International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Improving Security in WiMAX using Evolutionary Algorithm

Sachin Magithia
Asst. Prof., M.Tech. (IT)
CGC Landran, Mohali
sachinmagithia@gmail.com

Kamalpreet Kaur
M.Tech. (IT)
CGC Landran, Mohali
kamal_8188@yahoo.co.in

***Abstract* — The evolution of new technologies wireless is not secured as like others networking technologies. A lot of security concerns are needed to secure a wireless network. To achieve End-to-end secure communication then the security has to be kept in mind. By keeping in mind the importance of security, the wireless network has been designed with several security mechanisms to provide protection against unauthorized access and malicious threats, but still facing a lot of challenging situations. An authentication and authorization model provides protection for a network or technology and protects its resources from unauthorized use. It proposed some enhancements to the existing model to improve its capabilities and encryption strength for security.**

***Keywords* — Wireless networks; WiMAX 802.16; Authentication; Authorization.**

I. INTRODUCTION

Many wireless networks are based on radio waves, which makes the network medium inherently open to interception. Properly protecting radio transmissions on any network is always a concern for protocol designers. 802.11 or 802.16 did not build in much in the way of security protocols. Coping with the inherent unreliability of the wireless medium and mobility required several protocol features to confirm frame delivery, save power, and offer mobility. Poorly implemented network and device security opens the door for service disruption and theft. Not only must the users of broadband service protect their own personal information, but public networks must be designed and implemented with security in mind. Security of a network plays a key role in the performance of a network. Security is more important than ever before due to many reasons. When a network is implemented poorly, security threats and attacks always exist. But if that network is made fully secure by implementing high level of security, there will be a fewer amounts of security threats. Applying security to a network is too much costly than its advantages. Both Network operator and the network user are playing a key role in the security providence to a network and are concerned over network security.

There has been great evolution in wireless communications over the last few years. The wireless communication is so much open to threats. Radio transmission should be made secure so that the communication becomes secure. WiMax is an emerging wireless technology used for deploying broadband wireless metropolitan area network (WMAN). WiMax technology offers many features with a lot of flexibility and has replaced many of the existing telecommunication technologies. Not only does 802.16/WiMax provide network access anytime anywhere, but it also offers higher speed at longer distances. A lot of security concerns are needed to secure the end users, the core network, the application servers, and everywhere in between. Strong security mechanisms are needed for WiMax to secure it from vulnerabilities and threats. Because the security mechanisms used by old technologies are not applicable for new technologies.

II. CLASSES OF WIRELESS ATTACK

Intruders can inflict four major classes of attack on a system: interception, fabrication, modification, and interruption. A fifth classes of attacks-repudiation-is an attack against the accountability of information. A fifth class of attacks-repudiation-is an attack against the accountability of information, see Table1.

A. Interception

Interception is a passive attack on confidentiality where an intruding entity is able to read the information that is sent from the source entity to the destination entity.

We take eavesdropping and sniffing as an example of interception attack, in this attack; gathering information about the network (such as the SSID, the MAC address of the Access Point (AP), and information about whether WEP is enabled) is getting easier with the release of several products. Interception can occur far outside the user's working range by using high-gain antennas (many of which are standard offerings from some vendors).

Table 1, Five classes of attacks

Attack	On	Solved By
Interception	Confidentiality and privacy	Encryption/Decryption
Fabrication	Authenticity	Authentication
Modification Replay Reaction	Integrity	Digital signatures on every message.
Interruption	Availability	No effective solutions exist for interruption / Denial of Service attacks on availability.
Repudiation	No repudiation	Non-repudiation currently still suffers of cases of identity theft.

B. Fabrication

Fabrication is an active attack on authentication where an intruder pretends to be the source entity. Spoofed

packets and fake e-mails are examples of a fabrication attack.

Man-in-the-Middle Attacks is an example of fabrication, in order to execute a man-in-the-middle attack, two hosts must be convinced that the computer in the middle is the other host. Spoofing, Insertion Attacks and Brute Force Password Attacks are also examples of fabrication attacks.

C. Modification, Replay, and Reaction Attacks

Modification is an active attack on integrity where an intruding entity changes the information that is sent from the source entity to the destination entity .The insertion of a Trojan horse program or virus is an example of a modification attack. Virus Infection is another issue that affects both wired and wireless networks. There have been viruses that are capable of sending text messages to cell phones. Two of these are VBS/Timo-A and the Love Bug. Replay is an active attack on integrity where an intruding party resends information that is sent from the source entity to the destination entity. Examples of Replay attacks are Traffic Redirection and Invasion and Resource Stealing. Reaction is an active attack where packets are sent by an intruder to the destination.

D. Interruption

Interruption is an active attack on availability where an intruding entity blocks information sent from the originating entity to the destination entity. Examples are denial of service (DoS) attacks and network flooding.

The intruder may try to exhaust all network bandwidth using ARP flooding, ping broadcasts, Transmission Control Protocol (TCP) SYN flooding, queue flooding, smurfs, synk4, and other utilities.

Examples of Interruption Attack are Denial of Service (DoS) attacks and Rogue Networks. Rogue Networks and Station Redirection a rogue AP is one owned by an attacker that accepts station connections and then intercepts traffic and might also perform man-in-the-middle attacks before allowing traffic to flow to the proper network. The goal of a rogue is to move valid traffic off the WLAN onto a wired network for attacking (or to conduct the attack directly within the rogue AP) and then reinsert the traffic into the proper network.

E. Repudiation

Repudiation is an active attack on no repudiation. Either the source or the destination denies sending or receiving a message.

III. FUNDAMENTALS OF WIMAX

WiMax is an emerging broadband wireless last mile technology to provide higher speed at longer distances from 30 to 50 miles and its transfer rate is up to 70 Mbps. Initial version of the 802.16 standard was operating in 10 to 66 GHz providing line-of-sight connectivity and supports data rate up to 134Mb/s. The other standard 802.16a provide non line-of-sight transmission and provide lower frequency band (2 to 11 GHz). These two classes of WiMAX systems are fixed WiMax and mobile WiMax. Fixed WiMax provide fixed services while the mobile WiMax provides mobility. IEEE designated standards for fixed wireless applications as 802.16-2004 and 802.16e-2005 for mobile WiMax. The latest 802.16 standard adds support for mobility of SS (Subscriber Station). So when there is mobility the threats and attacks also increases. According to additional 802.16 standards are in the works and will cover:

- 802.16b – Quality of service (QoS),
- 802.16c – Interoperability, with protocols and test suite structures,
- 802.16d – fixing things not covered by 802.11c, which is the standard for developing access points,
- 802.16e – Support for mobile as well as fixed broadband.

802.16/WiMax operates on two layers, the physical (PHY) layer and the Media Access Control (MAC) layer. Threats are always there to both layers. But the physical layer is much vulnerable to threats as compared to MAC layer. The physical layer handles signal connectivity, error correction, initial ranging, registration, bandwidth requests, and connection channels for management and data. The MAC layer manages connections and security. Physical layer is below the security sub layer, that's why the physical layer is open to the threats. The threats to the physical layers of WiMax are *scrambling* and *jamming*. The security implemented at the MAC layer has several shortcomings especially with respect to Authentication and confidentiality. The serious threats are to the level of authentication. While establishing new connection many problems arise regarding the authentication level and also to authorize the authenticate person. Many of the security problems are solved but still some attacks are not yet been countermeasure, and new attacks are taking birth on daily basis may be on hourly basis.

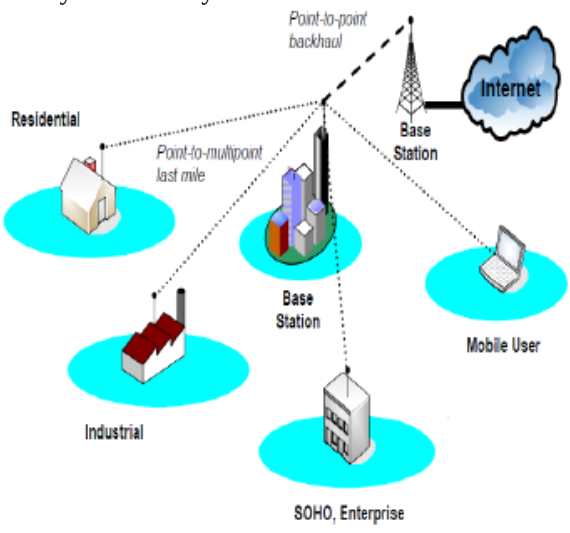

Figure 1: Wimax Applications

In WiMax applications, there is a Base Station (BS) and multiple Subscriber Stations (SSs). The connection between the Base Station (BS) and the Subscriber Stations (SSs) may be Point-to-Point or may be Point-to-Multi Point. IEEE 802.16 Point-to-Multi Point (PMP) mode is a networking infrastructure where every SS (Subscriber Station) communicates directly with the BS.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

IV. Pretty Good Privacy (PGP) Security Services

A. Key Generation and Storage

PGP allows a user to generate multiple key pairs (public key/private-key pairs) for each public scheme supported. Different key pairs are generated for public key encryption and for digital signatures. The key pairs, together with public keys of other users, are stored in a file called the key ring.

Information stored with a public key includes the user's name, email address, trust and validity indicators, key type, key size, expiry date, fingerprint (e.g., the 160-bit SHA-1 hash of the formatted public key), and a key ID (e.g., the low order 64 bits of the fingerprint).

Private keys are not stored directly in the key ring. Instead, the user selects a passphrase which is salted and hashed to derive a key k for a symmetric encryption scheme. The private key is encrypted using k, the passphrase is discarded, and the encrypted private key is stored. Subsequently, when the user wishes to access a private key (in order to decrypt a message or sign a message), the passphrase must be supplied so that the system can regenerate k and recover the private key.

B. Cryptographic Services

PGP uses a combination of symmetric-key and public-key methods to provide authentication and confidentially.

A message can be signed using the private key from a suitable public-key signature scheme. The recipient can verify the signature once an authentic copy of the signer's corresponding public key is obtained. The OpenPGP standard requires support for SHA-1 as a hash algorithm and the DSA, and encourages support for the MD5 hash function and RSA as a signature algorithm.

The use of symmetric-key algorithms (such as DES) alone for encryption is supported, although PGP is known more for the confidentiality provided by a combination of public-key and symmetric-key schemes. Since public-key encryption schemes tend to be computationally expensive, a session key is used with a symmetric-key scheme to encrypt a message; the session key is then encrypted using one or more public keys (typically, one for each recipient), and then the encrypted message along with each encrypted session key is delivered. The standard requires support for an ElGamal public-key encryption scheme and Triple-DES; support for RSA, IDEA, and CAST is encouraged.
Signatures and encryption are often used together, to provide authentication and confidentiality. The message is first signed and then encrypted as described above.
first signed and then encrypted as described above.

C. Key Management

The OpenPGP standard does not have a trust model. An OpenPGP-compliant PGP implementation could support a hierarchical X.509-based public key infrastructure (PKI). The trust model employed by existing PGP implementations is a combination of direct trust and the web of trust. In the former, user A obtains B's public key directly from B; fingerprints facilitate this process as only the fingerprints have to be authenticated. In the web of trust model, one or more users can attest to the validity of B's public key by signing it with their own signing key. If A possesses an authentic copy of the public key of one of these users, then A can verify that user's signature thereby obtaining a measure of assurance of the authenticity of B's public key. This chaining of trust can be carried out to any depth.

V. Experimental Results And Discussions

Due to some complexities in various models of WiMax networks, security has been more stringently placed into WiMax. It is the responsibility of the network service provider to develop comprehensive security strategies for designing a secure network. Otherwise, the network and the users will become vulnerable to threats and hackers. To study the security of WiMax we have to understand the primary protection methods of WiMax security. If we want to achieve end to end secure communication then the security has to be kept in mind. WiMax is designed with a lot of security mechanisms to make it secure form the threats, but still not so secure from threats. We can countermeasure these attacks by using wireless protocols and strong encryption techniques.

The encryption strength of both the techniques is the same but the key size matters. The description is shown in Figure 2. In the given figure we can see in detail that the key size of PGP is much smaller than that of RSA but having the same encryption strength. So the result may show that the cracking of both the techniques will take the same time.

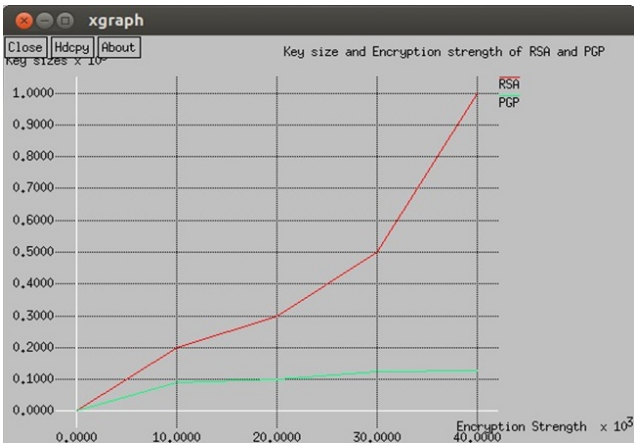

Figure 2: Key Size and Encryption Strength of RSA and PGP.

We construct two duplicate scenarios, one uses RSA and other one uses PGP for Authorization in Authentication phase. Figure 3, shows the delay in authentication phase in both the scenarios.

We run the simulation scenario for 19 times and from the results we conclude that PGP has less delay than RSA while having a smaller key as compared to RSA as shown in Figure 3. In the scenario we have compared two different techniques to choose the best of both and we concluded that PGP is better than RSA.

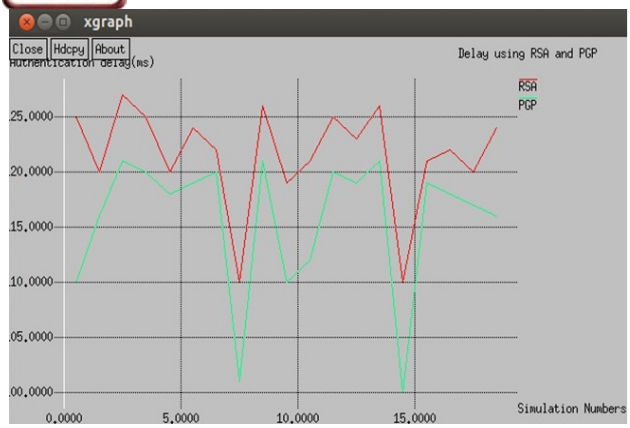

Figure 3: Delay using RSA and PGP.

VI. CONCLUSION

IEEE 802.16, known as WiMax, is at the top of communication technology drive because it is gaining a great position in the next generation of wireless networks. Due to the evolution of new technologies wireless is not secured as like others networking technologies. To achieve End-to-end secure communication then the security has to be kept in mind. By keeping in mind the importance of security, the wireless network has been designed with several security mechanisms to provide protection against unauthorized access and malicious threats, but still facing a lot of challenging situations.

An authentication and authorization model provides protection for a network or technology and protects its resources from unauthorized use. It proposed some enhancements to the existing model to improve its capabilities and encryption strength for security. We have proposed some enhancements to the existing model to improve its capabilities and encryption strength for security. The comparison of the RSA and PGP was done and we conclude that PGP is much better that RSA having a smaller key size than RSA. The delay was calculated and the delay in PGP was smaller than RSA.

REFERENCES

[1] Masood Habib, Tahir Mehmood and Fasee Ullah, “Performance of WiMax Security Algorithm” Proceeding on 2009 International Conference on Computer Technology and Development.

[2] M. Nasreldin, Heba Aslan, M. El-Hennawy, A. El-Hennawy, “WiMax Security” International Conference on Advanced Information Networking and Applications 2008, IEEE.

[3] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El-Hennawy, “WiMax Security” International Conference on Advanced Information Networking and Applications 2008, IEEE.

[4] Deepak Pareek “WiMax Taking Wireless to the MAX” By Auer Bach Publications, Taylor & Francis Group Boca Raton New York, 2006.

[5] Hao Yang, Fabio Ricciato, Songwu Lu, and Lixia Zhang, “Securing a Wireless World,” IEEE Commun. Mag., vol. 94, no.2, pp 442-454, Feb 2006.

[6] Dr. Kitti Wongthavarawat “IEEE 802.16 WiMAX Security” Presented at 17th Annual FIRST Conference, Singapore July 1, 2005.

[7] Michel Barbeau, “WiMax/802.16 Threat Analysis” ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet ’05, October 13, 2005.

[8] Matthew Gast, “802.11 Wireless Networks The Definitive Guide,” O’Reilly April 2005.

[9] IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), “IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems,” 2004.

[10] IEEE Std 802.16a-2003, “IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access System Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz” 2003.