International Journal of Engineering & Technology, 7 (4) (2018) 2558-2564

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.14993
Research paper

Design and analysis of physical layer security aspects in MIMO-OFDM based WiMAX network

Budhaditya Bhattacharyya [1] *, Ipsita Deb [1], Nalini Sharma [1]

[1] Department of Electronics and Communication Engineering, VIT Vellore, Vellore, Tamil Nadu, India
**Corresponding author E-mail: budhaditya@vit.ac.in*

Abstract

The protocol 802.16 of the IEEE proposed a technology of wireless broadband called WiMAX which overcomes the limitations of other wireless technologies that came prior to WiMAX. WiMAX has acquired significant attention owing to its mobility support, longer transmission range and higher transmission rate. In order to ensure usability and reliability, a number of security concerns are required to be addressed in WiMAX. The first part of this work is to analyze the performance of a MIMO-OFDM based WiMAX under Rayleigh fading channel using SIMULINK environment under diverse encoding algorithms and adaptive modulation schemes in terms of throughput and bit-error-rates. The second objective being its performance analysis using various standard cryptographic algorithms such as Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES), which enhances the security and efficiency of a WiMAX networks.

Keywords: *AES; DES; MIMO Alamouti; OFDM; RSA; STBC.*

1. Introduction

WiMAX is a long range wireless broadband access that can deliver large amount of information economically and is primarily intended to provide coverage to areas of difficult access, whereby a wiring may be difficult. It also provides consumers uninterrupted access to a wide variety of applications such as online games, digital music, television, video and other real-time services. WiMAX is based on OFDM (Orthogonal Frequency Division Multiplexing), may cover an area of 50 km allowing connection with obstacles interposed, and has a capacity to transmit data up to 75 Mbps with a spectral efficiency of 5.0 bps / Hz. Today the two major types of WiMAX (fixed WiMAX and mobile WiMAX) use sector antennas or adaptive antennas with modulations that allow exchange bandwidth range, known as smart antennas [1].
Network security has become a crucial problem in recent years. In real-life applications, everyday a huge amount of security related data is accessed. When data is transferred from the transmitter to the receiver over the communication link, there is a possibility of eavesdropping by an intruder and thus it is viewed as a continuous risk to the confidentiality or secrecy of the information. The technique that safeguards the confidentiality of the information is cryptography. Encryption and decryption are the most commonly used terms associated with the cryptographic process. The procedure for encoding the plaintext into a cipher text is defined as Encryption and the reverse process of decoding the cipher text to a plaintext is termed as Decryption. The Cryptographic process uses an algorithm along with a secret value which is also termed as key. The key can be the same for encryption as well as the decryption process. It can also be different based on the type of encryption algorithm used. Cryptography techniques are divided into two different categories depending upon the type of key used - Symmetric (secret) and Asymmetric (public) key encryption which has been broadly discussed in this paper.

The main objective of the paper is the analysis of the performance of WiMAX layers under different modulation schemes and encoding techniques. Multiple transmitters and receivers are used at both the ends of the communication link and the results are analyzed accordingly. The MIMO-OFDM technology is generally considered to be the most effective technique to enhance system throughput and spectral efficiency. This paper also presents a detailed analysis of the two categories of cryptography algorithms and their comparison on the basis of several parameters. In order to secure the information, it is mandatory to determine which algorithm performs better in comparison to the other algorithms.

2. WiMAX layers

A system whose architecture uses IEEE 802.16 protocol is mainly composed of a base BS (Base Station) station and one or more subscriber stations SS (Subscriber Stations), which communicate through a protocol and data structures serving as a reference communication between the 802.16 MAC (Media access control) layer and PHY 802.16 OFDM (physical layer of the OSI model). The WiMAX standard uses the OFDM (Division Multiple Orthogonal Frequency) technology that provides advantages such as efficient use of the radio frequency spectrum and advanced antenna support, which results in superior performance. Reed-Solomon codes and Convolutional Coding techniques are incorporated in the model design. The data propagates through the WiMAX transmitter, enters the AWGN channel and the multipath fading channels (such as Rayleigh and Rician) followed by the WiMAX receiver section where the data is decoded [2]. The concept of MIMO-Alamouti is illustrated in the design. The fundamental idea behind MIMO is that the transmitted signals and the received signals are merged in such a way that the data rate (bits/sec) of the system will be improved for each MIMO user. MAC layer is a sub-layer in the Data Link Layer of the OSI model. The WiMAX-

MAC layer has also been carefully designed and duly optimized to facilitate point to multi-point wireless communication. It also provides an interface between the physical layer of the OSI and the other higher application layers.

2.1. WiMAX model

The input data obtained from the source is initially randomized, then coded and further mapped onto QAM symbols. This physical layer makes use of orthogonal frequency division multiplexing (OFDM) that involves 256 subcarriers. There are 192 data subcarriers, 8 pilot subcarriers, 1 zero DC subcarrier, along with 55 guard carriers in each OFDM symbol. Zero padding is carried out after the assembling process gets over. Channel coding comprises of three processes which take place in the Transmitter section of WiMAX physical layer in the following order: randomization, forward error correction and interleaving. The randomization of data is supposed to be performed independently on every burst of both uplink and downlink data [3]. The Forward Error Correction comprises of the concatenation of a rate-compatible convolutional inner code and a Reed-Solomon outer code which shall be sustained on both uplink and downlink. The Reed-Solomon error rectification functions by appending few redundant bits to the required sequence of digital data. This can be accomplished by oversampling a polynomial which is constructed from un-coded data. By sampling the said polynomial more frequently than required, the receiver can get back the initial data. The Reed-Solomon encoding is generated from a methodical (N = 255, K = 239, T = 8) code by means of Galois Field(2^8), where N stands for the number of total bytes obtained after encoding, K stands for the overall number of bytes before encoding and T gives the numerical value of data bytes which can be rectified. Puncturing patterns can be utilized to incorporate several code rates. Interleaving is meant for securing the transmission from extended arrangements of consecutive errors, which are quite tricky to rectify. After bit interleaving is successfully carried out, the data enter serially into the constellation mapper [4]. Upon application of inverse Fourier transform to the data, an OFDM waveform is created. The receiver performs the reverse function as the transmitter. Channel estimation turns out to be a major factor in revealing the unknown channel coefficients. The cyclic prefix is detached. The received signal is then converted into the frequency domain by the application of FFT algorithm. The guard bands are detached initially, then disassembling is carried out in order to obtain pilots, data and trainings. Trainings are utilized in the channel estimator which determines channel coefficients and these estimated coefficients can then be utilized in the de-mapper to carry out data equalization and to reimburse frequency-selective fading of the requisite multipath propagation channel. Once the de-mapping is done, the data goes into the decoder in order to get back the original transmitted signal. Fig. 1 illustrates the model diagram for WiMAX transmitter and receiver.

2.2. Space-time block codes

Space-time block codes (STBC) [5] are recognized to be the more generalized version of the Alamouti scheme [6], but are known to have similar features. STBC codes are known to be orthogonal in nature. They can also attain full transmit diversity identified by the number of antennas which are used for transmission. The encoding-decoding scheme in the STBC is same as the scheme used in the Alamouti space-time code on the transmitter and receiver side. The data is designed accordingly in a matrix in which the number of columns are equal to the number of the transmit antennas and the rows are equal to the number of the time slots which are necessary for data transmission. The signals received are initially combined at the receiver end and then decision rules are applied in the maximum likelihood detector [7].

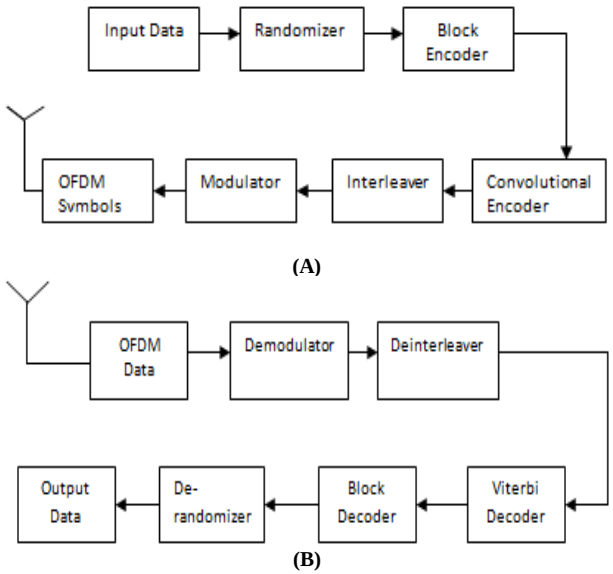

Fig. 1: System Model: (A) Wimax Transmitter and (B) Wimax Receiver.

2.3. MIMO in wireless networks

MIMO, which stands for Multiple-Input-Multiple-Output, describes a link in which multiple antennas are fitted in the transmitting and the receiving end of an arbitrary wireless communication system. The basic idea underlying MIMO is that the signals which are propagated through the transmitting antennas and the signals received at the receiving antennas are merged in such a way that the data rate (bits/sec) of the communication link or the bit-error rate (BER) will be enhanced for each MIMO user [8]. This proves to be quite advantageous in enhancing the quality of service of the network apart from influencing operator's revenues [9]. The model design of multiple transceivers is complex in Simulink and the design becomes even more unrealistic when it comes to hardware implementation.

2.4. Security in WiMAX

Security is essential in data networks more specifically in wireless networks. In wireless communication, jamming and scrambling are considered to be the potential physical layer threats. Jamming can be accomplished by introducing a noise strong enough to considerably reduce the channel capacity of WiMAX. Jamming can be reduced either by increasing the power of the signals or by increasing the bandwidth of the signals and this can be accomplished via spreading techniques such as direct sequence spread spectrum or frequency hopping. Other options include introducing a more powerful WiMAX transmitter, a high gain WiMAX transmission antenna, or a high gain WiMAX receiving antenna. Scrambling is typically activated for short duration and is targeted to specific frames of WiMAX or certain parts of the frames and is relatively more difficult to detect [10]. There are quite a large number of threats associated with MAC layer also. Hence, strong security mechanisms are required to shield the WiMAX from vulnerabilities and threats. Keeping in mind the threats and vulnerabilities to the WiMAX layers that arise during authorization and authentication, this paper presents some enhanced techniques for the security and performance. These algorithms will be more reliable and secure and will also save space and time. A number of security techniques can be implemented in the network layer of the OSI model. Security is usually handled at several layers inside a system. Each layer deals with diverse aspects of security, although in certain cases, there may be some redundant mechanisms. This paper focuses on the implementation of certain encryption algorithms on the WiMAX layers to prevent over-the-air eavesdropping. The ciphered data propagates through the WiMAX lay-

ers and is finally decoded at the receiver end of the WiMAX model. This ensures the confidentiality of the information transmitted.

3. Classification of cryptography algorithms

The type of encryption methodology where the sender and receiver use the same secret key for encryption as well as the decryption process is defined as Symmetric key encryption. It is called symmetric because a single key is used for both encryption and decryption. It is also known as private or secret key algorithm. The symmetric key is of two types: stream cipher encryption and block cipher encryption. Some notable examples of symmetric cryptography algorithms are DES, 3DES, AES, Blowfish, RC6 and CAST-128 [11].

The encryption method in which two different keys (private and public keys) are used in the encryption and the decryption process is defined as asymmetric key encryption. The keys used in the encryption and decryption process are different but are complementary in function. Data that is being encrypted with the help of public key can only be decrypted with the synonymous private key of the set where both the keys are interrelated mathematically. Public key, as the name indicates, is known to everyone while the information about the private key is only known to the receiver of the data or message. Some examples of asymmetric cryptography are RSA, SSH and SSL [11].

4. Rivest-shamir-adleman (RSA)

RSA (Rivest, Shamir and Adleman) is a public-key cryptographic algorithm. The RSA algorithm comprises of three steps: generation of key, encryption and decryption of data. Key generation in RSA involves a private key and a public key. The public key is used for encrypting the messages and is known to everyone. Messages which are encrypted with public key are decrypted with private key [12].

The algorithm for key generation in RSA can be explained in the following manner:

- Two distinct prime numbers a and b are chosen. For the purpose of security, two integers a and b are chosen at random, and their bit-length should be the same. Using primality test, efficient prime numbers are used.
- Compute N= ab where N is used as the modulus for both private and public keys.
- Compute $\varphi(N) = (a-1)(b-1)$, where φ is Euler's totient function.
- Choose an integer f such that $1 < f < \varphi(n)$ and $\gcd(f,\varphi(n)) = 1$, i.e. f and $\varphi(n)$ are co-prime. f is described as the public key exponent. Since f has small hamming weight and short bit-length, it results in more efficient encryption - generally 65537. However, small values of f (such as 3) have been shown to be less secure.
- Determine $d = f^{-1} \bmod \varphi(N)$ where d is the multiplicative inverse of f mod $\varphi(N)$. This is computed using the extended Euclidean algorithm. d is the private key exponent. The public key consists of the modulus N and the public exponent f. The private key consists of the decryption (or private) exponent d which is kept secret.
- Let us take an example. Priya transmits her public key (n,e) to Ajay and keeps the private key secret. Let us take an example of Rohit then wishes to send message M to Naina. He turns M into an integer such that m is between o and n by using padding scheme. Then he calculates the cipher text denoted by C corresponding to $C = m^e \pmod n$. Decryption can recover m from C by using her private key exponent d via computing $m = c^d \pmod n$.

5. Data encryption standard (DES)

Data Encryption Standard is considered to be the first encryption algorithm published by the National Institute of Standards and Technology. IBM designed DES on the basis of their Lucifer cipher and it turned out to be a standard in 1977. It is an extensively used methodology for symmetric data encryption which makes of a single private key for both encryption and decryption. DES algorithm is based on the Feistel function which includes 4 stages which are expansion, key-mixing, substitution and finally permutation. The function splits the blocks into two equal halves and then applies 16 rounds of processing to encode the data. A 56-bit key is applied to each block of data consisting of 64-bit. Security is a major issue in DES owing to its small key size. The size of the private key in DES is actually 64-bit although the key-size used is only 56 bits as the 8 bits used as parity bits are used for error correction. This process maps a 64-bit input block into an output block of size 64-bit [13]. The algorithm functions according to the given steps:

- DES, as has been already mentioned, accepts a 64-bit long plaintext and a 56-bit key along with 8 bits of parity as inputs and produces a 64-bit block size output e plaintext block has to shift the bits around.
- The plaintext block has to shift the bits around.
- The parity bits should be removed from the private key by subjecting the key to key-permutation.
- The plaintext and key are processed according to the following steps:

i) The 56-bit key is divided into two equal halves.
ii) Each half is shifted or rotated by one or two bits depending on the round.
iii) The halves are then recombined and subjected to compression permutation which reduces the key size from 56 to 48 bits. The compressed keys are then used to encrypt the plaintext block of that particular round.
iv) The rotated or shifted key halves from step b are then used in the next round.
v) The 64-bit data block is split into two equal halves.
vi) One half of the data block is subjected to expansion permutation to increment its size from 32 to 48 bits.
vii) Output of the previous step vi is exclusive-OR'ed with the 48-bit compressed key from step iii.
viii) Output of step vii is then provided to an S-box, which substitutes the bits of the key and reduces the 48-bit block back to 32-bits.
ix) Output of step viii is subjected to a P-box to permute its bits.

The output from the above mentioned P-box is exclusive-OR'ed with other half of data block. The two data halves are then swapped and this becomes the input for the next round.

6. Advanced encryption standard (AES)

Advanced Encryption Standard (AES) is used in data security. There are different types of cryptography algorithms, but AES is considered one of the best security algorithms. The implementation is done in various hardware devices and software languages. A MATLAB code is developed for cipher text decryption and plaintext encryption.

AES is based on the block cipher Rijndael and it turned out to be the designated successor of Data Encryption Standard (DES) algorithm. It works on the group of bits which are of fixed length, known as Blocks. The input block size is taken of 128 bits and the output is generated of the same size .The second input taken is secret key. AES uses three different types of key sizes: 128, 192 and 256 bits.

The AES algorithm uses a round function which is composed of four different byte-oriented layers for cipher and inverse cipher [14].

- Byte substitution is done using a substitution table (Sbox).
- Rows of the state array are shifted by different offset.

- Data is mixed within each column of State array.
- Round key is added to the state. The algorithm uses round function for 10 times. During the execution of the algorithm, the number of rounds is dependent on the key sizes. Nr is the representation of the number of rounds, where Nr=10 for 128bits, Nr= 14 for 256 bits and Nr= 12 for 192 bits.

The pseudo-code for AES algorithm is given below:
Input: Byte A1 [4 × N_b], Word k [N_b × (Nr + 1)];
Output: Byte c [4 × N_b];
Byte state [4, N_b];
State: = A1;
AddRoundKey (state, k [0, N_b − 1];
For round: = 1 to Nr − 1 do SubBytes (state);
ShiftRows (state);
MixColumns (state);
AddRoundKey (state, k [round×N_b, N_b (round+1))
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, k [Nr × N_b, N_b (Nr + 1) − 1]);
C: = state; return c;
End
The pseudo-code given above describes four distinct operations that take place during the process of encryption in AES.

- In SubBytes, each byte in the S state is replaced with another byte, based on a look-up table known as the S-box which is obtained from the inverse function over the Galois Field and is known to possess good nonlinearity properties. Even though the S-table can be derived mathematically, most implementations merely have the substitution table for the same, stored in the memory.
- In ShiftRows, each row is cyclically shifted by a predetermined number of steps. More precisely, the elements in row 1 are kept as it is, the elements of row 2 are left- shifted by one column, the elements in row 3 are left-shifted by two columns, and the elements of the last row are left- shifted by three columns. This particular operation guarantees that every column in the output state of this specific operation is composed of bytes taken from each column of the input state.
- In MixColumns, every column is transformed linearly. It is accomplished by multiplying it with a matrix in the finite field. Specifically, each column is considered as a polynomial over Galois Field and is modulo- multiplied with a fixed polynomial. This transformation, along with the ShiftRows operation, offers diffusion in the cipher.
- In AddRoundKey, each byte in the state is exclusive OR'ed with a round key. The AES encryption involves deriving eleven round keys from cipher key which is being forwarded to the encryption engine. The round keys are specifically obtained from the cipher key, by using a simple algorithm.

7. Results and Discussion

Simulation results suggest that transmission quality decreases with the increase in the number of symbols transmitted per block. This happens due to the mapping which is performed in transmission values. The probability of error rises with increase in the number of options available for mapping. The BER performance with respect to SNR is observed for several adaptive modulation techniques using different coding rates and at different cyclic prefix which is shown in Figure 2 and Figure 3. Figure 2 infers that the performance of the system under lower modulation schemes is more satisfactory in comparison to the ones with higher orders of modulation schemes. The potential of higher order modulations can be augmented with the use of smart antennas namely beam switch, phase array and adaptive beam forming. Cyclic prefix is a crucial factor in WiMAX systems. It is known for combating the effects of multipath fading which is an advantage. Hence, large cyclic prefix is required for decreasing the effects of multipath fading. However it reduces the rates and speeds of transmission of data. As a solution to decreasing values of cyclic prefix, lower modulation schemes are preferred in comparison to higher modulation schemes. Higher value of cyclic prefix implies large time gaps between two time frames; hence it gives excess time to receivers to receive signals. Again, larger value of cyclic prefix augments coverage areas to long distances. Therefore, based on the necessities of the system, the value of cyclic prefix needs to be defined and used for OFDM symbols. Figure 3 shows that BER values for a particular cyclic prefix remain almost constant up to a particular SNR and then steadily decreases.
Figure 4 illustrates the nature of throughput at different SNR values. The graph shows that the throughput increases with increase in the value of SNR but becomes almost constant after a certain value of SNR. It is clearly seen in the figure that the use of multiple transceivers in the communication link enhances the throughput and hence the capacity, compared to a system where a single transmitter and a single receiver is used, hence MIMO has a wide variety of applications.

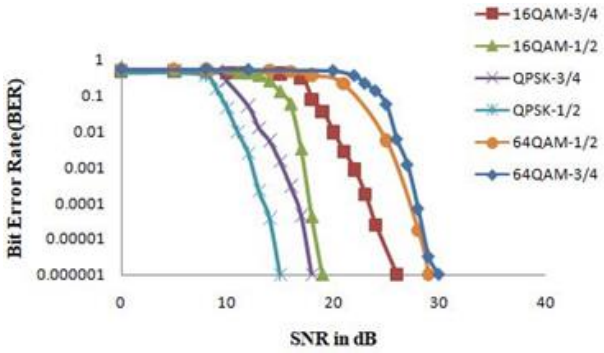

Fig. 2: Bit Error Rate Performances of Different Modulation Schemes.

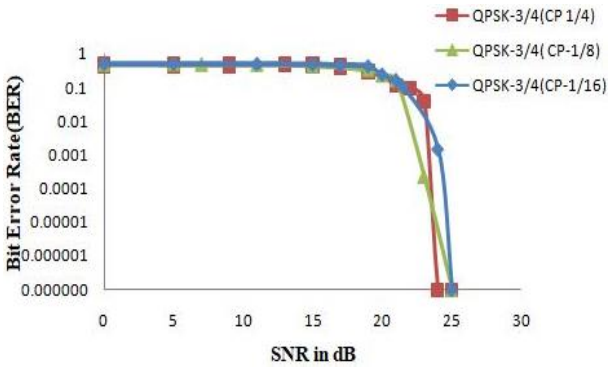

Fig. 3: Bit Error Rate Performance at Various Cyclic Prefix.

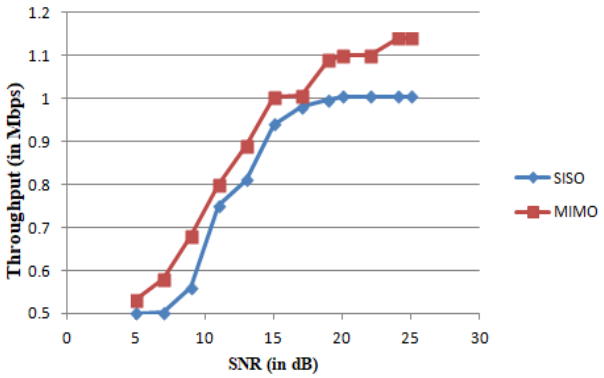

Fig. 4: Throughput Performance at Several Values of SNR.

The BER performance is also analyzed when the signal propagates through several multipath fading channels. The signals in the multipath fading channel are subjected to noise and therefore suffer from high attenuation. Hence, higher SNR values are needed, thus requiring higher power for the bits to be transmitted through a high fading channel from the base station to the receiver station. Simulation infers that Rayleigh channel shows improved perfor-

mance in terms of bit error rate in comparison to AWGN channel. Similar results are obtained when Rician channel is used with AWGN channel. The results are illustrated in Figure 5 where after a certain value of SNR, BER for AWGN channel remains almost zero for the remaining values of SNR. But Rician fading & Rayleigh fading channels have more non-zero values of BER compared to AWGN channel.

Reed-Solomon Convolutional encoder enhances the performance of OFDM systems. Figure 6 infers the nature of BER performance in the absence and presence of Reed-Solomon Encoder. The figure shows improved performance of WiMAX system in terms of BER in the presence of Reed-Solomon encoder.

Code-rate 1/2 implies that for every 2 bits transmitted, one of them is useful and the other one is redundant, so it might not be the most optimal for certain applications. Rate 3/4 implies 1 bit is redundant among every 4 bits transmitted, hence it is a better choice since it makes better use of the channel. However, BER performance is more satisfactory with code rate 1/2 than with code rate 3/4. Hence, the decision of choosing the suitable code rate depends on the application for which it is being used just like cyclic prefix. Figure 7 shows that for QPSK with code-rate 1/2 and code-rate 3/4, 1/2 shows better performance in terms of BER in comparison with code- rate 3/4.

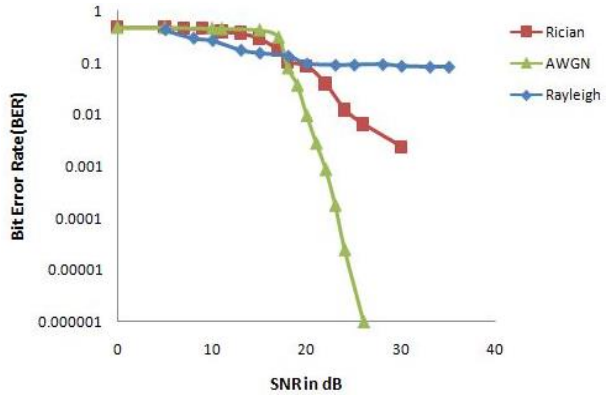

Fig. 5: BER Performances in Different Multipath Fading Channels.

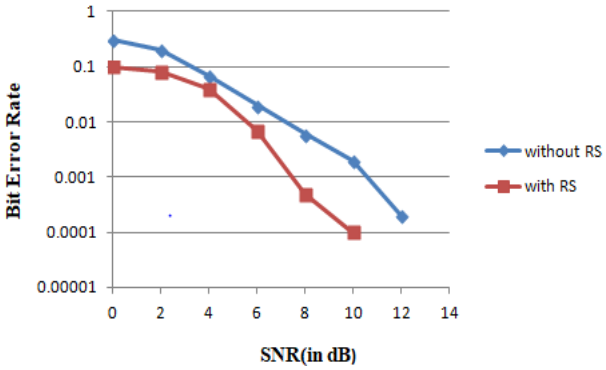

Fig. 6: BER Performances in the Presence and Absence of Reed-Solomon Encoder.

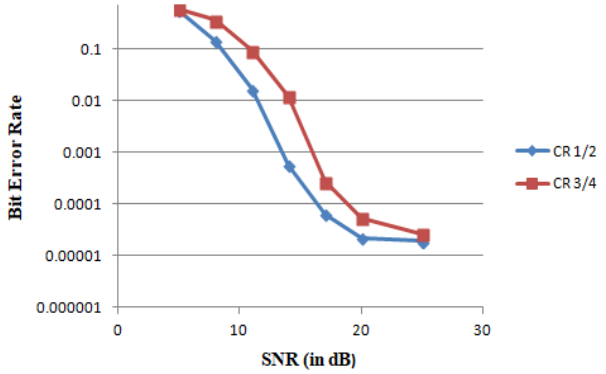

Fig. 7: BER Performances at Different Code Rates.

In order to reduce the effect of fading and hence, enhance the capacity and throughput of the system, multiple antennas are used at both the ends of the communication link. Bit Error Rate drops at lower values of SNR (as seen in Figure 8) for MIMO compared to MISO and SISO which suggests that OSTBC Encoding algorithm combined with Reed Solomon Convolutional coding effectively reduces the bit error rate in comparison to the model where RS-CC algorithm was used alone.

Figure 9 shows the encryption time taken by RSA, DES and AES in seconds for different bits. The results reveal that encryption time taken by AES is quite less in comparison to DES and AES. In the main program, tic-toc command is used at the beginning and end to measure the encryption time.

Decryption time is measured in the same way as encryption. Figure 10 illustrates the decryption time in seconds for the three encryption algorithms. From the results, we can conclude that RSA consumes the highest time for decryption while AES takes the least time. The encryption and decryption simulation is perhaps the most essential type of cryptographic analysis that can be carried out on the algorithms under study. AES and DES algorithms exhibit a very minor difference in the time consumed for encryption and decryption process.

The time taken by an algorithm to completely process a particular block of data is known as the simulation time. It depends on several factors; some of which are complexity of the algorithm, speed of the processor, etc. A small value of simulation time is desirable

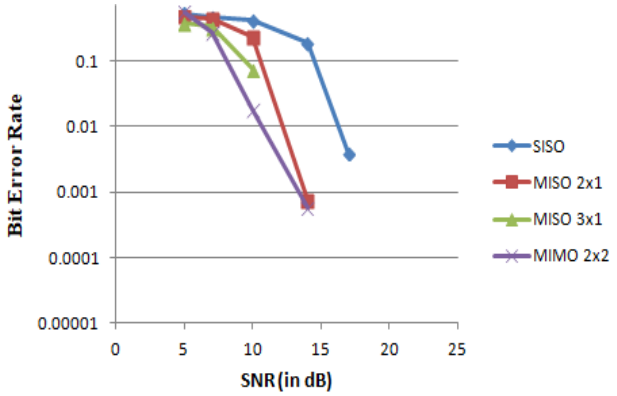

Fig. 8: Comparison of BER Performance of SISO, MISO and MIMO.

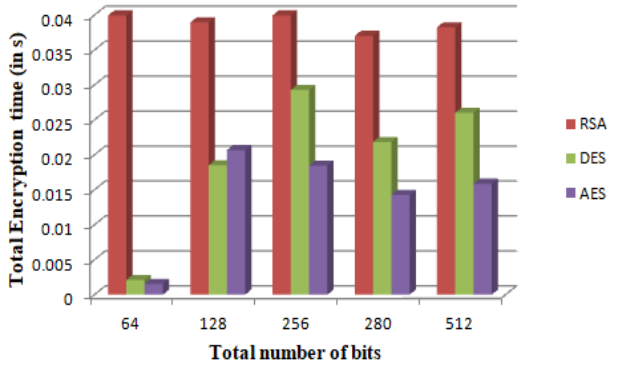

Fig. 9: Comparison of Encryption Times of RSA, DES and AES.

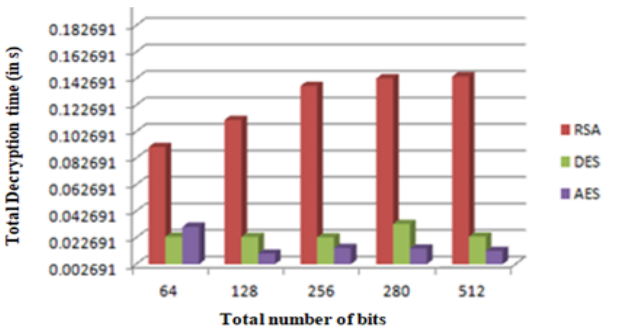

Fig. 10: Comparison of Decryption Times of RSA, DES and AES.

For any algorithm. Figure 11 shows the total simulation time in seconds taken by RSA, DES and AES. The figure reveals that RSA takes the highest simulation time while AES takes the lowest simulation time. Therefore, AES is mostly preferred for encryption of data over the communication link.

Throughput is known to vary inversely with respect to encryption and decryption time and also with respect to the power consumed by a particular algorithm. Therefore, AES has higher throughput in comparison to the other two algorithms. The throughput also explains that the encryption speed of AES is higher than DES and RSA algorithm.

It is found that each algorithm possesses its own benefits according to several parameters. It is further observed that the strong point of the each cryptographic algorithm depends upon the type of cryptography, key management, number of keys used and the total number of bits used in a key. The length of the key used for a cryptographic algorithm determines the level of security it can offer. The keys are based upon mathematical properties and it has been observed that their strength decreases with time. The keys containing higher number of bits require more time for computation which implies that the system requires more time to encode or encrypt the data. Practically it is said that asymmetric algorithms, like RSA are utilized for key exchange and symmetric algorithms like DES and AES are used for encryption and decryption.

Table 1 and Table 2 summarize the fundamental features of the three cryptographic algorithms – RSA, DES and AES. The respective block sizes, key sizes, number of rounds taken for encryption and certain other features are highlighted in the table.

It has been analysed that AES is fast, secure, effective and a better encryption algorithm among all these cryptographic algorithms with lesser storage space, higher encryption performance and without lesser limitations and weaknesses while other algorithms have certain weaknesses and differences in performance and storage space.

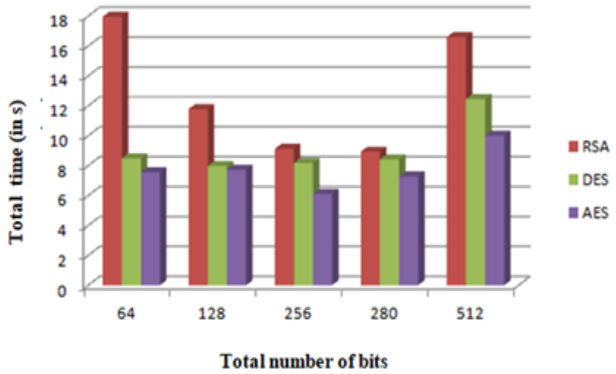

Fig. 11: Comparison of Total Time Taken for RSA, DES and AES.

Table 1: Properties of Cryptographic Algorithms

Sr. No.	Algorithm	Block Size (in bits)	Key Size (in bits	Number of rounds
1.	RSA	Any byte length	1024-4096	1
2.	DES	64	56	16
3.	AES	128, 192, 256	256	10, 12, 14

Table 2: Features of Cryptographic Algorithms

Algorithm	Features
RSA	i) Simple and fast encryption. ii) Easier to implement and understand. iii) Slower than other encryption algorithms. iv) Consumes more resources.
DES	i) Ideally suited for hardware implementation. ii) Suited for voice and video. iii) Vulnerable to attacks because of small key-size. iv) Can break the key by brute force attack.
AES	i) Advantageous in terms of time consumption and throughput. ii) Key is stronger due to its long length. iii) Occupies less memory space. iv) Software implementation is difficult.

8. Conclusion

This paper illustrates the present trend in WiMAX systems which can be used for attaining relatively faster wireless access services and also outlines the technologies sustaining the WiMAX systems. The performance of the WiMAX physical layer model is studied using parameters like SNR, BER and throughput. The simulations illustrate that BER decreases with increase in the value of SNR. The throughput performance is also shown. The combination of MIMO with OFDM shows better BER performance with improved channel capacity.

Rapidly rising cybercrimes and the ever-increasing prospect of the internet becoming more and more vulnerable to attacks generate a major challenge for the security of networks. Three well-known cryptographic algorithms have been analysed in this paper to illustrate the major differences between them in terms of nature and performance. It has been concluded that AES exhibit better performance compared to DES and RSA. AES is also proven to be more secure than DES and RSA since it takes significantly more time to break by the brute force program for a known length of the key.

Acknowledgement

We would like to articulate our sincere gratitude to our guide who has always been our motivation during the course of this work. We would also like to express our sincere gratitude to the entire Electronics and Communication Department of Vellore Institute of Technology, Vellore for providing all the essential facilities during the work and encouraging us from time to time. We are immensely grateful for giving us such an amazing opportunity. And thanks to all other people who directly or indirectly supported and helped us to fulfill our task. Finally, we heartily appreciate our family members for their motivation, love and support.

References

[1] S. Bhambure, A.D. Jadhav and S.A. Shirsat, "Simulation of IEEE 802.16e physical layer", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, Vol. 7, Issue 4, (2013), e-ISSN: 2278-2834, p- ISSN: 2278-8735, pp 23-28, available online: http://www.iosrjournals.org/iosr-jece/papers/Vol7-Issue4/E0742328.pdf.

[2] T. S. Rappaport, *Wireless Communications*, Upper Saddle River, NJ: Prentice Hall, (1996), Chap. 3 & 4.

[3] H. Schulze and C. Luders, *Theory and Applications of OFDM and CDMA: Wideband Wireless Communications*, John Wiley and Sons, (2005). https://doi.org/10.1002/0470017406.

[4] L. Nuaymi, *WiMAX: Technology for Broadband Wireless Access*, John Wiley and Sons, (2007). https://doi.org/10.1002/9780470319055.

[5] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time block codes from orthogonal designs", *IEEE Trans. Information Theory*, Vol. 45, (1999), pp. 1456-1467, https://doi.org/10.1109/18.771146.

[6] S. Alamouti, "A simple transmit diversity technique for wireless communications", *IEEE Journal on Selected Areas in Communications*, Vol. 16, (1998), pp. 1451-1458, https://doi.org/10.1109/49.730453.

[7] D. Gesbert, M. Shafi, D. Shiu, P. J. Smith and A. Naguib, "From theory to practice: An overview of MIMO space-time coded wireless systems", *IEEE Journal on Selected Areas in Communications*, Vol. 21, No. 3, (2003), https://doi.org/10.1109/JSAC.2003.809458.

[8] D.W. Bliss, K.W. Forsythe and M. C. Amanda, "MIMO Wireless Communication", *Lincoln Laboratory Journal*, Vol.15, No.1, (2005).

[9] R.S. Bansode and P. Borole, "Hardware implementation of an OFDM transceiver for 802.11n systems", *International Journal of Scientific and Engineering Research*, Vol. 4, Issue 6, (2013).

[10] R.K. Jha and U. D. Dalal, "A performance comparison with modulation schemes in WiMAX physical layer security aspect", *International Journal of Computer Applications (0975 – 8887)*, Vol. 6, No.8, (2010).

[11] O. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Performance analysis of data encryption algorithms", *Proceedings of the third International Conference on Electronics Computer Technology (ICECT)*, (2011), pp. 399-403.

[12] H. Wang, Z. Song, X. Niu and Q. Ding, "Key Generation Research of RSA Public Cryptosystem and Matlab Implement", *Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)*, (2013), https://doi.org/10.1109/SNS-PCS.2013.6553849.

[13] S.M. Seth and R. Mishra, "Comparative analysis of encryption algorithms for data communication", *International Journal of Computer Science and Technology (IJCST)*, Vol. 2, Issue 2, (2011), available online: http://www.ijcst.com/vol22/2/shashi.pdf.

[14] D.L. Kumar, A.R. Reddy and S.A.K. Jilani, "Implementation of 128-bit AES algorithm in MATLAB", *International Journal of Engineering Trends and Technology (IJETT)*, Vol. 33, No. 3, (2016).