ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Modern Coding Theory Based On Fountain Code Implementation In Embedded System

S.Thilagavathi[1], J.Sathyapriya[2], T.M Minipriya[3], T.Mohanapriya[4], C.Subashini[5]

PG Scholar, Embedded System & Technologies, S.A Engineering College, Chennai, India[1,2,3,4]

Associate Professor, S.A Engineering College, Chennai, India[5]

Abstract: Fountain codes are used in delay tolerant networks with low performance and encoding decoding complexity. Packet erasure is the major problem during transmission on wireless channel resulting in packet collisions. A digital fountain solves these problems by introducing the concept of segmentation and reassembly in order to avoid the total delay and packet loss. In addition to that the concept of cryptography is used to transmit the data in a secure manner. For that purpose the use of erasure code like Luby Transform(LT) code with LT encoder and LT decoder to achieve secure transmission of data. The LT encoder that are used at the source level for encoding the original data. Similarly the LT decoder that are used at the destination level are used for decoding the original data from the encoded data. The fountain codes are now used in the embedded systems for data encoding using Tarang F4 module. It is used to perform the data transfer between two terminals via serial port communication. The data transfer is done in wireless netwoks with the use of AT commands.

Index Terms: Segmentation And Reassembly, Luby Transform code, LT Encoder, LT Decoder, AT commands

I. INTRODUCTION

In wireless networks, reliable packet transmission can be achieved with minimal packet loss using LT codes. Some techniques are used to decompose LT codes into Distributed LT (DLT) codes to independently encode data from multiple sources in a network, when the DLT-encoded packets are combined as common to produce the resulting bit stream called a Modified LT (MLT) code.It has a compatible degree distribution approximately that of an LT code, with simulations indicate the comparable performance between DLT code and MLT code. DLT codes are designed to detect the final stage of encoding for error correction and is carried out by a low convolution relay that discriminatively XORs the bit streams that are created at each source level and transmits the result to the destination level [1]. Rateless codes are designed to decode all the original input symbols from a certain number of coded symbols that are received at the destination. It is possible to recover the splitted input symbols from the actually received coded symbols, and this process is called fractional decoding. The number of recovered input symbols is termed as the effective performance of rateless codes. The problem of optimality of the fractionally decoding process is determined. We say that a fractional decoding algorithm is optimal if, given rateless code is able to maximize the intermediate performance of the code, i.e. it is able to retrieve the maximum number of input symbols when a certain number n of coded symbols has been received, for every n. An optimal fractional decoding algorithm for all rateless code, proving its optimality [2]-[4]. The widespread use of mobile and handheld devices makes use of Ad-hoc networks instead of infrastructure based networks. The nodes of mobile and ad-hoc networks are communicated via routers. The communication may be achieved by means of single hop or multi-hop paths as a peer-to-peer fashion. Quality Of Service (QOS) is the major factor concerned in Mobile Ad-hoc VehicularNetworks[5].

Cooperative communication in wireless networks using parallel relays may forward information to a destination node parallel can greatly improve the energy efficiency of ad-hoc networks. However, current networks do not fully utilize its potential because it only uses traditional energy accretion technique, which is often used in combination with repetition coding. The concept of mutual information accretion can be realized with the help of fountain codes, and it leads to a lower energy consumption and transmission rate compared to energy accumulation. Then provide an analysis of the performance of mutual information accretion in relay networks with multiple relay nodes. First analyze the synchronization concept, when the source stops sending data and the relay nodes start sending after individual relay nodes have successfully decoded the source data.

Considering the closed form equations for the efficiency of energy savings that can be attained by the use of mutual information accretion at the receiver end. Then analyze for the scenario that each relay node starts its transmission to the destination after it decoded the source data, independent of the status of other relay nodes in wireless networks. This approach further reduces the transmission time of data between nodes, because transmission of the relay nodes that are completing its work helps the other relay nodes that are still receiving without any interruption[6]-[7].

II. ENSURING PRIVACY USING ERASURE CODES

According to coding theory, fountain codes are like erasure codes with an impact that more sequence of encoded symbols can be generated from a given set of original symbols and also the original basis symbols can ideally be decoded from any subset of the encoded

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

symbols of size equal to or little more greater than the number of original source symbols. Fountain is a general term like fountains in theme parks. It simply refers to the splitting of bulk data in different channels with a fixed rate. LT codes are rateless because the encoding algorithm can produce more number of message packets to perform encoding operation to ensure security. Mostly LT codes are error correcting codes because they can be used to transmit reliable digital data on an wireless channel.

A. LT ENCODER

The encoding process starts by dividing the uncoded message into N blocks of equal length. Encoded packets are then produced with the help of a random number generator.

The degree *n* is considered as the random number with the range, $1 \leq n \leq N$, and the next packet is chosen at random. Exactly *n* blocks from the source message is randomly chosen.

If M_i is the *i*th block of the message, the data partition of the packet is computed as follows:

$$M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{in} \quad (1)$$

where $\{i_1, i_2, \ldots, i_n\}$ are the randomly chosen keys for the *n* blocks included in this packet.

A prefix is appended to the encoded packet, that define the total blocks as N in the source message, determine *n* blocks have been exclusive-ored into the data segment of this packet, and the list of keys $\{i_1, i_2, \ldots, i_n\}$. Finally, some of the error-detecting code is applied to the packets to determine error, and then only that packet is transmitted.

This process continues until the receiver send signals to the sender that the message has been received and it is successfully decoded.

B. LT DECODER

The decoding process uses the xor operation used by the sender to retrieve the encoded message. If the currently received packet isn't pure, or if it replicates a packet that has already been processed, the current packet is discarded. If the current cleanly received packet is of degree $n > 1$, it is first processed with all fully decoded blocks in the message queuing area, then stored in a buffer area if its degree is greater than 1. Whenever a clean packet of degree $n = 1$ is received, it is moved to the message queueing area, and then it is matched against all the packets of degree $n > 1$ residing in its buffer. It is x-ored with the data portion of any buffered packet that was encoded using the block M_i, the degree of that matched packet is decremented, and the list of keys for that packet is adjusted to reflect the application of M_i. When this process unlocks a block of degree $n = 2$ in the buffer, that block is deducted to degree 1 and is in need to move on to the message queueing area, and then processed against the packets remaining in the buffer area.

When all N blocks of the data packets have been directed to the message queueing area, the receiver signals the sender that the data packets has been successfully decoded. This decoding procedure works because $A \oplus A = 0$ for any string *A*. After $n - 1$ divided blocks have been exclusive-ored into a packet of degree *n*, the original encoded content of the mismatched block is all that remains as same. In symbols we have

$$(M_{i1} \oplus \cdots M_{in}) \oplus (M_{i1} \oplus \cdots M_{ik-1} \oplus M_{ik+1} \oplus \cdots \oplus M_{in})$$
$$= M_{i1} \oplus M_{i1} \oplus \cdots \oplus M_{ik-1} \oplus M_{ik-1} \oplus M_{ik} \oplus M_{ik+1} \oplus M_{ik+1} \oplus \cdots \oplus M_{in} \oplus M_{in}$$
$$= 0 \oplus \cdots \oplus 0 \oplus M_{ik} \oplus 0 \oplus \cdots \oplus 0$$
$$= M_{ik}$$

III. PROPOSED BLOCK DIAGRAM

In Fig.1 The block diagram specifies the encoding and decoding of messages using LT encoder and LT decoder. The LT encoder composed of LT distribu-tion generator, Random number generator and XOR array for matrix computing to transmit the coded symbols to the LT decoder using wireless communication channel. The LT decoder in turn composed of LT distribution generator,Random number generator and matrix searching to obtain the decoded symbols. In Fig.2 the flow of the fountain code algorithm describes the encoding and decoding of original data. The input is first obtained from the user.The inputs obtained are character and key. The character may be either capital letters or small letters. It may be encoded by the use of ASCII values that are obtained from the ASCII table.

Using that character and keys the values are encrypted to some other human unreadable form because of fountain array encoder. The encoded output that are obtained is fed into the fountain array decoder to decrypt the encoded output to decoded output using the same key that is used by the sender.

LT DISTRIBUTION GENERATOR FOR ENCODER

LT distribution generator the messages that are given as input is segmented as several blocks and it is distributed over different channels in order to avoid data loss over the wireless network. The distributed messages over different channels are reassembled at the receiver end in order to get the original data message.

RANDOM NUMBER GENERATOR

A random number generator (RNG) is a computational device designed to generate a sequence of numbers or symbols as a key that ensure any regular pattern, i.e. consider randomly. Cryptographically secure computation based methods of generating random numbers is necessary. Using that random numbers only the input messages are encrypted in order to transmit the original data in some human unreadable form. This will provide secure transmission of data.

MATRIX COMPUTING

Consider there are eight possible six bit strings corresponding to valid codewords: (i.e., 000000, 011001, 110010, 101011, 111100, 100101, 001110, 010111). This LT code fragment represents a three-bit message encoded as six bits. Redundancy of bits is used here, to improve the chance of recovering from channel errors. This is a (6, 3) linear code with $m = 6$ and $n = 3$.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

The parity-check matrix representing this graph fragment as

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad (2)$$

In the above matrix, each and every row represents one of the three parity bit check constrictions, while each column represents any one of the six parity bits in the received coded words. In this example, the eight coded words can be obtained by putting the parity check matrix Q into this form $[-P^T|I_{m-n}]$ through basic row operations.

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \quad (3)$$

From this, the generator matrix R can be obtained as [In|P] (noting that in the special case of this being a binary code (P = -P), or specifically:

$$R = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \quad (4)$$

Finally, by multiplying all of the eight possible 3-bit strings by R, all eight valid codewords are obtained. For example, the codeword for the parity bit string '101' is obtained by:

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad (5)$$

IV. EXPERIMENTAL SETUP

The experimental setup for the flow of fountain code algorithm is based on both the approaches of software simulation and hardware implementation. The simulation is performed by using the MATLAB software. Specifically in this software this project makes use of only Matlab codings to run the project. The hardware used in this project is Stellaris LM4F120 Series Launchpad. Matlab codings for encoding and decoding concepts are explained using the range of ASCII values. In ASCII the value of small 'a' is 97 and small 'z' is '122'. The ASCII value of capital 'A' is 65 and the value of capital 'Z' is 90. The specific hardware used is Stellaris LM4F 120XL series regard to ARM processor.

The TARANG F4 module is used for data transfer between the two terminals in wireless network.One terminal is considered as the root and the another terminal is considered as the slave. Using the serial port the data entered in one terminal are send to another terminal via wireless medium with the power supply applied on both the terminals. Transformer is essential for providing power supply to both the terminals available in the wireless network for uninterrupted data transmission. Tarang F4 module comprised of data module and command module. Data module is used for data transfer and command module is used for sending commands to the memory for exchanging the source and destination address. Some of the commands of Tarang F4 module include ATNMY, ATNDA, ATWGR,ATGEX etc., Here AT is a prefix command, N stands for Network address and G stands for General address. All these commands are used for setting the source and destination address manually.

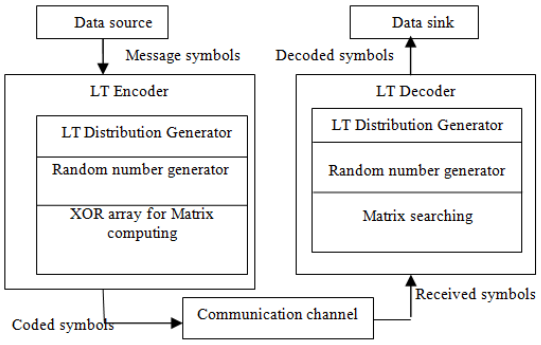

Fig.1 Proposed block diagram

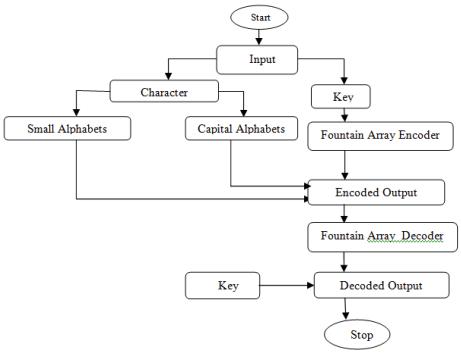

Fig.2 Flow of the fountain code algorithm

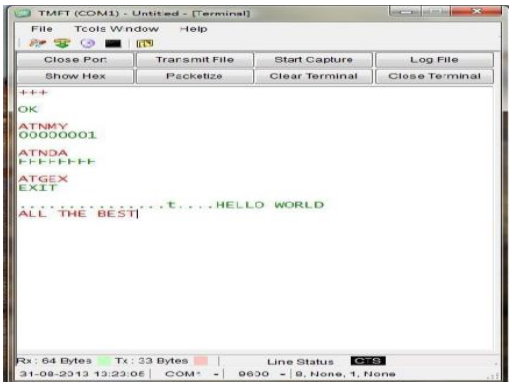

Fig.3 Data send from the root

In Fig.3 it shows the data that are transmitted from root to the slave terminal that is located at the remote end via wireless medium.

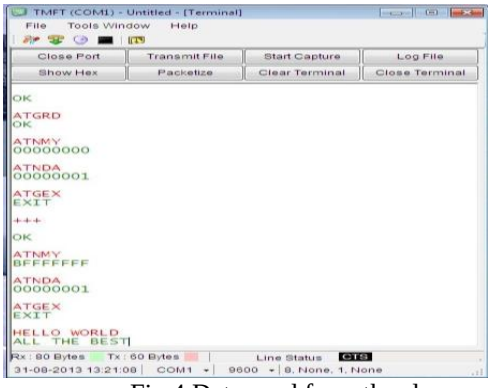

Fig.4 Data send from the slave

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

In Fig.4 it shows the data that are send and received from slave to the root terminal that is located at the remote end via wireless medium The Tarang F4 module starts with data mode and can be requested to move to AT command mode by sending an escape character sequence. Whenever two terminals are connected via modems the connection status is checked by means of using ”Query Modem”. If the connection between two terminals is achieved then the status is returned as “OK” else the error message is displayed. The conversion from data mode to escape mode is achieved by using ‘+++’. The default escape sequence to switch over to some other mode consists of three consecutive slash characters i.e.'///'. Pressing the refresh button on the Serial Port Adapter, when it is powered on, restores the default escape character sequence to set the source and destination address. After sending all commands the command mode is switched over to data mode for serial transmission using ATGEX. Generally AT is a prefix command and EX stands for exit operation. It may be possible to use n number of terminals in wireless network. For each and every terminals that are present in network have their own address and destination address in order to achieve secured transmission of data among their own dedicated channels. So congestion is reduced and also the transmission time is comparatively lower than previous transmission methods. Thus the Fountain Codes are a new class of codes designed for robust, resynchronized, and scalable transmission of information from multiple senders to multiple receivers in a reliable manner over computer networks. The hypothesis of Fountain Codes is very exciting, and also provides new imminent into the theory of parity check codes. New asynchronous multicast applications using Fountain Codes is utilized by software simulation and hardware implementation using Tarang F4 module

V. CONCLUSION

In this paper, the fountain codes are transmitted over the network by means of using relays as an intermediate and also to ensure secrecy cryptographic mechanism is used. The major advantage of using this is to transmit the packets without any packet loss by using the concept of segmentation and reassembly. Here the packets that are decided to transmit from the sender are segmented at the source level and it is transmitted via different relays.

And finally the segmented packets obtained from different relays are reassembled at the destination level. The resulting packets obtained at the receiver may be in different order due to delayed delivery of some relays. It can be sequentialized by the packet’s frame numbers attached by the sender. This fountain code technique combines application layer channel based on Luby Transform codes with multicast delivery of packets in a wireless networks. The main goal of this project is to achieve a realtime service with an high QOS level in a lossy vehicular network. Simulation results of LT codes provide the effeciency of our technique contrast with the traditional data propagation approach, and the concept of fountain codes is applicable in the hardwares like dish antennas, iphone, ipad and anrodid phones that are used in our day today life. So a hardware based coding theory is needed instead of software coding theory.

REFERENCES

[1] Srinath Puducheri, Jörg Kliewer, Senior Member, IEEE, and ThomasE. Fuja,Fellow, “TheDesign and Performance of Distributed LT Codes” IEEE transactions on information theory, vol. 53, no. 10, october 2007.

[2] V. Bioglio, M. Grangetto, R. Gaeta, and M. Sereno, “An optimal partial decoding algorithm for rateless codes”, in Proc. IEEE ISIT, pp. 2731-2735, July 2011.

[3] A. F. Molisch, N. B. Mehta, J. S. Yedidia, and J. Zhang, “Performance of fountain codes in collaborative relay networks,” IEEE Trans. Wireless Commun., vol. 6, no. 11, pp. 4108-4119, Nov. 2007.

[4] D. Sejdinovic, R. Piechocki, and A. Doufexi, _Note on systematic raptor design, in Proc.IEEE Winterschool on Coding and Information Theory, 2007, p. 31.

[5] P. Mohapatra, J. Li, and C. Gui, “QoS in mobile ad hoc networks,” IEEE Wireless Commun. , vol. 10, no. 3, pp. 44-52, June 2003.

[6] D. Sejdinovic, D. Vukobratovic, A. Doufexi, V.Senk, and R. Piechocki, Expanding window fountain codes for unequal error protection, IEEE Transactions on Communications, vol. 57, no. 9, pp. 2510_2516, 2009.

[7] D. Vukobratovic, V. Stankovic, D. Sejdinovic, L. Stankovic, and Z. Xiong, Scalable data multicast using expanding window fountain codes, in Proc. Allerton Conf. Comm., Control,and Computing, 2007.