PERFORMANCE EVALUATION OF SECURE VIDEO TRANSMISSION OVER WIMAX

FarrukhEhtisham, Emmanouil A. Panaousis and Christos Politis

Wireless Multimedia & Networking (WMN) Research Group
Kingston University London, UK
{f.ehtisham,e.panaousis,c.politis}@kingston.ac.uk

ABSTRACT

WiMAX is a wireless digital communication system based on the IEEE 802.16 standard which provides broadband wireless Internet access at very high rates that is up to 70 Mbps or a data rate of about 3 Mbps within a radius of 30-mile (data rate increases as the distance decreases). With the rapid increase in the wireless broadband use, the need for wireless fixed and mobile metropolitan area networks has ever been increasing. Multimedia communications, including audio and video are highly bandwidth demanding and error sensitive. When the coverage area of the wireless network technology is as high as with WiMAX, security becomes one of the most important issues.WiMAX, both mobile and fixed, has many attractive features such as connection-oriented MAC layer, provision of the Quality-of-Service (QoS) for different applications, efficient mobility and power save mode features. Needless to say, all these attractive features must be protected against malicious activities by security mechanisms.Providing secure multimedia communications by using a broadband wireless technology like WiMAXis likely to be challenging due to time or space overhead that occur. Security mechanisms might increase packet sizes thus delay, jitter and throughput are increased. In this paper, we evaluate the performance of secure video transmission over WiMAX networks under different cryptographic algorithms by using the OPNET simulator. The outcome of the results show negligible overhead introduced by the security extensions giving credence to their application in security sensitive scenarios.

KEYWORDS

Security, WiMAX, Video Transmission, IPSec

1. INTRODUCTION

There is an increasing demand of high-speed data rate, quality of service with mobility in the world of technology. Using wire medium like DSL (Digital Subscriber Line), fibre optic and cable networks, although providing high-speed data rate and good quality of service but fails to provide mobility. Not only that, wire medium adds an extra burden of managing the cable architecture thus increasing the cost. The solution for the problem is to use wireless as a medium to provide the broadband services to users. However, wireless medium is always vulnerable to errors and security threats. With advancement of technology however, researchers are able to discover some techniques in order to utilize wireless in the best possible manner.

Technological advances in wireless and broadband communications are changing the way people work, interact and exchange information. Interactive services such as video conferencing, Voice over IP (VoIP) [1], and both cached and live streaming video [2] are enabling people to stay in touch and to exchange multimedia content anywhere and at any time. These services have opened up new markets and business opportunities of great interest to the equipment manufacturing and service industries. To sustain these services and accompanying revenues, there is a requirement for constant adaptation to the fast changing technological

DOI : 10.5121/ijcnc.2011.3608

environment through the improvement of existing applications and the development of new ones.

Multimedia communications, audio and video, are highly bandwidth demanding and error sensitive applications. Providing multimedia communication on broadband wireless technology like WiMAX (Worldwide Interoperability for Microwave Access) is a big challenge, due to time sensitivity issues. Additional security features increase packet size, and as a result delay increases and throughput decreases.WiMAX is a wireless digital communication system based on the IEEE 802.16 standard which provides broadband wireless Internet access at very high rates that is up to 70 Mbps or a data rate of about 3 Mbps (data rate increases as the distance decreases). With the rapid increase in the wireless broadband use, the need for wireless fixed and mobile metropolitan area networks has ever been increasing. The main idea in Europe is to provide wireless metropolitan area network, mainly last mile connectivity with the line of sight as well as non line of sight transmission covering the area in between 30 to 50kilometers. Initially IEEE came up with the LoS (Line of Sight) WiMAX standard operating in the frequency range of 11-66 GHz. Later, there were significant changes and the solution was the IEEE 802.16 2004 operating in the 2-11 GHz range. IEEE announced the IEEE 802.16e version in 2005 to support mobility.The IEEE 802.16 uses OFDM (Orthogonal Frequency Division Multiplexing) on the physical layer, FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing) along with OFDMA (Orthogonal Frequency Division Multiple Access) in order to divide the resources between the Subscriber Stations (SSs.) In addition, the WiMAX technology supports two basic architectures namely point-to-multipoint and mesh architectures.

The biggest advantage of using WiMAX is its easy deployment in areas (hilly, rural areas) where no other forms of ISP's (Internet Service Providers) are present. WiMAX technology is capable of supporting live or cached streaming of audio, video and data. As multimedia communications are highly bandwidth demanding and error sensitive, delay and jitter are very important parameters. The coverage area of WiMAXconsists of the base station (BS) and one or more subscriber stations (SS), whereas SS is considered as customer premises equipment (CPE), and BS is connected to the core networks (CN).There is no doubt that wireless systems are more prone to security hazards than wired ones. On the other hand, the adoptability of any wireless network technology is mainly dependent on the security features it provides. When the coverage area of the wireless network technology is as high as with WiMAX, security becomes one of the most important issues. WiMAX, both mobile and fixed, has many attractive features such as connection-oriented MAC layer, provision of the Quality-of-Service (QoS) for different applications, efficient mobility and power save mode features. Needless to say, all these attractive features must be protected against malicious activities by security mechanisms.

For instance, application layer software based threat management and secure access solutions are as important as ever. The solutions include firewalls, virtual private networking (VPN), Internet key exchange (IKE) tunnelling, and intrusion prevention systems (IPS). However, popular application layer services, such as Voice over Internet Protocol (VoIP), it could be broken by hackers who initiate the download of remote configuration settings and resynchronize clients' Customer Premise Equipment (CPE) settings to their specifications.Hackers may also replicate, or spoof the address of the intermediary router or server and deceive other clients into believing their connection is secure, thus opening them up to a malicious attack. These routers and gateways will require robust security measures to ensure that unprotected clients remain protected behind the intermediary access point.

This study focuses on secure video transmission over WiMAX communications by splitting the video into small chunks, and transmitting them over an IP network. We mainly examine how security extensions in the current WiMAX technologyaffect the QoS in the communication channels by simulating video transmission over WiMAX in the OPNET network simulator and

add some optimised IPSec security extensions. This paper is organised as follows. In the section 2, we discuss the fundamental issues of WiMAX, including its security architecture, the IPSec protocol, the encryption algorithms that we have used to encrypt/decrypt video, as well as the basics of the scalable video. In section 3, we describe how video is transmitted over WiMAX networks. Whilst in section 4, we illustrate the performance evaluation of IPSec over WiMAX when video is transmitted for different cryptographic standards. Section 5 concludes this article.

2. BACKGROUND

2.1. WiMAX

The IEEE 802.16 standard, 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 [5]. WiMAX promises to be one of the wireless access technologies capable of supporting real time applications like video and voice requiring minimum service guarantee, in a low price.The transmission range allows using one base station to cover long distances [4]. WiMAX operates in outdoorand indoor environments and supports data, voice, and video services. WiMAX consists of two layers of the Open System Interconnection (OSI) reference model; the Physical (PHY) layer, and the Media Access Control (MAC) layer, which provides QoS and security [6]. The latest versions of WiMAX support a frequency range from 2 GHz to 66 GHz and each country has its own standard.

In this paper WiMAX MAC layer will be exploited to deliver real time services. MAC layer provides the interface between the upper layers and the physical layer. In WiMAX, the MAC layer consists of three sublayers and these layers interact with each other using service access points (SAPs). The Service Specific Convergence Sublayer (SSCS) and the service dependent sublayer assurereliable data transmission. The Common Part Sub layer (CPS) is the middle MAC sublayer provides services like system access, establishing and maintaining connection and bandwidth management. CPS also provides QoS for service flow [7]. The Security Sub layer (SSL) – SSL is at the bottom of MAC layer and provides security features like authentication, and encryption.

The three basic entities of the WiMAX architecture are Mobile Station (MS), Access Service Network (ASN) and Connectivity Service Network (CSN).

- Mobile Station (MS): is at the customer site and also known as CPE or (Customer Premises Equipment).
- Access Service Network (ASN): consist of several BSs (Base Stations)
- Connectivity Service Network (CSN): is responsible for providing the IP connectivity to the WiMAX radio equipment.

ASN and CSN have special functionalities, which communicate with each other through special points known as the reference points. These reference points are used for different control and management services [15].

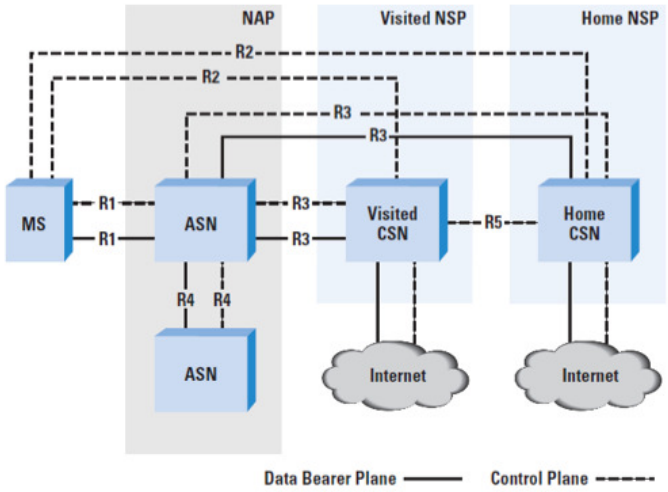

Figure 1: Reference Model for WiMAX [15]

Figure 1 shows the reference model for both mobile and fixed WiMAX. Reference point R1 specifies the air interface between Mobile Station (MS) and the Base Station (BS). Reference point R2 is used for management and mobility management purposes, whereas R3 also serve the same purpose of management and mobility management but, this time it is between ASN and CSN. Reference point R5 provides the interworking between CSN's during macro mobility (opposite of micro mobility (local movement)) [15].

Being a wireless system, WiMAX has security vulnerabilities, which do not exist in the wired networks [3]. 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 addressed in the newer WiMAX standard though for instance the resource constraints in wireless mobile devices keep security in MAC layer in minimal levels. Security in WiMAXhas two goals; 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 BS and the 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.

2.2. IPSec

Security is one of the key issues that have been taken into account in this article. Providing a secure mechanism to real time communications like multimedia communication especially VoIP on wireless environment like WiMAX is very challenging. This is due to the reason that by adding security, the packet size will increase and, once the packet size is increased, the processing time increases adding additional delay during the conversation.

Among the different technologies that have been developed to secure networks, the IPSec protocol [1] is maybe the most effective and suitable protocol to secure the end-to-end network layer communication. The protocol provides security services such as confidentiality, integrity and authentication.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.

IPsec operates at network layer and encapsulates both TCP and UDP traffics. The major components of the IPsec protocol can be divided into the following four categories defined by [16] as such:

- **Encapsulating Security Payload (ESP):** ESP is header for data confidentiality, integrity and authentication. It also includes an additional sequence number. Basically it scrambles the data by using hard-core encryption.

- **Authentication Header (AH):** is used for data integrity and authentication. Just like ESP it also include the sequence number

- **Internet Key Exchange (IKE):** is used for generating cryptography keys for ESP and AH. IKE also authenticates the remote system

- **Manual Keys:** cryptographic keys for ESP and AH are generated statically and manually distributed. Manual keys are usually used when the remote system does not support IKE as in a Mobile IPv6 client.

IP's strength lies in its ability to easily route packets. However, IP has also weaknesses exposing security threats like spoofing, sniffing, etc. since IP does not have in-built security capabilities. Thus Internet Engineering Task Force (IETF) has proposed the IP Security (IPSec) protocol suite. IPSec can be defined as a set of IP extensions that provide security at the network level, which is based on cryptographic technologies. Nowadays IPSec is one of the most effective technologies to secure network layer end-to-end communications. The advantage is that all network communications are protected at the network layer without modifying the applications running at the above layers. The protocol increases the security level by applying different cryptographic algorithms to send and receive encrypted data over secure channels. Originally IPSec was designed for wired networks and the wireless networks' limitations, such as processing power of mobile devices and the limited resources of wireless channels were not considered initially [8].

IPSec supports two security protocols: the authentication header (AH) and the encapsulating security payload (ESP). Both protocols support transport and tunnel modes of operations, connectionless integrity, anti-replay protection, and data origin authentication. Unlike AH, ESP supports confidentiality as well. In transport mode, only the packet payload is encrypted, whereas in tunnel mode, the entire packet is encrypted, including the IP header, and it is encapsulated as a payload in a new IP packet.IPSec supports a series of cryptographic algorithms to encrypt original unencrypted packets. The security level of the encrypted packets depends on the block sizes, number or encryption rounds, and keys [9]. Great block sizes and/or key sizes introduce great security level but, unfortunately, introduce more delays caused by encryption and decryption operations. The processing time is different for different encryption algorithms. A brief description of encryption algorithms appears next.

The AES (Advanced Encryption Standard) is an encryption standard comprising of three block ciphers: AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively. It is widely used because the algorithm is fast in both software and hardware, easy to implement, and does not require vast amount of memory [9]. AES has been designed to be resistant to well-known attacks and exhibits simplicity of design. In [8], the authors have proven that decrypting an AES data block requires more number of processing cycles than the encryption of the actual data. The standard defines the following number of rounds (N_r) for phase depending on the key lengths:

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

Formula (1) is used to calculate the number of processes ($T_{AES-enc}$) required to encrypt one block of data using AES [8]:

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

, where T_a, T_o and T_s are the number of processing cycles for a byte-wise AND, OR and shift respectively, and the $N_b = 32\ bits$ is the block size. In the simplest case, when T_a=T_o=T_s=1, from the equation (1) we will have that:

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

The number of processing cycles to decrypt one block of data [8] can be calculated using the equations (1) and (2) as:

$$\begin{aligned} T_{AES-dec} &= T_{AES-enc} + 96N_bT_a + (N_r - 1)\times(72N_bT_o - 32N_bT_s) = \\ &= (46N_bN_r - 30N_b)T_a + [31N_bN_r + 12(N_r - 1) - 20N_b]T_o + \\ &+[64N_bN_r + 96(N_r - 1) - 61N_{b)}]T_s + 96N_bT_a + (N_r - 1)\times(72N_bT_o - 32N_bT_s) \end{aligned} \quad (3)$$

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

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

Comparing (3) and (4) it is obvious, 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 [8]:

$$U_{AES}(S_d) = \frac{8 \acute{} S_d}{128} \acute{} T_{AES} \quad (5)$$

Then we calculate the time required by a processor to encrypt or decrypt a data packet using the following formula [8]:

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

, 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 [10] 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 [11].

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 [8].

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 [8]:

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

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 [8]:

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

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

2.3. WiMAX QoS Classes

The MAC common part sublayer (CPS) manages the QoS associated with the different MAC protocol data units (MPDUs) by creating appropriate buffers (queues) for their classification and

storage prior to scheduling and transmission. An application's QoS is managed by observing its requirements and then associating to it a predefined QoS class. Each QoS class is associated with well defined QoS requirements. The job of the scheduler is to manage the resources assigned to all active application with the goal of satisfying each of their QoS requirements. WiMAX recommends five QoS classes [12], which are briefly examined below.

- The Unsolicited Grant Service (UGS) Class: The UGS QoS class is designed for real-time applications that require constant bit rate. The QoS requirements for this class are a sustained data rate, maximum end-to-end delay and delay variation (jitter).

- The Extended Real Time Polling Service (extPS) Class: This class is designed to optimise voice over IP (VoIP) services by not sending any traffic during silent periods otherwise known as silence suppression. The QoS requirements are same as for UGS with the exception that bandwidth is allocated only during active periods.

- The Real Time Polling Service (rtPS) Class: The rtPS service class supports applications with variable bit rates and real-time traffic requirements. Real-time transmission of compressed video is an example of a service that belongs to this class. Scheduling for this class requires constant bandwidth adjustments bounded by a separately specified minimum and maximum reserved traffic rate. Additional QoS requirements are guaranteed end-to-end delay and jitter.

- The Non Real-Time Polling Service (nrtPS) Class: The nrtPS class is designed for non real-time variable bit rate applications without requirements for delay guarantees. The QoS criterion for this class is the guarantee of only a minimum throughput or data rate.

- The Best Effort (BE) Class: The best effort class as the name implies has no QoS guarantees. Only left over resources are granted to connections of this type. Although no QoS guarantees are specified for this class of service it is still possible to impose a minimum throughput to it for reasons of fairness.

2.4. Scalable Video

The scalable video coding (SVC) standard [13], is a video compression method that is designed to provide temporal, spatial and signal to noise ratio (SNR) or quality scalabilities through the use of advanced video coding techniques. SVC employs hierarchical prediction through the use of "I", "B" and "P" type frames in its implementation of the various types of scalabilities listed above.The H.264/AVC is the latest coding technology standardized by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), Moving Picture Experts Group (MPEG) and International Communication Union (ITU-T). Higher compression efficiency and network friendliness for video applications are the main achievements of this standard.

The Video Coding Layer (VCL) and the Network Abstraction Layer (NAL) are the two fundamental concepts used in implementing the SVC standard. VCL groups all the core video encoding functionalities while the NAL is mainly concerned with adapting the bit stream to the characteristics of the underlying transport network for more efficient transmission. Reduction of the impact of error on the SVC bit stream is achieved by the network abstraction layer through effective separation and packaging of important video data and decoding information. SVC employs non-VCL NAL units for the packaging of slowly changing information that is used for the decoding of a whole picture or entire sequence made up of VCL NAL Units. Because of

their importance, VCL NAL units must not be dropped or corrupted during transmission and should be handled with care.

3. SECURE VIDEO OVER WiMAX

In this article we have used the network simulator OPNET (Optimized Network Engineering Tool) to model a scenario. OPNET is a network simulation tool and it consists of different modellers, which incorporate protocols and technologies and enable modelling of all network types. In our simulation we have used the OPNET Wireless Modeler, which supports any network with mobile devices including WiMAX,WiFi, LTE and other cellular networks.Three configuration models are used for the above defined network model for simulation. These configuration models as shown in Fig.1 include profile configuration (for setting up profile), application configuration (for defining the different applications like VoIP, FTP, WEB and so on) and WiMAX configuration (defining WiMAX parameters like scheduling algorithms maximum sustained data rate and so on). For this setup a profile name "Voice Profile" has been defined in profile configuration. For application configuration VoIP application has been defined using G.711 PCM Codec producing 80 Byte of codec sample size with 10ms codec interval.The path loss parameter for the SS's has been set to Free Space. The modulation and coding scheme selected for this setup is QPSK 1⁄2.

The WiMAX standard is capable to provide data, voice and video technologies with mobility in a single network. In this article we have used OPNET to model a scenario where 2 WiMAX SSs communicate to the server through a BS using 2 different video transmission rates. To ensure confidentiality and integrity of the transmitted data as well as authentication of the different identities, we have used the IPSec protocol. We have used different cryptographic algorithms in IPSec to encrypt the traffic and compare them in terms of delay and throughput.

The process involves receiving a video source directly from the video transmission after encoding it into MPEG-2 format at a constant bit rate (CBR) [14]. The MPEG-2 stream is encapsulated into IP and is sent. Then, the IPSec processor encrypts (decrypts when receiving) packets and thus adds time overhead and space overhead. IPSec space overhead is added to the packet irrespective the type of application. The impact of time overhead depends on the application type. For real time applications the processing time for each of the packet is calculated and the processing delay is added to each of the packet.Results of above defined network model of WiMAX have been gathered keeping in mind three parameters like jitter, throughput, end-to-end packet delay.

- **Jitter**: Jitter can be defined as non-uniform packet delays. Due to jitter, packets arrive and process out of sequence. When jitter is high packets arrive in form of spurts. If two consecutive packets leave the source then the jitter is:

Jitter = (T4-T3) – (T2-T1)□(T2-T1) = Time to leave source node (T4-T3) = Play back time at destination node

If the value of jitter is negative this means that time difference between destination nodes is less than at source node. In order to understand jitter better let's take an example of multiple packets sent consecutively from source to destination with 10ms time interval. If network is behaving ideally the destination should receive them with the same10 ms time interval. On the other hand, if there are delays then the delay between packets may be greater or less than 10 ms. Using the defined example if packets arrive with 15 ms time interval then positive jitter is 5 ms, if they arrive at 5ms time interval then the jitter is negative.

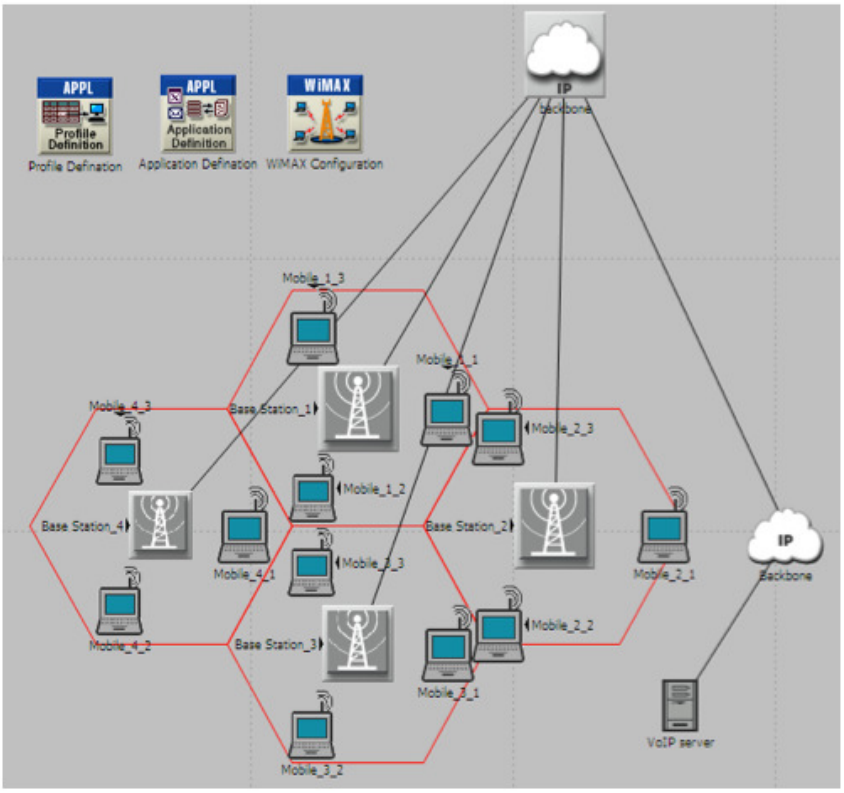

Figure 2. Experimental Setup for Simulation

- **Throughput**: Presents the amount of successful data delivery over a specific period of time. Throughput is measured in bits/second or packet/second.

- **Packet End-to-End delay**: Packet end to end delay is also known as total mouth to ear delay and consists of three components i.e. codec delay, network delay and playout delay. Packet end-to-end delay less than 150 ms is considered good and less than 400 ms is considered acceptable or fair. In OPNET generally the results gathering category, is generally divided in two groups i.e. Global Statistics and Node Statistics. Global Statistics indicates the results for overall network model whereas Node Statistics indicates results for each and every individual node present in the network model. For this project Global Statistics results are taken into consideration.

In this section we discuss the simulation results. In Table 1 we show the processing times required for different packet sizes to encrypt/decrypt when AES, DES and 3DES algorithms are used. In this scenario a processor of 1000 MIPS capability has been used to encrypt and decrypt the packets. The processing times are shown below:

Original Packet Size (Bytes)	Final packet size (Bytes)		Time (milliseconds)			
	AES	DES	AES (En)	AES (De)	DES	3DES
3840	3872	3864	1.492656	1.934064	1.302651	3.907953

Table 1. Processing time in milliseconds for a 1000 MIPS processor.

The table shows that the 3DES algorithm has the highest processing time. This is because 3DES repeats the DES algorithm 3 times. The AES requires slightly more processing time than the DES. In Figure 3, we illustrate the aforementioned results.

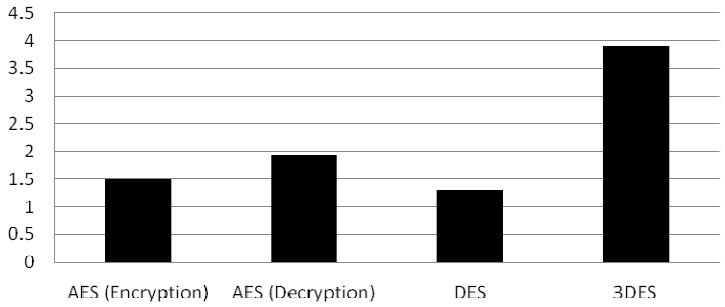

Figure 3. Packet processing times for a 1000 MIPS processor when transferring video

Figure 4 shows the space overheads of the IPSec for each security algorithm. This figure shows the calculated payload ratio, which is application packet size or final packet size.

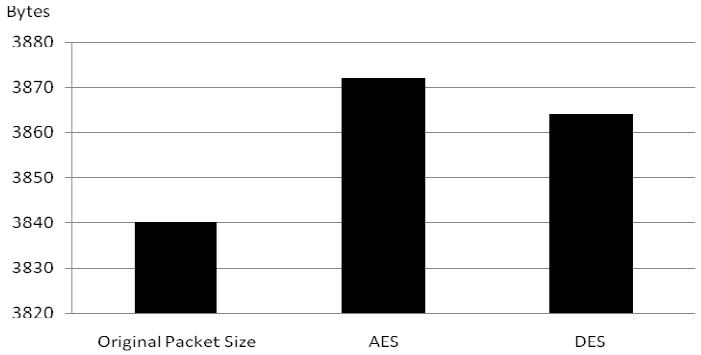

Figure 4. The space overheads of the IPSec for each security algorithm

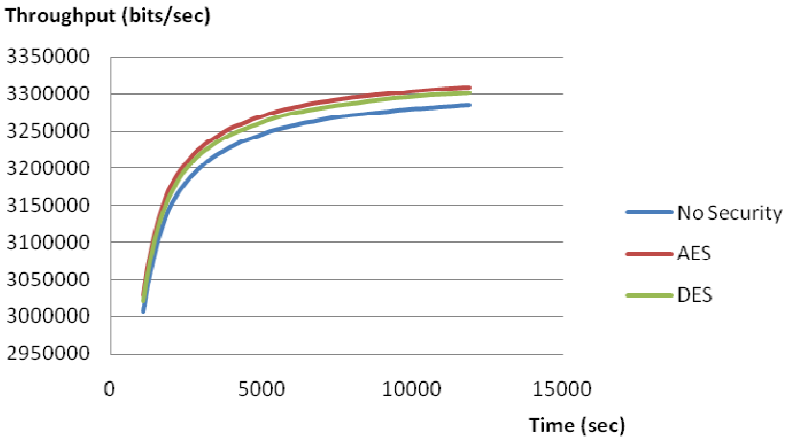

Figure 5. The Throughput for video traffic

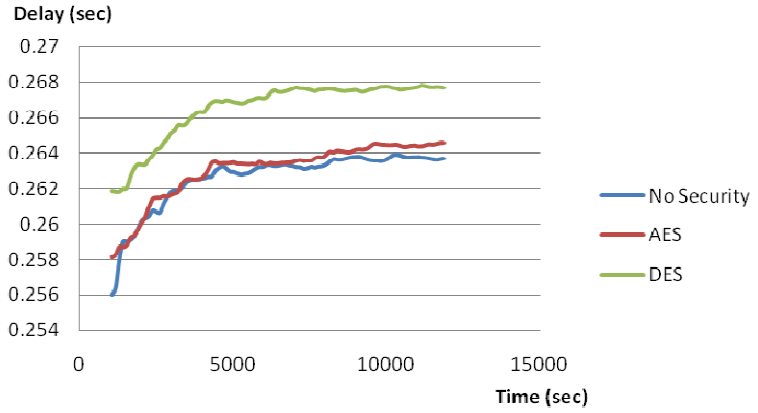

Figure 6. The Delay for video traffic

The space overheads are calculated using transport mode of ESP (Encapsulating Security Payload) for encryption algorithms [8]. Figure 5 shows that the throughput for video traffic when 1000 MIPS processor is used. From the results it is depicted that AES is the best algorithm for encrypting the packets as they do not require much processing power like other algorithms and at the same time AES considered more secure than DES or 3DES. Figure 6 shows that packet end-to-end delay is very small (almost around 268 ms: packet end to end delays less than 150 ms is considered good and less than 400 ms is considered acceptable or fair).

4. CONCLUSIONS

In this study, we have used IPSec to secure video transactions over WiMAX networks. IPSec is considered as one of the most secure protocols nowadays. It protects traffic between endpoints at the network layer by using different cryptographic algorithms and does not modify the applications running at the above layers.

We have simulated a WiMAX scenario where 2 SSs communicate to the server through a BS using 2 different video transmission rates. The traffic is protected at the network layer by using IPSec.A number of simulations and experiments have observed that AES is the best cryptographic algorithm in IPSec to secure video communications over WiMAX. The reason is that AES does not require lots of processing power and at the same time it introduces the highest throughput among all the examined security approaches. Moreover, AES is easy to implement and is considered to be secure enough.
The WiMAX standard is capable to provide data, voice and video technologies with mobility in a single network. The process involves receiving a video source directly from the video transmission after encoding it into MPEG-2 format at a constant bit rate (CBR) [14]. The MPEG-2 stream is encapsulated into IP and is sent. Then, the IPSec processor encrypts (decrypts when receiving) packets and thus adds time overhead and space overhead. IPSec space overhead is added to the packet irrespective the type of application. The impact of time overhead depends on the type of application. For real time applications the processing time for each of the packet is calculated and the processing delay is added to each of the packet.

As a future work, we would like to simulate a WiMAX system where several SSs will transfer voice and video streams through multiple BSs to evaluate the performance of the network. This work completes one more step toward the final cross-layer security solution for WiMAX networks. Later we will implement security protocols in PHY, MAC, and network layers.

Especially for the network layer, the methodology followed in this article will be considered for the purposes of the final cross-layer security mechanism.

REFERENCES

[1] Kahun, R., Walsh & T., Fries, S. (2005). Security Consideration for Voice over IP Systems. National Institute of Standards and Technology, USA

[2] Vishwanath, A., Dutta, P., Chetlur, M., Gupta, P., Kalyanaraman, Sh. & Ghosh, A. (2009). Perspectives on Quality of Experience for Vodeo Streaming over WiMAX

[3] Fernandez, E. & VanHilst, M. (2008). An Overview of WiMAX Security. In WiMAX Standards and Security (pp. 197-205). CRC Press, USA

[4] Wu, L. & Sandrasegaran, K. (2008). Overview of WiMAX Standards and Applications. In WiMAX applications. CRC Press, USA

[5] Tsao, S. & Chen, Y. (2007). Mobility Management in Mobile WiMAX. In Wireless Metropolitan Area Networks. Auerbach Publications, CRC Press, USA

[6] Zhang, Y. & Chen, H. (2008). Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks. State: Auerbach Publications

[7] Jubair, A., Hasan, I. and Obaid Ullah, Md. (2009). Performance Evaluation of IEEE 802.16e (Mobile WiMAX) in OFDM Physical Layer. ING/School of Engineering, Sweden

[8] Xenakis, C., Laoutaris, N., Merakos, L. & Stavrakakis, I. (2006). A generic characterization of the overheads ay IPSec and associated cryptographic algorithms. Computer Networks, Athens, Greece

[9] Daemen, J. & Rijmen, V. (2002). The Design of Rijndael. Secaucus, NJ. State: Springer-Verlag

[10] NIST FIPS PUB 46-3 (1997). Data Encryption Standard. Federal Information Processing Standards, National Bureau of Standards. U.S. Department of Commerce

[11] Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A. and Schimmele, M. How to Break DES for EUR 8980. Ruhr University Bochum and Christian-Albrechts-University of Kiel, Germany

[12] Ahson, S. & Ilyas, M. (2008). WiMAX Standards and Security. State: CRC Press

[13] Schawrz, H. & Wien M. (2008). The Scalable Video Coding Extension of the H.264/AVC Standard. IEEE Signal Processing Magazine, p. 135-141

[14] Jianfeng Wang; Venkatachalam, M.; Yuguang Fang; , "System architecture and cross-layer optimization of video broadcast over WiMAX," Selected Areas in Communications, IEEE Journal on , vol.25, no.4, pp.712-721, May 2007

[15] Piri, E, Pinola, J., Fitzek, F., Pentikousis, K., "ROHC and aggregated VoIP over fixed WiMAX: An empirical evaluation,"IEEE Symposium onComputers and Communications, pp.1141-1146, 6-9 July 2008.

[16] IPsec Protocol Suite. [Online] Available from: http://docs.hp.com/en/J4256-90015/ch01s02.html, 2005

Authors

Farrukh Ehtisham is currently working as a Software Support Engineer at Scheidt & Bachmann (UK) Ltd. He was previously with Wireless Multimedia & Network (WMN) Research Group at Kingston University, UK. Farrukh received his MSc., with distinction in Networking and Data Communication from Kingston University London and BSc. in Computer Sciences from National University of Modern Languages, Islamabad, Pakistan.

Emmanouil A. Panaousisis currently a PhD candidate at Kingston University London, Faculty of Science, Engineering and Computing (SEC). He is also working towards his PhD dissertation entitled 'Security for Emergency Mobile Ad-hoc Networks'. He works within the Wireless Multimedia & Networking (WMN) research group as well as giving the occasional lecture on IT security and wireless networking field within the SEC faculty. His specialties fall within the areas of mobile communications, security for security & mobile communications, computer & network security, Internet security and game theory for optimising computer/wireless networks performance and security. Emmanouil has over 4 years of research and development experience in the field of wireless communications and mobile computing and he has 2 years project management experience working in the European Union (EU) ICT Framework Programme 7 (FP7) PEACE project. Emmanouil contributed in various research challenges, in PEACE, mainly including design and implementation of security solutions and frameworks for next generation ubiquitous wireless emergency networks. He has also been involved in software analysis project for iPhone and Android mobile applications and he holds some temporary IT consultancy experience. Emmanouil has co-authored few EU and Engineering and Physical Sciences Research Council (EPSRC) project proposals in the past and he is an author of over 25 publications published in international conferences, journals and standardisation bodies. He holds a BSc degree in Informatics & Telecommunications, an MSc degree in Computer Science from University of Athens and Athens University of Economics & Business, correspondingly.

Dr Christos Politisis a Reader (Assoc. Prof.) in Wireless Communications at Kingston University London, UK, Faculty of Science, Engineering and Computing (SEC). There, he leads a research team on Wireless Multimedia & Networking (WMN) and teaches modules related to communications. Christos is the Field Leader for the 'Wireless Communications' and 'Networks and Data Communications' postgraduate courses at Kingston. Prior to this post, he was the Research and Development (R&D) project manager at Ofcom, the UK Regulator and Competition Authority. There he managed a number of projects across a wide range of technical areas including cognitive radio, polite protocols, radar, LE Applications, fixed wireless and mobile technologies. Christos' previous positions include telecommunications engineer with Intracom Telecom in Athens and for many years he was a post-doc research fellow in the Centre for Communication Systems Research (CCSR) at the University of Surrey, UK. He is being active with European research since 2000 and has participated in several EU, national and international projects. Christos was the initiator and the project manager of the IST UNITE project. He is a patent holder, and has published more than 100 papers in international journals and conferences and chapters in two books. Christos was born in Athens, Greece and holds a PhD and MSc from the University of Surrey, UK and a B.Eng. from the Technical University of Athens, Greece. He is a senior member of the IEEE and a member of Technical Chamber of Greece.