RESEARCH REVIEW JOURNALS
Volume-03
Issue-09
September-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

IEEE 802.16 (WIMAX) Security Issues

Jagdish Kaur

Assistant Professor, DAV College for Women, Ferozepur Cantt, Punjab (India)

ARTICLE DETAILS

Article History
Published Online: 07 September 2018

Keywords
IEEE 802.16, WIMAX, Authentication, Authorization, PKMV1 & PKMV2, Security Mechanism

ABSTRACT

Worldwide Interoperability for Microwave Access (WiMAX) is going to be an emerging technology for the future. IEEE 802.16 standard is designed to provide better security as compared to other wireless networks. It comes with lotof security features to protect the information in the network as well as to protect the network from unauthorized access, still it vulnerable to many attacks. IEEE 802.16 is a standard used for authentication and authorization which provides protection for a network or technology and protects its resources from unauthorized use. A global overview of the WiMAX technology is provided followed by security concerns and problems associated with WiMAX/IEEE 802.16 broadband wireless technology. This paper will address the security aspects of the IEEE 802.16 Standard and point out the security issues associated with MAC layer and Physical layer of WiMAX. This paper examines the security flaws in the standard as well as in related works, and key management protocols. Solutions in the standard were also proposed to prevent these attacks.

1. Introduction

The latest development in wireless metropolitan area networks is IEEE 802.16 that is most widely acknowledged with the name as WiMAX (Worldwide Interoperability for Microwave Access).This standard provides us higher range and speeds as compared to IEEE 802.11.The IEEE 802.16 standard is originally meant to specify a fixed wireless broadband access technique for point-to-point and point-to-multipoint links. IEEE802.16 was established in 1999 to prepare specifications for broadband wireless metropolitan area networks. December 2001 marked the release of the first 802.16 standard, which uses a single-carrier (SC) physical (PHY) standard. The initial version of 802.16 distributed a standard for point-to-multipoint broadband wireless transmission in the 10-66 GHz band. It featured only a line-of-sight (LOS) capability. The amendment succeeding the foremost version of 802.16 was famous as 802.16a. This improvement was ratified in January 2003.It delivered a point-to-multipoint ability in the 2-11 GHz band, which required a non-line-of-sight (NLOS) capability to function. 802.16b Defines wireless metropolitan area networks on frequency bands from 10 to 60 GHz inclusive. 802.16c delivered a system profile for the 10-66 GHz 802.16 standard. Fixed WiMAX is the 802.16d standards or as it is sometimes called 802.16-2004.The Fixed 802.16 standard supports time division duplex (TDD) and frequency division duplex (FDD) services. Time division multiplexing is more popular with mobile wireless providers than the newer TDD approach. 802.16e is the standard for WiMAX offers significant security improvements over 802.16-2004. IEEE 802.16e is often called Mobile WiMAX. It introduces a service for Multicast and Broadcast communication. This facilitate the BS to distribute data simultaneously to multiple MSs.802.16e, alternately known as "Mobile WiMAX," comes with a number of enhancements, including better support for Quality of Service (QoS) and the use of Scalable OFDMA (Orthogonal Frequency Divison Multiple Access). Accomplished in 2005, 802.16e is the latest modification of the 802.16 family to have been unconfined so far. It uses Scalable OFDMA for data transmission, supporting channel bandwidths from 1.25 MHz up to 20 MHz, with up to 2048 sub-carriers. The 802.16m mobile WiMAX standard is follow-on to 802.16e standard and considered as an IMT advanced (4G) technology. The new 802.16m standard will provide increased performance advantages over 802.16e. 802.16m, is considered to congregate or go beyond the requirements of IMT-Advanced (the 4th generation of cellular systems).

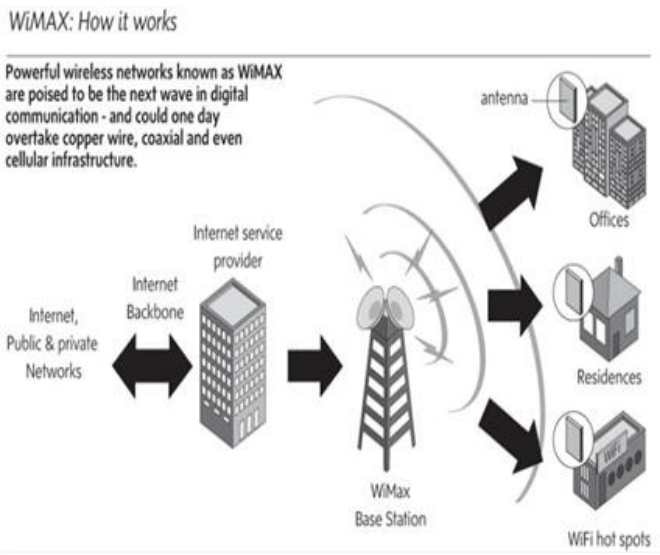

Figure1. Working of wimax

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 fully 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:MAC layer consists of three sub-layers. The first sub-layer is the Service Convergence Sub-Layer(CS), this layer mapshigher level data

services to MAC layer service flows and connections. 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.

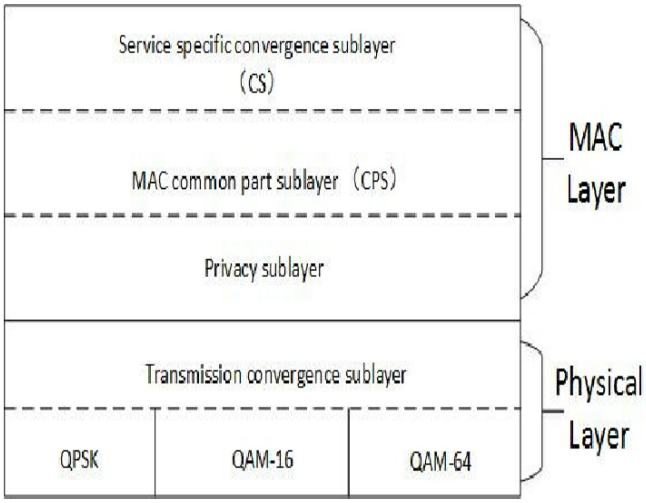

Figure2. The IEEE 802.16 Protocol Structure

2. Authentication

We can perform theAuthentication with the help of a public key interchange protocol which ensures not only authentication but also the establishment of encryption keys. Each subscriber station must (SS) have a X.509 certificate that will uniquely identify the subscriber. 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. 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.

3. Authorization

The IEEE 802.16 standard that is generally refers to authorization for the main process of authenticating all the WiMAX nodes and yielding them access to the network. 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.

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).

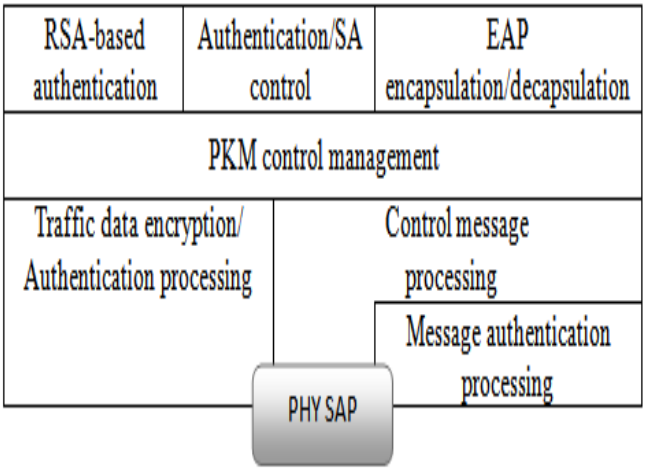

Figure 3. Authorization and Authentication

The Protocol that The WiMAX standardemploys for security that is Privacy and Key Management Protocol 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. If just

the once the user'suniqueness is validated and verified for the access, the WiMAX network uses the public key to create the authorization key, and sends the authorization key to the mobile station. The mobile station and the base station use the authorization key to derive an identical encryption key that is used with the advanced encryption standard (AES) algorithm.

PKMv3 adds an extensible framework for previous PKM protocols for supporting key agreement in multi hop relay for broadband wireless access. The PKMv3 protocol provides mutual authentication and establishes a shared secret between the MS and BS. The shared secret is then used to exchange or derive other keying material.

4. Conclusion

This paper started by describing what WiMAX is and especially how its authentication and authorization works. Then after we came across atsuch security issues and described the solutions projected in the literature. It can be seen that WiMAX provides a robust user authentication, access control, data privacy and data integrity using sophisticated authentication and encryption. Even though some issues are no longer valid since the recent amendments and security solutions in 802.16, some remain unsolved and need to be carefully reviewed to avoid the same mistake as 802.11/Wi-Fi.

References

1. http://www.computerworld.com/article/9215414/IEEE_approves_next_WiMax_standard
2. IEEE Std. 802.16e, air interface for fixed and mobile broadband wireless access systems. IEEE Standard for local and Metropolitan Area Networks, February 2006.
3. Arkoudi-VafeaAikaterini, Security of IEEE 802.16, Royal Institute of Technology 2006 http://people.dsv.su.se/~x04-aia/Final%20Document.pdf
4. Certicom Corp., SEC 1: Elliptic Curve Cryptography, published September 20, 2000, http://www.secg.org/download/aid-385/sec1_final.pdf

