EBAUB Journal Volume 3 January 2021

EBAUB Journal

ISSN: 2617 - 8338

An Academic Journal of
EXIM Bank Agricultural University Bangladesh

Analyzing a Secure Message Transmission Process over WiMAX Communication System with Implementation of AES Encryption Algorithm

Ridwan Ul Islam Mahdi[1]*, Halida Homyara[2], Md. Ashraful Islam[2]

[1]Department of Computer Science and Engineering, EXIM Bank Agricultural University Bangladesh, Chapainawabganj-6300, Bangladesh
[2]Department of Information and Communication Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh

ARTICLE INFO

Received date: Nov. 25, 2020
Accepted date: Dec. 30, 2020

ABSTRACT

This paper aims to develop and analyze a Secure Message Transmission System over a WiMAX (Worldwide Interoperability for Microwave Access) communication system with the implementation of the Advanced Encryption Standard (AES) encryption algorithm using AWGN communication channel. WiMAX has many potentials to be the leading communication technology, offering high-speed internet service up to the customer. The WiMAX technology standard 802-16 wireless MAN is configured as a traditional cellular network with base stations using point to multipoint architecture and can provide a service coverage of a few kilometers. However, wireless data transmission systems are not secured as other networking technologies. Many security concerns are required to secure a wireless network. Simulation is done using Matlab 7.5 simulation tool with necessary parameters for WiMAX communication system and AWGN channel. The results indicate that the shared secret key is adequate to properly hide the plain text over AWGN communication channel using AES. Leading us to believe that with necessary security measures WiMAX could provide privacy and security over a larger distance.

Key words: AES, AWGN, Communication system, Encryption, IEEE, MAN, Security, WiMAX

CORRESPONDENCE
* sohan.ridwan.cse@ebaub.edu.bd
Senior Lecturer, Department of Computer Science & Engineering, EXIM Bank Agricultural University Bangladesh, Chapainawabganj-6300, Bangladesh

1. INTRODUCTION

Security in computer networks has been a topic of intense research due to the increasing use of computers in recent decades with their interconnecting networks of all kinds and sizes, often via the Internet. With all these possibilities of exchanging information and accessing data stored in databases scattered around the world, organizations and even home users have viewed the need to define mechanisms to ensure that their information is properly protected. Increasing bandwidth reducing cost and improving security is the demand of modern society (Pigatto et al., 2011).

When a network is implemented poorly, security threats and attacks always exist. Applying security to a network is expensive often providing diminishing returns. Both the Network operator and the network user are playing a key role in the security providence to a network and are concerned over network security (Habib et al., 2009).

The purpose of network security is to encrypt information from unauthorized access or malicious attackers.

To Cite: Mahdi, R. I., Homyara, H. & Islam, M. A. (2021). Analyzing a secure message transmission process over WiMAX communication system with implementation of AES encryption algorithm**,** *EBAUB J*., 3, 94-101

Chart. WiMAX standards overview

Standard	802.16a	802.16d-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz-66GHz	2GHz-11GHz	2GHz-11GHz for fixed; 2GHz-6GHz for mobile
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps-134.4Mbps	1Mbps-75Mbps	1Mbps-75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/OFDMA	Burst TDM/TDMA/OFDMA
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission Scheme	Single carrier only	Single carrier only, 256 OFDM or 2048 OFDM	Single carrier only, 256 OFDM or scalable OFDM with 128, 512, 1024, 2048 subcarriers
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN
Security	DES3 and AES	DES3 and AES	PPTP, SSL, or VPN
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS

This requirement has given birth to different kinds of cryptographic primitives including symmetric and asymmetric cryptography, hash functions, digital signatures, message authentication codes, etc. (Hasib et al., 2008).

Due to the demands of better bandwidth and mobility support, IEEE 802.16 working group has developed standards with mobility access called the IEEE 802.16e-2005 amendment. It has also been developed by many working groups of the Worldwide Interoperability for Microwave Access (WiMAX) Forum, similar to Wi-Fi in IEEE 802.11 standards.

Mobile WiMAX technology is considered as one of the best next-generation wireless technologies because it can support high-speed, broadband data transmission, wide-coverage, and high capacity. A lot of security concerns are needed to secure the end-users, the core network, the application servers, and everywhere in between (Habib et al., 2009).

A Wi-Fi hotspot can be imagined as a data transfer hotspot covering a limited area. As a user travels, their smart devices connect to one data transfer hotspot after another to replenish their data transmission requirements.

In between and beyond these Wi-Fi coverages there are vast expanses of dead air where a smart device or notebook is unconnected. WiMAX will make these dead zones come alive with the high-speed of broadband Internet access (Ergen, 2009).

Fig. 1 WiMAX system diagram.

WiMAX is an IP-based, novel wireless broadband access technology that provides performance similar to Wi-Fi networks with the coverage and QoS (quality of service) of cellular networks. The meaning of WiMAX is Worldwide Interoperability for Microwave Access. WiMAX is a

wireless digital communications system, also known as IEEE 802.16, that is intended for wireless "metropolitan area networks" MAN.

WiMAX is wireless communications that can reach an upload download speed of about 30 to 40 megabit-per-second data rates, with the 2011 standard update providing up to 1 Gbit/s for fixed stations. It is a part of a "fourth generation," or 4G, of wireless-communication technology.

It can be used in both point-to-point and the typical WAN type configurations that are also used by 2G and 3G mobile network carriers. WiMAX can provide broadband wireless coverage up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations.

In contrast, the Wi-Fi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30-100m). WiMAX is built with advanced, efficient wireless technology that provides higher speeds than today's wide-area wireless technologies. It will be able to completely transform our mobile Internet lifestyle, enabling us to connect in ways we have only dreamed about (Ergen, 2009).

The current WiMAX incarnation, Mobile WiMAX, is based upon IEEE Std 802.16e-2005 was approved back in December 2005. It is a supplement to the IEEE Std 802.16-2004 and so the actual standard is 802.16-2004 as amended by 802.16e-2005 the specifications need to be read together to understand them. Basic data on IEEE 802.16 as well as WiMAX standards are given through the following chart (Bakkoury et al., 2016; Andrews et al., 2007).

WiMAX networks can easily interface with different types of networks including IP, TDM voice, and ATM. A design has also been kept for service-specific support by providing quality-of-service classes based on characteristics of different services. WiMAX networks can support VoIP, video, voice, or data using the same architecture by merely defining appropriate classes of service.

They are also capable of multicasts as well as web syndication feeds such as RSS simultaneously with other services, providing a rich user experience. These advantages of WiMAX, however, do not indicate that these networks will immediately start replacing the mobile networks. These will continue to work side-by-side providing voice data and multimedia options to users in the foreseeable future**.**

Our objective in this paper is to implement the WiMAX communication system with AES algorithms over an AWGN channel and to determine if the shared secret is adequate to ensure a safe data transmission. In the section below, we will cover the concept of AES and its encryption and decryption process with all necessary simulation models followed by a short description of simulation model.

2. MATERIALS AND METHODS

2.1. Advance Encryption Standard (AES) Cipher

AES is an iterated cipher that was proposed by Joan Daemen and Vincent Rijmen (Rijndael) (Daemen & Rijmen, 2020). The proposed algorithm could support variable-length block and key sizes e.g. multiple of 32 bits. Only the 128 bit block size and 128, 192, and 256 bits keys are specified as AES standard. An important feature of AES is that its structure is not based on the Feistel network like its predecessor DES in which half of the data block is used to modify the other half of the data block and then the halves are swapped. Rather AES is based on an S-P network in which the entire 128 bits input block is organized as a 4x4 bytes array called State and is processed in several rounds. The number of rounds is determined by the length of the key e.g. 10 rounds for 128 bit keys, 12 rounds for 192 bit keys, and 14 rounds for 256 bit keys. In both in the encryption and decryption process, the State array is modified at each round by a round function those defines four different byte-oriented transformations.

a) SubBytes transformation: a non-linear substitution step where each byte is replaced with another byte according to a substitution table (S-box). The S-box is invertible and has two operations.

- Inversion in the GF (2^8) field, modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.
- Affine transformation defined as $Y = AX^{-1} + B$, where A is an 8×8 fixed matrix and B is an 8×1Vector.

b) ShiftRows transformation: A transposition step where each row of the state is shifted cyclically a certain number of steps. This transformation can be defined as follows: $S'_{r,c} = S_{r,((c+shift(r,4))mod\ 4)}$ where shift value shift(r,4) depends on the row number are as follows: shift (1,4) = 1; shift(2,4) = 2; shift(3,4) = 3;

c) MixColumns: A mixing operation that operates on the columns of the state, combining the four bytes in each column. The transformation can be written as the following matrix multiplication formula.

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad for\ 0 \le c < 4$$

d) AddRoundKey: a simple bit-wise XOR operation is performed between each byte of the state and the round key which is generated from the cipher key using the Rijndael key schedule algorithm. The operation is described through the expression:

$$\begin{bmatrix} S'_{0,c} S'_{1,c} S'_{2,c} S'_{3,c} \end{bmatrix} = \begin{bmatrix} S_{0,c} & S_{1,c} & S_{2,c} & S_{3,c} \end{bmatrix} \oplus \begin{bmatrix} W_{round*r+c} \end{bmatrix} \quad for\ 0 \le c < 4.$$

2.2. Encryption and Decryption Process

The encryption and decryption process is composed of several rounds depending on the size of the cipher key where each round performs some specific functions. In this paper, we have considered the encryption and decryption process for a 128 bit cipher key that requires 10 different rounds to complete the process. Fig. 2 depicts the steps involved in the AES-128 algorithm.

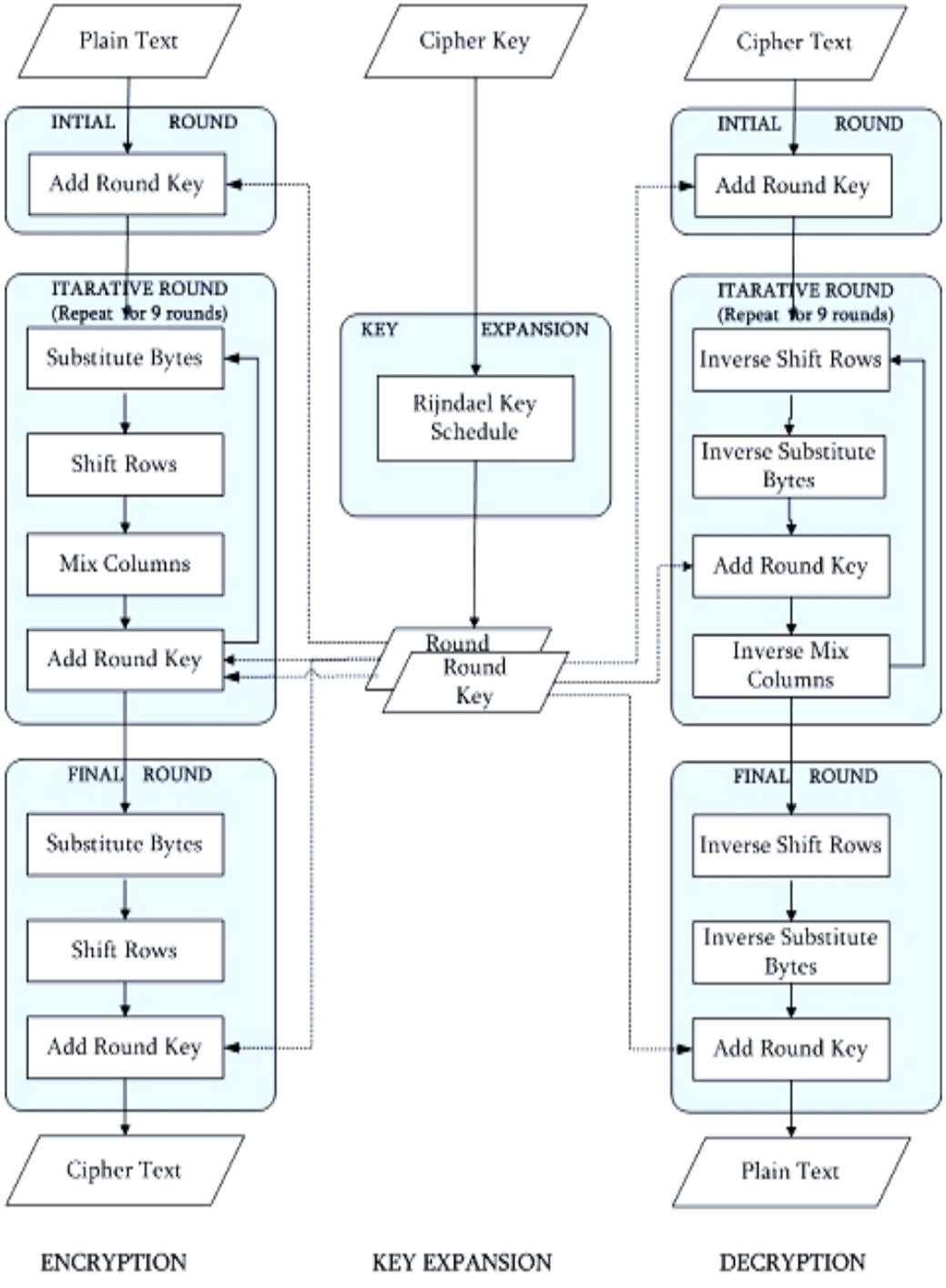

Fig. 2 AES-128 algorithm encryption and decryption.

Both encryption and decryption process begins with the initial round i.e. round 0 performs only the AddRoundKey transformation on the state array and provides the security as this is the only stage that makes use of the secret key. Nine identical rounds are followed by the initial round where each round includes SubBytes, Shiftrows, MixColumns, and AddRoundKey transformations respectively on the state array. The final round is three functions other than MixColumns transformation which is slightly different compared to the other rounds.

2.3. Simulation Model

OFDM-based WiMAX communication system simulation model with Least Mean Square (LMS) equalizer was

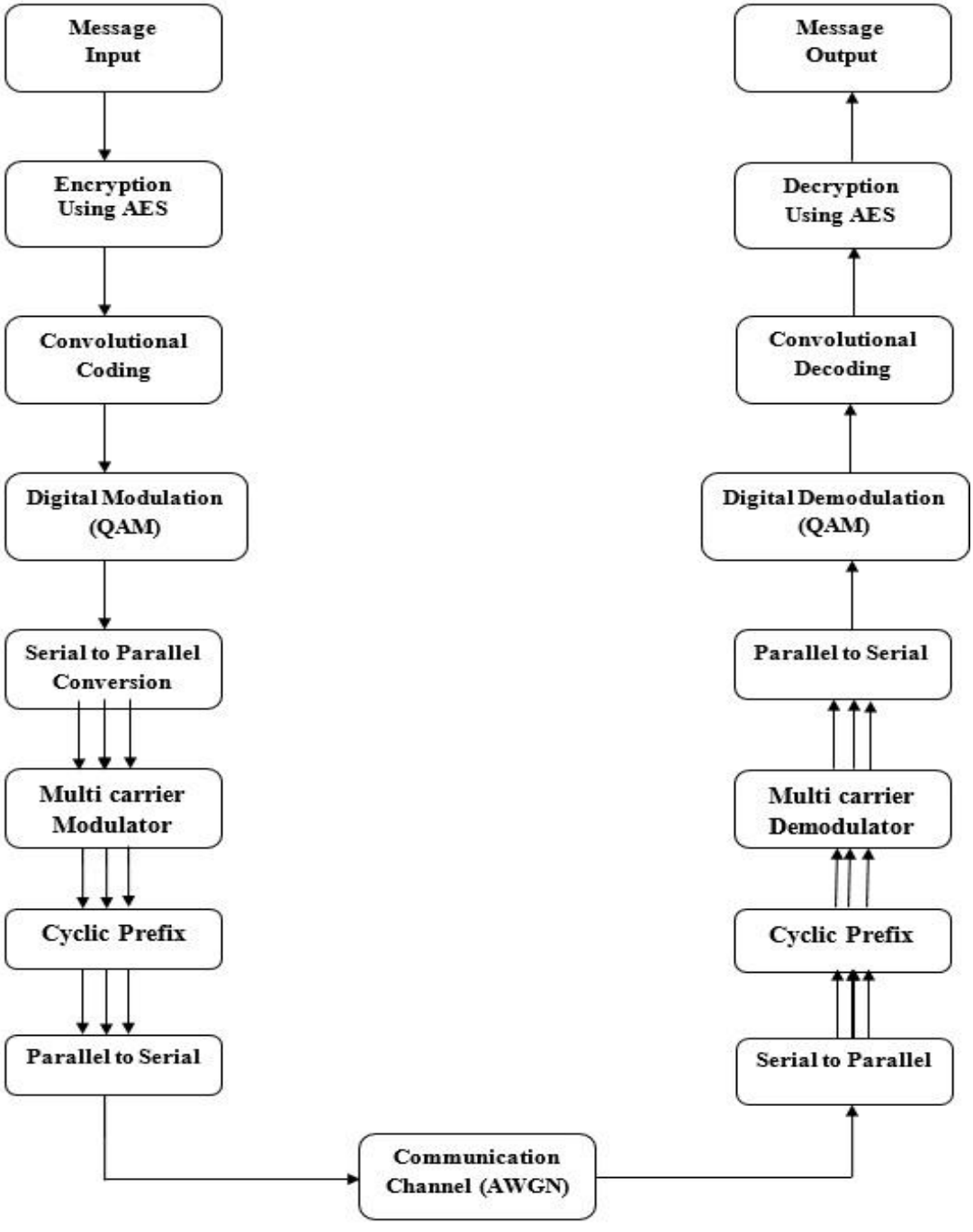

Fig. 3 A block diagram of an OFDM wireless communication system with Convolution Coding (CC).

implemented. It is ought to be mentioned here that the real communication systems are very much complicated and due to the non-availability of the algorithms to simulate the performance evaluation of their various sections, generally, simulations are made based on some assumptions to simplify the communication system(s) concerned. Figure 3 shows a simulation model for OFDM system with Least Mean Square (LMS) equalizer. It consists of various sections. A brief description of the simulated model is given below (Nasreldin et al., 2008).

2.3.1. Message Input

This indicates the place from where the original message or, data is to be conveyed. A data source is a notepad object.

2.3.2. Data Encryption
Input messages are encrypted using the AES encryption algorithm, which is discussed, in the previous section.

2.3.3. Convolution Coding
In this case, the encoder output is not in block form but is in the form of an encoded sequence generated from an input information sequence. The encoded output sequence is generated from present and previous message input elements, in a continuous encoding process that creates redundancy relationships in the encoded sequence of elements.

2.3.4. Digital Modulation
The digital modulations used in the present study is Quadrature amplitude modulation (QAM) In the case of QAM (quadrature amplitude modulation), a finite number of at least two phases, and at least two amplitudes are used. QAM is both an analog and a digital modulation scheme.

2.3.5. Serial to Parallel / Parallel to Serial Conversion
A combination of serial and parallel processing is involved in this step, for example, binary decimal coded (BDC) numbers are regularly processed as 4 bits in parallel, and successive 4-bit units are processed serially.

Table 1 Summary of model parameters

Parameters	Values
Length of the message	128 bytes
Number Of Subscribers	200
FFT Size	256
CP	1/4
Coding	Convolution Coding (CC)
Code rate	2/3
Constraint length	7
K-factor	3
Maximum Doppler shift	100/40Hz
SNR	0-20
Modulation	QAM, 16-QAM, 64-QAM
Noise Channels	AWGN
Encryption Algorithm	AES
Block size	128 bits
Key size	128 bits
Number of rounds	10
Round key size	4 words
Expanded key size	44 words

2.3.6. Multi Carrier Modulator
Multi-carrier modulation is the generic term used for any orthogonal pulse amplitude modulation (OPAM) where the orthogonal pulses are roughly localized in the frequency domain.

2.3.7. Cyclic Prefix
To combat the effect of multipath a cyclic prefix is added. Four different duration of the cyclic prefix is available in the standard. Being G the ratio of CP time to OFDM symbol time, this ratio can be equal to 1/32, 1/6, 1/8, and 1/4.

2.3.8. Additive White Gaussian Noise (AWGN) Communication Channel
A reasonable assumption for a fixed, LOS wireless channel is the additive white Gaussian noise (AWGN) channel (Proakis J. G. 1995)**,** which is flat and not "frequency-selective" as in the case of the fading channel. Particularly fast, deep frequency-selective fading as often observed in mobile communications is not considered in this paper, since the transmitter and receiver are both fixed. This type of channel delays the signal and corrupts it with AWGN.

2.4. Model Parameters
Simulation parameters used in the Matlab codes are shown below in Table 1.

3. RESULTS AND DISCUSSION

First, we will present the structure of the implemented simulator and then we will present the simulation results both in terms of validation of implementation and values for various parameters that characterize the performance of the WiMAX security.

3.1. Description of Simulation Tool
Matlab 7.5 has been used to write a computer program designed for the simulation study. The developed program provides different replaintext by decrypting different ciphertext for different values of signal to noise ratio.

3.2. Simulation Results
The plain text message is shown in figure 4 which is encrypted using a shared secret key. The secret key must be shared before transmitting the messages. The ciphertext produces by the shared secret key is shown in figure 5.

This is a specimen text to be encrypted with WiMAX AES encryption algorithm.

Fig. 4 Plaintext Message

Ù¾+bË[ð#BîF¢y´ËïcÁòævßcÒådåL¤ßÀÝW • tE¶ï9F
{¦äÍûÂÊ3í¸Çl6u;/r[â¢+Hl¦tJYÿ°G-öäA_VÑyOõL^ûfRp)
HMNÜ_Ú²#□nº

Fig. 5 Encrypted plaintext with a shared secret key.

Then encrypted messages are transmitted in a WiMAX system. To modulate the encrypted message modulation order16 and 64 are used. The channel used in this simulation is AWGN channel. In the receiver end for various values of signal to noise ratio various ciphertext is found. These ciphertexts are then decrypted using the shared secret key. For modulation order 16 and 0,4,7,10 values of signal to

noise ratio the replaintext messages are shown in figure 6., 7, 8, 9 respectively.

H$Ë¬ÞûvDÏÑfD´*§E»ïd°¨ßrÕJÂKÙèöâýËÆÚ¬ü)AÈ¨p Û0Ö¯\EÅ • Ëã³¥û§qÅÏnei8h[´t§ÇcÔ>ZÀxÄ/vjõeæxù{¿ /3ZúC üz YÚ

Fig. 6 Replaintext decrypted by shared secret key for SNR=0.

H$Ë¬ÞûvDÏÑfD´*§E»ïd°¨ßrÕJÂKÙèöâýËÆÚ¬ü)AÈ¨p Û0Ö¯\EÅ • Ëã³¥û§qÅÏnei8h[´t§ÇcÔ>ZÀxÄ/vjõeæxù{¿ /3ZúC üz YÚ

Fig. 7 Replaintext decrypted by shared secret key for SNR=4.

ÛÈµA|µSÅ¨=Ðªä(• ûV1´ù`-W-@éáíj1¾Ðõ • ç÷¬~ \èpR§Ik_o9Õ:Sgné¢Mªìæì#%+ßE&dí+Pá#Õû48¨këÅÿ Æ¢*_I« .¸À¯Á0=nS¦@çæîBÙ

Fig. 8 Replaintext decrypted by shared secret key for SNR=7.

This is a specimen text to be encrypted with WiMAX AES encryption algorithm.

Fig. 9 Replaintext decrypted by shared secret key for SNR=10

kOÅÂÕÖ+uÙ7 • ¥ùüx$EJ(r(µi÷Ô?xR¸{Ãó.Q-?□/!Ç{_ Bõ»Í!Æë2±\ÙQÕú`]M • âæâ-g¹îRxo¬w7ý[Æ-Yó¤NÉ¦! KKãüÖH.±5õ`nÆúñ

Fig. 10 Replaintext decrypted by shared secret key for SNR=0.

• Í8êVH«tµv.æaùÔ.,= • c>ñVzÁÆAÔµFGÛïøÄed°ü\øï 6Àã¤ý6&AGòÌdTné • Ö>WÊèì[B-êÂ¦^~§f • D@ 5¿ØKìÐ÷´±-¬V

Fig. 11 Replaintext decrypted by shared secret key for SNR=4.

• ç²1ã½ú¤ Þ²È°@Í6n0Ñ¤XÄã¨u63Þö-6M??<,{7*é °^ò\| mî$Ñ1QMO*xîÒë-«MnúAÊJSÎl_ÿÓznàDÓqÖÄGGÎ& »îá2_}ØJÜYrÉ÷o¡øöuI

Fig. 12 Replaintext decrypted by shared secret key for SNR=7.

ë_½fÂç~úÏ84oD`'ËÇo'DÒüÛÕdÌ.ªûd·å£gÐÛÞÌ YI«äuÇ D¸çÛçå3ä±øV7T³ÃVÒMyÿoíû`üPùÙÖ¸UG:©ýÂÔÿW O6/Ç!¤íäüDÝæÌuFéL • WP#:s{¸øÙDñfÔ2Ú'%¿F¡°sèxí

Fig. 13 Replaintext decrypted by shared secret key for SNR=10.

For modulation order 64 and 0, 4, 7, 10 values of signal to noise ratio the replaintext messages are shown in figure 10, 11, 12, 13 respectively.

With the encryption and decryption process achieved in the above section, we would like to discuss some similar findings from researches carried out in recent years. The prior deployment of Wi-Fi gave us a better understanding of the shortcomings for a high bandwidth wireless network. Now as the threats are known and understood they have been addressed prior to WiMAX's deployment. AES is one of those few counter measures being applied (Sanjay & Collier, 2010). In another paper, WiMAX security measures were highlighted in terms of privacy across wireless network and access control. It was found that by encrypting connections between the subscriber station and the base station better privacy could be achieved (Luo, 2009). In another research of security threats, MAC Layer of WiMAX was analyzed. PKM (Privacy and Key management) protocol was implemented to achieve authorization and traffic keying between the Base Station to Subscriber Station (Shahzadi & Shahzad, 2009). Therefore, from the above discussion it is observed that WiMAX though still need a lot of improvement could be implemented for a secure wireless data transmission.

4. CONCLUSION

If we want to achieve End-to-end secure communication then security has to be kept in mind. WiMAX is designed with many security mechanisms to make it secure from threats, but still not so secure from threats. We can countermeasure these attacks by using wireless protocols and strong encryption techniques.

In this paper, we encrypt the message with the shared secret key using the advanced encryption standard algorithm (AES) encryption algorithm. Then the ciphertext is transmitted in the WiMAX communication system, which uses the AWGN channel as the communication channel. In the receiver, the received ciphertext is decrypted by the shared secret key. In this process shared secret key of the communicants provide security.

REFERENCES

Andrews, J. G., Ghosh, A. & Muhamed, R. (2007). *Fundamentals of WIMAX, Understanding Broadband Wireless Networking*. Prentice-Hall, Westford, Massachusetts, USA.

Bakkoury, J., Azeddine, K., Bahnasse, A. & Khaili, E. (2016). Study and evaluation of vertical and horizontal

handover's scalability using OPNET modeler. *International Journal of Computer Science and Information Security*, 14, 7-14.

Daemen, J. & Rijmen, V. (2020). Specification of Rijndael. *In*: The Design of Rijndael. Information Security and Cryptography, Daemen J & Rijmen V (Eds.), Springer, Berlin, pp. 31-51.

Ergen, M. (2009). *Mobile Broadband - Including WiMAX and LTE*, Springer, New York, USA.

Habib, M., Mehmood, T. & Ibrahim, F. U. M. (2009). Performance of WiMAX security algorithm (the comparative study of RSA encryption algorithm with ECC encryption algorithm). *International Conference on Computer Technology and Development*, (13-15 Nov., Kota Kinabalu). P. 108-112.

Hasib, A. A. & Haque, A. A. M. M. (2008). A comparative study of the performance and security issues of AES and RSA cryptography. *Third International Conference on Convergence and Hybrid Information Technology*, (11-13 Nov., Busan). P. 505-510.

Luo, C. (2009). A simple encryption scheme based on WiMAX. *International Conference on e-business and Information System Security*, (23-24 May, Wuhan). P. 1-4.

Nasreldin, M., Aslan, H., El-Hennawy, M. & El-Hennawy, A. (2008). WiMAX security. *22nd International Conference on Advanced Information Networking and Applications-Workshops*, (25-28 March, Okinawa). P. 1335-1340.

Pigatto, D. F., Da Silva, N. B. F., Lucas, K. R. & Branco, J. C. (2011). Performance evaluation and comparison of algorithms for elliptic curve cryptography with el-gamal based on miracl and relic libraries. *Journal of Applied Computing Research,* 1(2), 95-103.

Proakis, J. G. (1995). *Digital Communications*, McGraw-Hill Inc., New York, USA.

Sanjay, P. A. & Collier, N. (2010). An assessment of WiMAX security. *Communications and Network*, 2, 134-137.

Shahzadi, R. & Shahzad, A. (2009). AES based security architecture of WiMAX using OMNET++. *International Journal of Video & Image Processing and Network Security*, 9(10), 1-4.