A Survey of Security Threats and Authentication Schemes in WiMAX

Parampreet Singh
Deptt. Computer Science
Punjabi University, Patiala
India

JyotsnaSengupta
Deptt. Computer Science
Punjabi University, Patiala
India

ABSTRACT
WiMAX networks have advantages over the wired network, such as convenience, mobility, and flexibility. The security concerns in this network may prevent its further widespread adoption. Hence, improving the security of WiMAX is of considerable importance. In WiMAX networks by providing security features like authentication, authorization and encryption. The absence of proper authentication mechanism can lead to many threats like denial of service, masquerading and attacks on the authentication protocol. Authentication is the most difficult from the perspective of network security; hence, various forms and threats related to authentication are needed to be studied. The aim of this paper is to study the various authentication schemes such as RSA, EAP and HMAC.

General Terms
Security Threats, Authentication schemes.

Keywords
Wireless network,WiMAX, 802.16.

1. INTRODUCTION
Wireless networks are convenient and popular, but the security issues in these networks are of major concern.Some of the security threats to wireless network are denial of service, masquerading, interception, theft of service etc. To prevent these threats use of security features such as authentication, authorization and encryption, becomes very important in any wireless network. Authentication is the ability of the network to ensure that the subscriber and subscriber devices are original (legitimate) users and devices to be connected to the network. WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications technology that provides wireless and broadband data transmission with high bandwidth and transmission rates between point-to-point links and full mobile cellular access, as defined by IEEE standard as 802.16. WiMAX has some similarities with the Wi-Fi; however its security aspects are stronger than that of Wi-Fi.A desirable security solution for WiMAX network should satisfy the properties such as Confidentiality, Authenticity, Integrity and Access control.Authentication is important for many applications in a WiMAX network to avoid the various mentioned threats. As WiMAX is growing the security concerns over it are also increasing.WiMAXprovides a flexible means for authenticating subscriber stations and users to defendillegitimate use as shown in Figure 1.

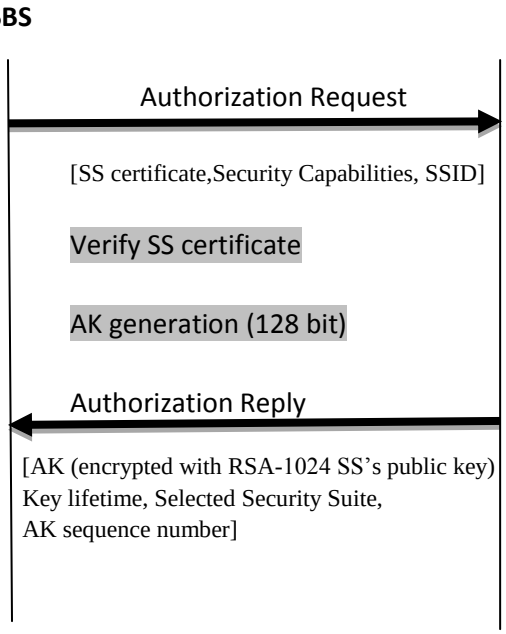

Figure 1: IEEE 802.16 Authentication [14]

Following are the steps in authentication:

- SS send authentication request using X.509 certificate
- No BS authentication
- Negotiate security capabilities between BS and SS
- Establish security association (SAID)
- Authentication Key (AK) exchange
  - AK serves as authorization token.
  - AK is encrypted using public key cryptography.
- Authentication is done when both SS and BS possess AK.

An enemy can easily inject messages in the transmission, Message authentication allows the senderto send a message to the receiverin such a way that if the message is modified/deleted during transportation, the receiver will able to detect any forgery messages. Data authentication is used by receiver to verify that the data was sent by the original(claimed) user.WiMAX network should have methodswhich ensure that a given user/device is the one it claims to be. Conversely, the user/device should also be capable of verifying the authenticity of the network to which it is connected. Together, the two are referred to as mutual authentication [8]. Mutual authentication is required for any

wireless medium; cabling cost reduction translates into increased credential management costs.The Privacy and Key Management (PKM) protocol allows for both mutual authentication and unilateral authentication. It also supports periodic reauthentication/ reauthorization and key refresh.There are two Key Management Protocols supported WiMAX: PKM version 1 and PKM version 2.

1.1 WiMAX Security Architecture

1.1.1 Protocol Layer

The IEEE 802.16 standard consists of a protocol stack with well-defined interfaces. The scope of protocol contains Physical layer and MAC layer[16].

i) Physical layer: The WiMAX's physical layer is based on orthogonal frequency division multiplexing (OFDM). OFDM is the transmission scheme that enablesefficient solutions for data, video, and multimedia communications with high peak rates.

ii) Media Access Control, MAC (data link) layer: The MAC layer takes packets from the upper layer; these packets are called MAC service data units (MSDUs). This layer organizes MSDUs into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse.

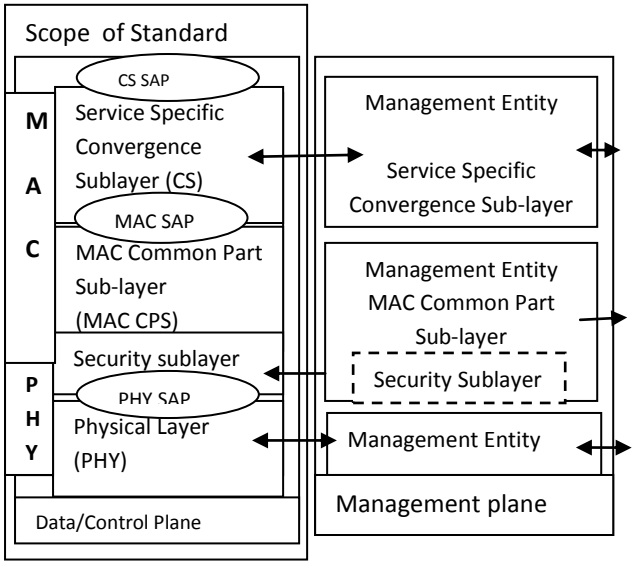

Figure 2: Protocol Layering in 802.16 [4]

MAC layer has three sub-layers shown in Figure 2. The Service Specific Convergence Sub-layer (MAC CS), the MAC Common Part Sub-layer (MAC CPS) and the Security Sub-layer.

The service specific Convergence Sub-layer (CS) provides higher level data services to MAC layer service flows and connections. The MAC Common Part Sub-layer (MAC CPS) specifies the rules and mechanisms for accessing system, allocation of bandwidth and connection management. Between MAC CPS and PHY layer, Security Sub-layer lies. This sub-layer isusedto encrypt and decrypt the data that travels to and from the PHY layer, also used for secure key exchange and authentication. PHY layer, targeted to operate in 10-66 GHz frequency band, is outlined with a high degree of flexibility so that service providers are capable to optimize system deployments with respect to cell planning, cost, radio capabilities and services [4].

1.1.2 Security Scheme

All the security issues in WiMAX are considered in security sub-layer, and are shown in Figure 3.

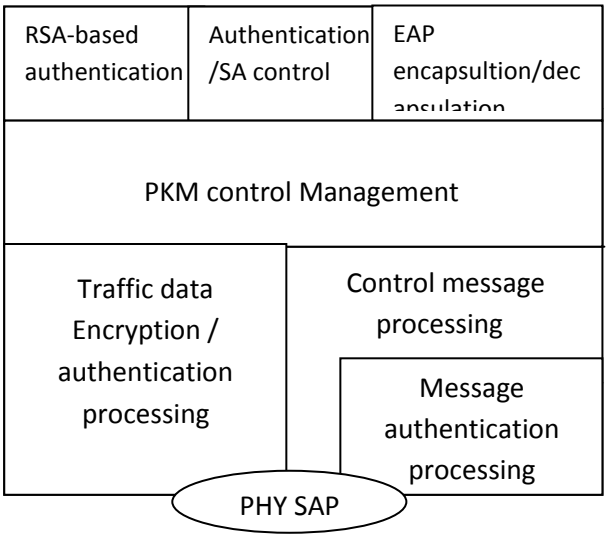

Figure 3: WiMAX Security Sub layer [13]

The security sub layer basically performs three functions viz. authentication, authorization and encryption

i) Authentication. It is concerned with confirming the identity of a person or software program, or ensuring that a product is what its packaging and label in claims to be.

*ii) Authorization.*The function of determining access rights to resources, related to information security and computer security in general and to access controlin particular can be termed as Authorization.This process follows the authentication process.

iii) Encryption. It is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. A Traffic Encryption Key (TEK) is used to encrypt the data traffic in security sub layer.

1.2Authentication Schemes

The most obvious flaw of the entire IEEE 802.16 security design is the lack of a BS certificate. In order toprotect the client against forgery or replay attack, replace the standard's authentication scheme with a scheme providing mutual authentication. Some different types of authentication schemes [8] used are:

1.2.1 RSA Authentication

The PKM RSA authentication protocol uses X.509 digital certificates that allow the base station to identify subscriber stations and the RSA public-key encryption algorithm that binds public RSA encryption keys to MAC addresses of Substations.

1.2.2 EAP Authentication

The IEEE 802.16e standard introduced an alternative to the authentication scheme based on X.509 certificates. It is considered to be more flexible and is based on the Extensible Authentication Protocol (EAP).EAP is a flexible framework created by the IETF (RFC 3748), which allows arbitrary and complicated authentication protocols to be exchanged between the supplicant and the authentication server and provides strong mutual authentication.

1.2.3 HMAC Authentication

Hashed Message Authentication Code (HMAC) is used to provide message authentication. By using HMACs, the receiver can verify who sent the message. This is possible because the sender creates an HMAC of the message it wishes to send using a key known only by the sender and receiver. When the receiver gets the message, it computes its own HMAC of the message using the same key and compares the one it computed with the one received from the sender. If the HMACs match then the sender is confirmed.

2. SECURITY THREATS IN WiMAX

In IEEE 802.16 security is considered the most important part in the design of the protocol. However, security mechanism of the IEEE 802.16 (WiMAX) still remains a question. WiMAX is relatively a new technology and it is not yet deployed widely to justify the evidence of threats and other risk in real situations.

Various security vulnerabilities found in WiMAX network were studied by Trung Nguyen [13]. They are associated with both layers in WiMAX (physical and MAC layers) and their solutions are discussed. Jamming can be considered a major threat at the Physical Layer. At MAC layer the threats include masquerading, eavesdropping of management messages, DoS attacks etc.The initial network entry procedure is very important at the MAC Layer because it is the first step to establish a connection to WiMAX by performing different steps including: initial Ranging process, SS Basic Capability (SSBC) negotiation, PKM authentication and registration process. Most of the attacks are done at the initial entry procedure. The vulnerability of using Ranging Request-Response (RNG-REQ, RNG-RSP) message is used in the initial ranging process. SS trying to join a network send the RNG-REQ message to request for transmission timing, power, burst profile information and frequency. The BS then respond by sending a RNG-RSP message to agree upon the set of negotiations for establishment of transmission link. At last, the uplink and downlink channel of the SS can be changed by using the RNG-RSP message.

The RNG-REQ message can be intercepted by the attacker and attacker can change the burst profile of SS to downgrade the service.Ranging messages can also be modified by the attacker to interrupt activities of network that are regular. Many of these issues have been fixed with recent security solutions in IEEE 802.16e. This paper proved that WiMAX is much stronger in sense of the security solutions in comparison with other wireless technologies. WiMAX is new technology and is under development and need more research on its security holes.

Security in WiMAX is implemented in the Privacy Sub layer. WiMAX provides a security architecture which basically secures the wireless transmission using different components. Eren, E. [3] summarized the most important elements of the WiMAX security architecture, presented some of its weaknesses, potential attacks and viable counter measurements. Some essential elements discussed are X.509 certificates (identity validation of the communications parties base stations (BS) and subscriber stations (SS)), the Security Associations (SA) (a set of security information by which secured communication between SS and BS can be established), encryption methods (securing data transmission against attacks using encryption of data) and the Encapsulation Protocol (specifying the encryption and authentication algorithms supported by the SS).This paper focused on Authentication of the SS - Man-in-the-Middle. One of the obvious weaknesses in WiMAXis lack of mutual authentication between SS and BS which leads to man-in-middle attack. SS authenticates itself through its certificate; however, the BS does not. A potential attacker who pretends to be a real BS but is rouge, could place himself between SS and real BS and force SS to authenticate itself and initiate a session by transferring an AK. The attacker can create Authorization Reply Message containing a self-generated AK and by this attacker can gain control over the communication of the attacked SS. This is a typical Man in- the-Middle attack. The SS is not able to recognize whether the messages of the authorization phase stem from a trustworthy BS. With the information of the SS the attacker could register himself at the BS. The security analysis depicted, that WiMAX is vulnerable in two phases: authentication and key exchange phase.

One method of attack involves burdening target machine with externally forged communications requests, such that it cannot respond properly to legitimate users or it responds so slowly as it seems to be unavailable. Such attacks usually lead to a server overload ,these type of attacks are called denial of service(DoS) attacks. A denial of service attacks are implemented across the Internet by the method of flooding the propagation medium with noise or with the forge messages. Yi Yang and Rui Li [16] discussed overview of the security issues on WiMAX. It explained the various attacks such as Replay- and DoS-Attack where the SS begins with an Authentication Information Message and a subsequent Authorization Request Message, with the aim to transmit all relevant information to the BS. The latter responds to the last message with an Authorization Reply Message. Although the message is transmitted in plaintext, it does not constitute a problem since the information is public anyway. The attacker can attack the BS by a replay attack which intercepts an Authorization Request Message which is being sent from an authorized SS and then the attacker stores it . Even though he will not be able to derive the original AK from the Authorization Response Message, he can repeatedly send the message to the BS to burden the BS with the effect that this declines the real SS.

A solution against Replay/DoS-Attacks is to provide the Authorization Request Message with a time stamp along with a signature of the SS. These additional parameters, would guarantee message authenticity. In order to protect sensible information within the message the signature should use the private key of the SS.

There are several threats to the security of the wireless networks. When more and more wireless devices are added up in the network the broadband wireless security also becomes more complicated. Ranking of the threats is done by the author in accordanceof the level of risk they present. Nasreldin et.al [11] introduced five classes of the attacks: interception attack, fabrication attack, modification, replay

and reaction attack, interruption attack, and repudiation attack. Then a special analysis of WiMAX/802.16 broadband wireless access network threats was examined and ranked according to the level of risk they presents. One of the main critical threats is: eavesdropping of management messages, which enables the attacker to gather sensitive data about the network infrastructure, used protocols, and authentication methods, other confidential information could be gathered if the network uses weak encryption techniques. Other critical threat is BS or MS masquerading where rouge BS or user MS masquerading techniques are used by the attacker to make legitimate users authenticate through rouge BS and gather more data about the user such as his username and password, or to gain access for a masqueraded MS. Strong authentication techniques for MS and mutual authentication for BS could reduce this attack. The main aim of the author was to examine Authentication in WiMAX (IEEE 802.16) using various kind of protocols so that it can be used to range the future directions of research in the Wireless security.

3. AUTHENTICATION SCHEMES

The purpose of authentication and authorization techniques mainly used in wireless systems are to prevent; snooping of the user ID, denial of service (DoS), man in- the-middle attack, offline dictionary attack, authentication method downgrading attacks, and also breaking a weak key. Adibi et.al [1] described EAP that offers an authentication scheme, which prevents the above mentioned problems. EAP allows for mutual authentication. It is basically a request-response protocol based on four different types of messages: EAP request, EAP response, EAP success, and EAP failure.In EAP protocol the different authentication methods are integrated to match the attributes of communication channel. This paper also described the authentication mechanism for WiMAX. For end-to-end authentication, WiMAX uses PKM-EAP (Privacy Key Management- Extensible Authentication Protocol), which relies on the TLS (Transport Layer Security) standard which uses public key cryptography. There are two Privacy Key Management Protocols supported in 802.16e - PKMvl and PKMv2. In this paper the PKMv2 with more enhanced authentication features are discussed. The PKM-EAP of WiMAX has been introduced into the area of WLAN in a more robust and secured way. Mutual authentication is provided in PKMv2, which could avoid "Man in the Middle" attacks. Paper gives description of X.509 certificate which is a digitally signed certificate,issued to each SS.The X.509 certificate cannot be easily forged. Hence,each of the base station in WiMAX has high performance security processor which is dedicated and which provide us to implement a mutual authentication system in WiMAX. The two main goals of the WiMAX security are to provide privacy across the wireless network and to provide access control to the network. The physical layer threat and MAC layer threat of WiMAX are studied by Lang Wei-min et.al [8] then it lists the security requirements of a WiMAX system which includes confidentiality, authenticity, integrity, and access control. Furthermore the security architecture of WiMAX is proposed which represent that the security sub layer of IEEE 802.16 provide subscribers with privacy across the network and confidentiality. Paper also describe that the management messages are exchanged between the SS and BS for authentication and then advance to key management prior to times; with the authentication time being on average fivetimes smaller for the simple EAP-MD5 method than the EAP-TLS and PEAP, and re authentication time being about two times smaller and packet loss during reconnection and throughput proved not depend on the authentication algorithm.

In IEEE 802.16, while designing the protocol the security aspect is considered as the main issue. Ziyi You et.al [17] transmission of data that is why authentication plays a critical role in securing connection in WiMAX and also in the transmission across WiMAX. In order to achieve the goal of authentication RSA authentication is described which with PKM uses X.509 digital certificates, and the RSA public-key encryption algorithm is used which is used to bind the public RSA encryption keys to the MAC addresses of SSs. X.509 certificates are used to allow the base station to identify subscriber stations.According to the 802.16 standard the 802.16-compliant SSs must have to use the X.509 Version 3 certificate formats which provide a public key infrastructure that is used for the purpose of secure authentication. The paper also recommends the use of other critical techniques, such as EAP and HMAC.

The subject of authentication within WiMAX (IEEE 802.16-2009) based wireless metropolitan networks is examined by Jacobs [6]. The two different WiMAX authentication mechanisms i.e. PKM v1 and PKM v2 are discussed. And a number of aspects which affect their authentication capabilities are presented. Managing digital certificates and the lack of multiple certificate authority support is studied. Due to the lack of multiple certificate authority support the interoperability of WiMAX devices produced by different manufactures is prevented. In this paper the recommendations are presented that should improve about the question that how WiMAX authentication operates and how to allow for mixed manufacturer device interoperability. This concluded RSA asymmetric encryption, when coupled with a PKI, provides highly reliable peer-entity authentication and non-repudiation. These security services are the result of a recipient of a message digitally signed by the sender's private key:

• Having high assurance that the sender's private key has not been stolen or lost, or is still valid for use by the signer.

• The message recipient possesses an authentic copy of the sender's public key.

The first point is achieved by the recipient being able to verify that the certificate associated with the sender's private key has not been revoked prior to the certificate's not After date.

The second point is achieved by the recipient being able to establish a chain of digital signatures on certificates starting from the sender's certificate to the certificate of the CA that issued the sender's certificate and continuing up a chain of CA certificates until a CA is identified that is within the hierarchy of CAs leading down to the CA that issued the recipient's Certificate.

In the concern of increasing data security the network access control has become a very important part of network security system. Chiornita et.al [2] analyzed different EAP authentication access methods that can be used with IEEE 802.Ix standard as a means to protect the computer network against the unauthorized access from attackers. Three of the most common methods, EAPMD5, EAP-TLS and PEAP, are compared with regard to time and packet performance both between each other and against a default situation, with no access control in place. The factors that are taken into consideration are authentication and re-authentication time, throughput and packet loss during reconnection are measured by using a specially designed test environment which is based on the test equipment capable of accurately measuring the time in the range of milliseconds and also the constant high rate traffic generation. The differences noticed weresignificant in the case of authentication and re authentication

designed a new WIMAX authentication protocol to better satisfy the security goals under the WiMAX security architecture. The new protocol primarily achieves the following two goals:

i) Identity authentication between principals.

ii) Secure session key distribution.

The protocol uses a dual-key authentication scheme based on trusted third party. The whole protocol consists of principals: mobile station (MS), access network (AN), and trusted server (TS), where, TS is only as a certification center which does not participant in the session key exchange.

The result showed that the protocol well solves two-way authentication, user identity confidentiality, preventing middle attack ...etc problems in WiMAX environments.

4. CONCLUSION

As WiMAX is emerging technology so it is necessary to study various threats associated with WiMAX. In this paper various security threats to WiMAX and different authentication schemes have beendiscussed. The different authentication schemes still need improvements for providing much secure networks.

5. ACKNOWLDGEMENTS

I express my sincere gratitude to Dr. JyotsnaSengupta, Professor, Computer Science Department, Punjabi University, Patialawho assisted me throughout the study. I thank her for providing me the reinforcement, confidence and most importantly the track for the study whenever I needed it.

6. REFERENCES

[1] Adibi, S.; Bin Lin; Pin-Han Ho; Agnew, G.B. Erfani,S. 2006. Authentication, Authorization and Accounting (AAA) Schemes in WiMAX. IEEE International Conference on Electro/information Technology, 210-215.

[2] Chiornita, Alexandra; Gheorghe, Laura; Rosner, Daniel. 2010.A Practical Analysis of EAP Authentication Method. 9th Roedunet International Conference, 31-35.

[3] Eren, E. 2007. WiMAX Security Architecture–Analysis and Assessment.4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications,673-677.

[4] Hasan S. S., Qadeer M.A. 2005. Security Concerns in WiMAX. First Asian Himalayas International Conference onInternet.

[5] Hashmi, R.M.; Siddiqui, A.M.; Jabeen, M.; Alimgeer, K.S. 2011.Towards Secure Wireless MAN: Revisiting and Evaluating Authentication in WiMAX. International Conference on Computer Networks and Information Technology, 165 - 173.

[6] Jacobs, S. 2011.WiMAX subscriber and mobile station authentication challenges. IEEE Communications Magazine, 166-172.

[7] Komu, Beth N.; Mzyece, Mjumo; Djouani, Karim.2012.SPIN-based Verification of Authentication Protocols in WiMAX Networks. IEEE Vehicular Technology Conference, 1-5.

[8] Lang Wei-min; Zhong Jing-li; Li Jian-jun; Qi Xiang-yu. 2008. Research on the Authentication Scheme of WiMAX. 4th International Conference on Wireless Communications, Networking and Mobile Computing, 1-4.

[9] Mei Song; Li Wang; Jianwen Huang; Junde Song. 2009.An Optimal Interworking Authentication Scheme Based on Eap-Aka forHeterogeneous Access Networks. Canadian Conference on Electrical and Computer Engineering, 794-797.

[10] Michail, H.E.; Kakarountas, A.P.; Milidonis, A.; Goutis, C.E. 2004.Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function.11th IEEE International Conference on Electronics, Circuits and Systems, 567-570.

[11] Nasreldin, M.; Asian, H.; El-Hennawy, M.; El-Hennawy, A. 2008.WiMAX Security.22nd International Conference on Advanced Information Networking and Applications-Workshops, 1335-1340.

[12] Sridevi, B.; Brindha, M.; Umamaheswari, R.; Rajaram, S. 2012. Implementation of secure and cost effective authentication process in IEEE 802.16e WiMAX. International Journal of Distributed and Parallel Systems, Vol. 3:No.2.

[13] Trung Nguyen: A survey of WiMAX security threats,Available: http://*www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2.pdf*, April 2009.

[14] Wongthavarawat K. 2005. IEEE 802.16 WiMAX Security. Annual FIRST Conference, Singapore.

[15] Yi Xiaolin; Chen Nanzhong; JiaZhigang; Chen Xiaobo 2010.Trusted Communication System based on RSA Authentication.Second International Workshop on Education Technology and Computer Science, Vol.1, 329-332.

[16] Yi Yang;Rui Li. 2009. Toward WiMAX Security. International Conference on Computational Intelligence and Software Engineering, 1-5.

[17] Ziyi You;XiaoyaoXie; WeihongZheng. 2010. Verification and research of a WiMAX authentication protocol based on SSM. 2nd International Conference on Education Technology and Computer, Vol. 5, 234-238.