ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

Performance of Secured Turbo Coding Scheme for Land Mobile Channels

[1]Nivedha.P, T.J Jeyaprabha,

PG Scholar, Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, India

Assistant Professor, Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, India

ABSTRACT: In real time communication system, channel coding schemes and encryption schemes are used to provide reliability and security respectively (confidentiality and authentication). An encrypted data without channel coding suffer from error – degradation effect, hence they both are done in sequential order to provide reliability and security. In this project a joint encrypted-coding is proposed that can reduce computational complexity and time complexity. When both are combined, an efficient coding can be obtained. The performance of the system can be enhanced using encryption technique Data Encryption Standard (DES) at the interleaver part. Comparison is going to be done on proposing available encryption and channel –coding algorithm that advice good error correction capability at low bandwidth added security.

KEYWORD*:* Crypto-coding, turbo coding, Data Encryption Standard (DES),

I. INTRODUCTION

Communication is the act of transmission of information. For communication to be successful, it is essential that the sender and the receiver understand a common language. Communication systems convey information from one point to another via physical channels that propagate electromagnetic, acoustic, particle density, or other waves. This information is usually manifest as voltages or currents; these may be continuous (often called analog) variables with an infinite number of possible values or discrete (often called digital) variables with a finite set of known possible values. They may communicate information in two directions, or only one way, and they may involve one node broadcasting too many, one node receiving from many, or a finite set of nodes communicating among themselves in a network. Digital communications and storage have created great impact in our daily lives. Robust data transmission and data storage are used. People realize that errors occur from time to time in data transmission and storage systems, and if the use of Error control techniques were not used, then the reliable data transmission and storage would not be done. Errors in data transmission and storage systems can come from many different sources such as random noise, interference, channel fading, or physical defects, to name a few. These channel errors must be reduced to a tolerable level.

A.CHANNEL DISTORTIONS

On propagating through a channel, signals are shaped and distorted by the frequency response and the attenuating characteristics of the channel. There are two main manifestations of channel distortions: magnitude distortion and phase distortion. Channel distortions can degrade or even severely disrupt a communication process, and hence channel modeling and equalization are essential components of modern digital communication systems. High latency due to interleaving and iterative decoding.

1. Complexing in time.
2. Data insecurity (in order to overcome it encryption technique can be used).

II .RELATED WORKS

Secure channel coding schemes based on convolutional codes are suggested to enhance the performance of combined cryptography and coding theory, which is called “Crypto-Coding”. In this Data Encryption Standard (DES)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

for security and channel coding algorithm such as convolutional code for efficient transmission are combined in a mono-block. This modification is required to improve the overall system performance. The combined System's performances are evaluated on Land Mobile Satellite (LMS) Channel. [1]. In this turbo code is embedded in public key cryptographic algorithm such as Rivest-Shamir-Adelman (RSA) to achieve security and reliability into a single step Secured data is efficiently transmitted over Land Mobile Satellite (LMS) channel with the help of turbo code having different interleaver.[2]It propose a joint encryption error correction coding scheme. In this scheme, a conflict-free interleaver parallel decoding method of Turbo codes is used, which is known simply as" efficient Turbo codes", and it is combined with chaotic encryption together.[3] The channel coding technique used is Turbo code that performs very well and provides results near Shannon's Limit. The design of interleaver used in turbo code provides security while channel coding. Puncturing pattern designed for channel coding further increases the security of the system and improves the code rate also. Security of the system is achieved by hiding the keys used in code generation and puncturing from unintended users. [4].The turbo encoder has been designed with shift register, modulo-2 adder, TDES interleaver. Viterbi decoder section includes Convolutional decoder and TDES interleaver and TDES de-interleaver [5].

III. TURBO CODING AND SECURITY

Secure channel coding schemes based on convolutional codes are suggested to enhance the performance by combining cryptography and coding theory, which is called "Crypto-Coding". In this work Turbo code is embedded with private key cryptographic. The algorithm used for private key cryptography is Data Encryption Standard (DES) Algorithm. This modification is required to improve the overall system performance by providing reliability, confidentiality and bandwidthefficiency. The combination of cryptography and error correction was firstdealt by McEliece time. Since then, unfortunately, very few researchers have tried to deal with this problem. Some authors argue that a crypto-coding has not fascinated more attention since the fact that error correction introduces redundant data (i.e. data expansion), which is usually not agreeable in cryptography. However, when secured data is transmitted over a noisy channel, then redundancy plays very important role in the correction of corrupted data at the decoder. In addition to decreasing computational costs, we discuss another advantage that one crypto-coding system may pose. Namely, we refer to the recently proposed crypto codingsystem which can have arbitrarily chosen redundant information. More precisely, the system is defined in a way that the redundant information used for error-correction is not pre-determined by the nature of the error-correction part of the algorithm but it can be chosen arbitrarily out of the whole set of possible strings. In in project, we propose a new scheme called crypto-coding.

A. TURBO CODE

Turbo codes are a class of high-performance forward error correction (FEC) codes. It was the first practical codes to closely approach the channel capacity, a theoretical maximum for the code rate at which reliable communication is still possible given a specific noise level.

i.Turbo Encoder

The fundamental turbo code encoder is built using two identical recursive systematic convolutional (RSC) codes with parallel concatenation.RSC encoder is termed as component encoder. The two component encoders are separated by an interleaver. Only one of the systematic outputs from the two component encoders is used, because the systematic output from the other component encoder is just a permuted version of the chosen systematic output. Fig.4.1 shows the fundamental turbo code encode.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

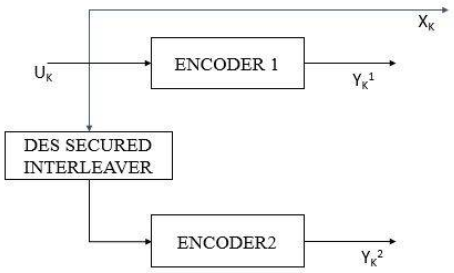


Fig.1. General Structure of secured turbo encoder

The first RSC encoder outputs the systematic code C_1 and recursive convolutional C_2 sequences while the second RSC encoder discards its systematic sequence and only outputs the recursive convolutional C_3 sequence.

ii.Interleaver Design

The interleaver is a very important constituent of the turbo encoder. It spreads the bursty error pattern and also increases the free distance. Thus, it allows the decoders to make uncorrelated estimates of the soft output values. The simplest interleaver is the "row-column" or "block" interleaver where the elements are written row-wise and read column-wise. The "helical" interleaver writes the data row-wise but reads diagonal-wise. There is also an "odd-even" interleaver, in this interleaver the odd positions of the input bits are encoded first. A "pseudo-random" interleaving of the input sequence follows this and the even positions are now encoded. The output consists of the input sequence and multiplexed sequence of odd and even positioned coded bits.

iii.Puncturing

Puncturing is a technique used to increase the code rate. A rate1/3encoder is converted to a rate1/2 encoder by multiplexing the two coded streams. The multiplexer can choose the odd indexed outputs from the output of the upper RSC encoder and its even indexed outputs from the lower one. An important application of puncturing is to provide unequal error protection where relatively unimportant bits.

IV.ALGORITHM FOR ENHANCEMENT

Secure channel coding schemes based on convolutional codes are suggested to enhance the performance of combined cryptography and coding theory, which is called "Crypto-Coding". Data Encryption Standard Algorithm (DES) is used at the interleaver part in order to provide security.

A. CRYPTOGRAPHY

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. With tremendous growth of internet, the need for optimal performance of the encryption algorithm is of main concern.

Within the context of any application-to-application communication, there are some specific security requirement, including:

- Authentication: the process of proving ones identity.
- Privacy/confidentiality: ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non- repudiation: A mechanism to prove that the sender really sent this message.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

i.Data Encryption Standard(DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration.

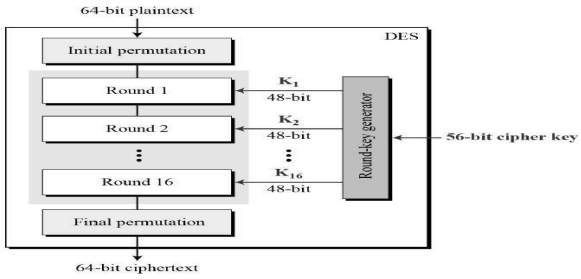


Fig. 2. Flow diagram of DES Algorithm

V.SIMULATION RESULTS

The implementation of proposed system involves the encryption of data using Data Encryption Standard (DES) in turbo code system.

A. *Simulated result for unencrypted channel coded data*

The BER Vs SNR graph is plotted for unencrypted data in presence of channel noise. The BER for this type of signal is considered to be very low, because of the absence of encryption technique. The network security for the information when transmitted through a wireless system is very poor as there is no encryption technique.

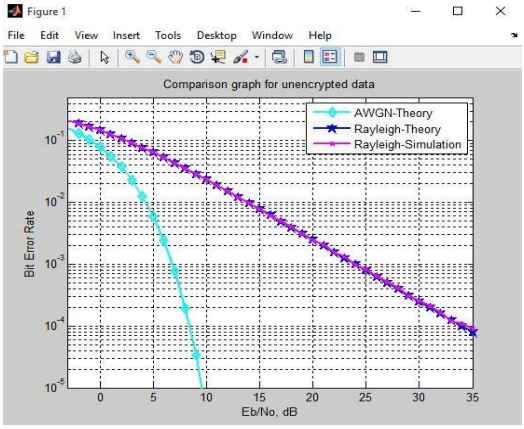


Fig.3. Comparison graph for unencrypted data

The above graph show the comparison between AWGN and Rayleigh Fading. The BER performance is better for AWGN channel when compared to Rayleigh Fading channel of turbo code system. In this process for AWGN channel BER is 10^-5 at SNR 10 dB at the same time For Rayleigh fading channel the BER is 10^-2 at SNR 10 dB.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

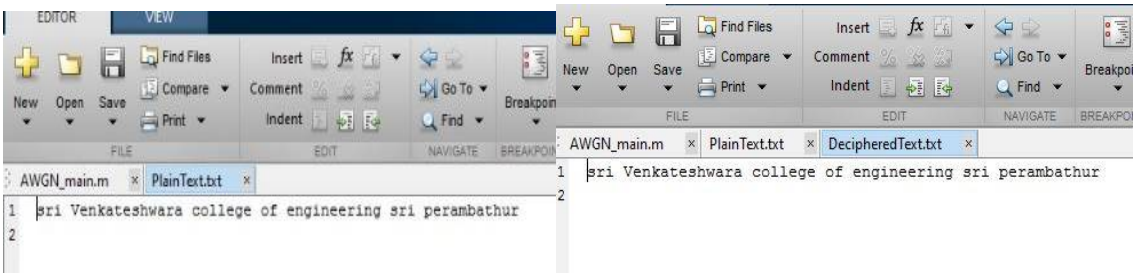
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

B.*Simulation result for des encrypted channel coded data*

Simulated result has been obtained using Data Encryption Standard. At first the input plain text is allowed to pass through the DES encryption Algorithm, in interleaver part which it generate a cipher text as well as the decipher text.as shown in the Fig. 4 the text is allowed to get generated from the interleaver part.



(a) (b)

(c)

Fig: 4. (a)Plain text,(b) Decipher text,(c)Cipher text

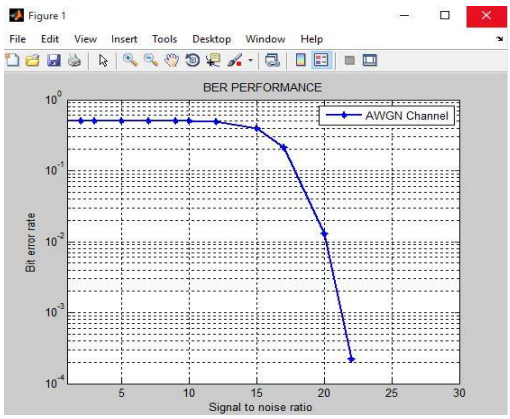


Fig.5. Turbo Coder with DES based Interleaver for AWGN Channel

Fig 5 shows the simulated result of encrypted data for AWGN Channel and the Modulation used QPSK modulation. The performance graph shows BER 10^-1 dB at SNR value of 10 DB, whereas the BER of unencrypted data is 10^-2 dB for same SNR Value, the security of the information is much more improved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

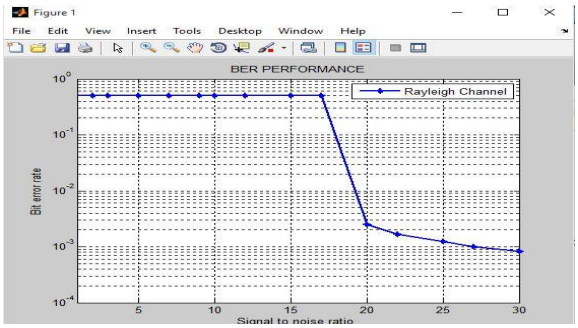


Fig. 6. Turbo Coder with DES based Interleaver for Rayleigh Fading Channel

In Fig 6 the BER is 10^-1 at SNR 10 dB for Rayleigh fading channel

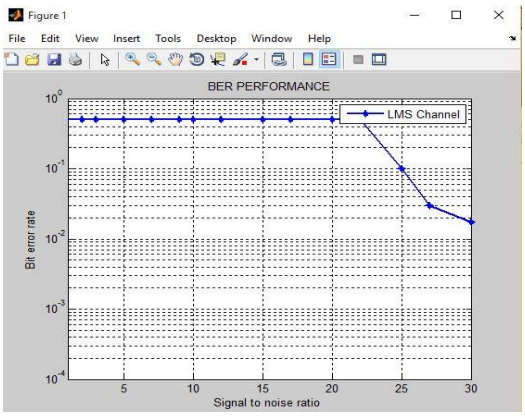


Fig.7 Turbo Coder with DES based Interleaver for LMS Channel

From the above Fig 7 the BER is 10^-1 dB at SNR value of 10 dB for LMS channel

VI .CONCLUSION AND FUTURE SCOPE

The concept of combining cryptography-error correction as a single algorithm, which is called here as "Crypto-Coding" has been done. The DES encryption and Rivest Shamir Adleman (RSA) algorithm is and investigated on land mobile satellite channel. The performance is also examined on Rayleigh and AWGN channels, the performance is analyzed and corresponding BER, SNR values are obtained. Even though the bit error rate performance is degraded optimization has been done for the security of the information for the users in the real time environment.

The same performance evaluation can be done for different encryption algorithm with different type of channel. The performance of the system can also be enhanced using hybrid algorithm encryption technique (i.e. combination of both Data Encryption Standard (DES) and Rivest Shamir Adleman (RSA)) at the interleaver part also by introducing an interleaver known as progressive edge growth interleavers ensures optimal growth of the minimum distance of turbo codes, which grows as log (N), where N is the interleaver size.

REFERENCES

1. RajashriKhanai, G. H. Kulkarni, Dattaprasad A. Torse (2015), "Crypto-Coding as RSA-Turbo for Land Mobile Satellite Channel",International Journal of Electronics and Electrical Engineering Vol. 3, No. 2
2. Jianbin Yao, Jianhua Liu and Yang Yang (2015),"Joint Encryption and Error Correction Technical Research Applied an Efficient Turbo Code",International Journal of Security and Its ApplicationsVol.9

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

3. RajashriKhanai, G. H. Kulkarni, Ph.D(2014),"Crypto-Coding as DES-Convolution for Land Mobile Satellite Channel"International Journal of Computer Applications (0975 – 8887) Volume 86 – No 18
4. RajashriKhanai, Dr. G. H. Kulkarni, Dattaprasad A. Torse. (2013),"Low Complex Crypto based Channel Coding with Turbo Code"International Journal of Computer Applications (0975 – 8887) Volume 61– No.16
5. Koka Hemant, Hamsavahini, PawanUpadhyay , Shamim Akhter (2007),"Design and Implementation of Crypto-Based Interleaver for Viterbi Encoder and Decoder using Turbo Codes",IEEE Publication
6. Sreelakshmi T S1, Noble C Kurian. (2015),"A Comparative Study of BER Performance in Deep Space Communication Based on Coding Techniques",International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 8.
7. Chuanyu Wang, Shanshan Wang, Ye Tian.(2013), "Yufeng Ma Research and Simulation on the Performance of Turbo Code and Convolutional Code in Advanced Orbiting Systems", IEEE pp. 502–507.
8. Mrs.K.M.Bogawar, Assistant Professor, Ms.ShardaMungaleDr.ManishChavan. (2014)," Implementation of Turbo Encoder and Decoder", International Journal of Engineering Trends and Technology (IJETT) – Volume 8 Number 2- ISSN: 2231.
9. RajashriKhanai, Dr. G. H. Kulkarni, Dattaprasad A. Torse. (2014)," Crypto-Coding Technique for Land Mobile Satellite Channel" Fifth International Conference on Signals and Image Processing.
10. RajashriKhanai, Dr. G. H. Kulkarni, Dattaprasad A. Torse. (2014),"Neural Crypto-Coding as DES: Turbo over Land Mobile Satellite (LMS) Channel," International Conference on Communication and Signal Processing, India.
11. Shao Xia1 and Zhang Weidang2. (2015),"Shortening the Turbo Codes Based on Unequal Error Protection", International Journal of Multimedia and Ubiquitous Engineering Vol.10, No.8 pp.73-82.
12. Sreelakshmi T S1, Noble C Kurian. (2015),"A Comparative Study of BER Performance in Deep Space Communication Based on Coding Techniques", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 8.