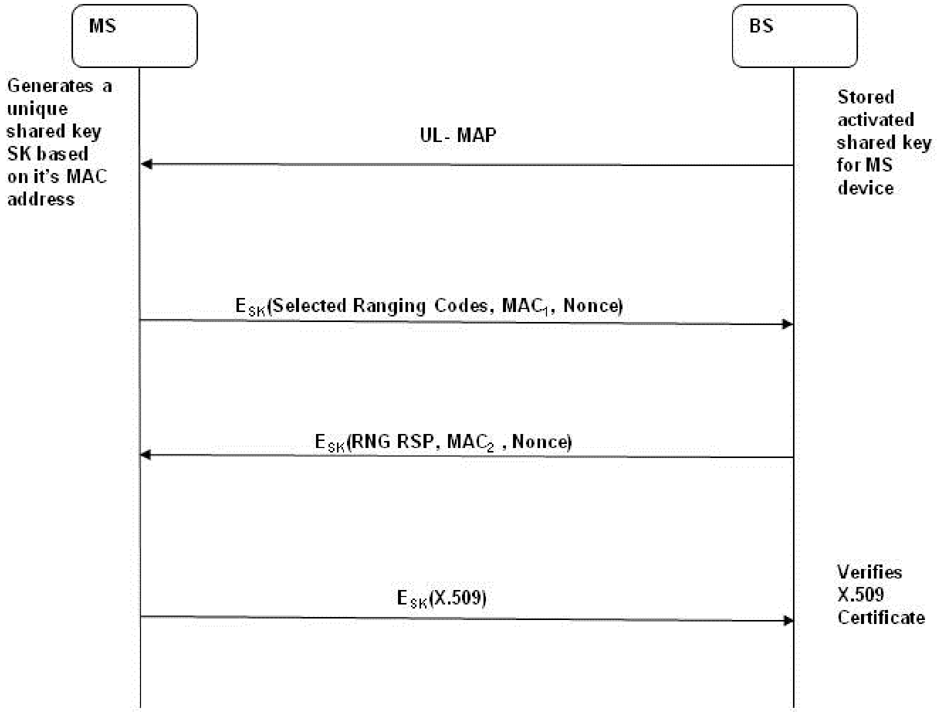

MS
BS
Generates a unique shared key SK based on it's MAC address
Stored activated shared key for MS device
UL- MAP
E_{SK}(Selected Ranging Codes, MAC_1, Nonce)
E_{SK}(RNG RSP, MAC_2 , Nonce)
E_{SK}(X.509)
Verifies X.509 Certificate

Figure 5.3 Ranging messages exchange with shared key protocol

On securely exchanging the management message, the X.509 certificate is exchanged with encryption by the shared key once the X.509 certificate is received the BS, it encrypts the authorization reply with the MS's public key. The MS upon receiving the reply continues the protocol as specified by the IEEE802.16 standard for exchange of authorization key AK, key encryption key KEK and traffic encryption keys TEKs. SeMMAN version B uses the AES cryptographic algorithm for encryption and decryption.

6. Conclusion

This paper has outlined WiMAX architecture and presented in detail the section that is vulnerable to attacks. It has identified DoS as one of the security threats that could degrade the quality of service that a WiMAX network can offer. DoS attacks can be reduced if some of the sources that make those attacks possible were eliminated or well protected from unauthorized access. This study has surveyed the current security methods and identified the Blowfish algorithm as the ideal one to be deployed with WiMAX to safeguard the messages used in a WiMAX network that are vulnerable to a DoS attack. A novel ways to secure the management messages have been outlined within this paper.

ACKNOWLEDGEMENTS

The authors would like to thank the UAE Police for sponsoring this publication!

References

[1] Ahson, Syed and Ilyas, Mohammad, (2008) “WiMAX Standards and Security”, Florida, CRC.

[2] Barrett, Daniel J, Silverman, Richard E. and Byrnes, Robert G., (2005) “SSH The Secure Shell”, California, O’reilly.

[3] Chang, William Y, (2007) “Network-Centric Service Oriented Enterprise”, Dordrecht, *Springer*.

[4] Chen, Kwang-Cheng, Roberto, and J. Marca, B. De, (2008),“Mobile WiMAX”, West Sussex, *Wiley*.

[5] Doe, Precious John, (2011). “How Secure Is WiMAX Technology”, Bright Hub, *[online].Available at<http://www.brighthub.com/computing/smb-security/articles/28129.aspx> [accessed 22 Dec 2012]*.

[6] Nuaymi, Loutfi, (2007), “WiMAX Technology for Broadband Wireless Access”, West Sussex: *Wiley*.

[7] NEC, (2012). “WiMAX Products”.*[online] Available at:<http://www.nec.com/en/global/solutions/nsp/WiMAX/products/index.html?> [Accessed 25 December 2012]*.

[8] Nguyen, Trung, (2009), “A survey of WiMAX security threats”, *Available at:< http://www.cse.wustl.edu/~jain/cse571-09/index.html >*

[9] Oppliger, Rolf, (2009). “SSL and TLS Theory and Practice”, Massachusetts, *Artech House.*

[10] Pachghare, V K, (2009). “Cryptography and Information Security”, Delhi, PHI.

[11] Paul, Goutam and Maitra, Subhamoy, (2012). “RC4 Stream Cipher and Its Variants”, Florida, CRC.

[12] Whitman, Michael E and Mattord, Herbert J, (2012),“Principles of Information Security”, Massachusetts, *Course Technology*.

Authors

Short Biography

Professor T Alukaidey is currently at the University of Hertfordshire leading research projects in security algorithms for 4G and 5G.