ISSN:0975-9646

A Journey on WiMAX and its Security Issues

Rakesh Kumar Jha[#1], Dr Upena D Dalal [#2]

[#]*Electronics and Communication Engineering Department, SVNIT*
Surat, Gujarat, India

Abstract— **Security has become a primary concern in order to provide protected communication in Wireless environment. We know the basic concept of communication is sent the information from source node to destination node but in my view the communication is not sent the information but the amount of secure information which is sent from source node to destination node. The much anticipated technology for wireless broadband access, the WiMAX (Wireless Interoperability for Microwave Access) is finally starting to be available in the market with the aim to provide high data rates and provide interoperability of vendor devices at the same time. In this report we give an overview on the different performance evaluations that have been conducted on WiMAX systems and show the current capabilities and future trends in the WiMAX technology. As a promising broadband wireless technology, WiMAX has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks in. This report is a survey of security vulnerabilities found in WiMAX network. Vulnerabilities and threats associated with both layers in WiMAX (Physical and MAC layers).**

Keywords— **WiMAX, Security Threats, Physical Layer, MAC Layer, Security Model, Towerstream, Authentication**

I. INTRODUCTION

This--Security has become a primary concern in order to pro-vide protected communication in Wireless environment .IEEE Standards Board in 1999 Established , the IEEE 802.16 is a working group on Broad Wireless Access (BWA).Developing standards for the global deployment of broadband Wireless Metropolitan Area Networks .In December 2001, the first 802.16 standard which was designed to specialize point to-multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised several times, the standard was ended in the final standard: 802.16-2004 which corresponds to revision D. These standards define the BWA for stationary and nomadic use which means that end devices cannot move between base stations (BS) but they can enter the network at different locations. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enables mobile stations (MB) to handover between BSs while communicating. This standard is often called “Mobile WiMAX7”’.The Fig provides a summary of the IEEE 802.16 family of standards. Based on the IEEE 802.16 standard, the WiMAX (Worldwide Inter-operability for Microwave Access) is “a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access”. The WiMAX is supported by the WiMAX forum, which is a non-profit organization formed to promote the adoption of WiMAX compatible products and services [1]. WiMAX is a very promising technology with many key features over other wireless technologies [2]. For instance, WiMAX network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc, and provides scalability and mobility with high data rates with NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMAX to achieve a maturity level and become a successful technology, more research on security threats and solution to these threats need to be conducted.

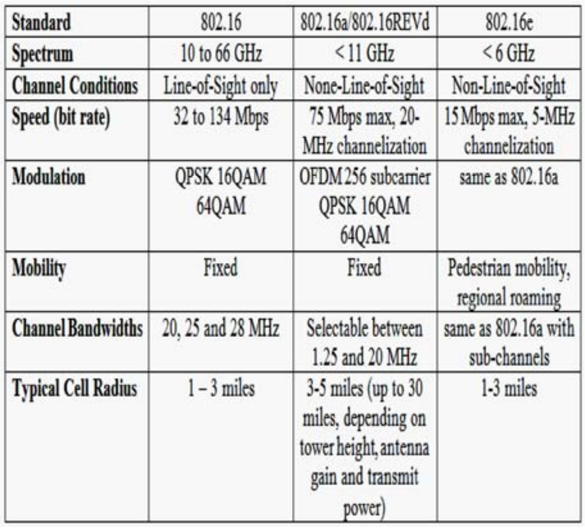
In the first section we are concentrate our study on security issue related to Physical Layer and Mac Layer. In the physical (PHY) layer, IEEE 802.16 supports four PHY specifications for the licensed bands. These four specifications are Wireless-MAN-SC (single carrier), OFDM (orthogonal frequency-division multiplexing), and OFDMA (orthogonal frequency-division multiple access). In addition, the standard also supports different PHY specifications (SC, OFDM, and OFDMA) for the unlicensed bands: wireless high-speed unlicensed MAN (Wireless HUMAN). Most PHYs are designed for non-line-of-sight (NLOS) operation in frequency bands below 11 GHz, except -SC, which is for operation in the 10-66 GHz frequency band. To support multiple subscribers, IEEE 802.16 supports both time-division duplex (TDD) and frequency-division duplex (FDD) operations. In the medium access control (MAC) layer, IEEE 802.16 supports two modes: point-to-multipoint (PMP) and mesh. The former organizes nodes into a cellular-like structure consisting of a base station (BS) and subscriber stations (SSs).The channels are divided into uplink (from SS to BS) and downlink (from BS to SS), and both uplink and downlink channels are shared among the SSs. PMP mode requires all SSs to be within the transmission range and clear line of sight (LOS) of the BS. On the other hand, in mesh mode an ad hoc network can be formed with all nodes acting as relaying routers in addition to their sender and receiver roles, although there may still be nodes that serve as BSs and provide backhaul connectivity. As a cost-effective solution, multihop communication is becoming more and more important to WiMAX system. To successfully deploy multihop WiMAX networks, security is one of the major challenges that must be addressed. Another important issue is how to support different services and applications in WiMAX networks. Since WiMAX is a relatively new standard, very little work has been conducted in the literature. In the authors provided a survey on the security schemes used in the IEEE 802.16-2001 standards. They further analysed the security flaws in the standard. Several improvements have been proposed since then. Nevertheless, we notice that the security mechanism of IEEE 802.16 is mainly focused on security in the MAC layer, which may not be able to provide sufficient security in multihop scenarios and satisfy the requirements of emerging applications in WiMAX networks.

II. WIMAX STANDARDS AND VERSIONS

Here i am describing a short table review for WiMAX technology standards and versions.

TABLE I

WIMAX STANDARDS AND VERSION SIZES FOR PAPERS



Standard	802.16	802.16a/802.16REVd	802.16e
Spectrum	10 to 66 GHz	< 11 GHz	< 6 GHz
Channel Conditions	Line-of-Sight only	None-Line-of-Sight	Non-Line-of-Sight
Speed (bit rate)	32 to 134 Mbps	75 Mbps max, 20-MHz channelization	15 Mbps max, 5-MHz channelization
Modulation	QPSK 16QAM 64QAM	OFDM 256 subcarrier QPSK 16QAM 64QAM	same as 802.16a
Mobility	Fixed	Fixed	Pedestrian mobility, regional roaming
Channel Bandwidths	20, 25 and 28 MHz	Selectable between 1.25 and 20 MHz	same as 802.16a with sub-channels
Typical Cell Radius	1 – 3 miles	3-5 miles (up to 30 miles, depending on tower height, antenna gain and transmit power)	1-3 miles

III. WIMAX: PROTOCOL ARCHITECTURE AND SECURITY SOLUTIONS

In order to understand WiMAX security issues, we first need to understand WiMAX architecture and how securities specifications are addressed in WiMAX. This section provides background and detailed information about WiMAX securities specifications in the security sub-layer.

A. *IEEE 802.16e protocol Architectures*

The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer [3] [4] and the Physical (PHY) [5][6] layer, as described in the **figure:1**. MAC layer consists of three sub-layers. The first sub-layer is the Service Specific Convergence Sub-layer (CS) [7], which maps higher level data services to MAC layer service flow [8] and connections [9]. The second sub-layer is Common Part Sub-layer (CPS), which is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocations and connection management. The MAC protocol data units are constructed in this sub-layer. The last sub-layer of MAC layer is the Security Sub-layer which lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers. The PHY layer provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals.

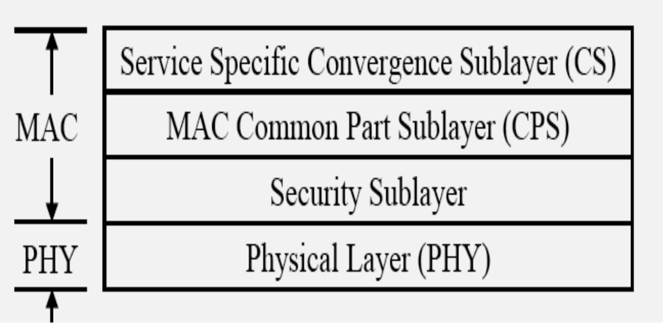

MAC
PHY
Service Specific Convergence Sublayer (CS)
MAC Common Part Sublayer (CPS)
Security Sublayer
Physical Layer (PHY)

FIGURE 1: THE IEEE 802.16 PROTOCOL STRUCTURE

B. *WiMAX security solutions*

By adopting the best technologies available today, the WiMAX, based on the IEEE 802.16e standard, provides strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization. In WiMAX, most of security issues are addressed and handled in the MAC security sub-layer as described in the **figure: 2** Two main entities in WiMAX, including Base Station (BS) and Subscriber Station (SS), are protected by the following WiMAX security features:

1) *Security association*: A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share [7]. Each SA has its own identifier SAID) and also contains a cryptographic suite identifier for selected algorithms), traffic encryption keys (TEKs) and initialization vectors.

2) *Public key infrastructure:* WiMAX uses the Privacy and Key Management Protocol (PKM) for secure key management, transfer and exchange between mobile stations. This protocol also authenticates an SS to a BS. The PKM protocol uses X.509 digital certificates, RSA (Rivest -Shamir-Adleman) public-key algorithm and a strong encryption algorithm (Advanced Encryption Standard - AES). The initial draft version of WiMAX uses PKMv1 which is a one-way authentication method and has a risk for Man-in-the-middle (MITM) attack. To deal with this issue, in the later version (802.16e), the PKMv2 was used to provide two-way authentication mechanism. The **figure: 3** provide an overview of public key infrastructure in WiMAX.

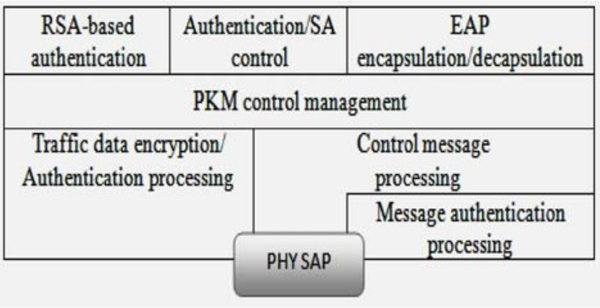

RSA-based authentication
Authentication/SA control
EAP encapsulation/decapsulation
PKM control management
Traffic data encryption/ Authentication processing
Control message processing
Message authentication processing
PHY SAP

FIGURE 2: MAC SECURITY SUB-LAYER

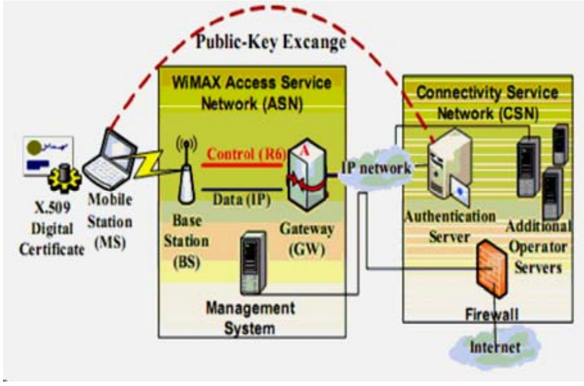


FIGURE 3: PUBLIC KEY INFRASTRUCTURE IN WIMAX [06]

C. Device/User Authentication

Generally, WiMAX supports three types of authentication which are handled in the security sub-layer. The first type is RSA-based authentication which applies X.509 certificates together with RSA encryption. The X.509 certificate is issued by the SS manufacturer and contains the SS's public key (PK) and its MAC address. When requesting an Authorization Key (AK), the SS sends its digital certificate to the BS, the BS validates the certificate, and then uses the verified PK to encrypt an AK and pass it to the SS the second type is EAP (Extensive Authentication Protocol) based authentication in which the SS is authenticated by an X.509 certificate or by a unique operator-issued credential such as a SIM, USIM or even by user-name/password. The network operator can choose one of three types of EAP EAP-AKA (Authentication and Key Agreement), EAP-TLS (Transport Layer Security) and EAP-TTLS MS-CHAP v2 Tunnelled Transport Layer Security with Microsoft Challenge Handshake Authentication Protocol version 2). The third type of authentication that the security sub-layer supports is the RSA-based authentication followed by EAP authentication. The **figure: 4** provide details of EAP based authentication.

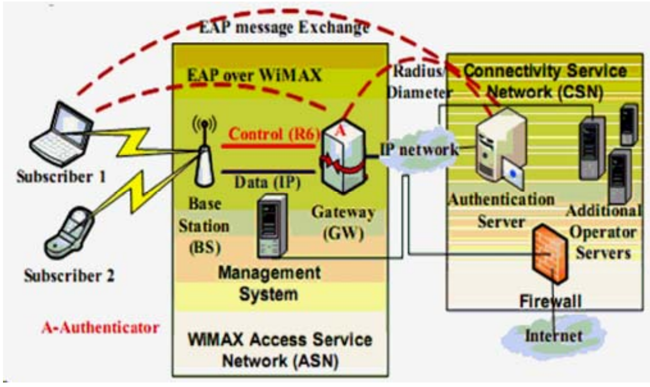


FIGURE 4: EAP-BASED AUTHENTICATION [7].

D. Authorization

The authentication process is the authorization process in which SS requests for an AK and a SAID from BS by sending an Authorization Request message. This message contains SS X.509 certificate, encryption algorithms and cryptographic ID. The BS then interacts with an AAA (Authentication, Authorization and Accounting) server to validate the request from the SS, and sends back an Authorization Reply which includes the AK encrypted with the SS's public key, a lifetime key and an SAIS.WiMAX adopts the AES algorithm for encryption. "The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A sets of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key" [3]. Since DES is no more secure enough, AES is recomended in WiMAX with many supported modes: CCM-Mode and ECB-Mode (in IEEE 802.16-2004), CBC-Mode, CTR-Mode, AES-Key-Wrap. WiMAX has been designed carefully with security concerns but it is still vulnerable to various attacks. The following section will present these security issues in WiMAX.

IV. WIMAX SECURITY THREATS

WiMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack including interception, fabrication, modification, and replay attacks [7].

Some vulnerabilities of WiMAX originate from flaws of IEEE 802.16 on which WiMAX is based. A lot of problems and flaws have been fixed in the enhanced version but WiMAX still has some exposes. In this section some possible threats or vulnerabilities will be reviewed.

A. *Threats to the PHY layer*

As described in 2.1, WiMAX security is implemented in the security sub-layer which is above the PHY layer. Therefore the PHY is unsecure [6] and it is not protected from attacks targeting at the inherent vulnerability of wireless links such as jamming, scrambling or water torture attack. WiMAX supports mobility, thus it is more vulnerable to these attacks because the attackers do not need to reside in a fixed place and the monitoring solutions presented below will be more difficult.

1) Jamming attack: Jamming is described by M. Barbeau as an attack "achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel" [6]. 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 and there is even a book by Poisel [10] which teaches jamming techniques.

2) Scrambling attack: Also described in [5], scrambling is a kind of jamming but only provoked for short intervals of time and targeted to specific WiMAX frames or parts of frames at the PHY layer. Attackers can selectively scramble control or management information in order to affect the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more difficult to perform an 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" [5].

3) Water torture attack: According to D. Johnson and J. Walker [3], this is also a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources.

4) Other threats: In addition to threats from jamming, scrambling and water torture attacks, 802.16 is also vulnerable to other attacks such as forgery attacks in which an attacker with an adequate radio transmitter can write to a wireless channel [3]. In mesh mode, 802.16 is also vulnerable to replay attacks in which an attacker resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process

V. THREATS TO THE MAC LAYER

This section begins with an overview of the WiMAX/802.16 MAC layer, including a description of its connections, the process used by an MS for joining the network, and the MAC security model. We then proceed to discuss the threats to confidentiality and authentication.

MAC Layer Connections: The MAC layer is connection oriented. There are two kinds of connections: management connections and data transport connections. Management connections are of three types: basic, primary, and secondary. A basic connection is created for each MS when it joins the network and is used for short and urgent management messages. The primary connection is also created for each MS at the network entry time, but is used for delay-tolerant management messages. The third management connection, the secondary one, is used for IP encapsulated management messages (e.g., dynamic host configuration protocol [DHCP], simple network management protocol [SNMP], trivial file transfer protocol [TFP]). Transport connections can be provisioned or can be established on demand. They are used for user traffic flows. Unicast or multicast can be used for transmission.

A. *Network Entry*

The network entry of an MS consists of the following Steps:

(i)Downlink, Scanning and synchronization with a BS.
(ii) Downlink and uplink description acquisition; available uplink channel discovery.
(iii) Ranging.
(iv) Capability negotiation.
(v) Authorization, authentication, and key establishment.
(vi) Registration.

During scanning, the MS looks for downlink signals by going through the available frequencies and searches for downlink subframes. Whenever a channel is found, the MS gets the downlink and uplink description. It obtains the downlink map and uplink map in the PHY frame headers, and these maps describe the structure of the subframes in terms of bursts. The downlink/uplink channel descriptors are obtained as MAC management messages, and they describe the properties of the bursts in terms of data rate and error correction. During ranging, the MS synchronizes its clock with the BS and determines the level of power required to communicate with the BS. Ranging is done using a special channel called the ranging interval, which uses contention-based multiple access. The basic connection and primary connection are assigned during ranging. Capabilities (e.g., the supported security algorithms) are negotiated on the basic connection.

Authorization and authentication can be device list based, X.509 certificate based, or EAP based. This is discussed in more detail below. The registration step results in the establishment of a secondary management connection and provisioned connections.

B. Security Model

The security keys and associations established between an MS and a BS during the authorization step at network entry are discussed in this section. A MAC layer PDU consists of a MAC header, a payload, and an optional cyclic redundancy check (CRC). The payload may consist of user traffic or management messages. The MAC header contains a flag, which indicates whether the payload of the PDU is encrypted or not. MAC headers themselves are not encrypted, and all MAC management messages are sent in the clear. According to the standard, this facilitates the operation of the MAC layer. A security association (SA) is a concept that captures the security parameters of a connection: keys and selected encryption algorithms. The basic and primary management connections do not have SAs, although the integrity of management messages can be secured, as discussed below. The secondary management connection can have, on an optional basis, an SA. Transport connections always have SAs. Each transport connection, a term used to refer to a MAC layer connection dedicated to user traffic, has either one SA for both the uplink and downlink, or two SAs, one for the uplink and another for the downlink. The security model is depicted in **figure: 6** rectangles depict entities; lines represent relations with cardinalities at the termination points; pre-existing elements are shown with solid lines; and dynamically established elements are shown using dashed lines. There are three types of SAs: the primary SA, static SA, and dynamic SA. Each SA has an identifier (SAID). It also contains a cryptographic suite identifier (selected algorithms), traffic encryption keys (TEKs), and initialization vectors. There is one primary SA for each MS. The primary SA is established when the MS is initialized. The scope of the primary SA is the secondary management connection, and it is shared exclusively between an MS and its BS. Static SAs are created by the BS during the initialization of an MS. For example, there is a static SA for the basic unicast service. However, an MS may have subscribed to additional services, and there are as many additional static SAs as there are subscribed additional services. Dynamic SAs are created dynamically when new traffic flows are opened and they are destroyed when their flow is terminated. Static SAs and dynamic SAs can be shared among several MSs, for example, when multicast is used.

Core security data entities are the X.509 certificate, authorization key (AK), key encryption Key (KEK), and hashed message authentication code (HMAC) key (message authentication key). Every MS is preconfigured with an X.509 certificate. The X.509 certificate is persistent and contains the public key (PK) of the MS. The MS uses it for its authentication with the BS. All other keys are established during authorization, and they are subject to an aging process, so they must be refreshed on a periodic basis through reauthorization. The BS determines the AK, which is encrypted using the PK, and passes it to the MS. The AK has a sequence number (from 0 to 15) and a lifetime. For the purpose of smooth transitions, two AKs may be simultaneously active with overlapping lifetime. The lifetime of an AK ranges from 1 to 70 days, with a default value of 7 days. The MS uses the AK to determine the KEK and HMAC key. The sequence number of the AK implicitly belongs to the HMAC keys as well. KEKs are used to encrypt TEKs during their transfer.

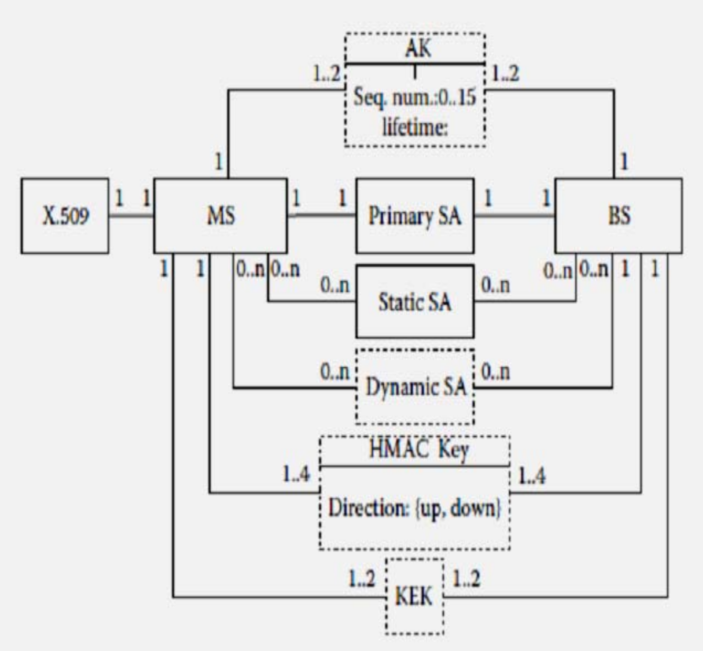


FIGURE: 6 Security Model

C. Threats to Confidentiality

The format of the MAC PDU payload is depicted in **figure:7** When applicable, before encryption, each packet is given a unique identifier as a new four-byte packet number which is increased from one data unit to another. Note that, for the sake of uniqueness, there are separate ranges of values for the uplink and downlink packets. The IEEE 802.16e standard uses Data Encryption Standard (DES) in the CBC mode or advanced encryption standard (AES) in the CCM mode to encrypt the payload of MAC PDUs. This standard introduces an integrity protection mechanism for data traffic which did not previously exist. CBC-MAC (as a component of AES-CCM) is used to protect the integrity of the payload of MAC data units.

D. Data privacy and integrity

In **figure: 8** provide values for the eavesdropping threat, first for management messages, then for user traffic. Management messages, which are never encrypted, can provide valuable information to an attacker, for example, to verify the presence of a victim at his location before perpetrating a crime. This provides a high motivation for an attacker. The messages can be intercepted by a passive listener within communication range, so there are no serious technical difficulties to resolve by an attacker. The threat is therefore likely to occur. From the user perspective, eavesdropping of management messages may result in limited financial loss if a crime is committed, resulting in an attack of medium impact. From the point of view of a system, eavesdropping in itself may not create outages, but it might be used by a competitor to map the network, making it a threat of high impact. Hence eavesdropping of management messages is a major threat for users and a critical one for a system.

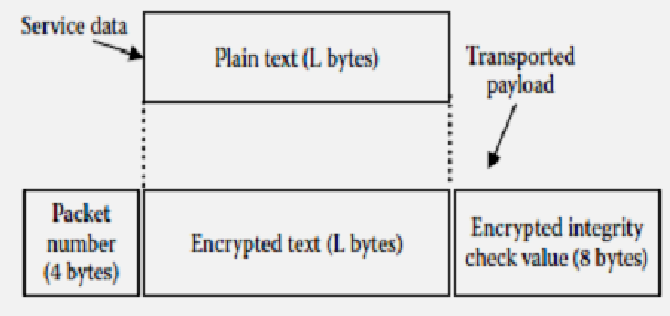
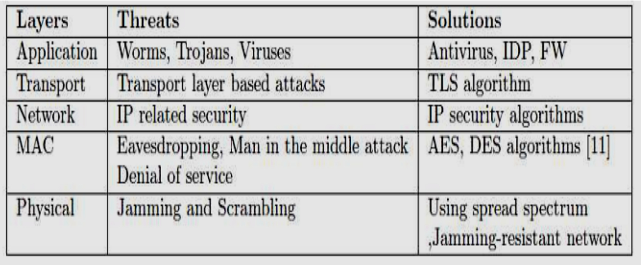


FIGURE: 7 MAC layer PDU payload format



Layers	Threats	Solutions
Application	Worms, Trojans, Viruses	Antivirus, IDP, FW
Transport	Transport layer based attacks	TLS algorithm
Network	IP related security	IP security algorithms
MAC	Eavesdropping, Man in the middle attack Denial of service	AES, DES algorithms [11]
Physical	Jamming and Scrambling	Using spread spectrum ,Jamming-resistant network

FIGURE: 8 Analysis Summaries from the User and System Points of View

E. Data privacy and integrity

Eavesdropping of data traffic is an unlikely threat because of the strong security measures provided by encryption, which presently pose unsurmountable technical difficulties. As a result, the threat is minor to both users and the system, and there is no need for countermeasures.

F. Threats to Authentication

The IEEE 802.16 standard states that identity can be verified via the X.509 digital certificate. This wording suggests that it is possible to disregard the X.509 certificate and base access control on a predetermined list of devices. In this case, a BS grants network entry only to MSs featured on a preconfigured list, while an MS is configured with its network identifier and joins a BS only if it belongs to that network.

Any weakness in authentication is an enabler for the BS or MS masquerading threat, which may result in important gains for an attacker in terms of misappropriation of resources such as air time from another user or from a system. We therefore rate the attacker’s motivation as high. Specific techniques for this threat include identity theft and the rogue BS attack there are three options for authentication: device list based, X.509 based, or EAP based. If only device list-based authentication is used, identity theft by device address reprogramming is greatly facilitated, and the likelihood of a BS or MS masquerading attack is likely because there are few technical difficulties to solve. The impact for a user is high because it can lead to a loss of service for long periods of time and the user can be billed for another user’s communication fee. The impact for a system is medium because it can lead to limited financial loss or theft of resources. The risk is therefore critical for a user and major for a system, and there is the need for countermeasures. Authentication of traffic messages also presents a moderate motivation for an attacker because it is an attack rooted in creating mischief.

The modification of data traffic is very unlikely to occur if AES is used because of the strong technical difficulties encountered and possible if AES is not used, given the lack of technical difficulty in carrying out an attack. We believe that 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. There is the potential for denial of service (DoS) attacks based on the fact that authentication operations of devices, users, and messages trigger the execution of long procedures. A DoS attack can be perpetrated by flooding a victim with a large number of messages to authenticate. With a moderate motivation on the part of the attacker bent on creating mischief, and with little technical difficulty to solve, this threat is possible. The impact is medium for a system, but could be high for a user because of lower computational resources available for handling a large influx of invalid messages. The DoS threat is therefore assessed as major for both the user and the system.

VI. TOWERSTREAM’S WIRELESS NETWORK [10]

Towerstream deploys a combination of Fixed Wireless Networks and WiMAX (802.16e). Fixed Wireless Networks have been in production since the 1970s. They were primarily used for backhaul in voice networks for phone companies, government agencies, etc.

One of the most popular questions is; "If the technology is so old, why you are still using it?" Similar to computers, the changes in size, speed and power have been dramatic. Radio's that once could once only push 1.5Mbs of traffic with eight foot antennas can now push a Gigabit of traffic attached to a one foot antenna.

1) *Towerstream's RF Security [11]:*

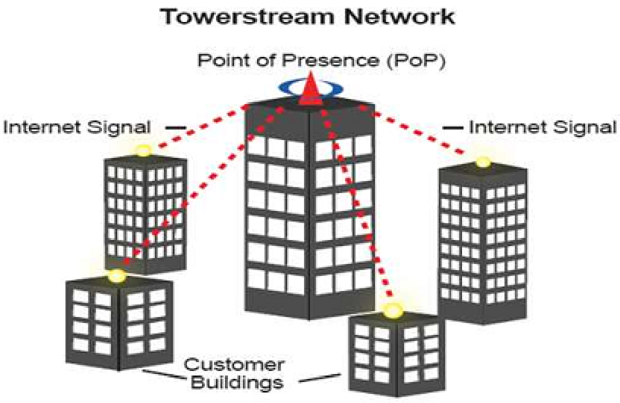


FIGURE: 9 Towerstream Network

A. Line of Sight

Unlike WiFi, the Towerstream RF devices do not advertise Service Set Identifiers (SSID's). Towerstream does not broadcast a frequency in 360 degrees. Towerstream service is considered "Line of Sight" (LOS). This means that a customer's antenna has to be pointed at a Towerstream facility and the corresponding Towerstream antenna has to be pointed at the customer. In order to interfere or intercept a signal, a potential intruder would have to be directly in that "Line of Sight". The intruder would have to have two antennas, one for each receiving end. Practically, an intruder would have to be hundreds of feet in the air to be in both data paths. Even if the data could be captured and stored, the radio manufacturers utilize proprietary communication protocols at the RF layer. These proprietary modulation and protocol schemes make it virtually impossible to decipher even if the data is captured.

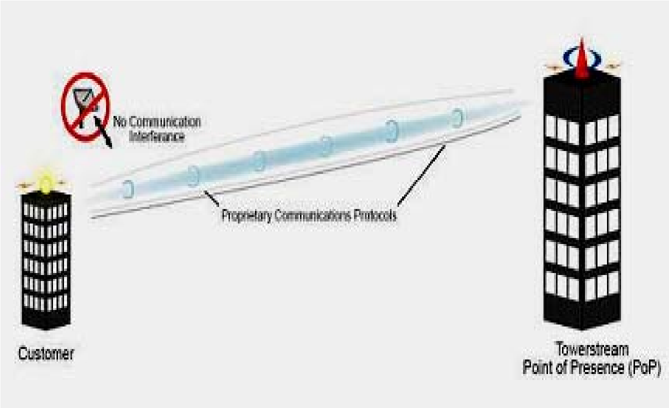

No Communication Interferance
Proprietary Communications Protocols
Customer
Towerstream Point of Presence (PoP)

FIGURE 10: Line of sight Communication.

B. Signal Theft

One of the most common questions is: "If a person was to obtain equipment from the manufacturer, would they be able to compromise the infrastructure and/or steal service." The short answer is, "No". First, each piece of equipment is provisioned with a Towerstream link identifier. Secondly, every radio has a manufacturer specific identifier "burned-in" by the manufacturer. This can never be changed. Without both sets of ID's matching, communication between the devices cannot occur.

C. Physical Security

All of Towerstream facilities are controlled access properties. Since the majority of our infrastructure is on roof tops, this is arguably the most difficult area of a building to compromise in this post 9-11 era. Since Towerstream's signal is out in the airwaves, the service cannot be compromised by a manmade disaster such as a broken telephone pole or a compromised street conduit. Comparatively, the customer side can be considered just as secure. For example, a typical T-1 generally terminates in a shared phone closet before it gets to the customer. Towerstream normally brings it service directly to the customer location bypassing common areas.

VII. CONCLUSION

In paper report, security solution, various vulnerabilities and possible attacks to WiMAX network have been discussed and illustrated. The threats apply to both layers of WiMAX. At PHY layers, jamming can be considered a major threat. At MAC layer, critical threats include eavesdropping of management messages, masquerading, management message modification or DoS attacks. Some of these issues have been fixed with the adoption of recent amendments and security solutions in IEEE 802.16 but some still exist and need to be considered carefully. However, through this review, we can see that WiMAX does offer much more strong security solutions in comparison with other wireless technologies such as Bluetooth or Wireless Fidelity (WiFi). WiMAX is still under development and need more research on its securities vulnerabilities. In the near future, when WiMAX achieves a maturity level, it would have a great opportunity to be a successful wireless communication technology.

VIII. FUTURE RESEARCH

In this paper we have described many security issues and solution till our researchers was given but the area of security in WiMAX has many issues which need to be resolved in the future. As our WiMAX network will reach all over world by 2012 than in that case our responsibility also increase how we can provide maximum data rate with maximum security. In this report, we have focused on the security issues related to Physical Layer, Mac Layer and lastly on-going project on Towerstream's RF Security. In my view in this area all security issues in Initial condition a lot of work we can do in the future. We are thinking research in following security issues with respect to above research. An analysis of the threats to the security of WiMAX/802.16 broadband wireless access networks was conducted. Critical threats consist of eavesdropping of management messages and BS masquerading. Major threats include jamming, MS masquerading, management message and data traffic modification, and DoS attacks. Countermeasures need to be devised for networks using the security options with critical or major risks. An intrusion detection system approach can be eve loped to address some of the threats, but more research is needed in this direction.

REFERENCES

[1] M. Barbeau, "WiMAX/802.16 threat analysis," in Proceedings of the 1st ACM international workshop on Quality of service security in wireless and mobile networks, Quebec, June 2005 .

[2] J. K. T. T. Andreas Deininger, Shinsaku Kiyomoto, "Security vulnerabilities and solutions in mobile wimax," vol. 7, no. 11, Nov 2007.

[3] M. E.-H. A. E.-H. Mahmoud Narsreldin, Heba Aslan, "Wimax security," in 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1335–1340.

[4] W. C. Taeshik Shon, "An analysis of mobile wimax security: Vulnerabilities and solutions," in Lecture notes in computer science, Springer, 2007

[5] R. Poisel, "Modern communications jamming principles and techinques," in Artech House Publishers, 2003.

[6] A. A. Ayesha Altaf, Rabia Sirhindi, "A novel approach against dos attacks in wimax authentication using visual cryptography," in The Second International Conference on Emerging Security Information, Systems and Technologies, securware, Cap Esterel, France, 2008.

[7] D. Park, in A Study of Packet Analysis regarding a DoS Attack in iBro Environments, vol. 8, no. 12.

[8] M. E.-H. A. E.-H. Mahmoud Nasreldin, Heba Aslan, "22nd international conference on advanced information networking and applications," in WiMAX Security, 2008.

[9] S.-G. H. Juan Li, "The 17th annual ieee international symposium on personal, indoor and mobile radio communications (pimrc06)," in Performance of IEEE 802.16 Based System in Jamming Environment and Its Improvement With Link Adaption, May 2006.

[10] B. Makarevitch, "communications laboratory helsinki university of tech-nology," in Jamming Resistant Architecture for WiMAX Mesh Network,Sep 2007.

[11] L. Cuilan, "Department of electronics jiangxi university of finance and economics nanchang," in A Simple Encryption Scheme Based on WiMAX, vol. 35, no. 5, Sep 2009, pp. 712–721

[12] RakeshKumarJha, U.D.Dalal SVNIT, Surat,India"WiMAX System Simulation and Performance Analysis under the Influence of Jamming". WET-Scientific Research, Vol 1, July 2010, pp 20-26

Mr. Jha Rakesh.

Mr. Jha Rakesh presently is full time Research Scholar at S. V. National Institute of Technology, Surat, INDIA. He has completed his B.Tech. (Hons in Electronics) from Bhopal and obtained M.Tech. (Wireless Communications) from NIT, Jalandhar, India.He have done live project in development and support both in Industries also. He has published many conferences and journal papers at national and international level including Scientific Research Journal. His one concept related to Router of Wireless Communication is accepted by ITU (International Telecommunication Union).He is now pursuing PhD in S. V. National Institute of Technology, Surat, INDIA. Surat. His research interest's area is Wireless and Optical Communication. Currently he is doing his research work in WiMAX and its Security issues. He is working on OPNET simulation and NS2 tools for Wireless Communication. Free to contact:jharakesh.45@gmail.com, https://sites.google.com/site/jharakeshnetworkcom/

Dr. (Mrs.) U. D. Dalal presently working as Associate Professor in Electronics Engineering Department of S. V. National Institute of Technology, Surat, INDIA. She has 18 years of academic experience. She completed her B.E. (Electronics) from SVRCET, Surat in 1991 and obtained M.E. (Electronics & Communications) from DDIT, Gujarat with Gold Medal. She is also awarded with 5th N.V. Gadadhar memorial Award by IETE. She has published many conference and journal papers at national and international level. She has guided many UG and PG projects, dissertations and seminars in the area of advance communication systems. She has completed Ph.D. in 2009 and guides 9 research scholars presently. Her book on "Wireless Communication" is published by Oxford University Press in July 2009. One more book edited by her and Dr Y P Kosta titled "WiMAX New Developments" is published by Inteh, Vienna, Austria. She is honored by "Rashtriya Gaurav Award" by India International Friendship Society. Recently she is received Best Technical Woman award by Divyabhaskar.