Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Hybrid Technique of PGP and PKM over RSA in WiMax Networks

Gurpreet Singh *
M. Tech Student CEC,Landran
India

Dr. Sandeep Singh Kang
Professor and Head,CGC Landran
India

Abstract*— Worldwide interoperality for microwave access was proposed to provide high speed data distribution through Wireless Metropolitan Area Networks (WMAN), with the advantage of rapid deployment scalability, and low upgrade cost. It and Management (PKM) protocol works as Authentication and Authorization to secure the information. . As we study also provides throughput broadband connections over long distances. The IEEE 802.16. WiMax applications, there is a Base Station (BS) and multiple Subscriber Station (SSs).The connection between the Base Station and Subscriber Station may be Point to Point and Point to Multipoint.IEEE 802.16.The privacy key and a management (PKM) protocol are also occur in model to improve the securities performance of IEEE 802.16, new version of the protocol. The Privacy Key about the PKM Protocol model various attacks should be attack on the PKM model of authentication protocol. The PKM have many security problems and no guarantee for secure transfer communication between the channels. 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. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography and finally public-key cryptography; each step uses one of several supported algorithms. . RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.

***Keywords*—PGP, PKM, RSA, WMAN, WiMAX.**

I. INTRODUCTION

The introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper. In this paper we have to discuss about the wireless communication technology. The technology is WIMAX has great for wireless communication and gain the top position in the wireless technology. But there is a lot of securities concerns while using wireless technologies [5]. WiMax security has two goals,one is provide to privacy across the wireless network and other is to provide control to the network. Privacy is accomplished by encrypting connection between the subscriber station and base station [3]. WiMax has some similarities with Wi-Fi,Wimax has security aspects are stronger than that of Wi-Fi[4].WiMax should be used like cellular networks, high speed internet access and "last mile" connections. The IEEE 802.16 standards that provide the privacy key and a management (PKM) protocol [6].WiMax Architecture, privacy key and management (PKM), giving the solutions of the securities problems and threats occurred in the networks. The comparison of Privacy Key and Management (PKM) of both model like PKMv1 and PKMv2 give the result, which show that the security in the PKMv2 is more confidentially than that of PKMv1.there for PKMv2 model should be used in the mainly application and secure communication [1].

PGP supports message authentication and integrity checking. The latter is used to detect whether a message has been altered since it was completed (message integrity) and the former to determine whether it was actually sent by the person or entity claimed to be the sender (digital signature). Because the content is encrypted, any changes in the message will result in failure of the decryption with the appropriate key. Public Key algorithms do the tricks with public and private keys. They can be slow, and are also more vulnerable to special kinds of attacks. Therefore these keys are only used to encrypt small pieces of random data, like randomly generated session keys of block ciphers and the outcome of hash functions [7]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages [8]. In this paper we have to implement the PKM and PGP Protocols by using the RSA encrypting algorithms. Because in the Wireless Wimax networks can have many securities problems. The various Protocols and Encrypting Algorithms are used for security purpose. But there is no guarantee of secure information.So, for improve the security of Wireless Networks working on Wimax we have to use protocols with encrypting algorithms. There foe we have to implement the PKM and PGP security protocols on the networks to enhanced the security and improve the performance of the networks.

II. SECURITY PROTOCOLS

There are various security protocols are used for secure the networks and information without affecting the performance of the networks. When security Protocol is implemented it is also measure that the protocol implemented on the networks would not affect the processing speed and performance of the networks. Such that we have to implanted the protocols like PKM and PGP in the network with encrypting algorithms.

2.1 Privacy Key and Management (PKM)

The Privacy Key Management (PKM) Protocol to gain authorization and traffic keying material from the Wimax Base Station (BS), and to maintain periodic reauthorization and key refresh. The Privacy Key Management (PKM) protocol uses X.509 digital certificates, and two-key triple Data Encryption Standard (DES) to secure key exchanges between a given Wimax SS (Subscribe station) and Wimax Base Station (BS), following the client-server model keys. The Privacy Key Management (PKM) Protocol first creates an Authorization Key (AK), which is a secret symmetric key shared between the Wimax SS and BS [9]. For this Subscriber uses the Authentication and Authorization process for communication. and key exchange method is used to protecting the Authorization Key (AK). PKMv1 and PKMv2 are mainly protocol used in WiMax (IEEE 802.16) network by which Authorization Key exchange (AK) and TEK exchange methods provides security. This paper gives the result of TEK exchange according to the used in both model PKMv1 and PKMv2.This paper shows the result of comparison of the model used like PKMv1 and PKMv2 in TEK exchange. After result compare there are many security problems occurs in PKMv1.of TEK exchange [10].

The Privacy Key and Management (PKM) of both model like PKMv1 and PKMv2, which show that the security in the PKMv2 is more confidentially than that of PKMv1.there for PKMv2 model should be used in the mainly application and secure communication. 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].

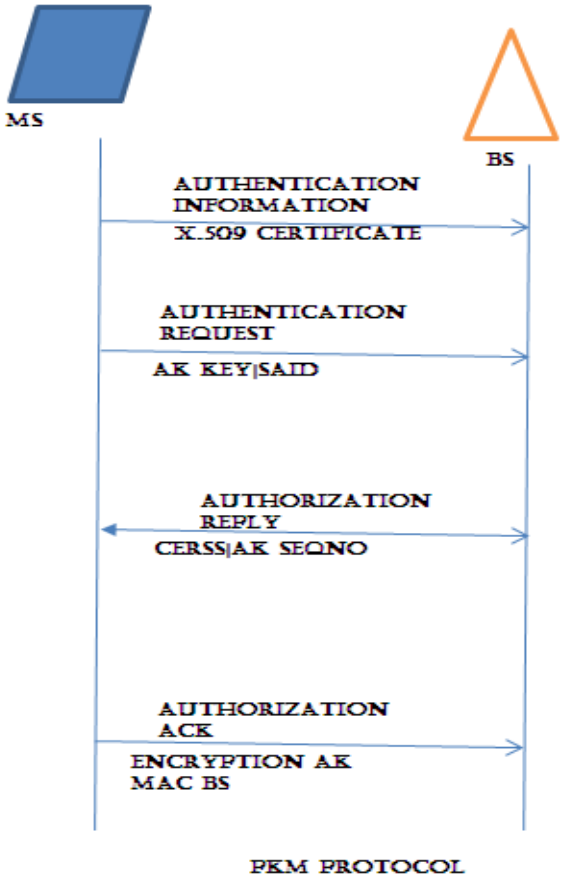

Fig:PKM Protocol Model

2.2 Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a computer program for personal privacy. It delivers privacy by making it impossible for other people to read your computer files and email, and by making it im-possible for other people to impersonate you. To achieve this it uses cryptographic techniques: en-cryption and digital signatures. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key. The message and its session key are sent to the receiver. The session key must be sent to the receiver so they know how to decrypt the message, but to protect it during transmission it is encrypted with the receiver's public key. PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Therefore these keys are only used to encrypt small pieces of random

data, like randomly generated session keys of block ciphers and the outcome of hash functions. Public key algorithms can normally be used for encryption and signing. These algorithms are not needed for the basic functions of PGP [7].

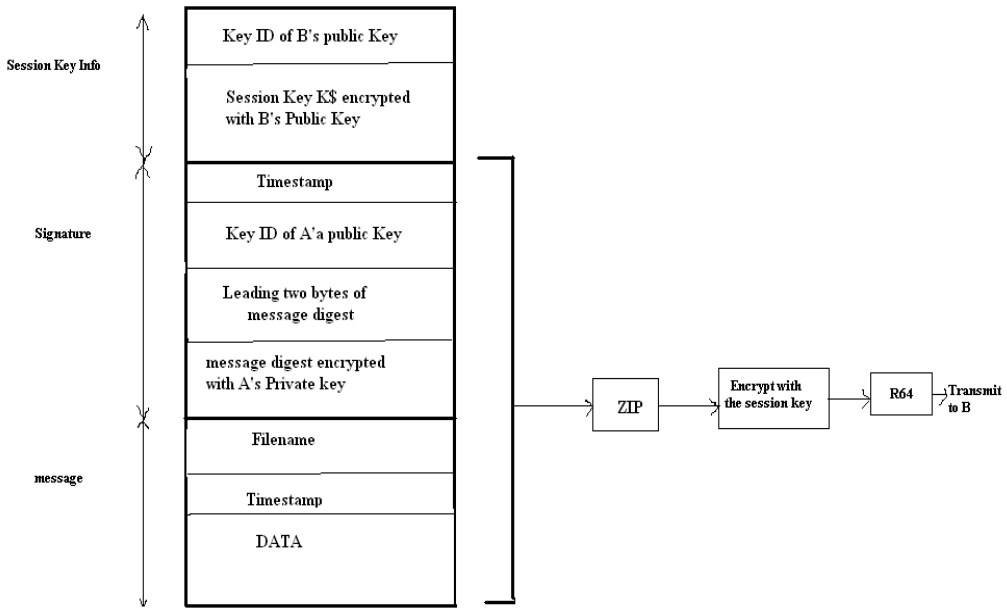

FIG:PGP PROTOCOL MODEL

III. ENCRYPTING MECHANISM

There are various encrypting mechanisms are used for secure communication like RSA, RC4 and AES Algorithms. I have to use for combinations of PKM and PGP protocols with RSA encrypting algorithms because it provide better encrypting than another algorithms and processing of the networks are not to be slow down. That's why I have to use RSA algorithm.

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 calculate d . The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute n = pq.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and φ(n) are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[
5. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).
   - This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent [8].

IV. THE PERFORMANCE PARAMETERS

In this section we analyze the simulation the 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.

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. FIGURES AND TABLES

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 of PGP and PKM protocol with combination. The networks shows delay as compared to PGP and PKM. The results describe that Hard Wimax shows high delay as compared to the Soft WiMAX with PGP and PKM.

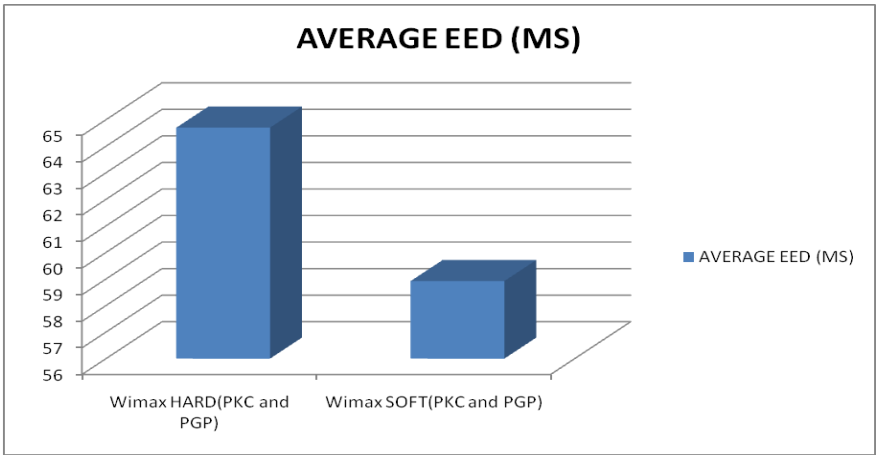

Fig.1: Delay for Hard WiMAX and Soft WiMAX

Table: Delay for Hard WiMAX and Soft WiMAX

TECNIQUE	AVERAGE EED(MS)
WiMax Hard (PKM and PGP)	64.7
WiMax Soft (PKM and PGP)	58.92

Throughput

The Fig. 2 shows the throughput of network with using PGP and PKM protocol in Wimax Networks. The networks give the throughput as compared to Hard Wimax and Soft Wimax with PGP and PKM on RSA algorithms. The results describe that Soft Wimax shows high throughput as compared to the Hard WiMAX with PGP and PKM.

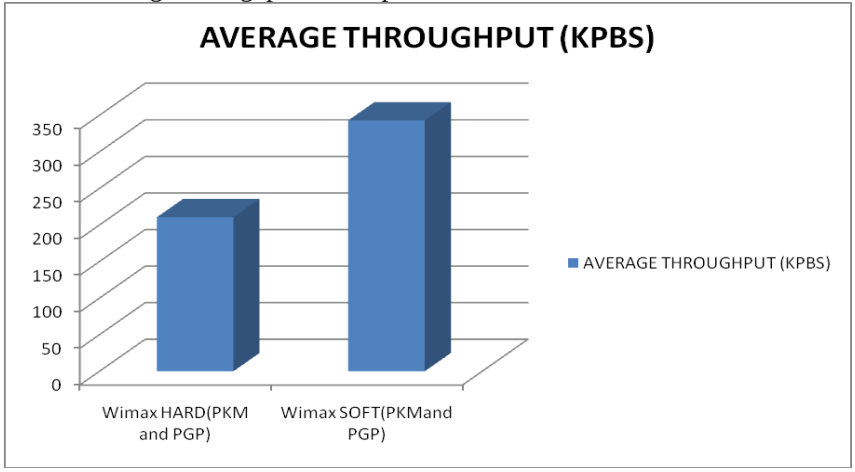

Fig. 2: Throughput for Hard WiMAX and Soft WiMAX

Table: Throughput for Hard WiMAX and Soft WiMAX

TECNIQUE	AVERAGE THROUGHPUT(KPBS)
WiMax Hard (PKM and PGP)	210.59
WiMax Soft (PKM and PGP)	342.92

Packet Delivery

The Fig. 3 shows the packet delivery in the network with using PGP and PKM protocol of Wimax Networks. The networks give the result of packet delivery as compared to Hard Wimax and Soft Wimax with PGP and PKM on RSA algorithms. The results describe that Soft Wimax shows better packet delivery as compared to the Hard WiMAX with PGP and PKM.

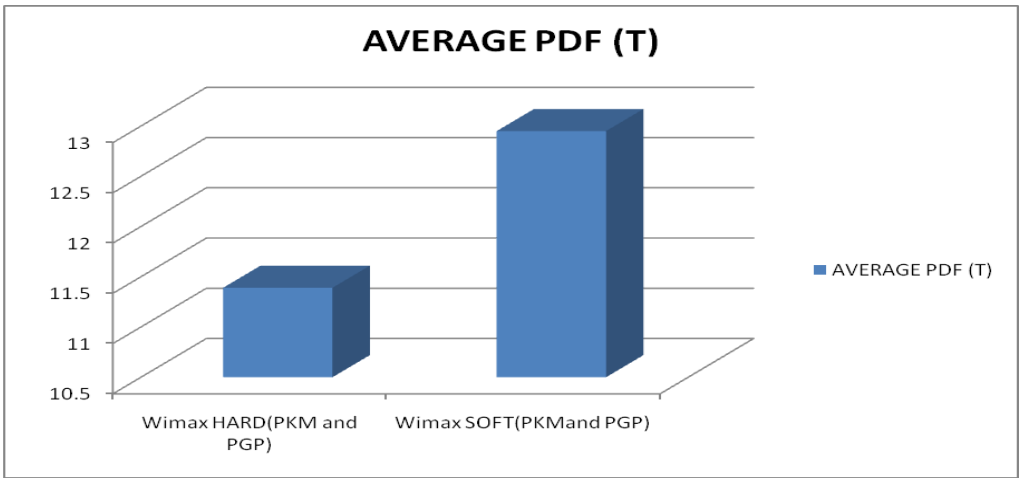

Fig. 2: Packet Delivery for Hard WiMAX and Soft WiMAX

Table: Packet Delivery for Hard WiMAX and Soft WiMAX

TECNIQUE	AVERAGE PDF(T)
WiMax Hard (PKM and PGP)	11.39
WiMax Soft (PKM and PGP)	12.92

VI. CONCLUSION AND FUTURE WORK

The conclusion of this paper is mainly works on wireless networks like IEEE Wimax. In Wimax network we have to compare the performance of Privacy Key and Management and Pretty Good Privacy Protocol with RSA algorithms the result shows that the performance of Soft Wimax gives the better performance than Hard Wimax on comparing with PKM and PGP in the Wimax network. The parameters are used for comparing the protocol like End to End Delay, Packet Delivery and Throughput. The discussion of these parameters gives the clear point that in case of Delay time the Hard Wimax have more delay time for transmitting the data in the network thus it will be affect the performance of the network while in case of Soft Wimax the parameters like Throughput and Packet Delivery to the networks.

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

[2] Habib. M., Mehmood, T., Ullah, F.and Ibrahim, M. (2009), *"Performance of WiMAX Security Algorithm".* IEEE 2009 International Conference on Computer Technology Development.

[3] Wei-min, L., and Run-sheng, W. (2008), *"A Simple Key Management Scheme based on WiMAX",* IEEE 2008 International Symposium on Computer Science and Computational Technology.

[4] 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.

[5]H abib. M., Mehmood, T., Ullah, F.and Ibrahim, M. (2009), *"Performance of WiMAX Security Algorithm".* IEEE 2009 International Conference on Computer Technology Development.

[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] http://en.wikipedia.org/wiki/Privacy_Key_Management.

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

