Performance Evaluation of Secure Video Transmission over WiMAX Networks

Levon Nazaryan and Christos Politis

Wireless Multimedia and Networking (WMN) Research Group,
Kingston University London, United Kingdom
{L.Nazaryan,C.Politis}@kingston.ac.uk

Abstract. The IEEE 802.16 standard, which is 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 guaranteed quality of service (QoS), security and mobility. Multimedia applications are bandwidth demanding and error sensitive, whereas wireless medium is unreliable and bandwidth limited. In this paper, we evaluate the performance of secure video transmission over WiMAX networks. We mainly illustrate the results of the simulations. To this end we depict the processing time and the throughput introduced when IP Security (IPSec) is applied over WiMAX. 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 (MD-5) are considered for this study.

Keywords: AES, DES, IPSec, MD-5, Security, WiMAX, Video Transaction.

1 Introduction

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 stored 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 environment, accomplishable through the improvement of existing applications and the creation of new ones. Modern communications systems are designed to be heterogeneous, presenting huge opportunities that can be leveraged by engineers to bring in the desired improvements and innovations. In this work we shall deal with the problem of increasing the security of video transmission over WiMAX which is a broadband wireless access system (BWA) designed to efficiently support different types of applications and devices with varying quality of service (QoS). Innovating or bringing significant improvement to any system or process has never been trivial and often demands considerable effort and dedication.

J. Rodriguez, R. Tafazolli, C. Verikoukis (Eds.): MOBIMEDIA 2010, LNICST 77, pp. 28–38, 2012.

The architectural design of the WiMAX technology [3], [4] is easy to implement. The coverage area of WiMAX (IEEE802.16) consists 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) [4].

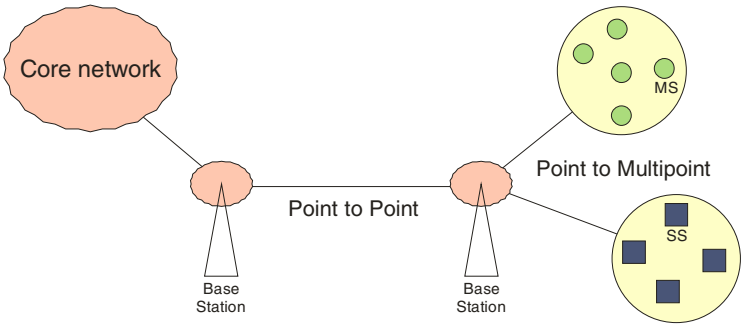

Fig. 1. An example of WiMAX architecture

This study focuses on secure video transmission over WiMAX communications. This is possible by breaking the video into small chunks, and transmitting them over an IP network.

This paper is organised as follows: In the "Background" section we will discuss the fundamental issues of WiMAX, including its security architecture, the IPSec protocol, the encryption algorithms we have used to encrypt/decrypt video, and the basics of the scalable video. In the "Video over WiMAX" section we describe how we have transmitted video over WiMAX networks. In the next "Performance Evaluation" section we illustrate the performance evaluation of IPSec over WiMAX when video is transmitted for different cryptographic standards. In the last section we conclude the paper.

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]. The transmission range allows using one base station to cover long distances [4]. WiMAX operates in outdoor and 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, which supports outdoor environment operations 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 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.

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 this paper WiMAX MAC layer will be exploited to deliver real time services. MAC layer provides the interface between the upper layers and physical layer. In WiMAX, the MAC layer consists of three sublayers and these layers interact with each other using service access points (SAPs).

- Service Specific Convergence Sublayer (SSCS) – this is the top MAC layer and service dependent sublayer assuring data transmission. This layer is used for Asynchronous Transfer Mode (ATM) and packet convergence [7].
- Common Part Sub layer (CPS) – CPS is the middle MAC sublayer and is responsible for providing services like system access, establishing and maintaining connection and bandwidth management. CPS also provides QoS for service flow [7].
- Security Sub layer (SSL) – SSL is at the bottom of MAC layer and provides security features like authentication, and encryption.

2.2 Security in WiMAX

Being a wireless system, WiMAX has security vulnerabilities, which do not exist in the wired networks [3]. 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 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 has 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.

2.3 IPSec

Internet Protocol (IP) is flexible, powerful and served network needs for many years. 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].

According to [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 in the next sub-section.

2.3.1 Encryption Algorithms

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 bit, 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]:

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

where T_a, T_o and T_s are the number of processing cycles for a byte-wise AND, OR and shift respectively, 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:

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

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

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

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

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

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]:

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

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

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

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]:

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

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:

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

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]:

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

$$N_p = 32 + (2 + N_i) \times 744 \tag{10}$$

2.4 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.

2.4.1 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).

2.4.2 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.

2.4.3 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.

2.4.4 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.

2.4.5 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.

2.5 The 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 Video over WiMAX

The WiMAX standard is capable to provide data, voice and video technologies with mobility in a single network. The model presented in Figure 2 is used in the analytical analysis as well as in the simulation study for video transmission. For example, 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 (see figures 3 and 4).

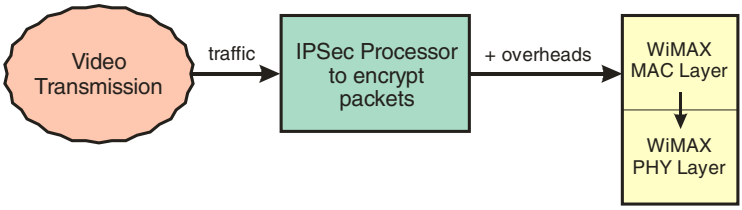

Fig. 2. IPSec analytical model

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.

4 Performance Evaluation

In this section we discuss the simulation results. We have used the network simulator OPNET to evaluate the video transmission performance over WiMAX using IPSec. We have used different cryptographic algorithms in IPSec to encrypt the traffic and compare them in terms of delay and throughput.

In Table 1 we show the processing times required for different packet sizes to encrypt/decrypt when AES, DES, 3DES and MD-5 algorithms are used. In this scenario a processor of 1000 MIPS capability has been used to encrypt and decrypt 400 Bytes and 600 Bytes packets. The processing times are shown below:

Table 1. The processing times for a 1000 MIPS processor in milliseconds

Application packet size	AES Encryption	AES Decryption	DES	3DES	MD-5
400 Bytes	0.166536	0.215784	0.142941	0.428823	0.008216
600 Bytes	0.240552	0.311688	0.210366	0.631098	0.010448

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. However, MD-5 does not require much processing power because it does not perform any encryption or decryption. It is just used to create a message digest for authentication and integrity. In Figure 3, we illustrate the aforementioned results.

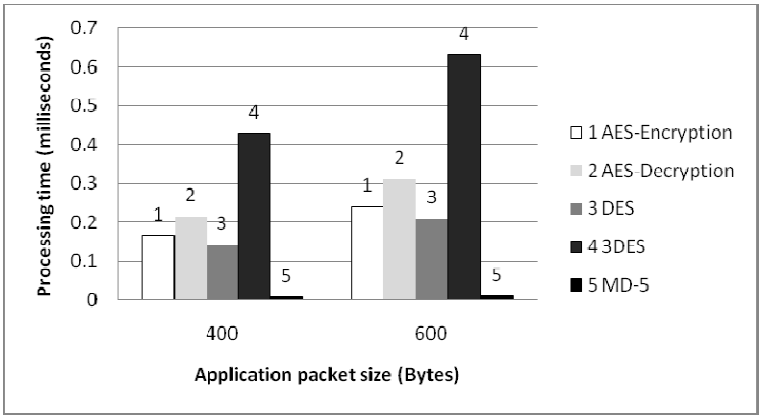

Fig. 3. Processing times for a 1000 MIPS processor when transferring video

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

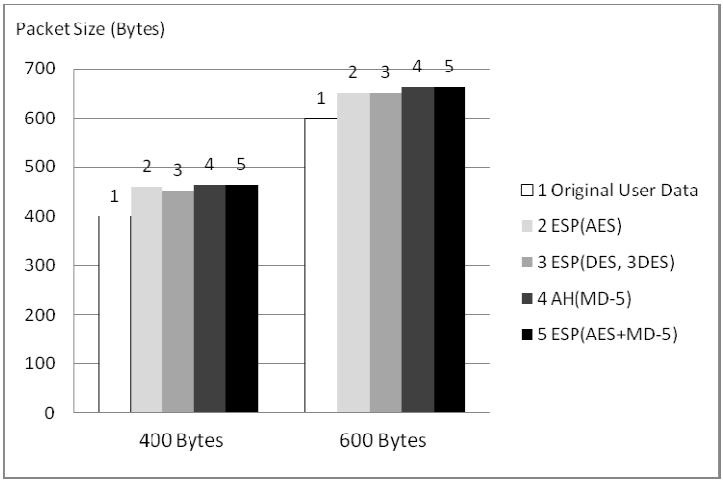

Fig. 4. The space overhead of the IPSec for each security algorithm

The space overheads are calculated using transport mode of ESP (Encapsulating Security Payload) for encryption algorithms and AH (Authentication Header) for MD-5 [8].

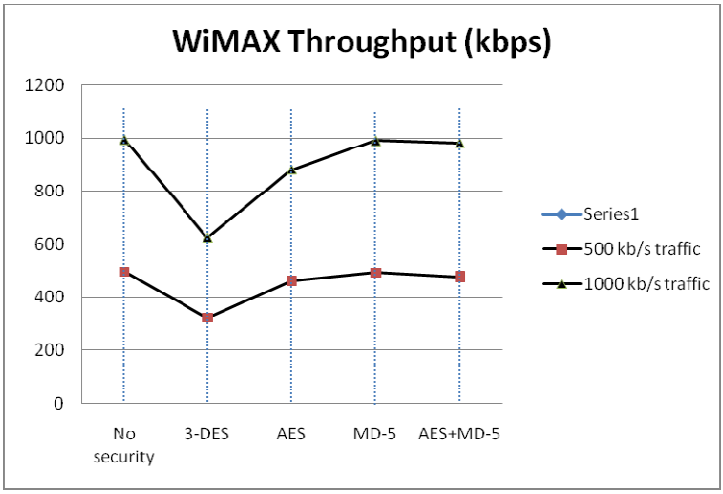

Fig. 5. The Throughput for 500 kb/s and 1000 kb/s traffics

Figure 5 shows that the throughput for 500 kb/s traffic is about 496 kb/s when 1000 MIPS processor is used and 996 kb/s for 1000 kb/s traffic using the same processor when no security mechanism is applied. When the traffic is encrypted using AES algorithm, the throughputs are 472 kb/s and 992 kb/s respectively.

By analysing the figure's results, we notice that the throughput is almost the same when there is no security mechanism and for MD-5. The reason is that MD-5 does not introduce high space and time overheads and thus it requires almost the same throughput as with no security cases.

From the results it is depicted 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 and at the same time AES considered more secure than DES or 3DES.

5 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.

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.: Security Consideration for Voice over IP Systems. National Institute of Standards and Technology, USA (2005)
2. Vishwanath, A., Dutta, P., Chetlur, M., Gupta, P., Kalyanaraman, S., Ghosh, A.: Perspectives on Quality of Experience for Vodeo Streaming over WiMAX (2009)
3. Fernandez, E., VanHilst, M.: An Overview of WiMAX Security. In: WiMAX Standarts and Security. CRC Press (2008)
4. Wu, L., Sandrasegaran, K.: Overview of WiMAX Standards and Applications. In: WiMAX Applications. CRC Press, USA (2008)
5. Tsao, S., Chen, Y.: Mobility Management in Mobile WiMAX. In: Wireless Metropolitan Area Networks. Auerbach Publications, CRC Press (2007)
6. Zhang, Y., Chen, H.: Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks. Auerbach Publications (2008)
7. Jubair, A., Hasan, I., Obaid Ullah, M.: Performance Evaluation of IEEE 802.16e (Mobile WiMAX) in OFDM Physical Layer. ING/School of Engineering, Sweden (2009)
8. Xenakis, C., Laoutaris, N., Merakos, L., Stavrakakis, I.: A generic characterization of the overheads imposed by IPSec and associated cryptographic algorithms. Computer Networks, Athens, Greece (2006)
9. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer, Secaucus (2002)
10. NIST FIPS PUB 46-3: Data Encryption Standard. Federal Information Processing Standards. National Bureau of Standards. U.S. Department of Commerce (1977)
11. Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A., Schimmele, M.: How to Break DES for EUR 8980. Ruhr University Bochum and Christian-Albrechts-University of Kiel, Germany
12. Ahson, S., Ilyas, M.: WiMAX Standards and Security. CRC Press (2008)
13. Schawrz, H., Wien, M.: The Scalable Video Coding Extension of the H.264/AVC Standard. IEEE Signal Processing Magazine, 135–141 (2008)
14. Wang, J., Venkatachalam, M., Fang, Y.: System Architecture and Cross-Layer Optimization of Video Broadcast over WiMAX