Security Issues of IEEE 802.16 Standard and Design Challenges

[1]Sheetal Kumar Dixit, [2]Amit Prajapati

[1]Assistant Professor, Computer Engineering, Mehsana, Gujarat, India
[2-]Programmer, CE/IT Engineering, Mehsana, Gujarat, India
[1,2]UVPCE, Ganpat University, Mehsana, Gujarat, India

***Abstract*: This article focuses on the privacy aspects of the IEEE 802.16 standard and point out the security issues combined with MAC , physical layer of WiMAX and also key management protocols and Design Challenges. Recently, Satisfy the growing demand of broadband wireless access by using resource of bandwidth is a large issue for researchers, that's why worldwide interpretability for microwave access emerged as a better solution. It provides fast internet connectivity in urban areas as well as rural areas. IEEE 802.16 is a standard used for authentication and authorization**

***Keywords*: IEEE 802.16, WiMAX, Authentication, Authorization, Security mechanism.**

I. INTRODUCTION

In broadways main purpose of WiMAX technology is to provide fast and reliable internet connectivity among huge number of subscribers with limited existing bandwidth and to accomplished that work the effective utilization of radio resources are required The scheduling algorithm is one of the way not only efficient utilization of radio resources but also satisfied the QoS requirements. WiMAX has the potential to do to broadband Internet access what cell phones have done to phone access. In the same way that many people have given up their "land lines" in favor of cell phones, WiMAX could replace cable and DSL services, providing universal Internet access. WiMAX (World Wide Interpretability for Microwave Access) is most prominent choice for Broadband Wireless Access (BWA) in metropolitan Area because of its unique qualities like effective recourses utilization and Adaptive modulation and coding . it is a better alternative approach against DSL (Digital Subscriber Line) and cable modem. The IEE 802.16 is a standard that defines the various family of broadband wireless radio interface. Theoretically, a WiMAX base station can provide broadband wireless access in range upto30 miles(50kms) for fixed stations and 3 to 10 miles (5 to 15 kms) for mobile station with a maximum data rate up to 70 mbps as compare to IEEE 802.11a with 54 Mbps up to several hundred meters. WiMAX technology defines the layer 1 as physical layer and layer2 is defined as MAC (medium access control layer) of OSI's seven layer model. The purpose of this research paper is to identify:

- Work with existing studies relate to WiMAX, network issues and commonly encountered problems.
- This paper is focusing on various security issues and their designing challenges.
- It shows a new challanges that overcomes the drawbacks of existing WiMAX algorithms to provide better solutions than the former.

WiMAX : How it works: It is a telecommunications technology that provides wireless transsmission of data using a variety of transmission modes, from point-to-multipoint links to portable and mobile internet access". 802.16/WiMAX: Protocol Architecture and protection solutions: - IEEE 802.16 Protocol Architecture is planned into two main layers : the Media Access Control (MAC) Layer and the Physical(PHY) layer , as describe in the following figure.

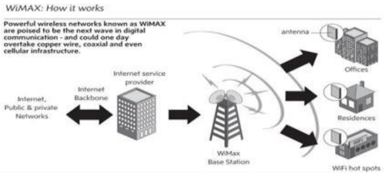

WiMAX: How it works
Powerful wireless networks known as WiMAX are poised to be the next wave in digital communication - and could one day overtake copper wire, coaxial and even cellular infrastructure.
Internet, Public & private Networks
Internet Backbone
Internet service provider
WiMax Base Station
antenna
Offices
Residences
WiFi hot spots

Figure 1: WiMAX working

MAC layer consists of three sub-layers. The first sub-layer is the Service Convergence Sub-Layer(CS)

The second sub-layer is Common Part Sub-Layer, 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 allocation and also connection management.

The very last sub-layer of MAC layer is the Security Sub-Layer which is associated in 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.

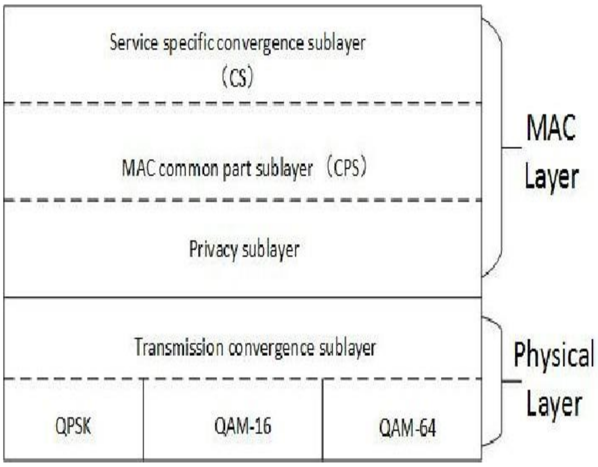

Service specific convergence sublayer
(CS)
MAC common part sublayer (CPS)
Privacy sublayer
MAC
Layer
Transmission convergence sublayer
QPSK
QAM-16
QAM-64
Physical
Layer

Figure 2: IEEE802.16 MAC and Physical Layer

The main problems with broadband access are that it is pretty expensive and it doesn't reach all areas. The main problem with WiFi access is that hot spots are very small, so coverage is sparse.

- What if there were a new technology that solved all of these problems? This new technology would provide:
- The high speed of broadband service
- Wireless rather than wired access, so it would be a lot less expensive than cable or DSL and much easier to extend to suburban and rural areas
- Broad coverage like the cell phone network instead of small WiFi hotspots
- The fastest WiFi connection can transmit up to 54 megabits per second under optimal conditions. WiMAX should be able to handle up to 70 megabits per second. Even once that 70 megabits is split up between several dozen businesses or a few hundred home users, it will provide at least the equivalent of cable-modem transfer rates to each user.

The biggest difference isn't speed; it's distance. WiMAX outdistances WiFi by miles. WiFi's range is about 100 feet (30 m). WiMAX will blanket a radius of 30 miles (50 km) with wireless access. The increased range is due to the frequencies used and the power of the transmitter. Of course, at that distance, terrain, weather and large buildings will act to reduce the maximum range in some circumstances, but the potential is there to cover huge tracts of land.

Coverage and Speed

The WiMax network operates similarly to a Wi-Fi connection, but with a few key differences. The system has two main components: A WiMax tower and a WiMax receiver. Like Wi-Fi, WiMax can connect directly to the Internet by sending a signal from a WiMax tower to a WiMax-enabled computer via a wired connection. A WiMax tower, however, can also connect to a second tower — this is what allows the network to provide long-range wireless service. WiMax transmiters can cover an estimated 30-mile radius whereas Wi-Fi’s range is about 100 feet. In other words, WiMax turns many small, scattered hot spots into one huge wireless hot spot.

WiMAX protocol stack:

This describes wimax protocol stack with functions of each in the system, which include wimax physical layer,WiMAX MAC layer and upper layers.

Physical layer

WiMAX physical layer are of five types viz. SC,SCa,HUMAN,OFDM and OFDMA as decribed in IEEE 802.16-2004/802.16e standards. Any one out of these will be used in the system. For example fixed wimax uses OFDM type of physical layer and mobile wimax uses OFDMA type. For more on OFDM and OFDMA refer following links.

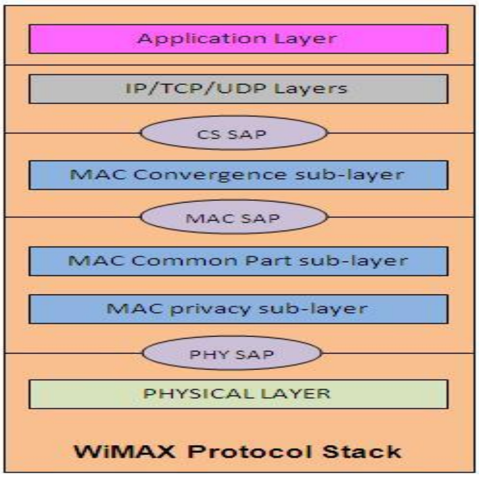


Figure 3. WiMAX protocol Stack

Physical layer takes MAC PDU consisting of MAC GMH, MAC payload and CRC and perform following functions.
1. Scrambling
2. Forward error correction
3. Interleaving
4. Modulation
5. IFFT
6. Cyclic prefix insertion
7. Pass the IQ data to RF module for radio frequency

MAC layer
MAC layer consists of three sub layers viz. MAC privacy sub layer, MAC common part sub layer and MAC convergence sub layer as mentioned in the figure.
MAC privacy sub layer:
It does Authentication,encryption and key management functions.
MAC common part sub layer:
It does ranging,scheduling,connection setup,bandwidth allocation,hybrid ARQ and QoS functions. Various QoS schemes and applications of each supported in wimax are as follows. It is Connection oriented protocol, which assigns connection ID (A 16-bit value that identifies a connection to equivalent peers in the MAC) to each service flow on both uplink and downlink pair between BS and SS. Each service flow (uniquely identified by a SFID, 32-bit value) has it own QoS parameter setting (latency, jitter & throughput).

BE-Best Effort, SS can request for bandwidth anytime, SS will get it or not that depends on the wimax system. It is used for data transfer and web browsing
For more on MAC frames used for establishing connection between Base Station(BS) and Subscriber Station(SS) or Mobile Station(MS) are mentioned in our article on wimax MAC frame.

- Make upper layer frames compatible to be used by wimax MAC/PHY layers.
- Map upper layer addresses into wimax protocol addresses.
- Translate upper layer QoS fields into wimax MAC format and more
- Classify external network data and associate them to proper MAC service flow identifier (SFID) and connection id (CID)
- Handle TCP/IP based traffic

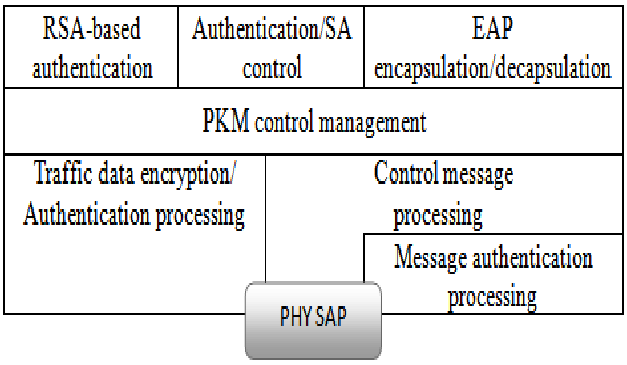
II. Authentication and Authorization

The distinction made by IEEE 802.16 is that authorization processes implicitly include authentication. The Privacy Key Management (PKM) protocol is the set of rules responsible for authentication and authorization to facilitate secure key distribution in WiMAX. Privacy Key Management (PKM) protocol supports three types of authentication.
The first type is RSA-based authentication which applies X.509 certificate together with RSA encryption. The SS manufacturer contained the SS's public key (PK) and its MAC address. When an Authorization Key is requested (AK), the SS sends its digital certificate to the BS, after validation and verification of 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 a unique operator-issued credentials such as a SIM or by username/password.
The third type of authentication that the security sub-layer supports is the RSA-based Authentication followed by EAP authentication.
We can perform the Authentication with the help of a public key interchange protocol(PKI) which ensures not only authentication but also the establishment of encryption keys. When a connection is established between SS and BS, then the management channel is opened using Privacy Key Management (PKM) protocol. 802.16e i.e based on Mobile WiMAX defines Privacy Key Management protocol in security sub-layer.
The PKM(Privacy Key Management)protocol based security is present where the BS authenticates a client SS during the initial authorization exchange. An SS used digital- certificate to get authentication from the BS.

After the authentication message SS sends an authorization message to BS regarding its verification. This message contains SS supported authentication and data encryption algorithms. If BS determines that SS is Authorized it sends a message back to BS containing an authentication key(AK). When these steps have been completed successfully, the SS has entered the network of BS and it can communicate with all the entities are available in its network. In figure MS refers to Mobile subscriber station (SS).

The Protocol that The WiMAX standard employs for security that is Privacy and Key Management Protocol

Figure 4 : Authorization and Authentication


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

for security transferring key material between the base station and the mobile station. This protocol is responsible for privacy, key management and authorizing an SS to the BS. The IEEE
802.16 standard was drawn up a security mechanism called Privacy Key Management version1 (PKMv1) which mainly manages keys and defines particular confidential and unidirectional authentication for later message delivery.
PKMv2 supports the use of the Rivest–Shamir-Adlerman that is RSA public key cryptography exchange. The RSA public key exchange necessitates that the mobile station ascertain identity using either a manufacturer-issued X.509 digital certificate or an operator-issued credential such as a subscriber identity module (SIM) card. The X.509 digital certificate contains the mobile station's Public-Key (PK)
and its MAC address. Then after the mobile station transfers the X.509 digital certificate to the WiMAX network, which then transfer the certificate to a certificate authority. The certificate authority validates the certificate, thus validating the user identity

III. Security issues and Design challenge

WiMAX security issues in MAC layer:
(Key exchange phase-Attacks) The attacker will be attack the link during authentication or key
exchange process.

- Attacker can act as a false Base station for subscriber and issue self generated keys to take over communication.
- Attacker can act as false subscriber to request to renew the keys again.

WiMAX security issues in physical layer:

- WiMAX/802.16 is vulnerable to physical layer attacks such as jamming and scrambling.
- Jamming is reducing the channel capacity.
- Scrambling is a sort of jamming, but for short intervals of time and targeted to specific frames or parts of frames.
- Intercept the radio signals in air.

Design challenges

To design the efficient scheduling algorithm the many design issue is need to take care by the researchers first one are fairness, designed algorithm having the fairness to allocate the bandwidth and each and every packet is need to transfer at least once. Most of the scheduling algorithm is channel unaware types in that always consider the channel is lossless but most of the practical channel is lossy. The third are implementation complexity, the algorithm should have the less complex the algorithm so that it can be implemented and modification could be done easily. The fourth and last one compatibility, implemented algorithm must be compatible with previous scheduling algorithm so that new algorithm can be implemented in older or existing system.

The design of today's WiMAX products requires a unified baseband and RF design methodology to help designers overcome the challenges of working with WiMax signals and take advantage of the market's windows of opportunity.
Such a design methodology uses realistic modulated signals and provides accurate performance for RF components, eliminating overdesign. This expanded methodology enables the use of system-level measurements that are defined in the WiMax specifications and which are common to all other wireless standards.

- Error Vector Magnitude(EVM)- it is an important measurement used to characterize the performance of RF components.
- Adjacent Channel Power Ratio(ACPR)- it is a measure of the interference caused to adjacent channels & used to characterized the distortion.
- Bit error rate(BER)- it is the ultimate performance matrix used to measure wireless standard.

IV . **Future work**

The future work that would further provide contributions to the scheduling in IEEE 802.16e and IEEE 802.16m mobile wimax and holistic admission control and the uplink and downlink algorithm of wimax analysis.

V**. Conclusion**

In this paper, we provided an extensive survey of recent privacy issues for WiMax. We presented by describing what WiMax , it's working and how it's authentication and authorization works. Then discussed security issues and described the solution challenges projected in the literature.

VI. **Acknowledgment**

The authors wish to thank the reviewers for their constructive comments and suggestions helped in improving this survey paper.

REFERENCES:

1. Arkoudi-VafeaAikaterini, Security of IEEE 802.16, Royal Institute of Technology2006 http://people.dsv.su.se/~x04- aia/Final%20Document.pdf
2. Certicom Corp., SEC 1: Elliptic Curve Cryptography, published September20,2000
3. http://www.computerworld.com/article/9215414/IEEE_approv es_next_WiMax_standard
4. Loutfi Nuyami ,*WiMAX Technology for BroadBand Access*,3rd ed. Wiley,2007