Performance Analysis of IDEA Encryption Model under Different Fading Environments

Gaurav Mahajan [1], Kavita Upadhyay[2]

Abstract— **As the technology advances day by day, there is an essential need of a secured data transmission for exchanging information from one user to the other. In Wireless Networks, various algorithms are used to encrypt/decrypt the message. An encryption scheme named International Data Encryption Algorithm (IDEA) along with baseband communication system is used. The performance of Idea encryption model is analyzed & compared on different fading environments (AWGN, Rayleigh, Rician & Nakagami fading channel).The performance parameter such as Bit error rate & throughput are determined & compared by varying signal to noise ratio from 0 db to 30 db. The modulation scheme used is BPSK.**

Index Terms—**AWGN, BER, IDEA, Nakagami, Rayleigh, Rician, SNR, Throughput.**

I. INTRODUCTION

It is important to evaluate the performance of wireless channel by considering wireless channel parameters. The performance of data transmission over wireless channels is well captured by observing their BER, which is a function of SNR at the receiver [1].

Fading or loss of signals is a very important phenomenon that related to the Wireless Communications Field. That leads us to the fading models which try to describe the fading patterns in different environments and conditions. Although no model can perfectly describe an environment, they strive to obtain as much precision as possible. The better a model can describe a fading environment, the better can it be compensated with other signals, so that, on the receiving end, the signal is error free or at least close to being error free. This would mean higher clarity of voice and higher accuracy of data transmitted over wireless medium. An important issue is in wireless application development is the selection of fading [2].

The four important and frequent model for describing the fading environments are AWGN channel model, Rayleigh fading channel (environment) model, Rician fading channel (environment) model and Nakagami fading channel (environment) model.

In wireless communication, any intruder, anywhere in the transmission path can easily extract the signal and recover the data with no privacy considerations .one way to overcome this deficiency is to encrypt the data before transmission process.so we used encryption for securing the wireless communication before transmission .

In this paper we propose an IDEA encryption model in which IDEA encryption is applied on the first block of each frame of data stream, the data stream then transmitted through four different fading environments (AWGN channel, Rayleigh fading channel, Rician fading channel & Nakagami fading channel), at the receiver end the Bit error rate (BER) and Throughput Performance is analysed, recorded and compared by varying the simulation parameter SNR from 0 to 30 db.

The rest of the paper is organised as follows. Section II introduce fading environments. The IDEA algorithm are explained in section III. Proposed Idea encryption model are presented in section IV.Experimental results are shown in section V. Finally some conclusions are drawn in section VI.

II. FADING ENVIRONMENTS (CHANNEL)

Fading Channel is known as communications channel which has to face different fading phenomenon’s, during signal transmission. In real world environment, the radio propagation effects combine together and multipath is generated by these fading channels [2].The important fading channels are as under.

A. **AWGN channel**: Additive white Gaussian noise (AWGN) channel is a universal channel model for analyzing any new scheme. In this model, the channel add a white Gaussian noise to the signal passing through it. Fading does not exist or if exists than it is of very less amount. The only distortion is introduced by the AWGN. AWGN channel is a theoretical channel used for analysis purpose only.

B. **Rayleigh fading channel**: The Rayleigh fading is primarily caused by multipath reception. Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal. Rayleigh fading is most applicable when there is no line of sight between the transmitter and receiver.

C. **Rician fading channel**: The Rician fading model is similar to the Rayleigh fading model, except that in Rician fading, a strong dominant component is present. This dominant component is a stationary (non-fading) signal and is commonly known as the LOS (Line of Sight Component).

D. **Nakagami fading channel**: It is possible to describe both Rayleigh and Rician fading channel with change in only one parameter which is generally denoted mainly as **m**. Here, as we increase or decrease the value of the

Manuscript received March, 2015.

***Gaurav Mahajan**, M.E. Scholar, Department of Electronics and Communication Engineering, I.E.S, IPS Academy, Indore, M.P., India.*
***Kavita Upadhyay,** Associate Professor, Department of Electronics and Communication Engineering I.E.S, IPS Academy, Indore, M.P., India.*

nakagami factor **m**, it changes the value of the probability distribution function towards the Rician or Rayleigh fading distribution, respectively. As we choose the value of **m**<1 than Nakagami channel acts as a Rayleigh channel. Similarly, as we increase the value of nakagami factor i.e. when it is **m**>1 (m=1.5, 2, 4, etc.) than Nakagami channel acts as a Rician channel [3].

III. IDEA Algorithm

International Data Encryption algorithm (IDEA) is a block cipher algorithm designed by Xuejia Lai and James L. Massey in 1991. As the IDEA is a symmetric key algorithm, it uses the same key for encryption and for decryption. This algorithm was patented in no of countries (U.S. and Europe), but the last patent was expired in 2012.Now IDEA is free to use for both commercial & non-commercial purpose. IDEA was used in Pretty Good Privacy (PGP) version 2.0.

The IDEA algorithm works on 64-bit plain text and cipher text block (at one time) and is controlled by a 128-bit key. For encryption, the 64-bit plain text is divided into four 16 bits sub-blocks. Each of these blocks goes through 8 rounds and one output transformation phase. In each of these eight rounds, some (arithmetic and logical) operations are performed. In the last phase, i.e. the output transformation phase, only arithmetic operations are performed [4].

First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks. The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks. The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated [5].

IV. Proposed Model

A) Transmitter and Receiver Section:

A conceptual structure for the transceiver of the proposed encryption model is shown in Figure 1. The transmitter structure for the proposed model is depicted in Figure 1 (a), where the incoming serial data stream (S in bits) is mapped into parallel data blocks, each with a common pre specified block length (β_l).The first block undergoes IDEA encryption algorithm satisfying a certain security level. All the remaining blocks are arranged systematically and enter a bitwise XOR operation with the first block (before encryption, i.e., plaintext), as can be seen from the figure 1(a).

Next, the data is mapped back into a serial format before transmission to enhance transmission reliability. The data stream is then modulated using BPSK digital modulation technique in order to be suitable for transmission.

The receiver structure, as can be seen in Figure 1 (b), completely reverses all the operations performed at the transmitter. Also, at the receiver side, only the first block is decrypted using the IDEA decryption algorithm and the decryption key, whereas all the other blocks are also bit-wise XORed with the first decrypted block (plaintext). As a result, all the data frame is transmitted securely by performing traditional encryption only on the first small amount of data (B_1 in Figure 1) within a frame or super frame.

B) Algorithm:

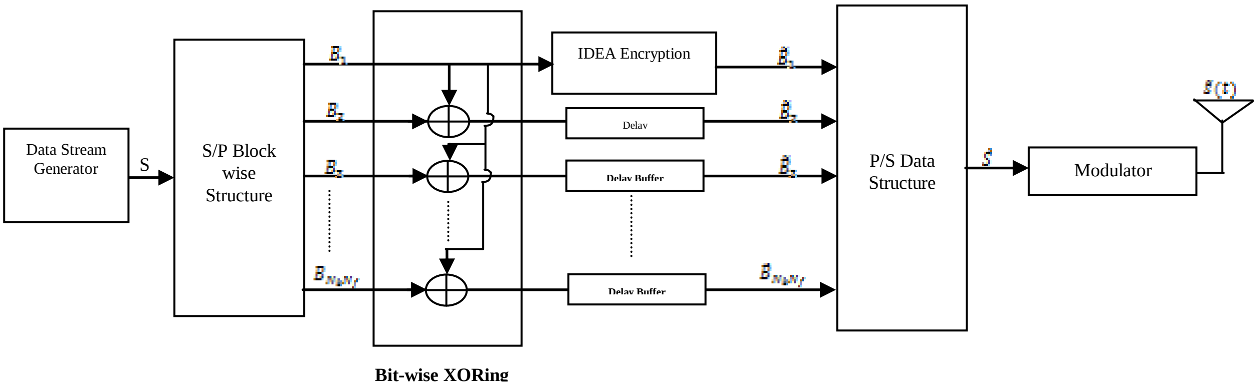
We assume that we have a data sequence composed of N super frames. Each super frame contains N_F frames, and each frame consists of N_b blocks, each of $K = \beta_l$ bits size.

Algorithm: Generating secure encrypted-coded data using the proposed encryption algorithm:

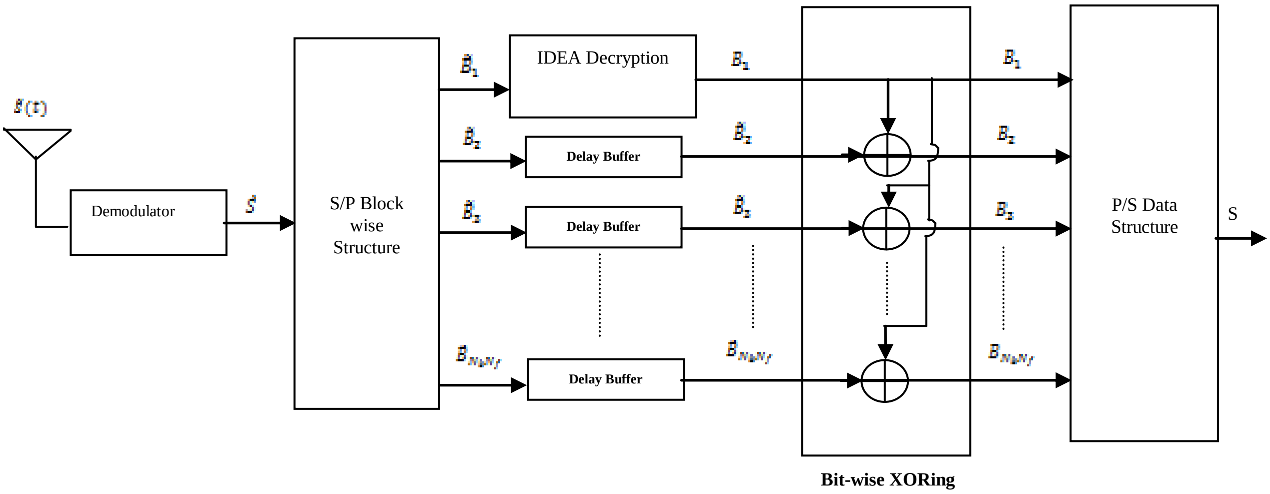
Input: Data stream as plaintext

Output: Data stream as cipher text

```
Divide the data sequence into $N$ super frames;
For each $N_i$ super frame ($SF_i$ ),$i = 1, \dots, N$, to be sent
 do
    Divide each super frame into NF frames;
    Divide the frame ($F_k$),$i = 1, \dots, N_F$, into $N_b$ blocks with block size of $K = \beta_i$;
    Encrypt the first block $B_1$ with an appropriate encryption algorithm, i.e. $\tilde{B}_1 = E_k[B_1]$
    For each of the remaining blocks $B_j, j \in \{2, N_b\}$ do
        $\tilde{b}_{i,j} = b_{i,j} \oplus b_{i,1}, i \in \{0, K-1\}$;
        Generate the coded blocks as
        $\tilde{B}_j = [\tilde{b}_{0,j}, \dots, \tilde{b}_{K-1,j}]$;
    end
    Generate the encrypted-coded frame.
 end
 Generate the encrypted-coded super frame. Repeat for other super frames;
```



(a) Transmitter



(b) Receiver

Figure 1: Transmitter and receiver section for the proposed system

Where,

$$S = [B_1, B_2, \ldots, B_{N_bN_f}] \qquad (1)$$

$$B_k = [m_1^k, m_2^k, \ldots, m_{\beta_l}^k], \ k = 1,2,3 \ldots, N_bN_f \qquad (2)$$

$$\tilde{B}_1 = E_k[B_1] \qquad (3)$$

$$\tilde{B}_k = B_1 \oplus B_k, \ k = 2,3, \ldots, N_bN_f \qquad (4)$$

$$\tilde{S} = [\tilde{B}_1, \tilde{B}_2, \ldots, \tilde{B}_{N_bN_f}] \qquad (5)$$

Algorithm Notations

B_j = The j^{th} block of data (plaintext).

$\tilde{B}_j$= The j^{th}block of the encrypted-coded data (cipher text).

β_l= Block length.

N_F= Number of frames within a super frame.

N_b= Number of block within a frame.

$b_{i,j}$= The i^{th} bit of the j^{th} block of the data (plaintext).

$\tilde{b}_{i,j}$= The i^{th} bit of the j^{th} block of the encrypted-coded data (cipher text).

As it is clear from the steps in Algorithm, we first encrypt the first block, B$_1$, with IDEA encryption. Following this step, the rest of the $N_b - 1$ blocks will be used as plaintexts (i.e., will not undergo IDEA encryption). In these steps that follow, a bit-wise XOR operation is performed between the plaintext of the first block with each of the remaining $N_b - 1$ blocks and then transmitted to the destination.

Consequently, the first block will not be recovered without performing the decryption process, which is assumed to be very immune for cryptanalysis, and therefore the other blocks will not be detected by the intruders since the plaintext of the first block is required to undo the XOR operation. This latter operation can be performed only after decrypting the first block (*B$_1$*) at the receiver (see Figure 1 (b)).

By performing the proposed IDEA encryption algorithm, where the first block is first IDEA encrypted and then the XOR operation is performed for the remaining blocks with the plaintext of the first block, the whole resultant data stream will then be secure with security level as high as the security level of the first block. The whole data stream will share the same security level since the XOR operation is a one- to-one mapping function and the data will not be recovered by any intruder without breaking the first cipher.

V. SIMULATION PARAMETER AND RESULTS

A. Simulation parameters

1) **Bit Error Rate (BER):-** The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferring bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage.

$$BER = \frac{No.\ of\ bit\ errors\ recieved}{Total\ number\ of\ bits\ transmitted} \qquad (6)$$

2) **Signal-to-Noise Ratio (SNR):-** Signal-to-noise ratio (SNR or S/N) is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. The ratio is usually measured in decibels (dB). A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise.

In other words, signal-to-noise ratio is defined as the power ratio between a signal (meaningful information) and the background noise (unwanted signal).

$$SNR = \frac{P_{signal}}{P_{noise}} \qquad (7)$$

3) **Throughput***:* - It is defined as the rate of successful message delivery over a communication channel. Mathematically it can be expressed as:

$$T = R(1 - p_e)^{B_l} \qquad (8)$$

Where,

R = Bit rate

p_e = Bit error probability

B_l = Block length

Table 1 is showing the values of simulation parameter used.

Table 1: Simulation Parameters

Simulation Parameter	Value
Encryption Technique	IDEA
Modulation Technique	BPSK
Communication Channels	4
No of bits	2560 bits
SNR	0-30 db
Throughput	1366-2560
BER	Varying (10^0 to 10^{-4})

B. Simulation Results

Bit error rate (BER) and Throughput Performance is analyzed, recorded and compared of IDEA encryption model for BPSK based secured communication system over AWGN, Rayleigh, Rician and Nakagami fading channels (environments) by varying the simulation parameter SNR from 0 to 30 db with a 128 bit key. Simulation is carried out using MATLAB 2010 a.

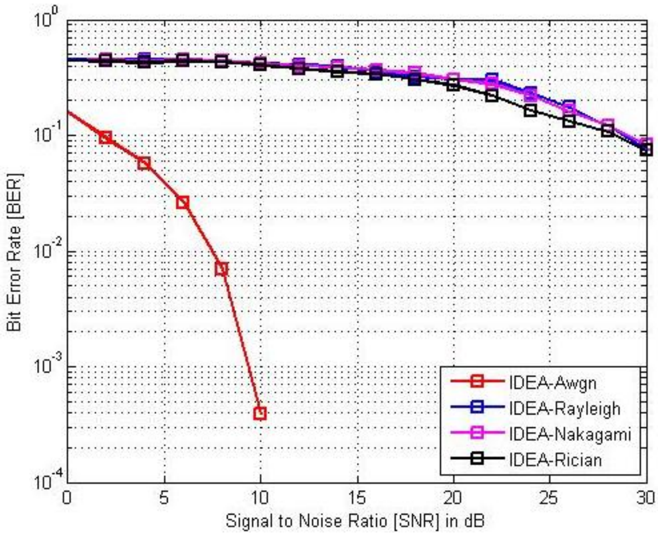


Figure 2: BER performance comparison of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels.

Figure 2 shows BER performance comparison of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels (environments).

Figure 3 shows the throughput performance comparison of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels (environments).

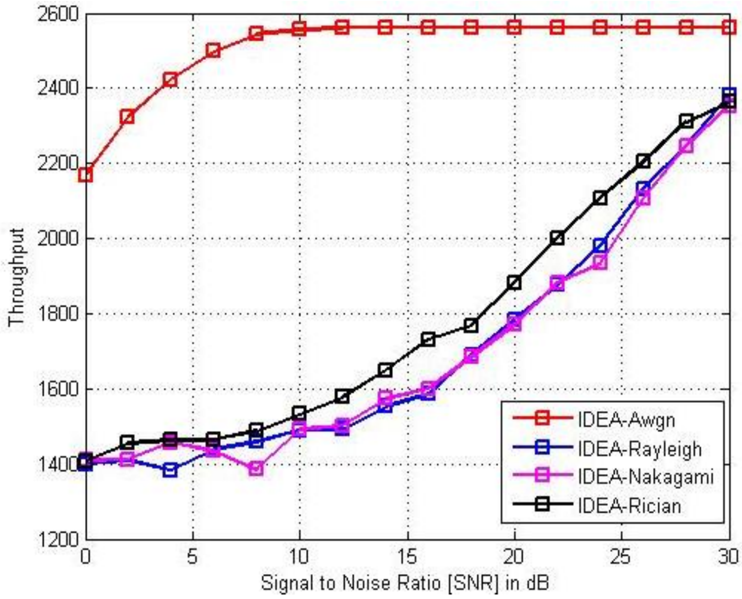


Figure3: Throughput performance comparison of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels.

VI. Conclusion

In this paper performance of IDEA encryption model is analyzed over different fading environments. It was found that the IDEA encryption model performs better in case of AWGN channel as compared to other communication channels on the basis of BER and Throughput results. It was observed that the performance of Rayleigh fading channel was worst among all channels on the basis of BER and Throughput results. Additionally it conclude that the performance of rician fading channel is worse than that of AWGN channel and better than that of Rayleigh and Nakagami fading channels in terms of BER and Throughput.

Direction of future work may be focused on the use of other encryption algorithms for enhancing the system throughput and reduction of the complexity. Error correction schemes can be applied to reduce the Bit Error Rate of existing research work.

REFERENCES

[1] Gary Breed, High Frequency Electronics , 2003 Summit, Technical Media LLC "*Bit Error Rate: Fundamental Concepts and measurement issues"*

[2] A. Sudhir Babu, Dr. K.V Sambasiva Rao, "Evaluation of BER for AWGN, Rayleigh and Rician Fading Channels under Various Modulation Schemes", *International Journal of Computer Applications, ISSN: 0975 – 8887,* Volume 26, No.9, July 2011.

[3] M. N. Rindani, A. A. Bavarva, "Evaluation of BER for AWGN, Rayleigh and Rician Fading Channels under Various Modulation Schemes," *International Journal of Computer Applications (0975 – 8887)* Volume 26– No.9, July 2011

[4] Sandipan Basu "International data encryption algorithm (IDEA*)" Journal of Global Research in Computer Science* Volume 2, No. 7, July 2011.

[5] Suying Yang*, Hongyan Piao, Li Zhang and Xiaobing Zheng, "An Improved IDEA Algorithm Based on USB Security Key" *Third International Conference on Natural Computation (ICNC 2007)*.

[6] Mustafa M. Matalgah, Amer M. Magableh, "Simple Encryption Algorithm with Improved Performance in Wireless Communications*", IEEE, Radio and Wireless Symposium (RWS),* January 2011.

[7] Vinod Shokeen, Niranjan Yadav, "Encryption and Decryption Technique for Message Communication", *IJECT*, Vol. 2, Issue 2, June 2011.

[8] Harivans Pratap Singh, Shweta Verma, Shailendra Mishra, "Secure-International Data Encryption Algorithm", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* ISSN: 2278 – 8875, Vol. 2, Issue 2, February 2013.

[9] Sutanu Ghosh, "Performance Analysis on the basis of a Comparative Study between Multipath Rayleigh Fading and AWGN Channel in the presence of various Interference", *International journal of Mobile Network Communications & Telematics (IJMNCT)* Vol. 4, No.1, February 2014.

Gaurav Mahajan was born in India, in 1988, received the B.E. degree in 2010, from Department of Electronics and Communication, Vindhya Institute of Science and Technology Indore, R.G.P.V. University, pursuing M.E. degree in digital communication from Department of Electronics and Communication, I.E.S. I.P.S. Academy Indore, India

Prof. Kavita Upadhyay received the B.E. degree from Department of Electronics and communication, M.E. degree from I.E.T. DAVV, Indore, pursuing Ph.D. from I.E.T. DAVV, Indore. Presently working as Associate Professor in I.E.S., I.P.S. Academy, Indore, India