Analysis of Security Protocols in Mobile Wimax

Rajesh Yadav
Department of Computer Science
Mewar University
Chittorgarh, India

Dr. S. Srinivasan
Department of Computer Application
P.D.M. College of Engineering
Bahadurgarh, India

***Abstract*— For wide area wireless networks, Mobile WiMAX has come up as an emerging technology. Based on Orthogonal Frequency Division Multiple Access (OFDMA), mobile wimax provides high speed Internet access to the subscribers within a coverage area of several kilometres in radius..This paper focus on different authentication protocols for Mobile Wimax. These protocols are different from other conventional authentication methods, those based on the mobility of Mobile stations. Security is a fundamental issue in M. Wimax. A lot of researcher proposed their work towards the security to make the M. Wimax secure. In this paper we investigate and present comparative study of existing security protocols over mobile wimax and discuss how they achieve better security against various types of security threats.**

Keywords- Mobile Wimax, Authentication, Mobile station, Base station.

I. INTRODUCTION

Mobile wimax has undoubtedly become interesting whenever there is need to deliver next-generation, high-speed mobile voice and data services.

Due to lack of potential related to QOS, it is not possible for service providers to take benefit of mobile voice and multimedia over IP.

By taking this into consideration, mobile wimax has been designed with five distinct classes of service quality thereby providing a more robust and resilient connectivity time for time-sensitive applications..

It can offer large wireless access network accessibility to subscribers and simultaneously providing higher throughputs just like wireless LAN. Mobile Wimax is ideal for next-generation converged data and voice services and streaming wireless multimedia.

As far as security is concerned , security sub layer is responsible for implementing it, at bottom of MAC layer and above to the PHY layer.IEEE 802.16e i.e. Mobile wimax is vulnerable to attacks such as scrambling, jamming ,water torture attack, most of all that supports mobility[1].Wimax has been embedded with many sophisticated authentication and encryption techniques, but there are still chances of various attacks in it In this paper we will discuss about mobile wimax security consisting of different type of algorithms, and will analyse the work done by several researchers w.r.t. ensuring security in Mobile wimax. [2].

II. MOBILE WIMAX SECURITY

As compared to fixed wimax, Mobile WiMAX is considered to be more vulnerable as different mobile stations moves openly throughout the network during data transmission. One important factor which needs to be focussed upon is that authentication process should be highly secure so that there are no chances of security threats. So the authentication process is to be focussed in a way for prevention of different category of attacks on network users especially in the station's initial network entry phase.Fig.1 gives an overview of different security protocols which are used in Mobile Wimax.

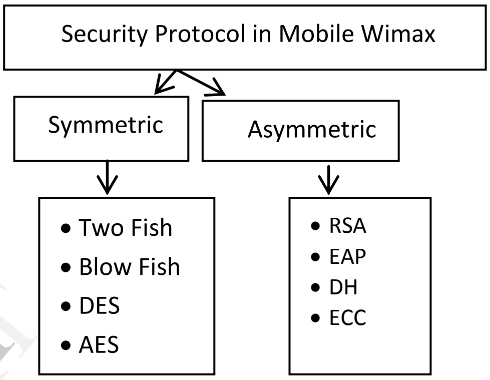

Fig.1. Security Protocols in Mobile Wimax

A. *Symmetric Algorithms*

This category of algorithms use trivially related, often identical, cryptographic keys for the process of encryption as well as decryption. It is of the following types:

a) Two Fish

Two fish algorithm uses one key of any length maximum up to 256 bits, it is considered efficient for both software running in smaller processors such as in case of smart cards as well as for embedding in hardware.

b) Blowfish

Blowfish kind of algorithm is actually fast one which provides compact and simple block encryption with variable length key thereby permitting a trade-off between security and speed [17].

c) DES

The Data Encryption Standard (DES) is a symmetric-key method for encryption of data, it works by using similar key for encrypting as well as decrypting the message, therefore it is necessary for both the sender and receiver to be aware of the same private key.

d) AES

Advanced Encryption standard is a symmetric 128-bitblock encryption technique which is being designed for replacing the DES encryption. It has the capability of working simultaneously at multiple network layers.

B. *Asymmetric Algorithms*

These are the category of Encryption techniques in which keys come in pairs. What one key encrypts, only the other can decrypt.

a) RSA

Public-key cryptography, also known as asymmetric cryptography, make use of two different but keys which are mathematically linked with each other, one public and the other private one. Public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both public and private keys can perform encryption of message; the opposite key from the one used to encrypt a message is used to decrypt it.

This is the reason why RSA is considered good to be used widely as an asymmetric algorithm.

RSA involves a method of assuring integrity, confidentiality, message authenticity.

b) EAP

The Extensible Authentication Protocol (EAP) is actually an authentication framework which is widely used for wireless networks like Wimax .EAP is a method to for transfer of authentication information between a network adn a client. It contains a basic request/response protocol platform over which to implement specific authentication algorithms which are of different types as explained below [18].

EAP Methods:

- EAP MD5
- EAP LEAP
- EAP PEAP
- EAP FAST
- EAP AKA
- EAP SPEKE
- EAP TLS
- EAP TTLS

i. EAP MD5

This EAP protocol provides minimal security; it has hash function is vulnerable to dictionary attacks, and it also does not support key generation. So it is considered unsuitable in case of dynamic WEP, or WPA/WPA2 enterprise.EAP-MD5 is different form methods in the sense that it only provides authentication of the EAP peer to the EAP server but there is nothing related to mutual authentication. Therefore it is prone to MITM attacks also.

ii. EAP LEAP

LEAP (Lightweight Extensible Authentication Protocol) is an authentication protocol which is used in wireless networks as well as Point-to-Point connections. LEAP is actually developed for providing better secure authentication for both fixed as well as mobile wimax networks.

iii. EAP PEAP

EAP-PEAP involves wrapping up of EAP methods within TLS (Transport Layer Security).This makes it good because EAP messages are encapsulated inside the TLS tunnel and are protected against various types of attacks.

iv. EAP FAST

EAP-FAST makes it possible for optional use of security weaknesses and it also makes use of a PAC (Protected Access Credential) for ensuring establishment of TLS tunnel. This tunnel is therefore used for verifying the client credentials.

v. EAP AKA

It is an authentication protocol method for Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement.EAP-AKA is an EAP mechanism for authentication distribution of session key using the UMTS Subscriber Identity Module (USIM).

vi. EAP SPEKE

EAP-SPEKE (Simple Password Authenticated Exponential Key Exchange) has the capability to provide mutual authentication between authentication server and client by making use of simple common password. It may be considered as replacement of EAP-TLS protocol which provides strong security and authentication of user and device both but lacks fast reconnection support which is an important EAP requirement [7].

vii. EAP TLS

EAP-Transport Layer Security protocol [3] is considered as one of the most secure EAP methods. Its requirement is that both peer and server should have X.509 certificates for mutual authentication, so each client requires a unique digital certificate.

It is difficult to manage these certificates, these certificates add administrative overhead. Hence, EAP-TLS is rarely deployed. Another issue is that a passive attack can easily obtain the usernames.

viii. EAP TTLS

EAP is extended from TLS (Transport Layer Security) to TTLS (Tunnelled TLS); this method allows legacy password-based authentication protocols to be used against existing authentication databases, thereby ensuring safety of these legacy protocols against eavesdropping, MITM and other attacks [3].

c) Diffie Hellman

It is also known as exponential key exchange, it is a technique of digital encryption which makes use of numbers raised to specific powers so as to generate decryption keys depending on the components that are never directly transmitted, making it difficult for the attacker to break its functionality.

d) ECC

Elliptic Curve Cryptography (ECC) was discovered in 1985 as an alternative method for implementation of public-key cryptography. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms which is much more difficult to challenge at equivalent key lengths.It is an encryption technique based on elliptic curve theory which can be utilised for creating smaller,faster, and more efficient cryptographic keys. ECC creats keys through properties of the elliptic curve equation rather than having traditional method of generation as the product of very large prime numbers. ECC can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.

It can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC assists to establish equivalent security with les computing power and battery usage, it is becoming widely used for mobile applications. ECC was designed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been designing its own version of ECC. Many other have included support for ECC in their products.

ECC algorithm is based on properties of a type of equation created from the mathematical group derived from points where axes is intersected by line ultiplying a point on curve by number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result.

III. REVIEW OF MOBILE WIMAXSECURITY PROTOCOLS

Young wook Kim et al. [4] proposed a mechanism for avoiding DDOS attacks in Mobile Wimax using Shared Authentication Information (SAI) technique. It makes use of unused 64 bits of CMAC. SAI has following advantages:

- Since SAI is outcome of CMAC calculation, so SAI need not be calculated at BS and MS.
- BS and MS are not required to exchange messages for SAI as they already get it during CMAC calculation and verification.
- No attacker can be aware of SAI as it is not being flown as information over the air.
- SAI provides uncompromised security as against validation process of CMAC value.

Bart Sikkens [5] analysed work done by several researchers towards DOS/Replay attack, authorization vulnerability, key space vulnerability, downgrade attack, WPKI. During analysis light is being thrown on possible solutions for the above mentioned problems and proposed solutions were analysed using criteria of focussing on solution performance, updation required in standards, scalability, improvement in authentication and authorization but for a complete solution all the proposed solutions should be combined and research should be conducted further in this regard.

Perumal Raju et al. [6] analysed MAC layer security issues and discussed their solutions. Issues related to PMP network were discussed like DOS/Replay attack during MS network entry, downgrade attack, computational efficiency of cryptographic algorithm and bandwidth spoofing solutions were recommended during analysis. Also issues related to mesh networks were analysed like MITM attack during network entry, during neighbour interaction, encryption load issues and bandwidth spoofing. However during analysis it is being found that mesh network is not analysed clearly and absence of complete security solution is there due to unsecured MAC management messages.

Anjani K. Rai et al. [7] proposed a new password based EAP TLS authentication protocol. Proposed protocol incorporates Diffie Hellman concept also. Efficiency of this protocol is compared with other EAP methods using parameters like mutual authentication, credential security, MITM attack, user authentication etc. the proposed protocol is an improvement over highly secure TLS method as it provides Mutual authentication between MS & AAA server using simple common password and don't make use of Public key certificates thereby saving a lot of additional administrative work as well as overhead.

Taeshik Shon et al. [8] proposed different secure approaches for handover, access network and initial network entry. Security approach called ROSMEX is applied enhancing network entry with modified DH key agreement. For securing access networks, secure channel is established using device certificate based simple and efficient key exchange .Also handover process is improved by having embedded mutual authentication parameters.

Mohammad Zabini et al. [9] proposed DH based authentication in Mobile Wimax and also compared the same with other protocols like RSA based PKMv2 and EAP. Proposed method is shown resistant towards MITM, Replay & Interception attack. It provides mutual authentication, key exchange between BS and MS, so chances of eavesdropping, MITM and Replay is reduced.

Deepak Kumar et al. [10] analysed security issues like Privacy protection, interruption attack. They proposed an authentication protocol based on public key cryptography to address the security issues. The proposed protocol provides one way authentication, while doing so it ensures consistency and freshness of session keys thereby enhancing mobile wimax network security.

D. David et al. [11] analysed different encryption algorithms like AES, two fish, blowfish, MD5. By taking processing time and throughput as parameters they proposed approach of (Twofish+MD5) to improve security for encrypting packet transmission between BS and MS.

Ahmed et al. [12] analysed PKMv1 and PKMv2 authentication protocol vulnerabilities. They also proposed and improved authentication protocol based on timestamp to prevent MITm and replay attacks. Proposed design is analysed thereby showing that intruder can't obtain SS/MS certificates, unauthenticated user can't access services provided and can't impersonate other user, and also an adversary can't obtain the unique Pre-PAK.

Do Hyeon et al. [13] proposed encryption of initial entry in mobile wimax using ECC. The proposed approach involves 3 steps i.e. initial ranging, periodic ranging and handover ranging. DOS attack can happen in Wimax environment due to parameter exposure, applying ECC to prevent parameter exposure enhances security against such attacks.

Zeinab et al. [14] Diffie Hellman- Digital signature scheme for securing initial network entry process in Mobile Wimax having less bandwidth and computational costs as against DOS attack, DOS vulnerabilities are being discussed like handover process, resource saving, network entry and Elliptic Curve –Dh key exchange method is developed for enabling authentication key agreement between BS and MS during initial network entry, handover and sleep mode.

Prakash et al. [15] proposed an authentication algorithm based on new linear block cipher cryptography (Nlbc) which can be used as replacement for RSA. It uses smaller key size there by requiring low computing time, computational power and less memory.

Aposotol et al. [16] proposed a new method for enhancing Mobile wimax security using digital certificate over EAP-TTLs method which is credential based. It also throw light on management channel protection where no unauthorised third party has access to the network, also security of management virtual network is taken into consideration for IP-CS and ETH-Cs subscriber functionality.

Table 1. presents the comparative analysis of research work done by different authors towards Mobile Wimax Security.

TABLE 1. Comparative Analysis

Author	Problem analysed/Solution proposed	Benefits
Deepak kumar et al.[10]	Analysed security issues like privacy protection/interruption attack. Proposed public key cryptography authentication protocol.	Proposed protocol provides one way authentication thereby ensuring consistency/session key freshness enhancing Mobile Wimax security.
D. David et al.[11]	Analysed AES, two fish,MD-5, blow fish algorithms by taking processing time/throughput as parameters. Proposed (two fish + MD-5) approach to improve security.	Proposed approach enhances security during encryption and packet transmission between MS & BS.
Ahmed et al.[12]	Analysed PKMv1 & PKMv2 vulnerabilities. Proposed improved authentication protocol based on timestamp to prevent MITM/Replay attack.	• Intruder can't obtain SS/MS certificate. • Unauthenticated used can't access services. • No impersonation attack. • Adversary can't obtain unique pre-PAK.
Zeinab et al.[14]	Proposed Diffie Hellman-Digital signature scheme to secure initial network entry procedure.	• Less bandwidth • Less computational costs • Works well against DOS attacks.
Do-Hyenchoi et al.[13]	Proposed encryption of initial network entry using ECC.	Using ECC for prevention of parameter exposure enhances security against DOS attacks.
Prakash et. Al[15]	Proposed authentication algorithm based on Nlbc.	• Nlbc can be replacement for RSA. • Smaller key size requires less computing time, low computation power & less memory.
Taeshik et al.[8]	Proposed secure approaches for handover, access network and initial network entry.	• Improved access network and handover process. • Enhancing network entry.
Apostol et al.[16]	Proposed digital certificate based security over EAP TTLS.	• Security based on minimum cost. • Digital certificate parameters are secret.
Young wook Kim et al.[4]	Proposed mechanism for avoiding DDOS attack using SAI.	• No SAI calculation at BS/MS. • BS/MS not required to exchange messages for SAI. • Attacker remains unaware of SAI.
Bart Sikkens[5]	Analysed research towards DOS/replay attack, authorizationvulnerability, key space vulnerability downgrade attack, WPKI.	Solution proposed for key space vulnerability & Downgrade attack.
Perumalraju et al.[6]	Analysed Physical and MAC layer security issues & discussed their solutions for.DOS, Replay attack, downgrade attack, computational efficiency of cryptographic algorithm. Bandwidth spoofing solution is recommended during analyses.	Solution proposed for DOS, Replay attack during MS initial network entry, Rogue BS attack, MITM during authorization, MITM during authentication and encryption load issues.
Anjani K Rai et al.[7]	Proposed password based EAP TLS authentication protocol incorporating Diffie Hellman concept also.	Suggested protocol is beneficial due to mutual authentication using simple common password and no requirement for Public key certificates saving overhead and administrative work.
Mohd. Zabini et al.[9]	Proposed Diffie Hellman based Mobile Wimax authentication & compared it with RSA/EAP/	Proposed method is resistant towards MITM, replay, interception attack. Eavesdropping, MITM and replay attack chances are reduced.

CONCLUSION

Security in Mobile Wimax is essential in many of the proposed applications. In this paper we presented a review of relevant authentication schemes suitable for Wimax against different attacks during communication. This comparative study of security based on different attacks in Wimax give a broad view for researcher, how to make an authentication protocol scheme to provide better security measure with removal of computational cost and its overhead.

REFERENCES

[1] Daniel Simion, Mihai-Florentin URSULEANU, Adrian GRAUR, “An Overview on WiMAX Security Weaknesses/Potential Solutions”,11th International Conference on Development and application systems , Suceava, Romania, May 17-19, 2012.

[2] Gaurav Soni, Sandeep Kaushal,” Analysis of Security Issues of Mobile Wimax 80.2.16e and their solutions”,InternationalJournal of Computing and Coorporate Research, volume 1 issue 3,November 2011.

[3] R. C. Roychaudhary, S.S. Telrandhe, C.N. Rokde, A. Y. Khobragade,” Analyzing Performance for Mutual Authentication Mechanism for Wimax: IEEE 802.16e”, Int. Journal of Engineering Research and Applications, Vol. 4, Issue 2(Version 1), February 2014, pp.429-438.

[4] Youngwook Kim, Hyoung-Kyu Lim, Saewoong Bahk,” Shared Authentication Information for Preventing DDoS attacks in Mobile WiMAX Networks”, IT R&D program of MIC/IITA, grant 2007-S001-01, and the NRL program of MOST/KOSEF, in Korea.

[5] Bart Sikkens, Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e), 8th Student Conf. on IT, 2008.

[6] Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan, Analysis on Mobile WiMAX Security, IEEE TIC-STH 2009, Information Assurance in Security and Privacy, September 27-29, 2009 Toronto, Ontario, Canada.

[7] Anjani K.Rai,Shivendu Mishra and Vimal Kumar, Strong Password Based EAP-TLS Authentication Protocol for WiMAX, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010.

[8] Taeshik Shon, Bonhyun Koo, Jong Hyuk Park, and Hangbae Chang, Novel Approaches to EnhanceMobileWiMAX Security, EURASIP Journal on Wireless Communications and Networking Volume 2010.

[9] Mohammad Zabihi , Ramin Shaghaghi, Mohammad Esmail kalantari, Improving Security Levels of IEEE 802.16e Authentication By Diffie-Hellman Method, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 3, November 2011.

[10] Deepak Kumar Mehto, Rajesh Srivastava, An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile Wimax, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011.

[11] D. David NeelsPon Kumar, Praveen David, S.Rimlon Shibi, K.Arun Kumar, Security Enhancement for Mobile WiMAX Network, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[12] Ahmed Mohamed El-Amin, Salah El-agooz, Alaa El-Din Rohiem Shehata and Essam Abd-Elwanees Amer, Design, Verification and Implementation of Enhanced PKM WiMAX Authentication Protocol, International Journal of Computer Science and Telecommunications [Volume 4, Issue 3, March 2013.

[13]Do-Hyeon Choi, Hyungjoo Kim, 3Jungho Kang, 4Moonseog Jun, ECC-based Mobile WIMAX Initial Network Entry with Improved Security, International Journal of Advanced Computer Technology (IJACT) : , Vol. 5, No. 13, pp. 505 ~ 517, 2013.

[14] Zeinab Kalantari, Maryam Shojaei, A DH-DSS Based Approach to Improve Mobile WiMAX Security against DoS Attack, International Journal of Computer Science Engineering (IJCSE), Vol. 2 No.05 Sep 2013.

[15] Prakash Kuppuswamy1, Sikandhar Shah, Improving Security Authentication of IEEE 802.16 WiMax with New Public key algorithm, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February, 2014.

[16] Apostol Cristian- Gabriel, Ciprian Răcuciu, Improving Mobile WiMAX EAP-TTLS Authentication with Minimum Downtime and Securing its Management Channel, Indian Journal of Research , Volume 3, June 2014.

[17] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid,” Symmetric Algorithm Survey: A Comparative Analysis” International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

[18] Lei Han, “A Threat Analysis of The Extensible Authentication Protocol”, School of Computer Science, Carleton University, April, 2006.