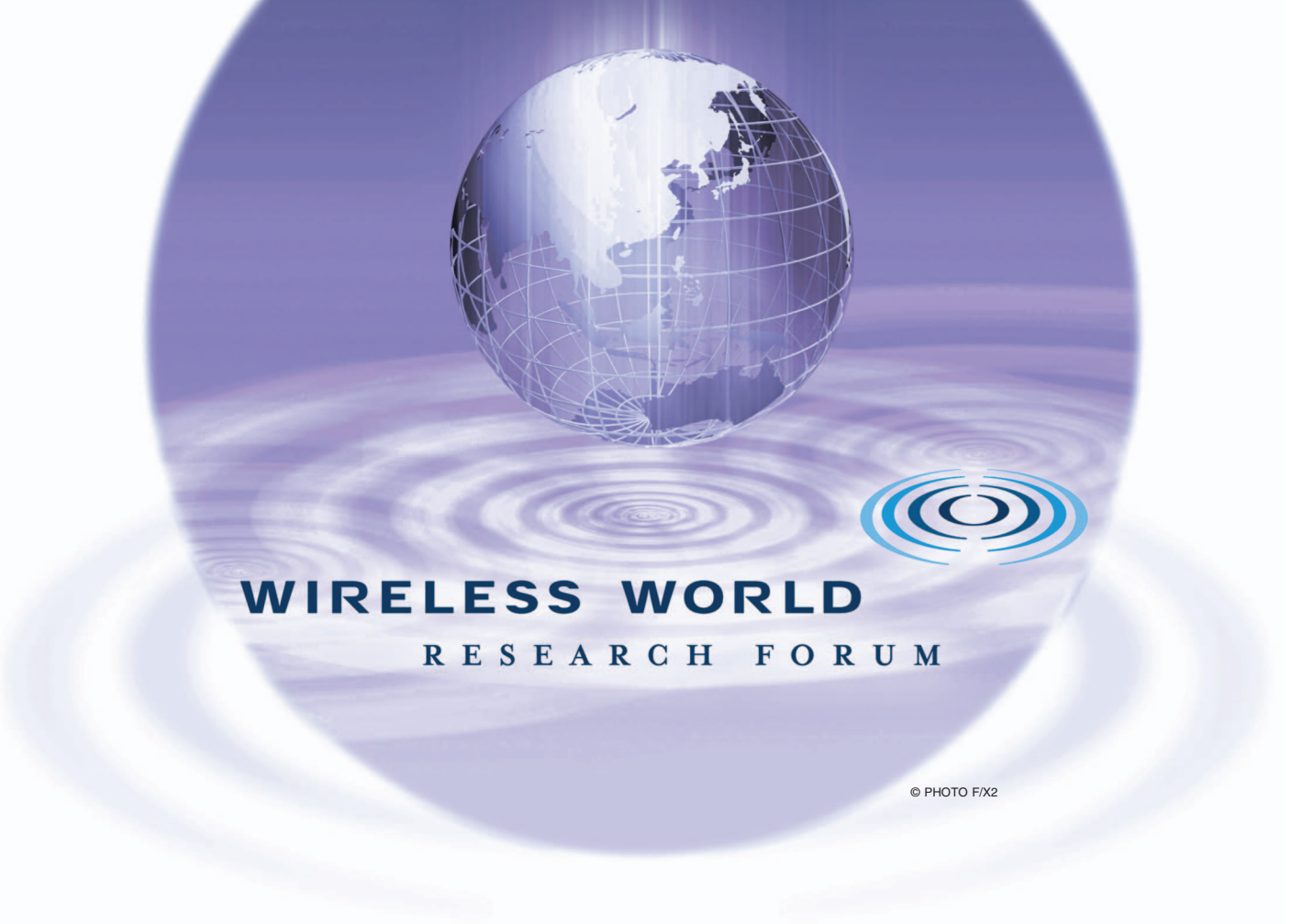

END-TO-END SECURITY PROTECTION

IPSec Provisioning in WiMAX Networks

Levon Nazaryan, Emmanouil A. Panaousis, and Christos Politis

The IEEE 802.16 standard [7] (mobile broadband wireless access system), 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 article, we have evaluated the performance of the Internet Protocol security (IPSec) over WiMAX networks. We have also illustrated the results of the simulations. We have also depicted the processing time and the throughput introduced when IPSec is applied over WiMAX technology (IEEE 802.16).

Digital Object Identifier 10.1109/MVT.2009.935542

WiMAX is a wireless digital communication system based on the IEEE 802.16 standard that provides broadband wireless Internet access at very high rates that is up to 70 Mb/s or a data rate of about 3 Mb/s within a radius of 50 km (data rate increases as the distance decreases) [1]. 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 a wireless metropolitan area network, mainly last mile connectivity, with the line-of-sight (LoS) as well as non-LoS transmission

 1556-6072/10/$26.00©2010IEEE

covering the area between 30 and 50 km. Initially, the IEEE came up with the LoS WiMAX standard operating in the frequency range of 11–66 GHz. Later, there were significant changes, and the solution was that the IEEE 802.16 2004 operated in the 2–11 GHz range. The IEEE announced the IEEE 802.16e version in 2005 to support mobility.

On the physical (PHY) layer, the IEEE 802.16 uses orthogonal frequency division multiplexing (OFDM), frequency division duplexing (FDD), and time division duplexing (TDD) along with OFDM access (OFDMA) 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 WiMAX consists of two layers: the open system interconnection (OSI) reference model; namely, the PHY layer that supports outdoor environment operations and the media access control (MAC) layer that provides QoS and security [3]. The latest versions of WiMAX support a frequency range from 2 to 66 GHz, and each country has its own licensed and license-free spectrums for WiMAX. For example, the international standard is 3.5 GHz, the license-exempt standard in the United States is 3.5 GHz while that of the licensed spectrum is 2.5 GHz.

As a wireless system, WiMAX has security vulnerabilities that cannot be found in the wired networks [4]. 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 successfully launched because the original MAC layer can be occasionally compromised. Some security weaknesses have been corrected in the newer IEEE 802.16e WiMAX standard.

This article evaluates the performance of IPSec over fixed WiMAX networks. We have used a WiMAX network as a backbone connection, and we have implemented the IPSec protocol to guarantee a secure end-to-end connection at the network layer [1]. Our goal is to simulate the scenario shown in Figure 1. The most commonly used cryptographic standards, such as advanced encryption standard (AES), data encryption standard (DES), and 3-DES in addition to message digest 5 (MD5), have been simulated in this scenario. We have illustrated the simulation results to show how each of these standards affects the performance of the WiMAX network in terms of processing time overhead and throughput.

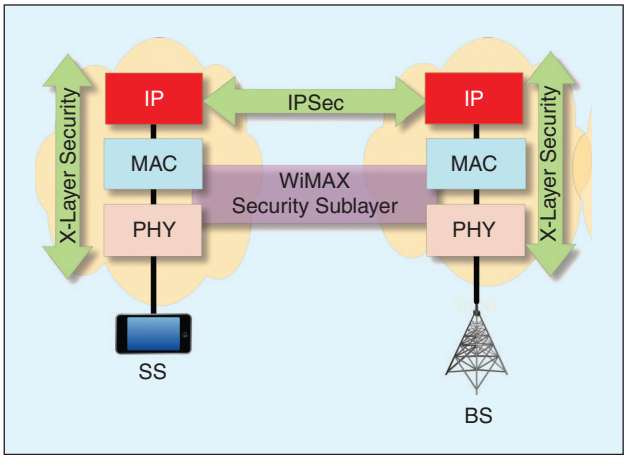

FIGURE 1 The IPSec protocol is used to encrypt, authenticate, and provide integrity to WiMAX communications.

This article is organized as follows. In "Security Issues in WiMAX" section, we have discussed the fundamental issues of security in WiMAX and basics of IPSec protocol. In the "IPSec Basics" and "IPSec over WiMAX" sections, we have illustrated the performance evaluation of IPSec over WiMAX for the different cryptographic standards and the different security modes. We have concluded this article by the "Conclusions" section.

Security Issues in WiMAX

There is no doubt that wireless systems are more prone to security hazards than the wired ones. On the other hand, the adaptability 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 in 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 QoS for different applications, efficient mobility, and power-saving 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) tunneling, and intrusion prevention systems (IPSs). However, popular application layer services, such as voice over IP (VoIP), 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.

Examining the lowest layer of the International Organization for Standardization (ISO)/OSI model, the PHY layer, we have realized that WiMAX networks are open to PHY-layer attacks such as jamming and rushing. Jamming is done by introducing a source of strong noise to significantly lower the capacity of the channel, therefore, denying services to all stations. However, jamming is detectable with radio analyzer devices. Rushing or scrambling is another type of jamming, but it takes place for a short interval of time aimed at particular frames.

In addition, the privacy sublayer security of the MAC layer has the main objective to protect service providers against theft of service but not securing network users. It is

obvious that the privacy layer only secures data at the data link layer, but it does not ensure complete encryption of user data. Furthermore, it does not protect the PHY layer from being interfered or even catastrophically fail. Hence, it is essential to include technologies to secure PHY layer and higher layers for a converged routable network and devices within the system and thus follow a cross-layer approach.

Generally, security in WiMAX has two main goals: to provide 1) privacy and 2) 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 SS. For instance, to protect a WiMAX network from unauthorized access, the BS encrypts the service messages. To control the distribution of the keys, BS uses the privacy and key management service (PKM), which deploys digital certificates and provides access control.

To provide privacy across the air interface, the WiMAX standard has introduced the concept of security associations (SAs). SA is a group of information about authentication and encryption algorithms and their associated keys. There are three types of SAS: primary, static, and dynamic.

- Both BS and SS share the security information at the initial authorization stage through a primary SA.
- Static SAs do not change. Actually, the BS is provided with a set of encryption and authentication algorithms in the form of static SA for which the SS has subscribed.
- Dynamic SAs are assigned to each service flow, and their lifetime is equal to the lifetime of the corresponding flow. In other words, each service flow requires a different set of security capabilities, therefore, dynamic SAs serve this purpose.

Two emerging questions from the security point of view are as follows: how strong is the current security sublayer of the WiMAX and does this provide an end-to-end security protection against attacks on the network layer? Actually, there is no standard for cross-layer security in WiMAX motivating us to apply well-known and effective mechanisms to finally protect the communication paths against network layer attacks.

IPSec Basics

Among the different technologies that have been developed to secure networks, the IPSec protocol [1] may be the most effective and suitable protocol to secure 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.

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 that runs above the network layer. Originally, IPSec was designed for wired networks, and limitations appearing in the case of wireless networks, such as the processing power of mobile devices and the limited resources of wireless channels, were not considered initially. The protocol allows the communicating nodes to set up secure channels to send and receive data. It also allows any cryptographic algorithm to be applied and increase the security to a desired level.

Furthermore, the IPSec supports two security protocols, namely, the authentication header (AH) and the encapsulating security payload (ESP) [1]. Both protocols support transport and tunnel modes of operations, connectionless integrity, antireplay protection, and data origin authentication. Unlike AH, ESP supports confidentiality as well [1]. In transport mode, only the packet payload is encrypted, whereas in tunnel mode, all the packets are encrypted, including the IP header, and it is encapsulated as a payload in a new IP packet.

As previously mentioned, IPSec supports different cryptographic algorithms to encrypt original plain-text messages into transforming cipher-text messages. Iterative block ciphers are widely used in IPSec. These make blocks of constant sizes from the data of the user and then encrypt each block independently using a 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. Encryption and decryption operations eventually introduce more delays in the packet transmission along with space overhead.

The time required for ciphering or creating a message digest is called computation cost, and it should be analyzed in advance to avoid unaffordable overheads. In fact, the computation cost is 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 this work.

The AES is an encryption standard comprising of three block ciphers: AES-128, AES-192, and AES-256. Each AES cipher has a 128-b block size, with key sizes of 128, 192, and 256 b, 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 [5]. AES has been designed to be resistant to well-known attacks and exhibits simplicity of design. In [1], the authors have proven that decrypting an AES data block requires more number of processing cycles than the encryption of the actual data.

The DES algorithm [1] is a symmetric block cipher with a block and key size of 64 b. DES requires the same processing time for both encryption and decryption, because it is a Feistel [1] cipher and uses a 56-b key and a block of 64 b.

TABLE 1 *The processing times for a 100-MIPS processor in milliseconds.*

Application Packet Size (B)	AES Encryption	AES Decryption	DES	3-DES	MD5
20	0.1850	0.2397	0.1618	0.4854	0.0375
50	0.3084	0.3996	0.2427	0.7281	0.0375
100	0.4934	0.6393	0.4315	1.2945	0.0449
200	0.8635	1.1188	0.7551	2.2654	0.0598
300	1.2952	1.6783	1.1057	3.3173	0.0672
400	1.6653	2.1578	1.4294	4.2882	0.0821
500	2.0354	2.6373	1.7800	5.3400	0.0896
600	2.4055	3.1168	2.1036	6.3109	0.1044
700	2.8372	3.6763	2.4542	7.3628	0.1193
800	3.2073	4.1558	2.7779	8.3337	0.1268

DES has been proven not to be a reliable cryptographic scheme, as a special hardware can hack it fast. This has been the reason to introduce the 3-DES (or triple DES) algorithm. This algorithm is the three 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 a new block is finally reencrypted using the initial key. However, the disadvantage of 3-DES is that it runs three times slower than the DES on the same platform [1].

MD5 is a one-way hash function and is used with cryptographic keys for authentication and integrity. MD5 actually processes 512-b input text blocks to generate a 128-b hash value. Then, the hash values are used to verify the correct message transfer. It uses padding and adds some bits to the original plain text to make its size a multiple of 512 b. However, MD5 on its own cannot be used as hashed-message authentication code (HMAC) algorithm because it does not include a secret key. One solution for this problem is using the MD5 with keyed-HMAC, which is a secret key-authentication algorithm. The HMAC-MD5 mechanism is suitable for IPSec protection, because it provides data-origin authentication and integrity protection services when AH mode is used. In this article, we have considered MD5 with AES and 3-DES cryptographic keys to compare the performance of the different HMAC schemes and their impact on WiMAX networks in terms of throughput and end-to-end packet delay.

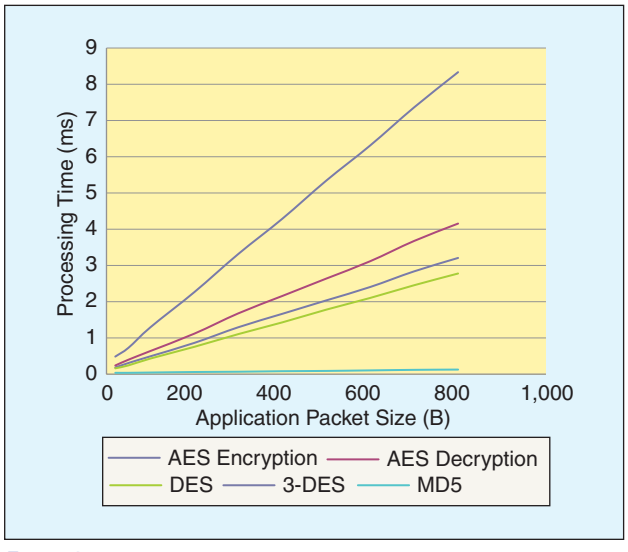

FIGURE 2 The processing times for a 100-MIPS processor.

The secure hash algorithm 1 (SHA-1) is a cryptographic hash function designed by the National Institute of Standards and Technology (NIST) along with the National Security Agency (NSA). SHA-1 provides the highest security level compared with SHA-0 and SHA-2, and it is widely used in many security protocols and applications. The function produces a 160-b digest from a message with a maximum length of 263 b. SHA-1 has a similar but more conservative design used in MD4 and MD5 message-digest algorithms. However, in our scenario where low-power devices are considered as the entities (BSs) of our network, SHA-1 introduces a significant higher overhead than does the MD5 hash function.

In the context of HMAC algorithms, the number of operations required in HMAC-SHA-1 and HMAC-MD5 depends on the number of input blocks. For instance, for each SHA-1 block and for each MD5 block, 1,110 and 744 operations are correspondingly required to produce a message digest according to the setup presented in [1]. Thus, we have only considered the HMAC-MD5 mechanism to avoid undesirable time and space overhead. Besides, the security level of MD5 is considered adequate for our scenarios.

IPSec over WiMAX

In this section, we have discussed the simulation results that have been taken by using the network simulator ns-3 [6]. We have actually evaluated the performance of IPSec over WiMAX when different cryptographic algorithms are used.

In Table 1, we have shown the processing times in milliseconds required for the different user data packet sizes when AES, DES, 3-DES, and MD5 algorithms are used. In this case, a processor with 100 millions instructions per second (MIPS) capability has been used.

In our simulations, we have considered three types of processors: 100, 400, and 800 MIPS. In Figure 2, we have illustrated the results derived from Table 1. We can see that the 3-DES algorithm has the highest processing time, whereas the AES requires slightly more processing time than the DES. Finally, MD5 does not require much processing power because it does not perform any encryption or decryption, and it is just used to create a message digest for authentication and integrity.

In the same context, Table 2 and Figure 3 show the required processing times for each security setup when a 400-MIPS processor has been used. We have noticed that 3-DES algorithm still has the highest required processing time, whereas AES and DES have approximately the same processing time.

Likewise, in Table 3 and Figure 4, we have analyzed the results for processing times when an 800-MIPS processor has been used. We have noticed that AES has about 50% less processing time than 3-DES. Again, AES has slightly more processing time than DES, but DES can be quickly cracked using a specialized hardware, whereas AES is considered to be secure enough.

Figure 5 is illustrated by using the space overheads of the IPSec for each security algorithm. The figure gives very important information, because it computes the payload ratio (application packet size/final packet size) for different security services and compares it with the payload ratio when WiMAX payload header suppression (PHS) is used. This reduces the upper layer headers to an average of 8 B.

In Figures 6 and 7, we have derived the throughput (the average rate of successful packet delivery) to the BS. The figures show that the throughput remains the same when there is no security mechanism and when only MD5 is applied. We have anticipated this trend of results due to the fact that MD5 does not require high processing power. However, in the cases that encryption algorithms are used (3-DES or AES), the 800 MIPS clearly outperforms in terms of throughput the other processors.

By analyzing the results, we have concluded that AES and AES+MD5 are the best algorithms for encrypting the packets as they do not require much processing power like other algorithms and provide the best security level for end-to-end communications.

For example, Figure 6 shows that the throughput for 500 kb/s data rate is about 400 kb/s for 100-MIPS processor, 430 kb/s for 400-MIPS processor, and 470 kb/s for 800-MIPS processor using AES.

TABLE 2 *The processing times for a 400-MIPS processor in milliseconds.*

Application Packet Size (B)	AES Encryption	AES Decryption	DES	3-DES	MD5
20	0.0462	0.0599	0.0404	0.1213	0.0093
50	0.0771	0.0999	0.0606	0.1820	0.0093
100	0.1233	0.1598	0.1078	0.3236	0.0112
200	0.2158	0.2797	0.1887	0.5663	0.0149
300	0.3238	0.4195	0.2764	0.8293	0.0168
400	0.4163	0.5394	0.3573	1.0720	0.0205
500	0.5088	0.6593	0.4450	1.3350	0.0224
600	0.6013	0.7792	0.5259	1.5777	0.0261
700	0.7093	0.9190	0.6135	1.8407	0.0298
800	0.8018	1.0389	0.6944	2.0834	0.0317

TABLE 3 *The processing times for an 800-MIPS processor in milliseconds.*

Application Packet Size (B)	AES Encryption	AES Decryption	DES	3-DES	MD5
20	0.0231	0.0299	0.0202	0.0606	0.0046
50	0.0385	0.0499	0.0303	0.0910	0.0046
100	0.0616	0.0799	0.0539	0.1618	0.0056
200	0.1079	0.1398	0.0943	0.2831	0.0074
300	0.1619	0.2097	0.1382	0.4146	0.0084
400	0.2081	0.2697	0.1786	0.5360	0.0102
500	0.2544	0.3296	0.2225	0.6675	0.0112
600	0.3006	0.3896	0.2629	0.7888	0.0130
700	0.3546	0.4595	0.3067	0.9203	0.0149
800	0.4009	0.5194	0.3472	1.0417	0.0158

Conclusions

In this article, we have examined the use of IPSec over WiMAX. IPSec is probably one of the most secure protocol nowadays. It protects traffic between endpoints at the network layer by using different cryptographic algorithms and HMACs.

In our simulations, we have considered an SS communicating with a BS, and its traffic is protected in the network layer by using the IPSec protocol.

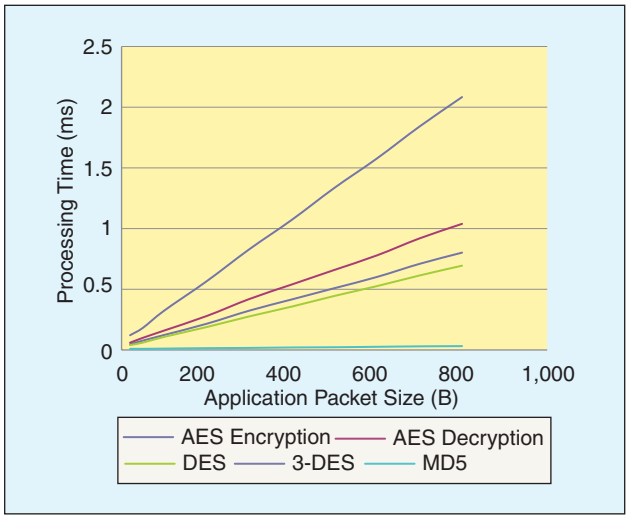

FIGURE 3 The processing times for a 400-MIPS processor.

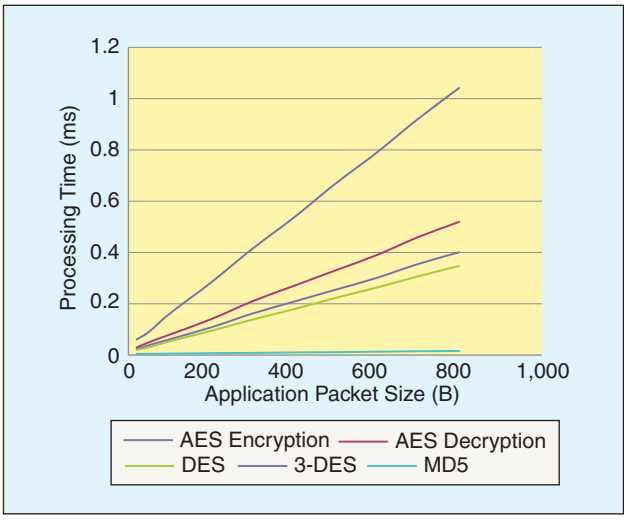

FIGURE 4 The processing times for an 800-MIPS processor.

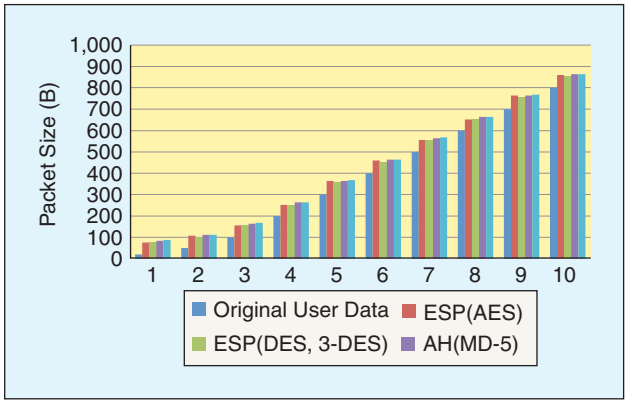

FIGURE 5 The space overhead of the IPSec according to each security algorithm option.

After a series of simulations and experiments, we have observed that AES is the best cryptographic algorithm to use in IPSec over WiMAX. This protocol 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 communicate with multiple BSs to evaluate the performance of both downlink and uplink traffic. This work constitutes first points toward the final cross-layer security solution for WiMAX networks. This 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.

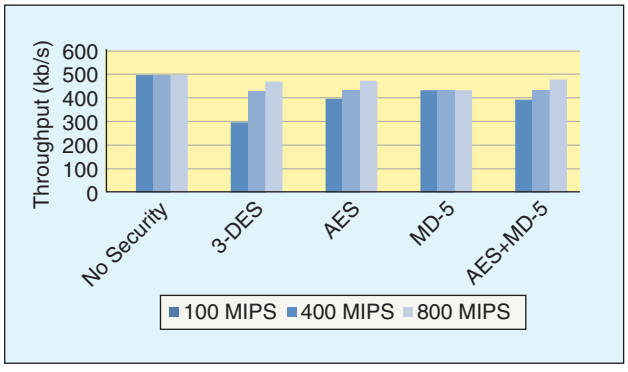

FIGURE 6 The throughput for 500 kb/s data rate with 100-, 400-, and 800-MIPS processors.

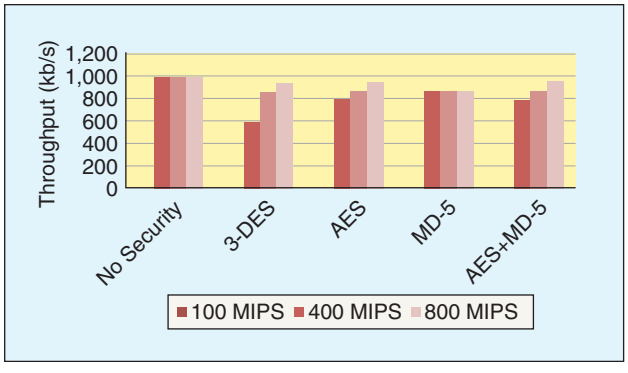

FIGURE 7 The throughput for 1,000 kb/s data rate with 100-, 400-, and 800-MIPS processors.

Author Information

Levon Nazaryan (l.nazaryan@kingston.ac.uk) obtained his first M.Sc. degree in automation and control at State Engineering University of Armenia (SEUA) and his second M.Sc. degree in networking and data communications with management studies at Kingston University, London. He is a Ph.D. student at Kingston University, London, Faculty of Computing, Information Systems, and Mathematics (CISM). His previous work experience includes computer network administrator and network designer. He is currently doing his research in cross-layer security in mobile WiMAX.

Emmanouil A. Panaousis received his B.Sc. degree in informatics and telecommunications at the National and Kapodistrian University of Athens and his M.Sc. degree in computer science at the Department of Informatics of the Athens University of Economics and Business. He is currently a researcher and a Ph.D. candidate at the Faculty of CISM of Kingston University, London, United Kingdom. He is a member of the British Computer Society and the IEEE.

Christos Politis holds a Ph.D. degree and M.Sc. degree from the University of Surrey, United Kingdom, and a B.Eng. degree from the Technical University of Athens, Greece. He was the R&D manager at Ofcom, the U.K. regulator and Competition Authority, where he managed a number of projects across a wide range of areas including cognitive radio (CR), polite protocols, radar, fixed wireless, and mobile technologies. He is currently an assistant professor with the Faculty of CISM of Kingston University, United Kingdom, where he leads a research group on wireless multimedia networks. He is a patent holder and has published more than 70 papers in international journals and conferences and chapters in two books. He is a member of the IEEE and the Technical Chamber of Greece.

References

[1] C. Xenakis, N. Laoutaris, L. Merakos, and I. Stavrakakis, "A generic characterization of the overheads imposed by IPSec and associated cryptographic algorithms," *Comput. Netw.*, vol. 50, no. 17, pp. 3225–3241, 2006.

[2] S. L. Tsao and Y. L. Chen, "Mobility management in mobile WiMAX," in *Wireless Metropolitan Area Networks*, Y. Zhang and H.-H. Chen, Eds. New York: Auerbach, 2007, pp. 220–232.

[3] Y. Zhang and H.-H. Chen, *Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks*. New York: Auerbach, 2008.

[4] E. B. Fernandez and M. VanHilst, "An overview of WiMAX security," in *WiMAX Standards and Security*, M. Ilyas, Ed. Boca Raton, FL: CRC Press, 2008, pp. 197–204.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael*. Secaucus, NJ: Springer-Verlag, 2002.

[6] NS-3 Project. (2009, Nov.). *NS-3 tutorials and manual* [Online]. Available: http://www.nsnam.org/tutorials.html

[7] C. Eklund, R. B. Marks, K. L. Stanwood, and S. Wang, "IEEE standard 802.16: A technical overview of the WirelessMANTM air interface for broadband wireless access," *IEEE Commun. Mag.*, vol. 40, no. 6, pp. 98–107, June 2002. VT