Investigation on Mobile Wimax: it's Security Issues

S.S. Dwivedi
M.Tech(Student), CSE Department
Bipin Tripathi Kumaon Institute of Technology
Dwarahat, Almora, India

S. Mishra
CSE Department
Bipin Tripathi Kumaon Institute of Technology
Dwarahat, Almora, India

V.K.Mishra
CSE Department
Bipin Tripathi Kumaon Institute of Technology
Dwarahat, Almora, India

Abstract— ***WiMax is a wireless based technology standard that provides high throughput broadband connections over long distances. Security is one of the major considerations in broadband wireless access especially when wireless devices are added to it. Wimax/802.16 is also not free from vulnerability, threats, risks or other attacks to provide secured and robust services like as other standards 802.11 and so on. With the high and effective security confirmation, this technology would be more reliable and trustworthy. This paper works on all possible attacks of Wimax standard and provided their solutions which separately came on light so far. This research found some difficulties in the security of 802.16 transmissions and then proposed solutions for that. Also, a simulation work has been done in dot net framework with C# language.***

Keywords- Mobile Wimax, Security vulnerability, Hash chasing and authentication.

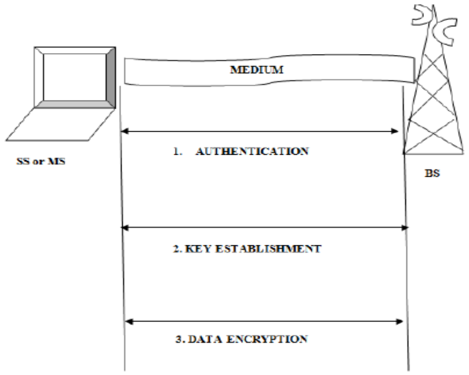
I. Introduction

The family of IEEE 802.16 standard is also known as Wimax has produced high expectations from hardware vendors and internet service provider. Wireless network have brought about major development in the way, the information is shared between individual to individual, individual to business and business to business. Which are yet too solved? We discuss security as protection of data being transmitted over a wireless networks. It is an important to know the problems that security systems need to address. These needs are confidentiality, integrity and authentication; these are defined as follows-Confidentiality-it allows only that the intended legitimate recipients to read encrypted messages. Integrity-it is referred to as ensuring that another party has not altered messages after it has been sent. Authentication-it makes sure that parties sending messages or receiving messages and have the right to undertake such actions. The wireless signal is transmitted through electromagnetic waves, which cannot be physically contained. Wimax builds on the security problems of 802.16 wireless networks and was developed to solve most of wireless shortcomings, especially security and long distance connecting coverage [1].

Adding mobility of standard through IEEE 802.16 makes the attacker's life even easier. This need to maintain a secured state while a mobile SS moves between BSs introduces new vulnerabilities. An attacker could forge new frames and capture, modify and retransmit frames from authorized parties. The design must therefore also provide a data authenticity mechanism. Interference and distance could allow an attacker to communicate with two authorized parties who cannot communicate directly with each other, and reorder and selectivity forward frames. Thus, design must detect replayed frames. Can resend a valid, already send frames unmodified. Also provide a data authenticity mechanism.

II. Literature Survey of Wimax Security

It was analyzed in many papers, especially in[2] where a lot of security vulnerabilities are outlined when the publication of the mobile Wimax amendment, most of these vulnerabilities were solved. The security of Wimax was



analyzed by a few papers, such as in[3] that examined in the 3-way TEK exchange and the authorization process and it could not find any security leak. Also [4] analyzed the key management protocol. It analyzes software. This is also discussed that the interoperation with other protocols could be a security problem, if these protocols have lower security characteristics. As that the Figure 1 shows the framework of the Wimax Security system.

Figure 1. Wimax Security Framework

III. Authorization and Authentication Issues

It is an essential issue for wimax security. In which, the entire IEEE 802.16.Security design is the lack of a BS certificate. The only way to defend the client against forgery or replay attack is to replace the standard's authentication scheme with a scheme providing mutual authentication. Mutual authentication is required for any wireless medium. The PKM authorization protocol that manages it possesses vulnerabilities. The IEEE 802.16 design's lack of a mean for authenticating the BS to the SS leaves the PKM protocol open to replay attacks.In a replay attack, the SS can not verify that any authorization protocol messages. It receives when generated by an authorized BS.The BS is responsible for authorization protocol responses it sends to an SS using entirely public information, So any rogue BS can create a response. Requiring the SS to authenticate to the BS can eliminate this vulnerability.

It is an essential issue for wimax security. In which, the entire IEEE 802.16.Security design is the lack of a BS certificate. The only way to defend the client againstt forgery or replay attack is to replace the standard's authentication scheme with a scheme providing mutual authentication. Mutual authentication is required for any wireless medium. The PKM authorization protocol that manages it possesses vulnerabilities. The IEEE 802.16 design's lack of a mean for authenticating the BS to the SS leaves the PKM protocol open to replay attacks. In a replay attack,the SS can not verify that any authorization protocol messages. It receives when generated by an authorized BS. The BS is responsible for authorization protocol responses it sends to an SS using entirely public information, So any rogue BS can create a response. Requiring the SS to authenticate to the BS can eliminate this vulnerability.

The authorization protocol subjects the SS to reply attacks. The simplest way to represent such an attack is to require the SS to generate a random challenge in the authentication protocol, and the BS to include the challenge in the state it returns authenticating itself to the SS. Arelated problem is the protocol failure to allow participants to distinguish one instance of the protocol from another. It will become an important as IEEE 802.16e facilitates mobility and roaming. By exchanging public random numbers, participants can uniqely identify the protocol instance as the 4-tuple BS's certified identity, SS's certified identity, BS's public random number for this instance. Participants could use this information to tie key management protocol instances to the governing authorization instance.

Atlast, this protocol assumes that certificates are correctly issued-that is no parties with different public or private key pairs are certified to use the same MAC address. If this condition not met, each party can masquerade as the other.The specification should explicitly call out its assumptions that every certified MAC address is distinct[5]. The key management and encryption portions of IEEE 802.16 security offer no assurance because the security of both rests on the authorization protocol's correctness.It failure demonstrates that securty algorithms can not be transferred from one of the content to another without great care.

IV. Data Protection

Data protection is very important in the Wimax network. When transferring data from one place to another place. In which, the scheme's failure to protect against forgeries or replies, the most serious threats against any wireless data protection scheme. Encryption only read protects the WMAN channel; it doesn't protect the channel from writes, even by someone without the encryption key[7].

Few protocols also exhibit a severe error in its use of encryption. IEEE 802.16 uses DSE in CBC mode.CBC mode requires a random initialization vector to secure the scheme[5]. But IEEE 802.16 uses a predictable initialization vector. Correcting this problem requites generating each per frame initialization vector randomly and inserting them into the payload. Although this increases the encryption overhead, no other alternative exists.

Recently it has been demonstrated that secret keys can be generated by a completely different method[5], as well. It is based on synchronization of network by mutual learning. The secret key is generated by the dynamics of a complex physical process, namely the competition between stochastic attractive and repulsive forces which act on the weights of the two dynamical systems which synchronize by mutual signals have an advantage over an attacker E which can only synchronize by listening to the exchanged signals[8].

V. Mordern Data Protection

In which, the IEEE 802.16e amendment recently adopted AESCCM-that is ,AES in CCM mode, as a new data link cipher.CCM13 combines counter mode encryption for data confidentiality with the CBC-MAC for data authenticity. Hence correct use of AES-CCM addresses the most fundamental deficiency in the original data protection scheme the lack of a data authenticity mechanism.

Designers choose AES-CCM for a variety of reasons, including its use in IEEE 802.11i and subsequent scrutiny. The US national institute of standards and technology has indicated that CCM will become an approved mode of operation for AES.CCM protects associated data, which lets the encryption scheme protect GMH. No intellectual property claims have been made against CCM.

AES-CCM requires that the transmitter constructor a unique nonce, which is a per packet encryption randomizer. Consistent with the IEEE 802.11i solution, IEEE 802.16e inserts a packet number into each MPDU to ensure each nonce's uniqueness. A receiver validates that received packets correctly decrypt under AES-CCM and have an increasing packet number.

IEEE 802.16i also describes AES in ECB mode to replace the triple-DES key wrapping in the PKM protocol. A better choice would be NIST's AES key-wrap algorithm[6].

VI. Conclusion

In this paper, we give a through explanation on the authentication and authorization security issues. To solve the security threats existing in a wimax authentication. In which, we can generate a pair of secret keys through synchronization. The proposed solution's are of efficiency and ready for real time processing. Finally, the advantage of the proposal has been thoroughly described.

Acknowledgment

We like to acknowledge our vigorous thanks to Mr. Dong Hu & Mr. Frank for providing such a good data on mobile wimax security system of their research work on internet which helped us a lot in our research work and we also want to thanks our friends and classmates for helping us in this research work by giving us there timely suggestions and feed backs on our research work.

References

[1] Westech Communication Inc(2005), Can Wimax Address your Application.Whitepaper,accessed on 3 october 2006.

[2] D.Johnston and J.Walker,"Overview of IEEE 802.16 security",IEEE Security and Privacy,PP.40-48,May/June.

[3] Datta A., He C;Mitchell J.C.,Roy A.,Sundararajan M."802.16e Notes,Electrical Engineering and Computer science Departments,Stanford University,CA,USA,2005.

[4] Yuksel E. "Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling",Technical University,Denmark,DTU,2007.

[5] Rachna Dhameja and J.D.Tygar.The Battle Against Phising:Dynamic Security Skins In Proceedings of the Symposium on Usable Privacy and Security(SOUPS).pages 77-78,july 2005.

[6] R.Poisal.Modern Communications Jamming Principles and Techniques.Artech House Publishers,2003.

[7] Rakesh Kumar Jha "A Journey on Wimax and its Security Issues,"International Journal of Computer Science and Information Technologies,ISSN-0975-9636,Vol.1,No.4,Page no.256-263,2010.

[8] Dong Hu,Yuyan Wang "Secure Authentication on Wimax with neural cryptography,"978-0-7695-3126-7/08,DOI 10.1109/15A.2008.16.