Performance Evaluation of IPsec over WiMAX

Levon Nazaryan, Nabeel Khan, Emmanouil A. Panaousis and Christos Politis
Wireless Multimedia & Networking (WMN) Research Group
Kingston University London
KT1 2EE London, United Kingdom
{l.nazaryan, e.panaousis, c.politis}@kingston.ac.uk

***Abstract*—The IEEE 802.16 standard, which is also known as Worldwide Interoperability for Microwave Access (WiMAX), is one of the latest technologies in the wireless world. The main goal of WiMAX is to deliver wireless communications with quality of service (QoS) guarantees, security and mobility. In this paper we evaluate the performance of the Internet Protocol Security (IPsec) protocol over WiMAX networks. We mainly illustrate the results of the simulations. To this end we depict the processing time and the throughput introduced when IPsec is applied over WiMAX. Then we research the best cryptographic algorithm to encrypt the end-to-end IPsec traffic. The most commonly used cryptographic algorithms and Hashed-Message Authentication Codes (HMAC), such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3DES, Secure Hash Algorithm 1 (SHA-1) and Message Digest 5 (MD5) are considered in the paper.**

***Index Terms*—WiMAX, Security, IPsec**

I. INTRODUCTION

Due to their open medium nature, wireless networks require a higher level of security than wired networks. Many technologies have been developed to secure networks and the IPsec protocol [1] is one of them. IPsec provides security services, such as confidentiality, integrity and authentication, to increase the security level in networks. IPsec operates at the network layer of the Internet protocol stack.

All network communications between two hosts or networks can be protected at the network layer without modifying any applications on the clients or servers. Hence, the reason why IPsec provides a much better solution than transport or application layer protocols is the difficulty to add security controls to individual applications. In addition IPsec provides a way for network administrators to enforce certain security policies.

This paper evaluates the performance of IPsec over WiMAX networks. We use a WiMAX network as a backbone connection and we implemented the IPsec protocol to guarantee a secure end-to-end connection at the network layer of the Internet protocol stack [1]. Our goal is to simulate the scenario shown in Figure 1. The most commonly used cryptographic standards, namely AES, DES and 3DES in addition to SHA-1 and MD5 (HMAC algorithms) have been simulated in the scenario.

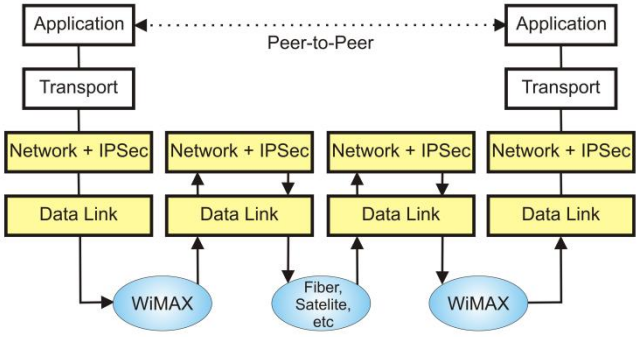

Fig. 1. The system architecture used in our scenario

We illustrate the simulation results to show how each of these standards affects the performance of the WiMAX network in terms of processing time and throughput.

This paper is organized as follows. In section II, we discuss fundamental issues of WiMAX and IPsec. In section III, we illustrate the performance evaluation of IPsec over WiMAX for difference cryptographic standards and different security modes. We conclude this paper in section IV.

II. BACKGROUND

A. WiMAX

The IEEE 802.16 standard, also known as WiMAX, is one of the latest broadband technologies in the wireless world. WiMAX offers packet-switched services for all accesses including mobile, fixed, portable and nomadic [2]. The main goal of WiMAX is to replace digital subscriber line DSL and T1 cable services and to reach 100 Mbps transmission rate [3]. The transmission range allows using one base station for instance to cover an entire city. WiMAX operates in outdoor environment and supports data, voice, and video services.

The WiMAX consists of two layers of the Open System Interconnection (OSI) reference model; namely the physical (PHY) layer, which supports outdoor environment operations and the Media Access Control (MAC) layer, which provides QoS and security [4]. The latest versions of WiMAX support a frequency range from 2 GHz to 66 GHz and each country has its own standard for WiMAX. For example, the international standard is 3.5 GHz, the license exempt standard in the US is 3.5 GHz while the licensed

spectrum is 2.5 GHz.

B. Security in WiMAX

As a wireless system, WiMAX has security vulnerabilities, which do not exist in the wired networks [5]. Security is a necessity in real world, especially for the military, environmental and health monitoring communications. Higher level attacks against the IEEE 802.16 standard may be launched because the original MAC layer can be occasionally compromised.

Some security weaknesses have been corrected in the newer WiMAX standard though for instance the resource constraints in wireless mobile devices keep security in MAC layer in minimal levels.

Security has two goals; namely to provide (i) privacy and (ii) access control. Privacy is important due to the wireless nature of the network and it is achieved by encrypting all the connections in the network between the Base Station (BS) and the Subscriber Station (SS).

For instance, to protect a WiMAX network from unauthorized access, the BS encrypts service messages. To control the distribution of the keys, the BS uses the Privacy and Key Management Service (PKM), which deploys digital certificates and provides access control.

C. IPsec

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.

IPsec supports two security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP) [1]. Both protocols support transport and tunnel modes of operations and support connectionless integrity, anti-reply protection and data origin authentication. Unlike AH, ESP supports confidentiality as well [1]. In transport mode all IP packet payloads are encrypted to provide end-to-end protection. In tunnel mode all IP packets are encrypted, including IP header, and encapsulated as a payload in the new IP packet.

IPsec supports different cryptographic algorithms to encrypt original plaintext messages into transforming ciphertext messages. Iterative block ciphers are widely used in IPsec. They make blocks of constant sizes from user data and then encrypt each block independently using different number of encryption rounds.

The security level of the ciphers depends on the block sizes, number or encryption rounds and keys [1]. The greater block sizes and/or the key sizes, the greater the security level. Unfortunately in these cases encryption and decryption speed reduces and as a result there are more delays and packet losses in transmissions.

The time, which is required for ciphering or creating a message digest, is called computation cost and important to be analyzed in advance. This will help us to evaluate the delay for different cryptographic algorithms. The computation cost is even more important when the end node is a mobile device with limited processing power and battery life. In IPSec, where different cryptographic algorithms are used, the processing times are different. The remaining paragraphs in this section briefly describe the encryption algorithms used in the paper.

The Advanced Encryption Standard (AES) is an encryption standard comprising of three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael (developed by Joan Daemen and Vincent Rijmen).

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 standard defines the following number of rounds for phase depending on the key lengths

$$N_r(128) = 10,$$
$$N_r(196) = 12,$$
$$N_r(256) = 14.$$

The number of processes required to encrypt one block of data is calculated using the following formula

$$\begin{aligned} T_{AES-enc} &= (46 N_b N_r - 30 N_b) T_a + \\ &+ [31 N_b N_r + 12(N_r - 1) - 20 N_b] T_o + \\ &+ [64 N_b N_r + 96(N_r - 1) - 61 N_{b)}] T_s \end{aligned} \quad (1)$$

where T_a, T_o and T_s are the number of processing cycles for a byte-wise AND, OR and shift respectively. In the simplest case, when $T_a = T_o = T_s = 1$, from the equation (1) we will have that

$$\begin{aligned} T_{AES-enc}(128) &= 6168, \\ T_{AES-enc}(192) &= 7512, \\ T_{AES-enc}(256) &= 8856. \end{aligned} \quad (2)$$

The number of processing cycles to decrypt one block of data can be calculated using the equations (1) and (2) as

$$T_{AES-dec} = T_{AES-enc} + 96 N_b T_a + (N_r - 1) \times (72 N_b T_o - 32 N_b T_s) \quad (3)$$

Again assuming, that $T_a = T_o = T_s = 1$ we will have that

$$\begin{aligned} T_{AES-dec}(128) &= 10992, \\ T_{AES-dec}(192) &= 13408, \\ T_{AES-dec}(256) &= 15824. \end{aligned} \quad (4)$$

From (3) and (4) it is clear, that decrypting an AES data block requires more number of processing cycles than the encryption of the actual data. To encrypt an unencrypted

S_d data packet, the required operations are derived by the following equation

$$U_{AES}(S_d) = \left\lceil \frac{8 \times S_d}{128} \right\rceil \times T_{AES} \quad (5)$$

Then we calculate the time required by a processor to encrypt or decrypt a data packet as

$$t_{AES}(S_d, C_p) = \frac{U_{AES}(S_d)}{C_p} = \left\lceil \frac{8 \times S_d}{128} \right\rceil \times \frac{T_{AES}}{C_p}, \quad (6)$$

where C_p is the number of operations in Millions Instruction Per Second (MIPS) that the processor can perform per second.

The Data Encryption Standard (DES) algorithm [1] 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 [1].

DES requires the same processing time for both encryption and decryption because it is a Feistel cipher and uses a 56 bit key and a block of 64 bit. To encrypt an unencrypted S_d data packet, the following number of operations is needed

$$U_{DES}(S_d) = \left\lceil \frac{8 \times S_d}{64} \right\rceil \times T_{DES} \quad (7)$$

where $T_{DES} = 2697$ and shows the required number of operations to encrypt one block of S_d data [3]. Then we calculate the time required by a processor to encrypt or decrypt a S_d data packet as

$$t_{DES}(S_d, C_p) = \frac{U_{DES}(S_d)}{C_p} = \left\lceil \frac{8 \times S_d}{64} \right\rceil \times \frac{T_{DES}}{C_p} \quad (8)$$

where C_p is the number of operations in MIPS.

In the context of HMAC algorithms, the number of operations required in HMAC-SHA-1 and HMAC-MD5 depend on the number of input blocks. For instance, for each SHA-1 block and for each MD-5 block 1110 and 744 operations are correspondingly required to produce a message digest. The formulas to calculate the number of blocks for the HMAC-SHA-1 and HMAC-MD-5 are the following [1]

$$N_i = \left\lceil \left(\frac{8 \times S_d + 64}{512} \right) \right\rceil + 1 \quad (9)$$

$$N_p = 32 + (2 + N_i) \times 744 \quad (10)$$

In our simulations we consider two types of processors: 100 million instructions per second (MIPS) and 400 MIPS.

III. Performance Evaluation

In this section we discuss the simulation results. We have used the network simulator ns-3 to evaluate the performance of IPsec over WiMAX when different cryptographic algorithms are used.

In Table 1 we show the processing times required for different packet sizes when AES, DES, 3DES and MD5 algorithms are used. In this case a processor of 100 MIPS capability has been used.

Application Packet size (Bytes)	Processing time (AES)	Processing time (MD5)	Processing time (3DES)	Processing time (DES)
20	0.185	0.038	0.485	0.162
50	0.308	0.038	0.728	0.243
100	0.493	0.045	1.295	0.432
200	0.864	0.06	2.265	0.755
300	1.295	0.067	3.317	1.106
400	1.665	0.082	4.288	1.429
500	2.035	0.092	5.34	1.78
600	2.405	0.105	6.31	2.1
700	2.837	0.112	7.362	2.454
800	3.207	0.1268	8.33	2.778

Table 1: The processing times for the 100 MIPS processor in milliseconds.

In Figure 2, we illustrate the aforementioned results. We see that the 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.

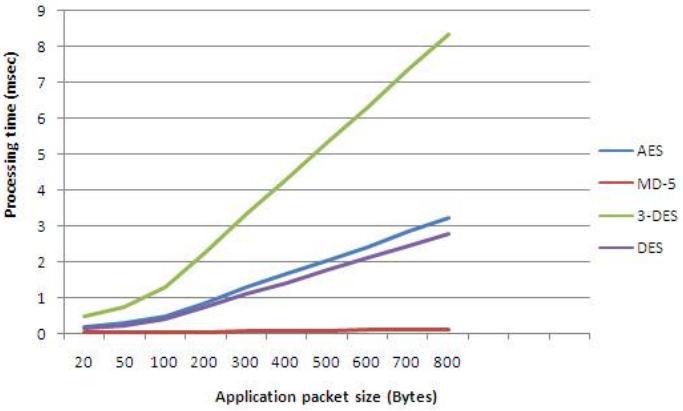

Fig. 2: The processing times for the 100 MIPS processor

In the same context, Table 2 and Figure 3 show the required processing times to run each security standard when a 400 MIPS processor has been used. We notice that 3DES algorithm has still the highest required processing time while AES and DES have approximately the same processing times. Additionally, in Figures 4 and 5, we depict the throughput in the network.

Application Packet size (Bytes)	Processing time (AES)	Processing time (MD5)	Processing time (3DES)	Processing time (DES)
20	0.046	0.0095	0.121	0.0405
50	0.077	0.0095	0.182	0.06
100	0.123	0.0113	0.323	0.108
200	0.216	0.015	0.566	0.189
300	0.324	0.017	0.829	0.277
400	0.416	0.0205	1.072	0.357
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

Table 2: The processing times for the 400 MIPS processor in milliseconds.

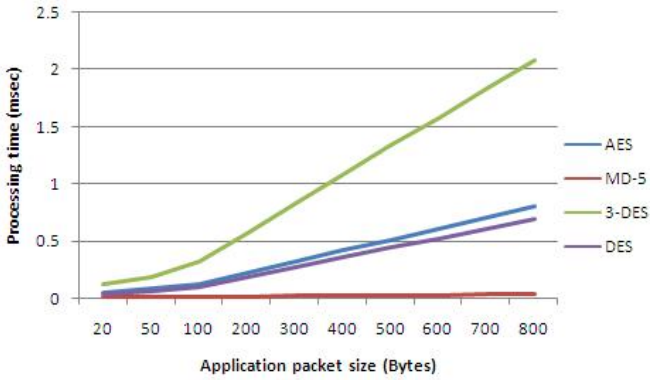

Fig. 3: The processing times for the 400 MIPS processor

In the next two figures (Figures 4 and 5) we have analyzed the throughput which is the average rate of successful packet delivery to the BS. We have calculated the number of packet sizes as well, which is the number of packets successfully received by the BS per second after each security service.

Figures 4 and 5 show, that the throughput is the same when there is no security mechanism and for MD-5. The reason is that for both Md-5 and with no security cases processing power is not necessary. By analyzing the results, it is essential that AES and AES+MD-5 are the best algorithms for encrypting the packets as they do not require much processing power like other algorithms.

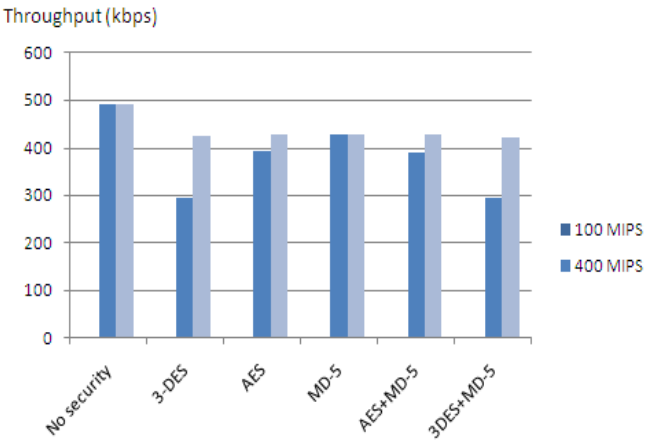

Fig. 4: The throughput for 500 kbps data rate with 100 and 400 MIPS processors

For example, the throughput for 500 kbps data rate is about 400 kbps for 100 MIPS processor and 430 kbps for 400 MIPS processor using AES.

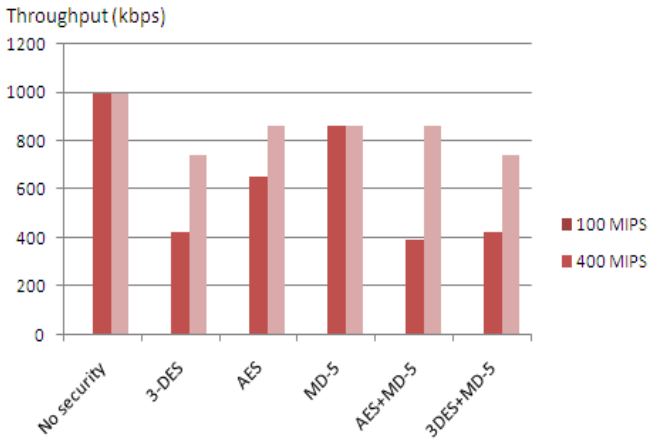

Fig. 5: The throughput for 1000 kbps data rate with 100 and 400 MIPS processors

The results are similar when 1000 kbps data rate is used (see Figure 5).

IV. Conclusions

In this paper we examine the use of IPsec over WiMAX. 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.

In our simulations we considered that a subscriber station (SS) communicates with a BS and its traffic is protected in the network layer level by the IPsec protocol.

After a series of simulations and experimentations we observed that AES is the best cryptographic algorithm to use. This protocol does not require a lot processing power and at the same time it introduces the highest throughput among all the examined security approaches.

As a future work we would like to simulate a WiMAX system where several SSs communicate with multiple BSs and to evaluate the performance of both downlink and uplink traffic.

References

[1] C. Xenakis, N. Laoutaris, L. Merakos and I. Stavrakakis, “A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms”, Elsevier Computer Networks, 2006

[2] S. L. Tsao, and Y. L. Chen “Mobility Management in Mobile WiMAX”, Book Chapter of “Wireless Metropolitan Area Networks”, Auerbach Publications, CRC Press, 2007

[3] A. Mishra and N. Glore, “Privacy and Security in WiMAX Networks”, Book Chapter of “WiMAX Standarts and Security”, CRC Press, 2008

[4] Y. Zhang, H.-H. Chen, “Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks”, Auerbach Publications, 2008

[5] E. B. Fernandez, M. VanHilst, “An Overview of WiMAX Security”, Book Chapter of “WiMAX Standarts and Security”, CRC Press, 2008

[6] Joan Daemen and Vincent Rijmen. The Design of Rijndael. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.