IPSec Provisioning in WiMAX Networks to Enhance the Security

S. Rimlon Shibi,
M.E Computer and Commn,
Dept of IT, National
Engineering College, Kovilpatti.

M. Kaliappan,
Assistant Professor,
Dept of IT, National
Engineering College, Kovilpatti.

L. Jerart Julus,
Assistant Prof,
Dept of IT, National
Engineering College, Kovilpatti.

ABSTRACT

The IEEE 802.16 (or) Worldwide Interoperability for Microwave Access (WiMAX) [7] is a standards-based technology enabling the delivery of last mile wireless broadband access with quality of service (QoS) guarantees, security, and mobility. For security in WiMAX the privacy sub layer of the MAC layer has the main objective to protect service providers against theft of service but not securing network users [12]. It is obvious that the privacy sub layer only secures data at the data link layer, but it does not ensure complete encryption of user data. To secure the networks, the IPSec protocol may be the most effective and suitable protocol to secure end-to-end network layer communication [2]. In the current scenario, existing method do not provide security level for end to end communications. The security algorithms namely TWOFISH [5] and BLOWFISH [26] are to encrypt the packets with best security levels for end to end communications. Analyses are done between these two algorithms with the existing encryption algorithms, from that TWOFISH is the best security algorithm and BLOWFISH is the fastest algorithm.

General Terms

Security, Algorithms, Throughput, Processing Time.

Keywords

Cryptographic Algorithms, Encryption, IPSec, Network Layer.

1. INTRODUCTION

WIMAX technology is a telecommunications system technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoint links. The WIMAX technology offers around 72 Mega Bits per second without any need for the cable infrastructure. WIMAX technology is based on Standard that is IEEE 802.16, it usually also called as Broadband Wireless Access. WIMAX Forum created the name for WIMAX technology that was formed in June 2001 to encourage compliance and interoperability of the WIMAX IEEE 802.16 standard [16]. WIMAX/802.16 is based on physical and data link layer of the OSI reference model where physical layer is single-carrier (PHY) layer and the data link layer is subdivided into logical link control (LLC) and medium access control (MAC) Sublayer. MAC layer is based on burst Time Division Multiplexing (TDM) layer and is again subdivided into Convergence Sublayer (CS), Common part Sublayer (CPS) and finally the security Sublayer (SS).

WIMAX physical layer is based on the orthogonal frequency division multiplexing. WIMAX MAC layer set an interface between the physical layer and the higher transport layer. In the MAC layer, security sub layer is responsible for authentication and encryption processes and privacy and key management protocol (PKM) [2] is responsible for user privacy from theft of services. Here the main theme is privacy sub layer of the MAC layer in WIMAX protects service providers against theft of service but not the network users. It is obvious that the privacy sub layer secures data only at the data link layer, but it does not ensure complete encryption of user data. The IPSec protocol may be the most effective and suitable protocol to ensure secured end-to-end network layer communication in NETWORK LAYER [11]. WIMAX Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services.

2. EXISTING WORK

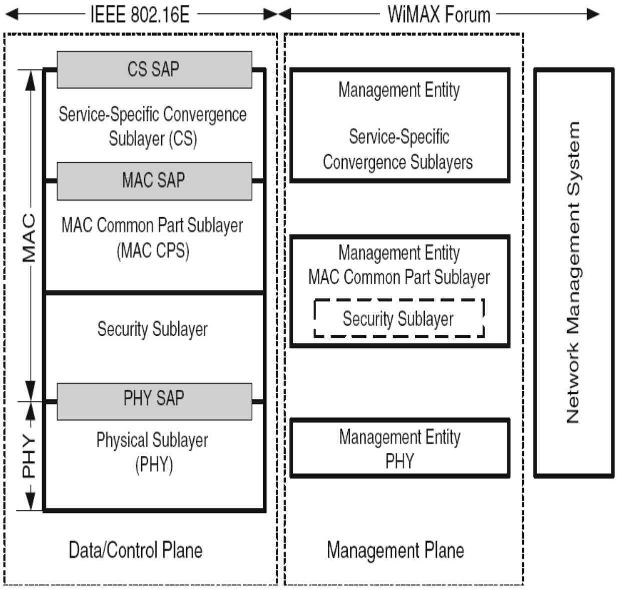


Fig 1: WiMAX Protocol Layers

In WiMAX, Privacy sub layer is used to provide security. Where more no of attacks are possible in this layer, in this case we need an alternate solution to provide better security between subscriber station and mobile station. The security concept in WiMAX is shown above.

3. RELATED WORK

Rizvi et al. [1] have discussed the basic design and the security issues of the AES and Twofish encryption algorithms for Text, Image and Sound Encryption. Both the algorithms have the equivalent safety factor. For the text encryption AES is faster than Twofish but with increasing RAM Twofish become faster than AES. For Image Encryption AES is faster but with increasing RAM Twofish performs at same speed. For Sound Encryption Twofish performs better than AES and with more RAM, its speed increases even more. So RAM size affects more the performance of Twofish. Nowadays, the system has high configuration such that RAM size and HARDDISK size is high. So with high configuration Twofish will perform faster.

Christos Xenakis et al. [2] have proposed IPSec packetization overhead depends on the selected security protocol are AH and ESP. The ESP header includes the security parameter index and sequence number field. The ESP trailer, which contains the padding, the pad length, and the next header fields, is placed after the IP packet. When the authentication service of IPSec is selected, an additional field, the ESP authentication data field is added after the ESP trailer. The AH consists of the fixed size fields and the field of authentication data. IPSec has two mode of operation as Tunnel and Transport Mode. In transport mode the aforementioned IPSec specific fields (i.e., ESP header, AH header, ESP trailer and authentication data field) are inserted within the transmitted IP packet. In tunnel mode, a new IP header is added in each IPSec-protected packet in addition to the IPSec specific fields. IPSec adds an additional space overhead with the processing overhead by increasing the size of the final transmitted packets. For better security and secured communication IPSec is the protocol.

Alex Biryukov et al. [3] have proposed the known attacks breaking 7, 10, 12 rounds for respective key sizes (128, 192, 256), with very high complexities. Where Related-key attacks on the full 14-round 256-bit key AES was said to be Biclique Cryptanalysis. Multi Collisions, Pseudo-Collisions, Local Collisions, Key Schedule and distinguisher are the problem with full AES. They show the first related-key attack on the full AES-256 with 296 data and time complexity and 265 memory which works for 1 out of every 235 keys on average. AES sub keys only have small differences between the round 10, 12, and 14, due to that to find an unknown key partition all the possible keys into a set of groups.

Trung Nguyen et al. [4] have mentioned that 802.16 standard was designed to specialize point-to-multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised the final standard was 802.16-2004 which corresponds to revision D. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enables mobile stations (MB) to handover between BSs while communicating. In WiMAX, MAC layer and Physical layer is used to send the packets over the network, but there is many attacks are possible in these layers, such as in physical layer Jamming attack, Scrambling attacks are possible. In MAC layer, the threats are Masquerading threat, Man in the middle attack and Denial of Service attacks are possible. In the near future, when WiMAX achieves a maturity level, it would have a great opportunity to be a successful wireless communication technology.

Bruce Schneier et al. [5] have proposed a Twofish - 128-bit block cipher that accepts a variable-length key up to 256 bits. The cipher is a 16-round Feistel network with a bijective F function made up of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix over GF(28), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule. Keys should be as short as possible. It is much harder to design an algorithm with a long key than an algorithm with a short key. They found it easier to design and analyse Twofish with a 128-bit key than Twofish with a 192- or 256-bit key in their design process. Twofish keys should be as short as possible. Twofish is Not breakable and with more rounds it gives high security, herewith it is theoretical but since no practical.

Aamer Nadeem et al. [6] have mentioned four of the popular secret key encryption algorithms, i.e., DES, 3DES, AES (Rijndael) and Blowfish have been implemented and the performance is compared by encrypting input files of varying contents and sizes on different hardware platforms. The performance of a block cipher and stream cipher varies with the block size and key size. The larger the block size, the faster will be the algorithm. The smaller the block size, the algorithm will be slower due to execution of cycles. In the end, the results were presented which conclude that the Blowfish is the fastest algorithm. A proposed direction for the future work could be to analyze the performance/security trade-off in greater depth. For instance, an algorithm with more complex rounds and a larger number of rounds is generally considered more secure.

Rakesh Kumar Jha et al. [7] has mentioned the anticipated technology for wireless broadband access, the WiMAX is finally starting to be available in the market with the aim to provide high data rates and provide interoperability of vendor devices at the same time. WiMAX has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. Vulnerabilities and threats associated with both layers in WiMAX (Physical and MAC layers). At PHY layers, jamming can be considered a major threat. At MAC layer, critical threats include eavesdropping of management messages. WiMAX is still under development and need more research on its securities vulnerabilities. In the near future, when WiMAX achieves a maturity level, it would have a great opportunity to be a successful wireless communication technology.

Naganand Doraswamy et al. [11] have mentioned that IP Packets have no inherent security. It is relatively easy to forge the addresses of IP packets, modify the contents of IP packets, replay old packets, and inspect the contents of IP packets in transit. Therefore, there is no guarantee that IP datagram's received are (1) from the claimed sender (the source address in the IP header); (2) that they contain the original data that the sender placed in them; or (3) that the original data was not inspected by a third party while the packet was being sent from source to destination. IPSec is a method of protecting IP datagram's. IPSec protects IP datagram's by defining a method of specifying the traffic to protect, how that traffic is to be protected, and to whom the traffic is sent. IPSec can protect packets between hosts, between network security gateways (e.g., routers or firewalls), or between hosts and security gateways. The method of protecting IP datagram's or upper-layer protocols is by using one of the IPSec protocols, the Encapsulating Security Payload (ESP) or the Authentication Header (AH). AH provides proof-of-data origin on received packets, data integrity, and antireplay protection. ESP provides all that AH provides in addition to optional data confidentiality.

Abdul Elminaam et al, [14] has described the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. The performance measure of encryption schemes will be conducted in terms of energy, changing data types such as text or document and images-power consumption, changing packet size and changing key size for the selected cryptographic algorithms. First there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Second in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Third in the case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. Finally in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. In decryption, Blowfish is better than other algorithms in throughput and power consumption. The second point should be notice here that RC6 requires less time than all algorithms except Blowfish.

Víctor A. Villagra [15] has described that IPSec has three main functionalities (1) Authentication only (AH), (2) Encryption + Authentication (ESP), (3) Key Management Functions (ISAKMP). IPSec has transmitted as a new header in the IP datagram between the original header and the payload. In ESP, data are encrypted and a new datagram trailer is added. Authentication Header provides support for the authentication and integrity of the IP datagram's. Encapsulating Security Payload provides (1) Content Confidentiality, (2) Limited traffic flow confidentiality, (3) Optionally authentication services like AH. Where IPSec is the protocol used to protect the packets between end-to-end networks in WiMAX. Encryption algorithms are used to protect the traffic for better security.

4. PROPOSED WORK

In our proposed work, WiMAX Network layer is used to provide End to End security with complete encryption of data. Later wise, important security algorithm is needed to avoid the attacks. For that case IPSec [22] is the protocol used in Network Layer in WiMAX and Twofish is the Encryption algorithm to encrypt the packets then MD-5 is the authentication algorithm used to authenticate the message.

4.1 IPSec

IPSec supports two security protocols, namely, the authentication header (**AH**) and the encapsulating security payload (**ESP**).

✓ The **Authentication Header** [23] Protocol is used when the integrity and authenticity of the IP packet or its payload must be protected but not necessarily the confidentiality of the packet itself.

✓ The **Encapsulating Security Payload** [24] Protocol is used to encrypt and encapsulate either the transport layer payload or the entire IP packet.

We used IPSec protocol for secured communication in network layer. For complete encryption of user data, tunnel mode is used to secure the packets from host to host, network to network, host to network.

IPSec protects IP datagram's by defining a method of specifying the traffic to protect, how that traffic is to be protected, and to whom the traffic is sent. IPSec can protect packets between hosts, between network security gateways (e.g., routers or firewalls), or between hosts and security gateways. For example, end-to-end authentication between hosts and security gateways, IPSec protect the data through a tunnel.

IPSec is a suite of protocols and it is important to understand how these protocols interact with each other and how these protocols are tied together to implement the capabilities described by the IPSec architecture. The ESP and the AH documents define the protocol, the payload header format, and the services they provide.

IKE generates keys for the IPSec protocols. IKE is also used to negotiate keys for other protocols that need keys. There are other protocols in the Internet that require security services such as data integrity to protect their data. IKE uses the language of ISAKMP to define a key exchange and a way to negotiate security services. IKE actually defines a number of exchanges and options that can be applied to the exchanges. The end result of an IKE exchange is an authenticated key and agreed-upon security services in other words, an IPSec security association. IKE defines how security parameters are negotiated and shared keys are established for other protocols.

IPSec [15] is a suite of protocols and it is important to understand how these protocols interact with each other and tied together to implement the capabilities described by the IPSec. The ESP and the AH define the protocol, the payload header format, and the services they provide.

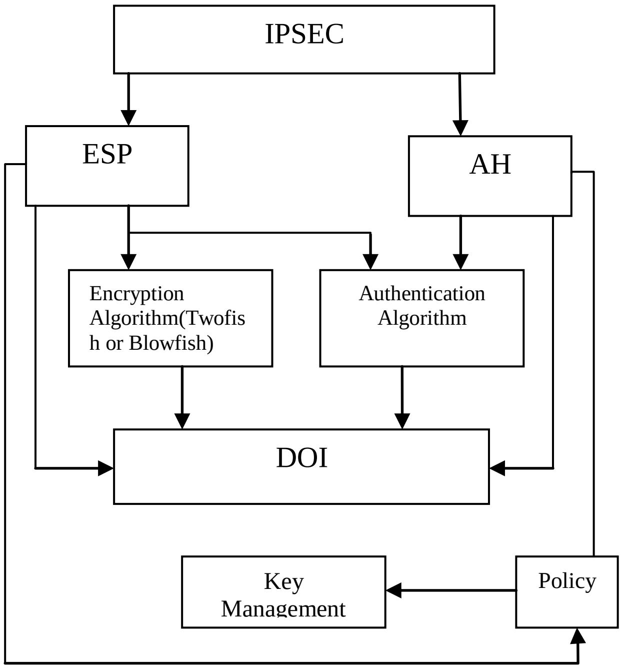


Fig 2: IPSec Architecture

A DOI (Domain of Interpretation) document defines many things: a naming scheme for DOI-specific protocol identifiers, the contents of the situation field of the ISAKMP SA payload, the attributes that IKE negotiates in a Quick Mode and any specific characteristics that IKE needs to convey.

Policy is the security interface between human and computer. Policy is not a standard. However, the main challenge with policy is its definition and representation at a higher level, and then mapping it so that IKE and IPSec protocols can access it efficiently and unambiguously.

Both the Authentication Header and Encapsulating Security Payload Protocol support two modes of use [15]:

Transport Mode:

It protects the upper layer protocols, only the packet payload is encrypted. In transport mode AH and ESP protect the transport header. The transport mode of IPSec can be used only when security is desired end to end.

Tunnel Mode:

All the packets are encrypted, including the IP header, and it is encapsulated as a payload in a new IP packet. In the case of tunnel mode, IPSec encapsulates an IP packet with IPSec headers and adds an outer IP Header. If the security services are provided end to end, transport mode is better because it does not add an extra IP header.

4.1.1 Authentication Data

MD-5 (Message Digest) is the algorithm used to authenticate the data for packet transmission. MD-5 does not perform any encryption or decryption, and it is just used to create a message digest for authentication and integrity.To mention the wired or wireless transmission TCP/UDP protocol is used in tunneled mode. The ICV is calculated by passing the key from the SA and the entire IP packet (including the AH header) to the algorithm identified as the authenticator in the SA. Since the mutable fields have been zeroed out the actual values are not included in the ICV. The ICV value is then copied into authentication data field of the AH and the mutable fields in the IP header can be filled in. AH processing is now complete and the AH-protected IP packet can be transmitted. Depending on the size of the packet, it might be fragmented prior to placing on the wire or it might be fragmented in transit by routers between the two IPSec peers.

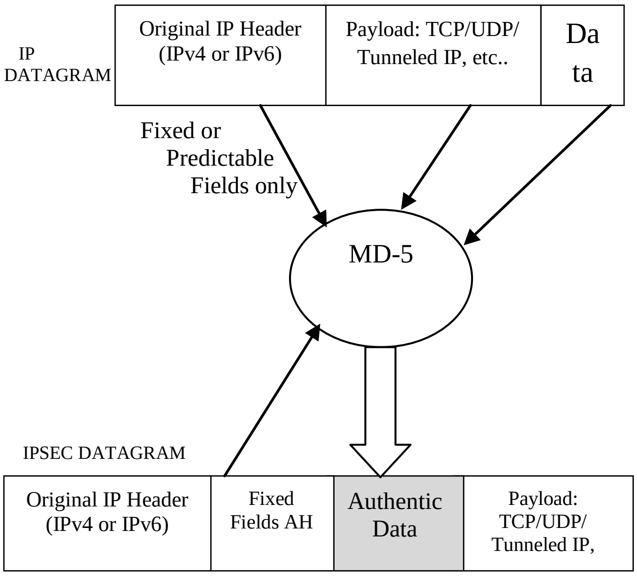

IP DATAGRAM
Original IP Header (IPv4 or IPv6)
Payload: TCP/UDP/ Tunneled IP, etc..
Da ta
Fixed or Predictable Fields only
MD-5
IPSEC DATAGRAM
Original IP Header (IPv4 or IPv6)
Fixed Fields AH
Authentic Data
Payload: TCP/UDP/ Tunneled IP,

Fig 3: Authentication Data

4.1.2 ESP Computation

To specify the protocol address, IPv4 or IPv6 is used to reach the destination from the source. To mention the wired or wireless transmission TCP/UDP protocol is used in tunneled mode. If the block size is 64 bits and the last block of input is only 48 bits, it may be necessary to add 16 bits of padding to the block prior to performing the encryption (or decryption) operation. The pad length field simply defines how much pad has been added so that the recipient can restore the actual length of the payload data. The next header field indicates the type of data that is contained in the payload data field what ESP is actually protecting. The SPI is a very important element in the SA. An SPI is a 32-bit entity that is used to uniquely identify an SA at the receiver.

Security context or SA is a contract between two hosts communicating securely and indicates the parameters, such as keys and algorithms. The sequence number is a 32-bit field and is used in outbound processing. The sequence number is part of both AH and ESP header. The sequence number is incremented by 1 every time the SA is used to secure a packet.

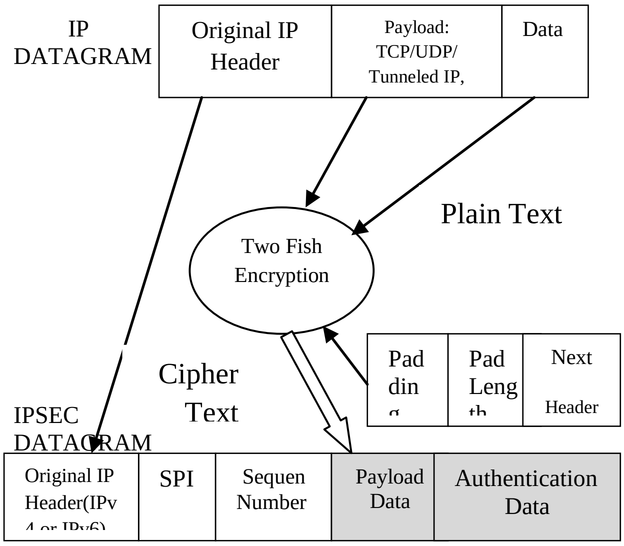


Fig 4: ESP Computation

This field is used to detect replay attacks by the destination. The actual data being protected by ESP is contained in the payload data field. The length of this field therefore depends on the length of the data. The protected data field is also used to contain any initialization vector that an encryption algorithm may require. To authenticate and to hide the data, ESP is used in IPSec protocol.

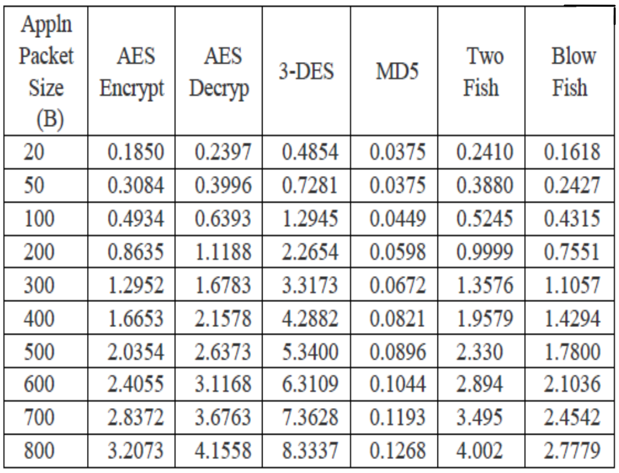
5. SIMULATION RESULTS AND DISCUSSIONS

5.1 Simulation Model and Parameters

We use NS 3 [9] to simulate our proposed work in Mobile WiMAX IEEE 802.16e, to provide End to End Security in the IPSec protocol. By analysis of various cryptographic algorithms we use the simulation tool to view the graphs for throughput, space overhead and for the processing time.

In our simulation, mainly Twofish and Blowfish is compared with the previously used algorithms as AES, DES, 3-DES, MD-5 [32] for analysis of each.

Table 1. Processing Time for 100-MIPS Processor in Milliseconds



Appln Packet Size (B)	AES Encrypt	AES Decryp	3-DES	MD5	Two Fish	Blow Fish
20	0.1850	0.2397	0.4854	0.0375	0.2410	0.1618
50	0.3084	0.3996	0.7281	0.0375	0.3880	0.2427
100	0.4934	0.6393	1.2945	0.0449	0.5245	0.4315
200	0.8635	1.1188	2.2654	0.0598	0.9999	0.7551
300	1.2952	1.6783	3.3173	0.0672	1.3576	1.1057
400	1.6653	2.1578	4.2882	0.0821	1.9579	1.4294
500	2.0354	2.6373	5.3400	0.0896	2.330	1.7800
600	2.4055	3.1168	6.3109	0.1044	2.894	2.1036
700	2.8372	3.6763	7.3628	0.1193	3.495	2.4542
800	3.2073	4.1558	8.3337	0.1268	4.002	2.7779

We have considered three types of processors in our simulations: 100, 400, and 800 MIPS [30]. In Figure 5, we have illustrated the results derived from Table 1. We can see that the 3-DES algorithm has the highest processing time, whereas the Twofish requires slightly more processing time than the AES due to the complexity of algorithm but it have high security. 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. Finally, Blowfish has low processing time because it is a fastest algorithm than any other encryption algorithm.

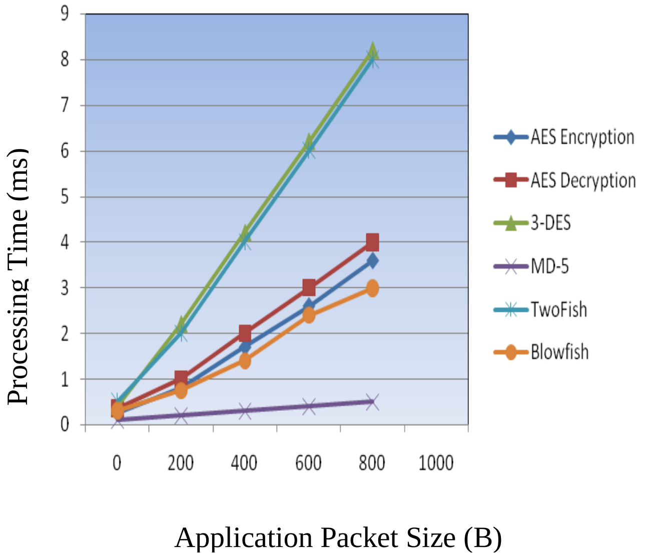
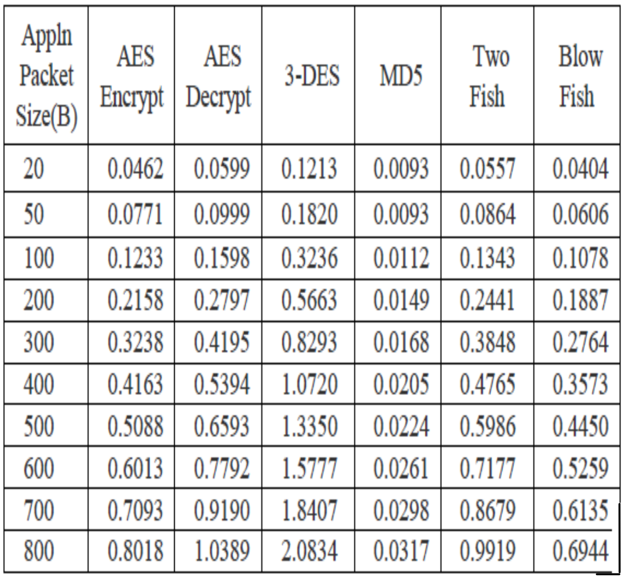


Fig 5: The processing times for a 100-MIPS processor

In the same context, Table 2 and Figure 6 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 Twofish have approximately the same processing time with light variation. Since Blowfish has low processing time due to its fastest encryption.

Table 2. Processing Time for 400-MIPS Processor in Milliseconds



Appln Packet Size(B)	AES Encrypt	AES Decrypt	3-DES	MD5	Two Fish	Blow Fish
20	0.0462	0.0599	0.1213	0.0093	0.0557	0.0404
50	0.0771	0.0999	0.1820	0.0093	0.0864	0.0606
100	0.1233	0.1598	0.3236	0.0112	0.1343	0.1078
200	0.2158	0.2797	0.5663	0.0149	0.2441	0.1887
300	0.3238	0.4195	0.8293	0.0168	0.3848	0.2764
400	0.4163	0.5394	1.0720	0.0205	0.4765	0.3573
500	0.5088	0.6593	1.3350	0.0224	0.5986	0.4450
600	0.6013	0.7792	1.5777	0.0261	0.7177	0.5259
700	0.7093	0.9190	1.8407	0.0298	0.8679	0.6135
800	0.8018	1.0389	2.0834	0.0317	0.9919	0.6944

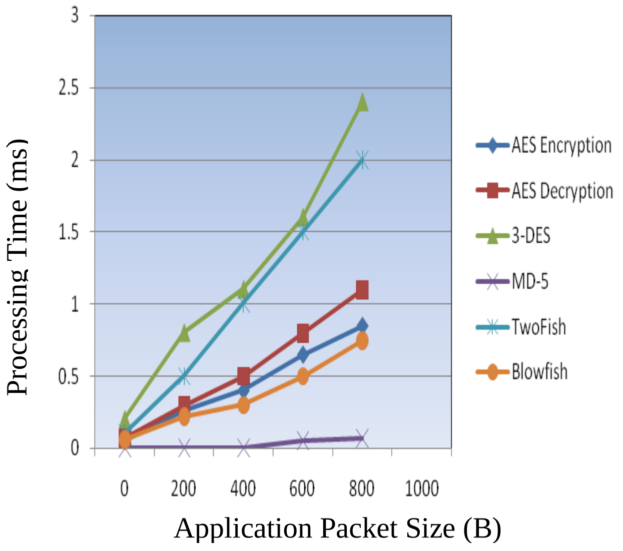


Fig 6: The processing times for a 400-MIPS processor

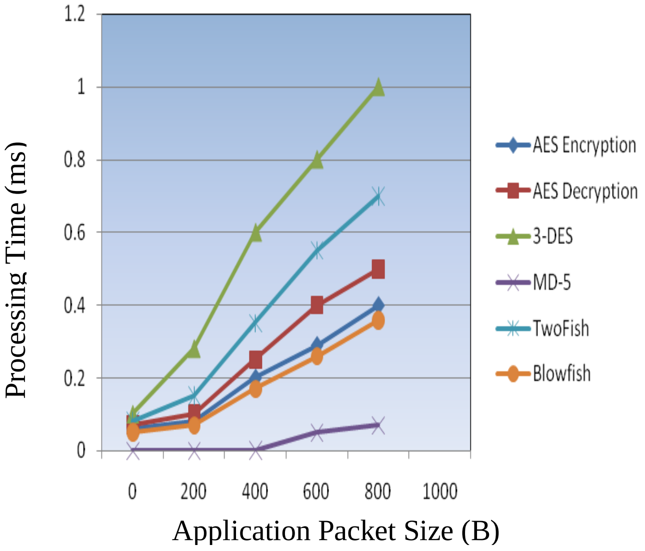


Fig 7: The processing times for an 800-MIPS processor

Likewise, Figure 7 and Table 3 have showed the processing time for 800 MIPS-processor, where the same 3-DES has highest processing time than any other algorithms. Moreover, when increasing the processor size the processing time for Twofish is reduced and equals the AES encryption algorithm. Such that there is not much delay in Twofish, when MD-5 is combined with Twofish it performs better than other algorithms and so Blowfish is the fastest algorithm in all cases.

The amount of data transferred from one place to another or processed in a specified amount of time is throughput. In fig 8, throughput is measured for various cryptographic algorithms, among those Twofish + MD-5 performs better result rather than any other algorithm. Hence one note is Blowfish performance is high but gives low security rather than Twofish. From these criteria we may know that when giving high security and larger RAM sizes with any algorithm it performs better than anyone. Similarly this is the figure which is used to preview the throughput for 500 kbps data rate with 100, 400, 800 MIPS processors in the WiMAX Network layer IPSec protocol.

Table 3. Processing Time for 800-Mips Processor in Milliseconds

Appln Packet Size(B)	AES Encrypt	AES Decrypt	3-DES	MD5	Two Fish	Blow Fish
20	0.0231	0.0299	0.0606	0.0046	0.0259	0.0202
50	0.0385	0.0499	0.0910	0.0046	0.0399	0.0303
100	0.0616	0.0799	0.1618	0.0056	0.0697	0.0539
200	0.1079	0.1398	0.2831	0.0074	0.1198	0.0943
300	0.1619	0.2097	0.4146	0.0084	0.1996	0.1382
400	0.2081	0.2697	0.5360	0.0102	0.2497	0.1786
500	0.2544	0.3296	0.6675	0.0112	0.2931	0.2225
600	0.3006	0.3896	0.7888	0.0130	0.3662	0.2629
700	0.3546	0.4595	0.9203	0.0149	0.4312	0.3067
800	0.4009	0.5194	1.0417	0.0158	0.5001	0.3472

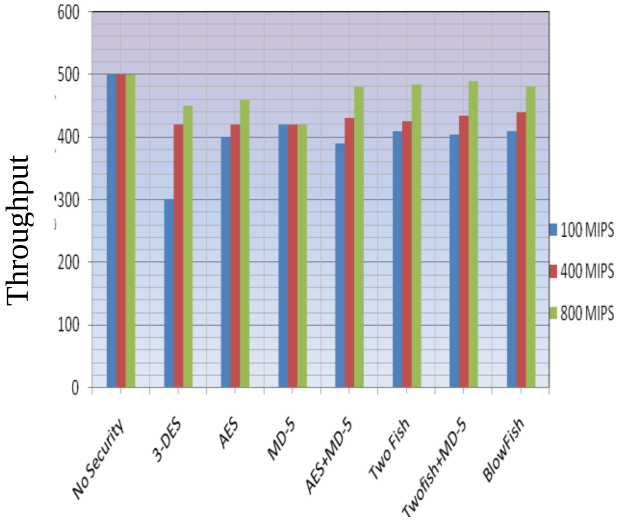


Fig 8: Throughput for 500 kb/s data rate with 100, 400 and 800 MIPS Processors

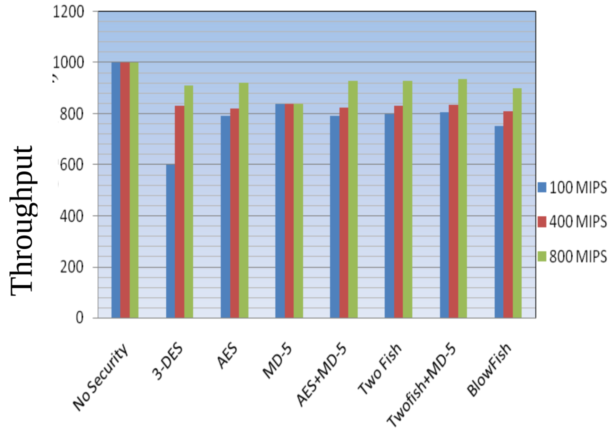


Fig 9: Throughput for 1000 kb/s data rate with 100, 400 and 800 MIPS Processors

In fig 9, throughput is measured for 1000 kbps data rate for various cryptographic algorithms, when the data rate is increased throughput is reduced for each encryption algorithm.

Figure 10 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.

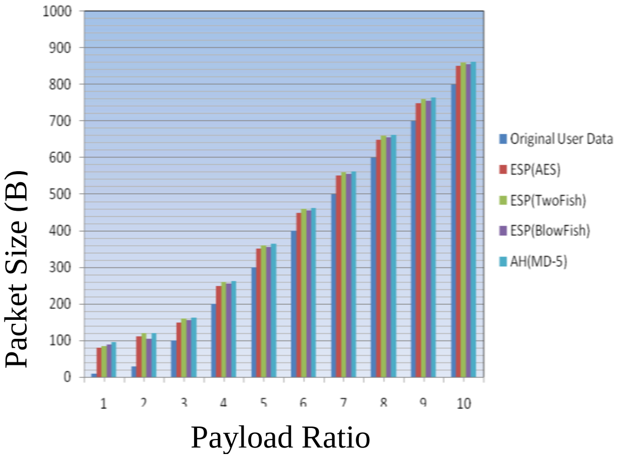


Fig 10: The space overhead of the IPSec according to each security algorithm option

By analyzing the results and Biclique cryptanalysis [13], we have concluded that Twofish and Twofish+MD5 are best algorithms rather than Blowfish and other 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 [38].

6. CONCLUSION

WiMAX technology is analyzed and the security issue has been found out in Security Sub Layer in Mac Layer. For End to End security in WiMAX networks, IPSec protocol is used for complete Encryption of user data in the Network Layer. In the IPSec protocol for encryption and authentication, Twofish [5] and Blowfish [26] algorithms are used for better security over WiMAX in Network Layer to provide the packet transmission as secured form. Communication between Base Station and subscriber station, IPSec is the protocol used to encrypt, authenticate and hide the data using ESP tunnel mode operation.

7. ACKNOWLEDGMENT

At the outset we whole heartedly thank the **living lord Jesus Christ,** the sole creator of all creations in this world. Hence S.Rimlon Shibi would like to thank Mr. M. Kaliappan and Mr. J. Jerart Julus for their guidance to do this work in the right time. Then S.Rimlon Shibi would like to acknowledge all the staffs those who guide me in the right path.

8. REFERENCES

[1] Dr. S.A.M Rizvi, Dr. Syed Zeeshan Hussain, "Performance Analysis of AES and TwoFish Encryption Schemes", Commn Sys & Network Tech's, IEEE, 2011.

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

[3] Alex Biryukov, Dmitry Khovratovich, Ivica Nikolic. “Distinguisher and Related-Key Attack on the Full AES-256”, University of Luxembourg, 2009.

[4] Trung Nguyen,Prof. Raj Jain, “A survey of WiMAX security threats”, www1.cse.wustl.edu/ jain/cse571-09/ftp/wimax2/index.html, 2010.

[5] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, “Twofish: A 128-Bit Block Cipher”, Counterpane Systems, 2000.

[6] Aamer Nadeem, Dr M. Younus Javed, “A Performance Comparison of Data Encryption Algorithms”, IEEE 2005.

[7] Rakesh Kumar Jha, D Dalal et al, “A Journey on WiMAX and its Security Issues”, IJCSIT, Vol. 1 (4), 2010.

[8] Mathieu Lacage, “Experimentation with ns-3”, Trilogy Summer School, 27th august 2009.

[9] NS-3 Overview, “www.nsnam.org\ ns-3 Tutorial” Release ns-3.13, Dec’ 2011.

[10] Elias Weingrtner, Hendrik vom Lehn and Klaus Wehrle, “A performance comparison of recent network simulators”, RWTH Aachen University,2009.

[11] Naganand Doraswamy, Dan Harkins, “IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks”, Prentice Hall PTR, , 2003.

[12] Ibikunle F.A., Jamshed hasan, “Security Issues in Mobile WiMAX (802.16e)”, Mobile WiMAX Symposium, pp. 117 – 122, 2009.

[13] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, “Biclique Cryptanalysis of the Full AES”, in 2011 Cryptology conference in Santa Barbara, California.

[14] D. S. Abdul. Elminaam et al.,“Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA, Vol 8, 2009.

[15] Víctor A. Villagra, “Security Architecture for the Internet Protocol: IPSEC”, DIT-UPM, 2002.

[16] E. B. Fernandez and M. VanHilst, ‘‘An overview of WiMAX security,’’ in WiMAX Standards and Security, M. Ilyas, Ed. Boca Raton, CRC Press, 2008, pp. 197–204.

[17] C. Eklund and S. Wang, et al., ‘‘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.

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

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

[20] 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.

[21] O. Elkeelany et al., Performance analysis of IPsec protocol: encryption and authentication, In: IEEE Communications Conference (ICC 2002), 2002, pp. 1164–1168.

[22] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[23] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, November 1998.

[24] S. Kent, R. Atkinson, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

[25] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[26] Bruce Schneier. “The Blowfish Encryption Algorithm” Retrieved October 25, 2008, http://www.schneier.com/blowfish.html.

[27] M. Barbeau, “WiMAX/802.16 threat analysis,” in Proceedings of 1st ACM international workshop on Quality of service in wireless and mobile networks, Quebec, June 2005 .

[28] Mahmoud Narsreldin, Heba Aslan, “Wimax security,” in 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1335–1340.

[29] W. C. Taeshik Shon, “An analysis of mobile wimax security: Vulnerabilities and solutions,” in Lecture notes in computer science, Springer, 2007.

[30] S.Z.S. Idrus, et al.,, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers, " IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008, PP 20-25.

[31] Dieter Schmidt, “Kameichel, anextension of Blowfish for 64-bit architectures”, September 30,2006.

[32] Diaa Salama Abd Elminaam, et al., “Evaluating the Performance of Symmetric Encryption Algorithms” International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

[33] Amit Soni, Harish Karnick and Manindra Agarwal, “Learning encryption algorithms from ciphertext”, IIT Kanpur, Department of Computer Science and Engineering, 2009.

[34] A. Murat Fiskiran and Ruby B. Lee, “Performance Impact of Addressing Modes on Encryption Algorithms”, 2001 IEEE.

[35] Othmar Kyas, “Mobile Wimax For Networks With Enhanced Security And Reliability Requirements”, Tektronix 4/2007 IEEE.

[36] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). The Internet Engineering Task Force - Request for Comments: 3748, June 2004.

[37] Mohammad Ahmed Alomari, Khairulmizam Samsudin and Abdul Rahman Ramli, “A Study On Encryption Algorithms And Modes For Disk Encryption”, 2009 International Conference on Signal Processing Systems, IEEE.

[38] WiMAX Forum: WiMAX End-to-End Network Systems Architecture (Stage 3: Detailed Protocols and Procedures) Release 1, V.1.3.0, 2008.