International Journal of Engineering Sciences & Emerging Technologies, Apr. 2013.
ISSN: 2231 – 6604 Volume 5, Issue 1, pp: 53-58 ©IJESET

A NOVEL COMMUNICATION SYSTEM WITH LT ENCODING FOR ERASURE CHANNEL

Jismi K[1], Deepthy J R[2]
[1]Department of Electronics and Communication Engineering, Trivandrum, India.
jis.ansal@gmail.com
[2] Department of Electronics and Communication Engg., Kerala University Trivandrum, India
deepthyreghu@gmail.com

ABSTRACT

A novel communication system model is proposed for erasure channels, whereby repeat request rates can be reduced and additional security can be achieved. The proposed system would make use of Luby Transform(LT) encoding to combat bit losses in the system and Triple Data Encryption Standard is used for encrypting the messages, so that secure transfer of information is made possible through the system. Luby Transform encoding can effectively recover original data from the received data even if only half of the encoded data is received properly. This property of Luby Transform encoding is made use of so that an opportunistic error correction layer is constructed. The bit losses in the system can be countered efficiently. Triple Data encryption Standard provides an additional security layer for messages whereby three 64-bit keys are used to encrypt the original data to obtain the cipher. The main real life applications are to enable secure communication within banking systems, online credit card payments, intranet password transfers, etc. with reduced rate of repeat request.

KEYWORDS: *luby transform, erasure channel, secure communication, repeat request rate.*

I. INTRODUCTION

A communication system is defined as a collection of individual communication networks which consists of transmission systems, relay stations, tributary stations and data terminal equipment usually capable of interconnection and inter-operation to form an integrated component. A novel communication system model for erasure channel is proposed whereby repeat request rates can be reduced and additional security can be achieved. The proposed system consists of Luby Transform encoding to combat bit losses in the system.

To alleviate transmission errors and losses over wireless network, Automatic Repeat reQuest (ARQ) and forward error correction (FEC) are widely used. ARQ increases delay because it has to retransmit lost data after receiving feedback information [1]. Thus ARQ may not be suitable for delay sensitive networks like online password transfers, internet banking etc. Forward Error Correction (FEC) or channel coding is a technique used for controlling errors in data transmission over unreliable or noisy communication channels.FEC requires some redundant data to compensate for errors and losses without any feedback information over the network [1]. This feature is generally appropriate for delay sensitive networks.

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key, which adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm, to randomly produce keys.

The paper is constructed as follows. The Communication system is described in section II, The system description includes LT encoding/ decoding section, Binary Erasure channel and Triple DES section. Simulation results are discussed in section III. Performance analysis is done in this section. Future works which includes TDES is described in section IV and conclusion is presented in section V.

II. SYSTEM DESCRIPTION

2.1. Luby Transform

Luby Transform codes are the first class of practical fountain codes that are near optimal erasure correcting codes. Fountain code is a type of erasure code with the property that a potentially limitless sequence of encoding symbols can be generated from a given set of source symbols such that the original source symbols can ideally be recovered from any subset of the encoding symbols of size equal to or slightly larger than the number of source symbols [2]. The main characteristics of Luby transform codes are high coding efficiency, low encoding/decoding processing time, and flexibility [1]. LT encoded symbols are generated by performing bitwise XOR operations on the selected source symbols. The process is repeated until the last LT encoded symbol is generated. The mapping process is controlled by the generator polynomial, which is one of the most important design factors [1].

LT-codes constitute a class of rate less codes, in which 'N' (N being potentially any value $\leq \alpha$) output symbols are produced randomly and independently according to a degree distribution. A decoding algorithm is then applied at the receiver side to recover the input symbols from the N output symbols. The LT-decoder is efficient in terms of the block-size N required to have a decoding success with high probability. The main drawback of LT codes is that, for vanishing error probability over erasure channels, the average degree of the output symbols grows logarithmically with the number of input symbols K [3].

For LT codes, each encoding symbol is generated independently of all other symbols. Generate a random number'd' from the degree distribution. Randomly select a message node incident on each of the'd' edges. The value of the encoding symbol is the XOR of the neighbouring encoding bits.

When the decoding process initiates all message symbols are uncovered. At the first step, all degree one encoding symbols gets released to cover their unique neighbour. These set of covered message symbols that have not been processed yet form a ripple. At each subsequent set one message symbol from the ripple is selected randomly and processed. It is removed as a neighbour of all encoding symbols. Any encoding symbol that now has degree one is now released and its neighbour is covered. If the neighbour is not in the ripple it gets added to the ripple. The process ends when the ripple is empty. It fails if at least one message symbol is uncovered [3].

There are two methods in which the decoder came to know which message nodes are the neighbours of a particular encoding symbol. One solution is to explicitly include this information as an additional overhead in the packet. Another possibility is to replicate the pseudorandom process at the receiver by supplying it with the suitable seed and/or keys [4]. LT codes were originally invented for multicast scenarios for the binary erasure channel (BEC) [5]. To recover the original packet, the LT decoder adopts the belief propagation (BP) technique. With the encoding degree and packet index information of each coded packet, a bipartite graph is formed. The decoder starts by releasing packets with degree one. Then all edges connected to the degree one packet(s) are removed. This is done recursively until no degree-one packet is left. If all 'k' input packets are recovered, then the decoding is successful, otherwise, a failure is reported [6].

2.2. Binary Erasure Channel

The Binary Erasure channel is the simplest non-trivial channel model imaginable. The emergence of the internet promoted the erasure channel into the class of "real world" channels. In this model, a transmitter sends a bit (a zero or a one), and the receiver either receives the bit or it receives a message that the bit was not received ("erased"). This channel is used frequently in information theory because it is one of the simplest channels to analyze. The BEC is a binary channel; it can transmit only one of two symbols (usually called 0 and 1). The channel is not perfect and sometimes the bit gets "erased", ie. The bit gets scrambled so the receiver has no idea what the bit was. The BEC is error-free. Unlike the binary symmetric channel, when the receiver gets a bit, it is certain that the bit is

correct. The only confusion arises when the bit is erased. This channel is often used by theorists because it is one of the simplest noisy channels to analyze. Many problems in communication theory can be reduced to a BEC. A Binary erasure channel with erasure probability pe is shown in Figure. 1.

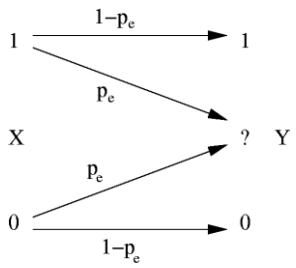

Figure. 1. Binary Erasure Channel

A binary erasure channel with erasure probability pe is a channel with binary input, ternary output, and probability of erasure pe. ie, let X be the transmitted random variable with alphabet {0, 1}. Let Y be the received variable with alphabet {0, 1, ?}, where ? is the erasure symbol. Then, the channel is characterized by the conditional probabilities

P (Y = 0 / X = 0) = 1-pe
P (Y = e / X = 0) = pe
P (Y = 1 / X = 0) = 0
P (Y = 0 / X = 1) = 0
P (Y = e / X = 1) = pe
P (Y = 1 / X = 1) = 1-pe

In a BEC, a code symbol is either erased with an erasure probability or received correctly by the receiver. This behaviour is an adequate model for packet transmission over computer networks, where a corrupted or un-received packet is considered an erased symbol. Through coding, the erased packets in the frame can be recovered by applying erasure-correcting decoding on its received/unerased symbols. Thus, coding is advantageous when compared to the acknowledgement-based protocols, especially under poor channel conditions or upon transmission from one server to multiple recipients [3].

2.3. Triple DES

The main function of an encryption system is to allow two parties to communicate in a manner such that transmitted information appears in an unintelligible form to an eavesdropping third party. Incoming plaintext is encrypted via some algorithm under the control of a key. This encrypted data, referred to as cipher text, is transmitted to the receiver, where it is decrypted under the control of a second key to restore the original plaintext [7].

Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DES and TDEA will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. FIPS 46-3 describes the Triple DES algorithm (also known as TDES). It can be used as a FIPS-approved encryption algorithm until 2030. TDES uses three rounds of DES encryption and has a key length of 168 bits (56 * 3). Brute force attacks against TDES are currently not practical. The FIPS-approved implementations of TDES uses three rounds applied in encrypt – decrypt – encrypt (EDE) order. EDE order also allows backwards compatibility with DES.[8] The block diagram of TDES is shown in Figure. 2.

Figure. 2. Block diagram of TDES

For TDES Algorithm, let Ek(X) and Dk(X) represent the DES encryption and decryption of 'I' using DES key 'k' respectively. Each TDEA encryption/decryption is a compound operation of DES encryption and decryption operations. In TDES encryption operation the 64-bit block 'X' is transformed into a 64-bit block 'Y'.[8]

Y = Ek3(Dk2(Ek1(X)))

In TDES decryption operation the 64-bit block 'X' is transformed into a 64-bit block 'Y'.

Y = Dk1(Ek2(Dk3(X)))

The security of any encryption algorithm against a "brute force" attack is directly related to the key length. DES's key length of 56 bits is small by today's standards, and custom "cracking machines" have been built which can break DES by brute-force in days.[8] For increased security, TDES is used which expands the effective key space to 112 bits. A TDES encrypted message is well out of reach of a brute-force attack for the foreseeable future [7].TDES is much more secure than DES, but it has the major disadvantage of also requiring more resources for encryption and decryption.

III. SIMULATION RESULTS

This section presents the MATLAB simulation results from some case studies to demonstrate the efficiency of the proposed communication system. Figure. 3. shows the plot of ARQ rate versus Probability of erasure of channel. From the analysis it is clear that with Luby encoding repeat request rate is reduced than with no encoding. Figure. 4. shows the plot of Bit loss rate versus Capacity of binary erasure channel. (1-Pe) is taken as the capacity of BEC.

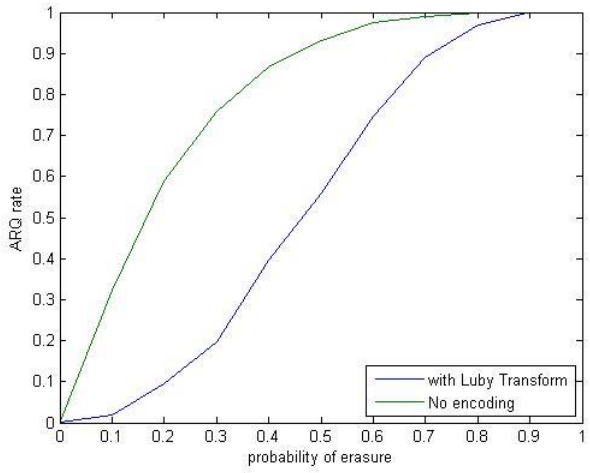

Figure. 3. ARQ rate versus Probability of erasure

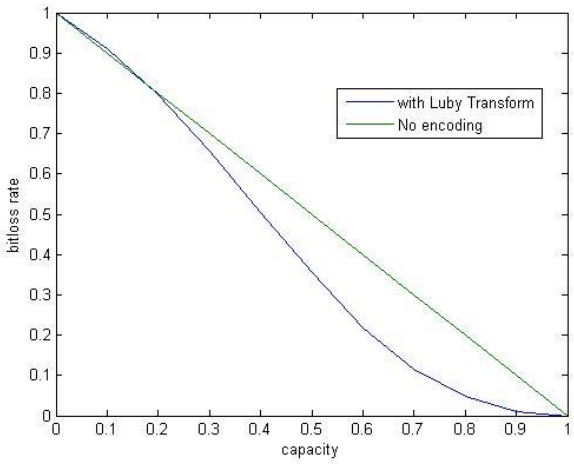

Figure. 4. Bit loss rate versus Capacity

IV. FUTURE WORKS

The binary erasure channel modelling and LT communication system is simulated. The future scope of the work is dedicated to TDES section. This section is provided in order to achieve additional security.

V. CONCLUSIONS

This paper presents the design and implementation of a novel communication system which provides additional security. The concept of Luby Transform and TDES is presented. Future effort will be devoted to validate the system in real application conditions.

ACKNOWLEDGEMENTS

We would like to thank Dr. Ibrahim Sadhar, HOD, EC department, MACE for his valuable guidance and encouragement in pursuing this paper. We also acknowledge our gratitude to other members of faculty in the Department of Electronics and Communication Engineering, MACE and all our friends for their whole hearted cooperation and encouragement.

REFERENCES

[1] Dongju Lee and Hwangjun Song, "A Robust Luby Transform Encoding Pattern-Aware Symbol Packetization Algorithm for Video Streaming Over Wireless Network," IEEE transactions on multimedia, vol. 13, no. 4, August 2011.

[2] M. Luby, "LT codes", Proceedings of the 43 rd Annual IEEE Symposium on Foundations of Computer Science, Nov.2002.

[3] Hady Zeineddine, Mohammad M. Mansour, Senior Member, IEEE, and Ranjit Puri, "Construction and Hardware-Efficient Decoding of Raptor Codes, ", IEEE transactions on signal processing, vol. 59, no. 6, June 2011I.

[4] Ashish Khisti, "Tornado Codes and Luby Transform Codes", http: //web.mit.edu/6.454/www/www_fall_2003=khisti=tor_summary.pdf, October22; 2003.

[5] Andrew Liau, Shahram Yousefi, and Il-Min Kim Senior Member, IEEE, "Binary Soliton-Like Rateless Coding for the Y-Network ", IEEE transactions on communications, vol. 59,no. 12, Dec 2011

[6] Rui Cao, Student Member, IEEE and Liuqing Yang, Senior Member, IEEE, "Decomposed LT Codes for Cooperative Relay Communications ", IEEE journal on selected areas of communications, vol. 30, no. 2, Feb 2012

[7] Toby Schaffer, Member, IEEE, Alan Glaser, Member, IEEE, and Paul D. Franzon, Senior Member, IEEE, "Chip-Package Co-Implementation of a Triple DES Processor", IEEE transactions on advanced packaging, vol.27,no.1,Feb2004.

[8] U.S Department of Commerce/ National Institute of Standards and Technology , "Data Encryption Standard (DES)", Federal Information Processing Standards Publication.

AUTHORS

JISMI K obtained BTech degree from IHRD under Cochin University of Science and technology, Kerala in 2004 and MTech in VLSI Design form Electronics and Communications Engineering Department Amrita Vishwavidyapeetham University in 2010. She is presently working as Assistant Professor in Department of ECE, MACE, Trivandrum, Kerala. Her current research interests are in the field of VLSI design, testing and cryptography.

DEEPTHY J R received her B Tech degree from Marian Engineering College, Trivandrum (Kerala) in the year 2006. Since 2008, she had been working as lecturer at Marian Engineering College. Her focus areas include network security, image processing, and communication systems.