Security Enhancement for Mobile WiMAX Network

D. David NeelsPon Kumar, Praveen David, S.Rimlon Shibi, K.Arun Kumar

Abstract- ***Security in wireless networks has traditionally been considered to be an issue to be addressed at the higher layers of the network.IEEE 802.16, known as WiMAX, is at the top of communication technology drive because it is gaining a great position in the next generation of wireless networks. Due to the evolution of new technologies wireless is not secured as like others networking technologies. A lot of security concerns are needed to secure a wireless network.Secure communication can only be provided after successful authentication and a robust security network association is established. By keeping in mind the importance of security, the WiMAX working groups has designed several security mechanisms to provide protection against unauthorized access and threats, but still facing a lot of challenging situations. WiMAX security architecture deals with all of the basic wireless security requirements like authentication, authorization, access control, data integrity, confidentiality and privacy.This paper examines the threats which are associated with MAC layer and physical layer of WiMAX and also proposes some enhancements to the existing model for improving the performance of the encryption algorithm and proposes some techniques in the existing model to enhance its functionality and capability.***

Index Terms- WiMAX, Authentication, Authorization, Access control, Data integrity, Confidentiality

I. INTRODUCTION

WiMAX stands for Worldwide Interoperability for Microwave Access. WiMAX technology is a telecommunications 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.

Actually 802.16-2004 or 802.16d is developed by the third party as a standard and it is also referred to call as Fixed WiMAX because this standard is lacking behind just because of the non-mobility feature that's why it's often called as Fixed WiMAX. During the maturity period of WiMAX technology some of the amendments were made to the above mentioned 802.16d. It introduced mobility and some other features amongst other standards and is also known as Mobile WiMAX.

Manuscript received on January, 2013

D. David NeelsPon Kumar, Professor, Department of ECE, Einstein College of Engineering, TN, India.

Praveen David, PG scholar, Department of ECE, Einstein College of Engineering, TN, India.

S.Rimlon Shibi, Lecturer, Department of IT, Saint Joseph Engineering College, India.

K.Arun Kumar, Assistant Professor, Department of ECE, Einstein College of Engg., TN, India.

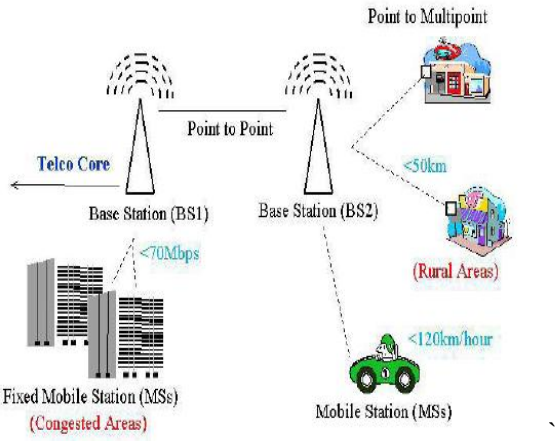

Fig -1: Simple WiMAX Environment

WiMAX/802.16 is based on the 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 the 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).

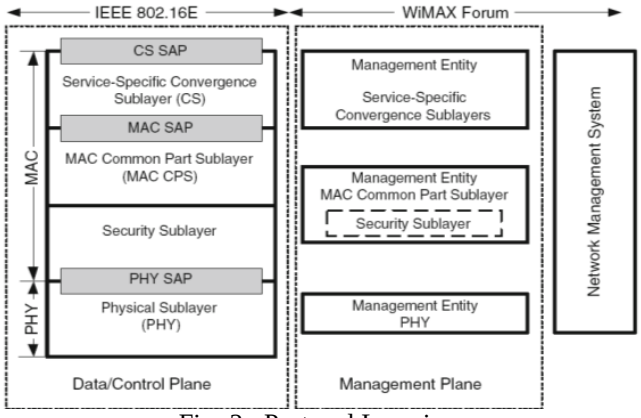

Fig -2: Protocol Layering

The 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.

WiMAX Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. In this case, these services are provided for IP traffic only. Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected. Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and

encrypting each IP packet of a communicationsession. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

II. LITERATURE SURVEY

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.Christos Xenakis et al. [2] have proposedIPSecpacketization overhead depends on the selected security protocol are AH and ESP. The ESP header, which includes the security parameters index and the sequence number fields, is inserted into the IP packet immediately prior to the transport-layer header.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. They have show a chosen key distinguisher for the 256-bit key AES with almost practical complexity of q * 2^{67} queries and negligible memory.Trung Nguyen and Raj Jain, [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. 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. AamerNadeem and YounusJaved, [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. Abdul Elminaam et al, [7] 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 datatypessuch as text or documentand images- power consumption, changing packet size and changing key size for the selectedcryptographic algorithms. Rakesh Kumar Jha and Upena D Dalal [8] 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 sametime. NaganandDoraswamy and Dan Harkins [12] 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. Víctor A. Villagra [13] 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.

III. ANALYSED SECURITY ALGORITHMS

3.1 Two Fish

It is a 128-bit symmetric block cipher. Its Key lengths are 128 bits, 192 bits and 256 bits. It has no weak keys. It is more efficient on both the Intel Pentium Pro and other software and hardware platforms.

Operation

Two fish uses a 16-round Feistel-like structure with additional whitening of the input and output. The only non-Feistel elements are the 1-bit rotates. The rotations can be moved into the *F* function to create a pure Feistel structure, but this requires an additional rotation of the words just before the output whitening step. The plaintext is split into four 32-bit words. In the input whitening step, these are xored with four key words. This is followed by sixteen rounds. In each round, the two words on the left are used as input to the *g* functions. (One of them is rotated by 8 bits first.) The *g* function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an MDS matrix. The results of the two *g* functions are combined using a Pseudo- Hadamard Transform (PHT), and two keywords are added. These two results are then xored into the words on the right (one of which is rotated left by 1 bit first, the other is rotated right afterwards). The left and right halves are then swapped for the next round. After all the rounds, the swap of the last round is reversed, and the four words are xored with four more key words to produce the cipher text.

Algorithm description of Two fish

Step 1: Feistel Networks

A Feistel network is a general method of transforming any function (usually called the Ffunction) into a permutation

Step 2: S-boxes

S-boxes are built using two fixed 8-by-8-bit permutations and key material.

s0(x) = q1 [q0 [q0[x] + k0] + k1]

s1(x) = q0 [q0 [q1[x] + k2] + k3]

s2(x) = q1 [q1 [q0[x] + k4] + k5]

s3(x) = q0 [q1 [q1[x] + k6] + k7]

Where q0, q1 are two fixed 8-bit permutations and ki (+ represents XOR)

Step 3: Key Schedule

Step 4: MD5 Matrices

Step 5: Pseudo-Hadamard Transforms

Step 6: Function F

The function F is a key-dependent permutation on 64-bit values. It takes three arguments, two input words R0 and R1, and the round number r used to select the appropriate sub keys

T0 = g (R0)

*T*1 = *g*(ROL(*R*1*;* 8))

*F*0 = (*T*0 + *T*1 + *K*2*r*+8) mod 232

F1 = (T0 + 2T1 + K2r+9) mod 232

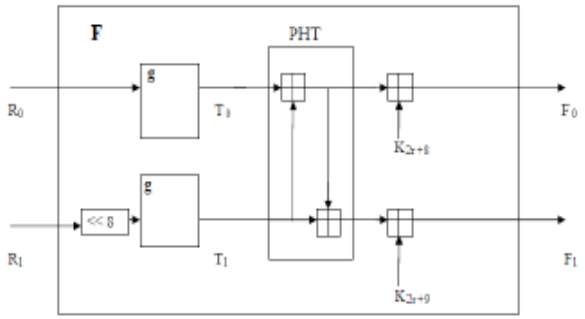

Fig -3: Functions F

Step 7: Whitening

Step 8: The Function G

It is the Heart of two fish. The input word *X* is split into four bytes. Each byte is run through its own key-dependent S-box. Each S box is bijective, takes 8 bits of input, and produces 8 bits of output.

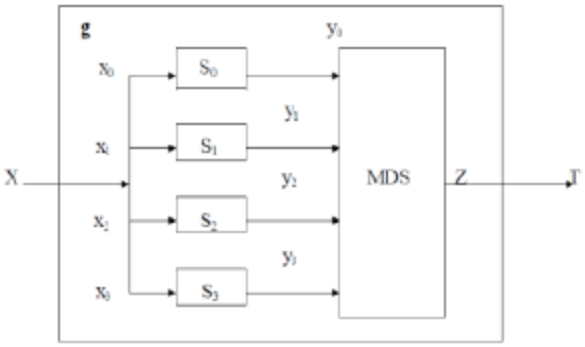

Figure 4: Functions G

MD-5

MD5 is a message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where alarge file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. The MD5 algorithm is designed to be quite fast on 32-bit machines. It does not require any large substitution tables; the algorithm can be coded quite compactly. The MD5 algorithm is an extension of the MD4 message-digest algorithm. MD5 is slightly slower than MD4, but is more "conservative" in design. MD5 was designed because it was felt that MD4 was perhaps being adopted for use more quickly than justified by the existing critical review; because MD4 was designed to be exceptionally fast, it is "at the edge" in terms of risking successful cryptanalytic attack. MD5 backs off a bit, giving up a little in speed for a much greater likelihood of ultimate security.

MD5 Algorithm Description

Here b-bit message as input and it is an arbitrary nonnegative integer; b may be zero, it need not be a multiple of eight, and it may be arbitrarily large,and the aim is to find message digest.The bits of the message written down as follows :

m_0 m_1 ... m_{b-1}

The following **five steps** are performed to compute the message digest of the message.

Step 1: Append Padding Bits

Step 2: Append Length

Step 3: Initialize MD Buffer

Step 4: Process Message in 16-Word Blocks

Step 5: Output

IV. PROCESSING TIME FOR 100 MIPS PROCESSOR

The time it takes to complete a prescribed procedure; "they increased output by decreasing processing time".

Application Packet Size (B)	AES	TWOFISH	BLOWFISH	MD-5	TWOFISH + MD-5
20	.187113	.218275	.271529	.0003902	.10934
50	.462897	.544218	.676966	.0006029	.27242
100	.919275	1.08496	1.34615	.0008994	.54295
200	1.83719	2.17133	2.68789	.001605	1.08647
300	2.75605	3.25011	4.02843	.0023015	1.62621
400	3.67722	4.33246	5.37294	.0030000	2.16773
500	4.59415	5.42515	6.73485	.003709	2.71443
600	5.51246	6.50039	8.07364	.004510	3.2525
700	6.42247	7.58163	9.39498	.005206	3.79342
800	7.33644	8.66985	10.7321	.005999	4.33793

Table -1: Processing Time for 100-MIPS processor in milliseconds

In my simulations, i have considered three types of processors: 100, 400, and 800 MIPS. In chart-1, i have illustrated the results derived from Table-1. I can see that the Blowfish 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, Twofish + MD-5 are a novel approach for authentication and encryption with low processing time for 100 MIPS processor. By varying the packet sizes in the specific algorithm, Processing Time also got varied in that scenario.

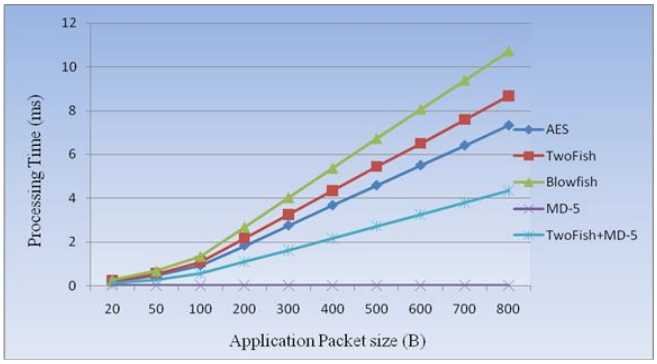

Chart -1: The processing times for a 100-MIPS processor

V. PROCESSING TIME FOR 400 MIPS PROCESSOR

In the same context, Table-2 and chart-2 show the required processing times for each security setup when a 400-MIPS processor has been used.

Application Packet Size (B)	AES	TWOFISH	BLOWFISH	MD-5	TWOFISH + MD-5
20	0.046 77825	0.0546	.06788	.0000 976	.02734
50	0.115 72425	0.1361	.169242	.0001 51	.06811
100	0.229 81875	.27124	.33654	.0002 249	.13574

200	0.459 2975	.5428	.6720	.0004 013	.27162
300	0.689 0125	.8125	1.00711	.0005 76	.40655
400	0.919 305	1.0831	1.3432	.0007 5	.54193
500	1.148 5375	1.3562	1.6837	.0009 273	.67861
600	1.378 115	1.6251	2.01841	.0011 28	.81313
700	1.605 6175	1.895	2.34875	.0013 02	.94836
800	1.834 11	2.1675	2.68303	.0015 00	1.08448

Table -2: Processing Time for 400-MIPS processor in milliseconds

I have noticed that Blowfish algorithm still has the highest required processing time, whereas AES and Twofish have approximately the same processing time with light variation. Since Twofish + MD-5 are a novel approach for authentication and encryption with low processing time for 400 MIPS processor.

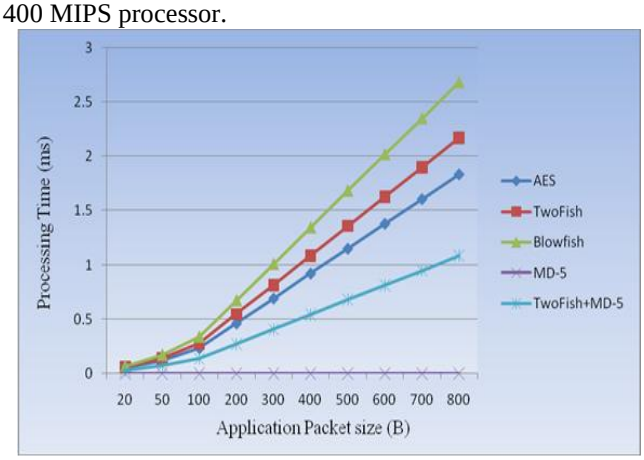

Chart -2:The processing times for a 400-MIPS processor

VI. PROCESSING TIME FOR 800 MIPS PROCESSOR

Application Packet Size (B)	AES	TWO FISH	BLOW FISH	MD-5	TWOFISH + MD-5
20	0.023389125	0.0273	.03394	.0000487 8	.01367
50	0.057862125	0.0680	.08462	.000754	.03405
100	0.114909375	.13562	.16827	.0001124	.06787
200	0.22964875	.2714	.33599	.0002006	.13581
300	0.34450625	.4063	.50355	.0002877	.20328
400	0.4596525	.5416	.67162	.000375	.27097
500	0.57426875	.6781	.8419	.000464	.33930
600	0.6890575	.8125	1.00921	.005638	.40656
700	0.80280875	.9477	1.1744	.0006508	.47418
800	0.917055	1.0837	1.34151	.0007499	.54224

Table -3: Processing Time for 800-MIPS processor in milliseconds

Likewise, chart-3 and Table 3 have showed the processing time for 800 MIPS-processor, where the same Blowfish has highest processing time than any other algorithms. Moreover, when increasing the processor size the processing time for Twofish is reduced and moreover equals the AES encryption algorithm. Such that there is not much delay in Twofish and when the MD-5 is combined with Twofish it performs better than any other algorithms, which is given in the specified scenario with varied Application Packet size.

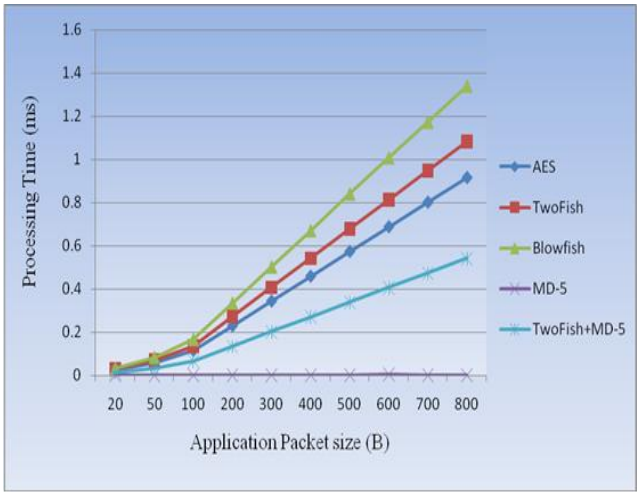

Chart -3: The processing times for a800-MIPS processor

Likewise in the graph the variations are clearly shown with various representations of lines for the given algorithms with varied Application Packet Sizes.

VII. THROUGHPUT

The amount of data transferred from one place to another or processed in a specified amount of time.From the chart-4 and chart-5, i can observe that throughput is increased gradually for the novel approach (Twofish + MD-5). So that rather than any other cryptographic algorithms, performance of the novel algorithm are good for the 500 MB/S data rate and 1000 MB/S data rate.

Then by evaluating the Throughput, Processing Time and security, this novel approach is a suitable algorithm for WiMAX Communications.

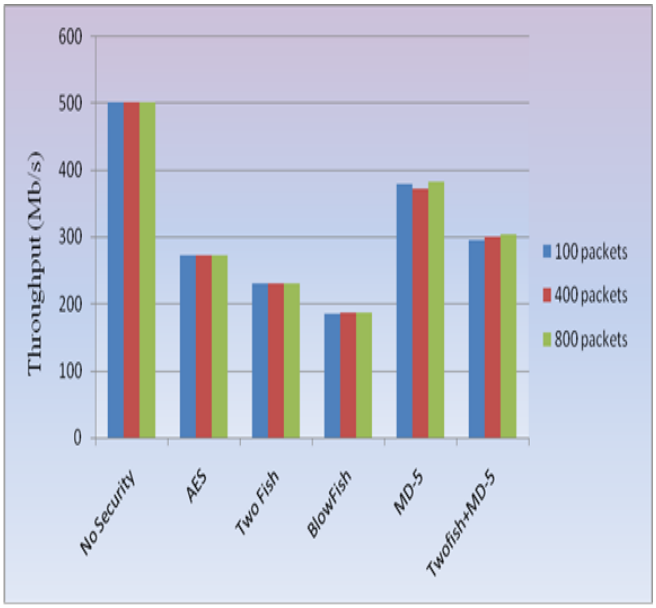

Chart -4: The throughput for 500 kb/s data rate with 100-, 400-, and 800-Packets

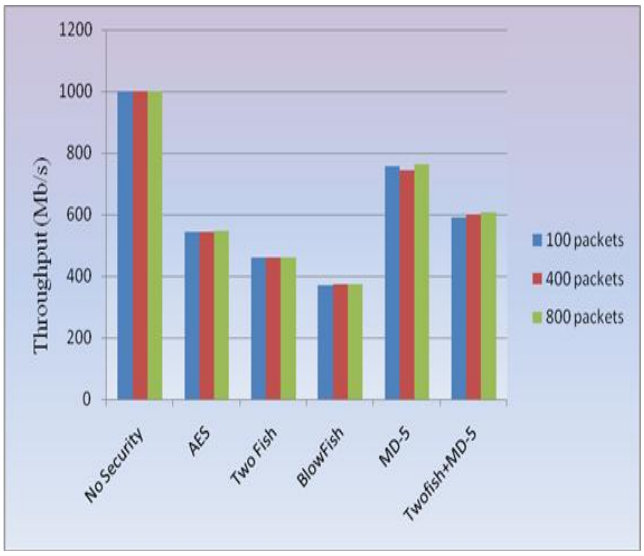

Chart -5:The throughput for 1000 kb/s data rate with 100-, 400-, and 800-Packets.

From these observations, i have concluded that TWOFISH + MD-5 are good in performance and most secured novel approach in Cryptographic algorithms. Here the simulations are done using Network Simulator-2.

VIII. FUTURE ENHANCEMENT

Here I have mentioned 100, 400, 800 MIPS of packets for improving and finding the throughput, more number of packets can be used for finding the throughput and its effect on the security layers.TheCross Layer security can be used to improve the Throughput, Processing Time, Delay, Performance and security to avoid attacks.

IX. 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 and Blowfish 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. In this case, among the analysis of algorithm AES is the best one based on Throughput and Processing Time, but to avoid the attacks in Network layer TWOFISH is the only one. To solve this case TWOFISH+MD-5 is used as a proposed algorithm to improve the security, throughput and processing time for encrypting the packets between base station and subscriber station in WIMAX.

REFERENCES

[1]. Dr. S.A.M Rizvi, Neeta Wadhwa, Dr. Syed ZeeshanHussain, "Performance Analysis of AES and TwoFish Encryption Schemes", Commn Sys & Network Tech's, IEEE, 2011.
[2]. C. Xenakis, N. Laoutaris, L. Merakos and I. Stavrakakis, "A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms", Elsevier Computer Networks, 2006.
[3]. Alex Biryukov, Dmitry Khovratovich, IvicaNikolic. "Distinguisher and Related-Key Attack on the Full AES-256", University of Luxembourg, 2009.
[4]. TrungNguyen,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]. AamerNadeem, Dr M. YounusJaved, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.
[7]. D. S. Abdul. Elminaam, H. M. Abdul Kader, M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Vol 8, 2009.
[8]. Rakesh Kumar Jha, DrUpena D Dalal, "A Journey on WiMAX and its Security Issues", IJCSIT, Vol. 1 (4) , 2010.
[9]. Mathieu Lacage, "Experimentation with ns-3", Trilogy Summer School, 27th august 2009.
[10]. "www.nsnam.org\ ns-3 Tutorial" Release ns-3.12, 2011.
[11]. Elias Weingrtner, Hendrikvom Lehn and Klaus Wehrle, "A performance comparison of recent network simulators", RWTH Aachen University, 2009.
[12]. NaganandDoraswamy, Dan Harkins, "IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall PTR, 2003.
[13]. Víctor A. Villagra, "Security Architecture for the Internet Protocol: IPSEC", DIT-UPM, 2002.
[14]. Ibikunle F.A., Jamshedhasan, "Security Issues in Mobile WiMAX (802.16e)", Mobile WiMAX Symposium, pp. 117 – 122, 2009.
[15]. 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.
[16]. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, "Biclique Cryptanalysis of the Full AES", in Crypto 2011 Cryptology conference in Santa Barbara, California.
[17]. RFC1321 - The MD5 Message-Digest Algorithm http://www.faqs.org/rfcs/ rfc1321.html.
[18]. Rivest, R., "The MD4 Message Digest Algorithm", RFC 1320, MIT and RSA Data Security, Inc., April 1992.

D. David NeelsPon Kumar was born in India, in 1971. He completed his B.E degree in ECE in 1992 and M.E degree in Digital Communication and Networking through Anna University Chennai in 2004. He is pursuing PhD in Wireless Networks through Anna University Chennai since 2007.He has 10 years of Industrial experience in India and abroad apart from 9 years of teaching experience at various cadres. Presently he is working as Associate professor in ECE department, at Einstein College of Engg., India. He has 8 publications in International journals and presented 10 papers in International and National conferences. He is a member of ISTE, IEEE and IAENG. He is a reviewer in IET Networks.

Praveen David was born in India in 1987.He completed his B.Tech in ECE from ThangalKunju Memorial Institute of Technology , through Cochin University of Science and Technology in 2009 and currently he is doing his ME in Applied Electronics from Einstein College of engineering through Anna University.

S.RimlonShibi was born in India in 1988.He completed his B.E degree in IT in 2010 and ME in Computer and Communication through Anna university, Tamilnadu.Currently he is working as a lecturer in Saint Joseph College Tansmania.

K. Arunkumar born in 1973 completed his B.E. in ECE from the Govt. College of Engineering, Tirunelveli and M.E. (Optical Commn.) from ACCET Karaikudi.He has more than 10 years of teaching experience and 7 years of Industrial experience.