Performance evaluation of Hard and Soft Wimax by using PGP and PKM protocols with RSA Algorithm

Gurpreet Singh[1], Dr. Sandeep Singh Kang[2]
[1]*(M.Tech student, Department of CSE, Chandigarh Engineering College, Landran)*
[2]*(Professor & Head, Department of CSE, Chandigarh Group of Colleges, Landran)*

Abstract: *Wimax is a wireless metropolitan area network (MAN) technology that provides interoperability, carrier class broadband wireless connectivity to fixed, portable for the last mile. Wimax (Worldwide interoperability for microwave access) is based on IEEE 802.16 standards that provide wireless access to metropolitan area networks and there are several security problems The Wimax technology has great impact in wireless communication and has notched the top position in the wireless technology. But there still are a lot of securities concerns while using such wireless technologies, especially for Wimax where we have to transfer secure data at high rate from one station to another station. Wimax works at the longer distances so there is more security required to protect the communication from attacks and threats. Wimax is a wireless network which is considered to be more vulnerable to attacks and threats than wired network as data transfer publicity in open areas. For secure the communication in Wimax various algorithms and security protocols are used. The researchers have developed various mechanisms which have made a great impact on secure communications in Wimax. Various encryption and authentication mechanisms are being used for secure communication. The concept of use multiple keys with RSA algorithms using PKM (Privacy & Key management) protocol has been used for secure communication. This concept is extended in this paper by combining PGP (Pretty Good Privacy) protocol with RSA algorithm to further improve the secure communication in Wimax. This paper compares the performance of Hard Wimax and Soft Wimax using PKM and PGP protocols over RSA. The performance is analyzed over NS 2.34 simulator using delay, throughput and packet delivery as performance metrics.*

Keywords - *PGP, PKM, RSA, WIMAX, WMAN.*

I. INTRODUCTION

Wimax(Worldwide interoperability for microwave access) is an emerging wireless communication system that is expected to provide high data rate communication in metropolitan area networks(WMAN).IEEE 802.16 working group has developed a number of standards for Wimax [1]. The Privacy Key Management (PKM) Protocol is used to gain authorization and traffic keying material from the Wimax Base Station (BS), and to maintain periodic reauthorization and key. Wimax CPE (Customer Premise Equipment) act as the client requests keying material while the Wimax Base Station (BS) act as the server act in response to those requests, ensuring individual Wimax CPE (Customer Premise Equipment) clients receive only the keying material for which they are authorized [5]. The authorization protocol for the both version of PKM model is used in Wimax network [3]. Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications [7]. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adelman. RSA involves a public key and a private key [8].

In this paper the focus lies on enhancement in security mechanism by combining PGP (Pretty Good Privacy) protocol with PKM (Privacy and Key Management) protocol over RSA algorithm. We combine these two protocols using RSA mechanism and compare Hard and Soft Wimax using three performance metrics of delay, throughput and packet delivery.

In Section II the security protocols used in this work are briefly discussed followed by the Encryption mechanism in Section III. The simulation environment and performance metrics are discussed in Section IV and the Section V contains the conclusion and future scope.

II. SECURITY PROTOCOLS

There are several protocols proposed for security in the wireless networks. We have to use the combinations of PKM and PGP securities with RSA algorithms for encrypting the information. We have to compare the performance of Soft Wimax and Hard Wimax of PGP and PKM protocol with security implanted by using RSA algorithms.

A: PKM (Privacy and Key Management) Protocol

The Privacy Key Management (PKM) Protocol is used to gain authorization and traffic keying material from the Wimax Base Station (BS), and to maintain periodic reauthorization and key. Wimax CPE (Customer Premise Equipment) act as the client requests keying material while the Wimax Base Station (BS) act as the server act in response to those requests, ensuring individual Wimax CPE (Customer Premise Equipment) clients receive only the keying material for which they are authorized. The AK is then used to protect subsequent Privacy Key Management (PKM) Protocol. [5]. The study Privacy Key and Management (PKM) shows that the security in the PKMv2 is more confidential than that of PKMv1 so the PKMv2 model is mainly used in secure communications. But in the wireless network security is not guarantee because PKMv2 model also suffers from various security threats and attacks, like replay and interleaving attacks [6].

B: PGP (Pretty Good Privacy) Protocol

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. To the best of publicly available information, there is no known method which will allow a person or group to break PGP encryption by cryptographic or computational means. As current versions of PGP have added additional encryption algorithms, the degree of their cryptographic vulnerability varies with the algorithm used. New versions of PGP are released periodically and vulnerabilities are fixed by developers as they come to light. Any agency wanting to read PGP messages would probably use easier means than standard cryptanalysis [7].

III. ENCRYPTION MECHANISM

There are various encrypting mechanisms are used for secure communication like RSA, RC4 and AES. In this paper we have to used the combination of PKM and PGP protocols with RSA encrypting algorithms because it provide better encrypting than other algorithms and processing of the networks also don’t slow down.

RSA algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adelman. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculated [8].

IV. SIMULATION ENVIRONMENT

The study of secure communication is based on experimental setup which is performed using NS 2.34 simulator. The encryption algorithm used in RSA and the security protocols chosen are PKM and PGP. The In general, NS 2.34 provides users with a way of specifying such network protocols and simulating their corresponding behaviours. NS 2.34 is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols [12].

PERFORMANCE METRICS:

The performance metrics are used to analyze the performance of Hard and Soft Wimax on the quantitavely based on values of the results. The results of our study are based on performance metrics as given below:

Throughput- Throughput is defined as the ratio of the total data reaches a receiver from the sender. The time consumed by the receiver to receive the last packet is called throughput. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).

Delay- The packet end-to-end delay is the average time of the packet passing through the network. It includes over all delay of the network like transmission time delay which to the networks, buffer, queues. It also includes the time from generating packet from sender to destination and express in seconds.

Packet Delivery- Packet dropped shows how many packets successfully sent and received across the whole network. It also explains the number of packet dropped during the transmission due to interference from other devices.

V. SIMULATION RESULTS

In this section we analyze the simulation results conducted on protocols. The main target of this paper is to analyze the performance of PKM and PGP with RSA algorithms. The results are based on experiments of delay, packet dropped and throughput. The results are shown below:

Delay

The Fig. 1 shows the entire delay for network with combination of PGP and PKM protocols. The results clearly show that the Hard Wimax shows high delay as compared to the Soft Wimax with PGP and PKM protocols using RSA algorithm. Initially both shows equivalent delay but later on Soft Wimax shows lower delay as compared to Hard Wimax.

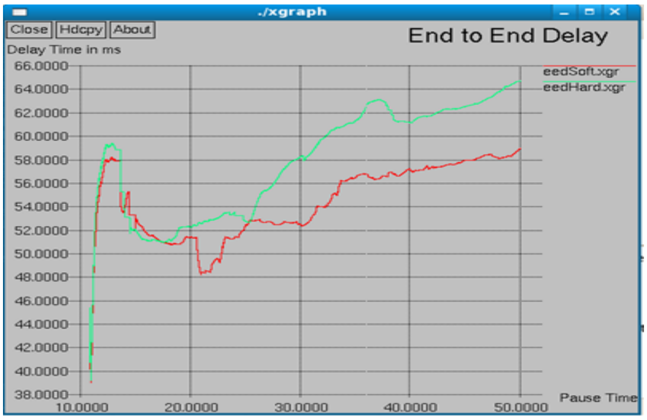

Fig 1: Delay for Hard Wimax and Soft Wimax

Throughput

The Fig. 2 shows the throughput of network with using combination of PGP and PKM protocol with RSA algorithm in Wimax Network. The result shows that the Soft Wimax shows high throughput as compared to the Hard WiMAX.

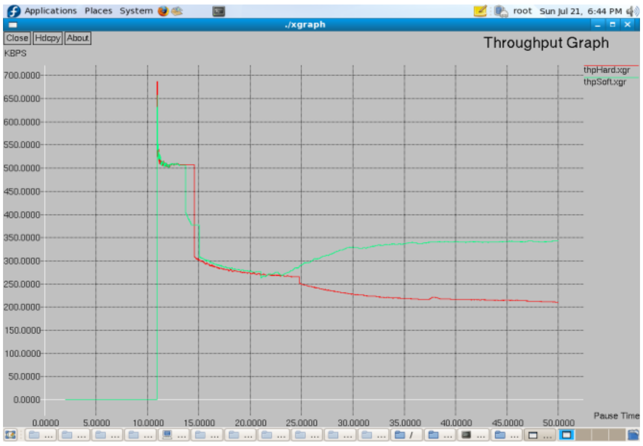

Fig. 2: Throughput for Hard Wimax and Soft Wimax

Packet Delivery

The Fig. 3 shows the packet delivery in the network with using combination of PGP and PKM protocol with RSA algorithm over Wimax Network. The results show that the Soft Wimax shows better packet delivery as compared to the Hard Wimax.

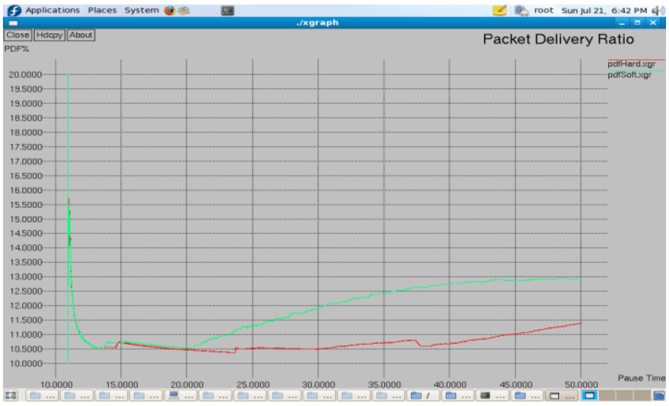

Fig. 3: Packet Delivery for Hard Wimax and Soft Wimax

VI. CONCLUSION AND FUTURE WORK

This study clearly shows that the Soft Wimax shows better performance over Hard Wimax. The study also shows an enhanced mechanism for secure communication over Wimax Network. The following points may be concluded from this experimental study:

- The Soft Wimax Shows lower delay. The discussion of shows that Hard Wimax have more delay time for transmitting the data in the network thus it will be affect the performance of the network
- The Soft Wimax shows higher throughput and hence a better performance.
- The Soft Wimax shows better packet delivery than Hard Wimax which is an essential factor for good performance.

Hence the overall result shows a better performance by Soft Wimax than Hard Wimax.

In the future work there are various encrypting algorithms and protocols used for secure communication that can be evaluated. A modified protocol with combination of PKM and PGP can also be developed for better performance.

References

[1] Lu, K., Qian, Y. and Chen, H. (2007), *"A Secure and Service-Oriented Network Control Framework for Wimax Networks", IEEE Communication Magazine, May 2007.*

[2] Habib, M., Ahmed, M. (2010), *"A Review of Some Security Aspects of Wimax & Converged Network",* IEEE 2010 Second International Conference on Communication Software and Networks.

[3] Altaf,A., Ahmed,A.and Javed,M. (2008), "*Security Enhancement for Privacy and Key Management Protocol in IEEE 802.16e-2005*".IEEE Ninth ACIS International Conference on Software Engineering, Artificial Intelligence,Networking and Parallel/Distributed Computing.

[4] Taha, A., Abdel-Hamid, A., and Tahar, S. (2009), *"Formal Verification of IEEE 802.16 Security Sub layer Using Scyther Tool",* 2009 ESR Grops France.

[5] http://freewimaxinfo.com/pkm-protocol.html.

[6] Altaf,A., Ahmed,A.and Javed,M. (2008), "*Security Enhancement for Privacy and Key Management Protocol in IEEE 802.16e-2005*".IEEE Ninth ACIS International Conference on Software Engineering, Artificial Intelligence,Networking and Parallel/Distributed Computing.

[7] http://en.wikipedia.org/wiki/Pretty_Good_Privacy.

[8] http://en.wikipedia.org/wiki/RSA_28algorithm.

[9] Yang, F. (2011), *"Comparative Analysis on TEK Exchange between PKMv1 and PKMv2 for Wimax",* IEEE 2011 School of Information and Security Engineering, Zhongnan University of Economics and Law.

[10] Xu, S., Huang, T., and Matthew, M. (2008), *"Modelling and Analysis of IEEE 802.16 PKM Protocol using CasperFRD"*, IEEE 2008.

[11] Adibi,S., Lin, B., Ho,P., Agnew,G., Erfani, S. (2006), "*Authentication Authorization and Accounting (AAA) Schemes in Wimax*", Electro/information Technology, 2006 IEEE International Conference on 7-10 May.

[12] Introduction to Network Simulator NS2_c 2009 Springer Science Business Media, e-ISBN: 978-0-387-71760-9