Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-270-272
Available online at http://www.bioinfo.in/contents.php?id=55

STUDYING THE BEHAVIOR OF DIFFERENT CRYPTOGRAPHIC TECHNIQUES OF IPSEC ON DIFFERENT WIMAX SCENARIOS

MONIKA RANI[1] AND SAINI K.K.[2]

[1]Electronics & Comm. Engg., DCRUST, Murthal (Sonipat)
[2]Electronics & Comm. Engg., IITM, Murthal (Sonipat)
*Corresponding Author: Email– [1]sneha_mnc24@yahoo.co.in and [2]dpiitm2011@gmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Worldwide Interoperability for Microwave Access (WiMAX) is a telecommunications technology providing wireless data, voice and videos over long distances." The main goal of WiMAX is to deliver wireless communications with quality of service (QoS) guarantees, security and mobility. With the help of Wimax technology, one can overcome the limitations of the existing wireless communication like short coverage area, lack of security and low data rate. In this study, different cryptographic techniques like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), (DES+MD5), (Message Digest) MD5 have been used for different packet sizes and evaluated their performances on the basis of trade of index. Also, these cryptographic techniques are applied for group communications in WiMAX networks. Here, 10 WiMAX scenarios are discussed based on these techniques, which can be further, extended for large no of scenarios for studying the behavior of IPSec over WiMAX.
Keywords- 2G, 3G, cryptography, IPSec, IKE

Citation: Monika Rani and Saini K.K. (2012) Studying the Behavior of Different Cryptographic Techniques of IPSec on Different WiMax Scenarios. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-270-272.

Introduction

In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user/device knows the private key whereas the public key is distributed to all users/ devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online. Whereas in private key cryptography, there is the same key to do the cryptographic operation.

We define security as protection of data being transmitted over a wireless networks. WiMAX is an emerging wireless communication system that is expected to provide high data rate communications in Metropolitan Area Networks (MANs) [2]. In the past few years, the IEEE 802.16 working group has developed a number of standards for WiMAX.

The first standard was published in 2001, which aims to support the communications in the 10–66 GHz frequency band. In 2003 IEEE 802.16a was introduced to provide additional physical layer Specifications for the 2–11 GHz frequency band. These two standards were further revised in 2004 (IEEE 802.16-2004).

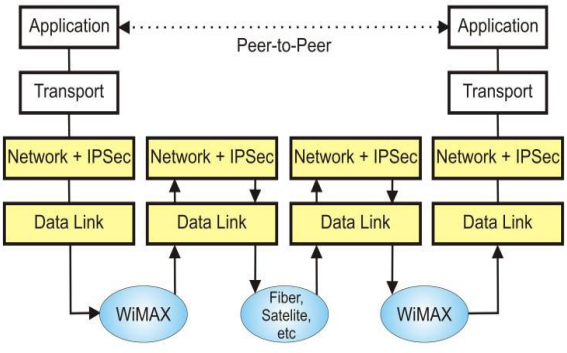

Fig. 1- Wimax Scenario

Recently, IEEE 802.16e has also been approved as the official standard for mobile applications. Encryption algorithms which use the same key for both encryption and decryption are known as symmetric key algorithms. A newer class of "public key" crypto-

graphic algorithms was invented in the 1970s which uses a pair of keys, one to encrypt and one to decrypt. These asymmetric key algorithms [6] allow one key to be made public while retaining the private key in only one location. They are designed so that finding out the private key is extremely difficult, even if the corresponding public key is known. A user of public key technology can publish their public key, while keeping their private key secret, allowing anyone to send them an encrypted message. Our goal is to simulate the scenario shown in Figure1.

The rest of this article is organized as follows: we will briefly review "IPSec" in Section 2. Section 3 introduces our "Methodology". Section 4 analyzes the "Conclusion and Future work".

IPSec basics

Internet Protocol Security (**IPSec)**[3] is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session[1]. IPSec is a suite of protocols for securing network connections, but the details and many variations quickly become overwhelming. This is particularly the case when trying to interoperate between disparate systems, causing more than one engineer to just mindlessly turn the knobs when attempting to bring up a new connection. According to [1], IPSec is a developing network layer security mechanism. It protects traffic between endpoints at the network layer and it is totally independent from any application, which runs above the network layer. Originally IPSec was designed for wired networks and the wireless networks' limitations, such as the processing power of mobile devices and the limited resources of wireless channels were not been considered.

The protocol allows the communicating nodes to set up secure channels to send and receive data. It also allows cryptographic algorithms to be applied and increase the security. Depending on the required security level for applications, different cryptographic algorithms may be applied.. One cause of the complexity is that IPSec provides mechanism, not policy: rather than define such-and -such encryption algorithm or a certain authentication function, it provides a framework that allows an implementation to provide nearly anything that both ends agree upon. There are several correlated parameters like:

- **AH *versus* ESP**

"Authentication Header" (AH) and "Encapsulating Security Payload" (ESP) are the two main wire-level protocols used by IPSec, and they authenticate (AH) and encrypt+authenticate (ESP) the data flowing over that connection. They are typically used independently, though it's possible (but uncommon) to use them both together.

- **Tunnel mode versus Transport mode**

Transport Mode provides a secure connection between two endpoints as it encapsulates IP's payload, while Tunnel Mode encapsulates the *entire* IP packet to provide a virtual "secure hop" between two gateways.

- **IKE versus manual keys**

Since both sides of the conversation need to know the secret values used in hashing or encryption, there is the question of just how this data is exchanged. Manual keys require manual entry of the secret values on both ends, presumably conveyed by some out-of-band mechanism, and Internet Key Exchange (IKE) is a sophisticated mechanism for doing this online.

- **Main mode versus aggressive mode**

These modes control an efficiency-*versus*-security tradeoff during initial IKE key exchange. "Main mode" requires six packets back and forth, but affords complete security during the establishment of an IPSec connection, while Aggressive mode uses half the exchanges providing a bit less security because some information is transmitted in clear text.

The Internet has a great many resources surrounding IPSec, some better than others. The starting point, of course, is always with the Requests for Comment (RFCs) that form the Internet standards defining the protocols. These are the main reference works upon which all other documentation — including this one — is based. Some of the RFCs are: RFC 2401, RFC 2403, RFC 4301, RFC 4302 etc[7].For further explanation on IPSec, it is advised to study the aictewwhitepaperprotocolsuite for IPSec[1].

Methodology

"Trade of Index" is a parameter to calculate the efficiency**.** In this study**, so** many cases have been taken to find trade of index by varying the packet sizes and cryptographic algorithms. After that average trade of index is calculated. Also different scenarios have been taken for selecting the best technique for encryption.

The techniques used are:

AES(128,196,256),DES,3DES,MD5,DES+MD5.

Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. It is used widely because the algorithm is fast in both software and hardware, easy to implement and requires little memory [6]. AES has been designed to be resistant to well known attacks and exhibits simplicity of design.

The DES algorithm [5] is a symmetric block cipher with block and key size of 64 bits. DES has been proven not a reliable cryptographic scheme as special hardware can break DES in a few hours. This has been the reason to introduce 3DES (or triple DES). 3DES algorithm is the 3 times repetition of the DES. First a data block is encrypted with the DES algorithm using an initial key, then the encrypted block is decrypted using a different key and then the new block is re-encrypted using the initial key. However, the disadvantage of 3DES is that it runs three times slower than DES on the same platform [7].

Performance evaluation

In this section, the simulation results have been calculated by using QualNet 5.0, in Table 1, different processing times are shown for AES, DES, 3DES, MD5 with a processor of 400 MIPS [1].

Table 1- Processing Times for 400 MIPS [4]

PKT	AES	MD5	3 DES	DES
500	0.508	0.023	1.335	0.445
600	0.6	0.026	1.578	0.525
700	0.709	0.028	1.84	0.6135
800	0.802	0.0317	2.083	0.695

After the simulation result, 3DES algorithm has the biggest processing time because it repeats the DES algorithm 3 times. The AES requires a little bit more processing time than the DES. Finally, MD-5 does not require more processing power because it does not do any encryption or decryption and it is just used to create a message digest for authentication and integrity.

The very first scenario is when taking 13 subscriber stations, 3 base stations, 2 cbr applications. The average Trade of Index is calculated by applying different cryptographic techniques. This is shown graphically as:

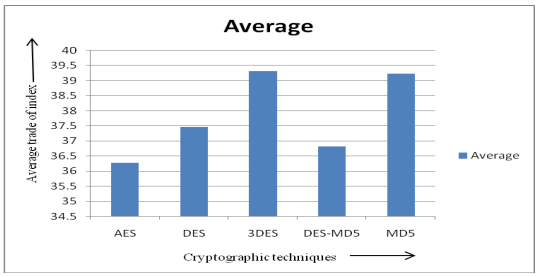

Fig. 2- Performance of 13SS+3 BS+2 CBR

This is the graph showing trade of index for 13ss+3bs+2cbr. on the basis of this, one can say that 3DES is best.
Next, we have the case of 13SS+3BS+3CBR. The average Trade of Index curve comes as:

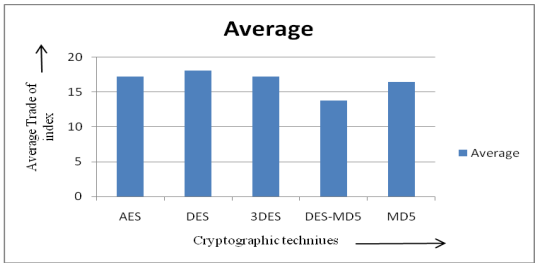

Fig. 3- Performance of 13SS+3BS+3CBR

Here also, we can say that 3DES is best cryptographic technique out of all others as DES gets cracked very easily and in almost all the cases 3DES comes out to be the best technique for encryption.
Similarly there are several cases, like we have done the group communication by using (1 CBR applications, 2BS, 20SS) then the best cryptographic technique on the basis of trade of index came out to be 3DES only irrespective of packet sizes. Moreover BS are increased then also 3DES came out to be the best technique. This is shown graphically as:

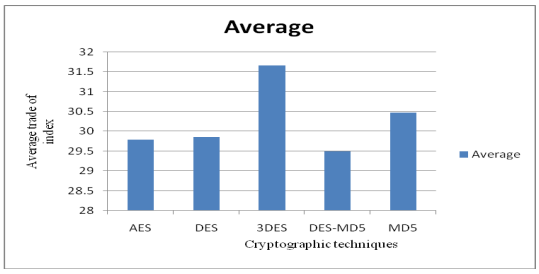

Fig. 4- Performance of 20SS+2BS+1CBR

Conclusion and future work

In this paper, IPSec protocol over WiMAX has been analyzed. IPSec is probably one of the most secure protocols nowadays. It protects traffic between endpoints at the network layer by using different cryptographic algorithms and hash message authentication codes.
After a series of simulations and experimentations we observed that AES is the best cryptographic algorithm in terms of throughput but if we take the concern of "Trade of Index" then 3DES comes out to be the best cryptographic algorithms in different CBR applications.
In future, we can also add one protocol "ISAKMP" which stands for "internet security association and key management protocol" with IPSEC that can increase its performance in terms of trade of index, throughput, processing time etc.

References

[1] Levon Nazaryan, Nabeel Khan, Emmanouil A. Panaousis and Christos Politis, *Performance Evaluation of IPsec overWiMAX*.
[2] Vaughan-Nichols S.J. (2004) *IEEE Comp.*, vol. 37, issue 6, pp. 10–13.
[3] Xenakis C., Laoutaris N., Merakos L. and Stavrakakis I. (2006) *A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms*.
[4] Mishra A. and Glore N. (2008) *Book Chapter of WiMAX Standards and Security*, CRC Press, 2008
[5] Xenakis, N. Laoutaris, L. Merakos and Stavrakakis I. (2006) *A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms*.
[6] *http:/www.wimaxforum.com*.
[7] *http:///www.ietf.org/rfc.*