IJETST- Volume||01||Issue||02||Pages 106-109||April 2014

Open access Journal International journal of Emerging Trends in Science and Technology

Error Free Cryptographic Secure Communication Using LDPC and Stopping Set Algorithm

Authors

Prof. Devendra.O.Shamkuwar
Dept of Information Technology, SPCOE (Otur)
E-Mail:- *Devendra8319@gmail.com*

Mrs. Kanchan Suresh Shinde
Dept. of information technology, SPCOE (Otur)
Sharadchandra Pawar College Of
Engineering,Dumberwadi (Otur)
Email: - *Kanchanshinde27@gmail.com*

Mr. Rameshwar.G.Wavhal
Dept of information technology,SPCOE (Otur)
E-mail:- *Wavhal1214@gmail.com*

Mr. Somnath.B.Nikam
Dept of information technology,SPCOE (Otur)
E-mail:-*Nikamsomnath1@gmail.com*

Mr. Somnath.R.Pande
Dept of information technology,SPCOE (Otur)
E-mail:-*spande27@gmail.com*

Abstract— In this paper we discuss how LDPC and Stopping set can be used in communication system design. In cryptographic secure communication we are transmitting data securely. LDPC algorithm implemented at sender side and stopping set algorithm are implemented receiver side to providing secure and error free communication. To make a strong security we are applying double encryption technique. LDPC algorithm protected under RSA algorithm. If hacker make modification in original data at that time that modified data can not received by the receiver. Whenever the eavesdropper attack on system and it has better channel Quality than the receiver at that time it difficult to receive original data or error free data. this security is achieved by using LDPC and stopping set algorithm.

Index Terms— Cryptography, LDPC, Stopping Set, Eavesdroppers.

I. INTRODUCTION

Coding for Cryptography using Stopping Sets are the technique to encrypt and decrypt the message to give high security to our data. Cryptography has been developed for the purpose to give security to data from unauthorized user. The module called as a Stopping Sets is introduced to decrypt the message for receiver. Many crypto systems in place today measure security computationally. If attacker attack on system at that time it is very difficult to identify it, due to that reason performance of system become low. To solve this complete security issue, we are applying different cryptographic strategies which will avoid attacker to modify the data and due to that reason receiver easily get the noise free data .We present a new enhanced cryptographic secrecy over a wide range of CSI parameters, and require no secret key. Using the LDPC & Stopping set algorithm we can maintain the Confidentiality of the data & correct data is received by receiver.

A] Main Contributions

The aim of these paper is to provide the complete security when the communication between two parties. They will maintain the confidentiality of data. To accomplish this goal we can use LDPC(Lower Density Parity Check) and Stopping Set algorithm. To achieve secure communication we are going to use encoding technique. While transferring of data from sender to receiver, if data get changed then question arises about the error free and accurate data for this solution is achieve in this paper.

II. Related Work

It has been shown by Shannon and others that a one-time pad can achieve perfect secrecy as a cryptographic encoding technique, meaning that knowing the codeword or encoded sequence gives no information on the value of the original message[1].

using theory and simulations for two different attacks that channel coding can be used to either increase the difficulty of the attack or make it very difficult to detect it, hence it will provide the better security at physical layer.[2]

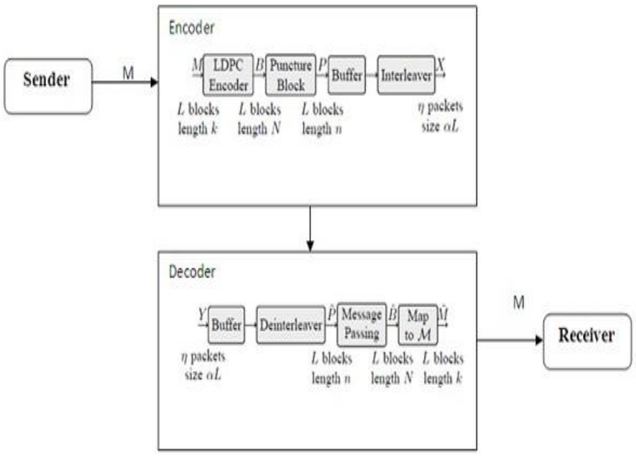
Traditional cryptography assumes an eavesdropper receives an error-free copy of the transmitted cipher text. Wieners wiretap channel model recognizes that at the physical layer both the intended receiver and the passive eavesdropper inevitably receive an error-prone version of the transmitted message which must be corrected prior to decryption.[3]

This paper considers the implications of using both channel and cryptographic codes under the wiretap channel model in a way that enhances the information theoretic security for the friendly parties by keeping the information transfer to the eavesdropper small. In previous paper the data is send by only bit by bit format but in this paper we can send the data in text format.

III. MAIN ALGORITHM

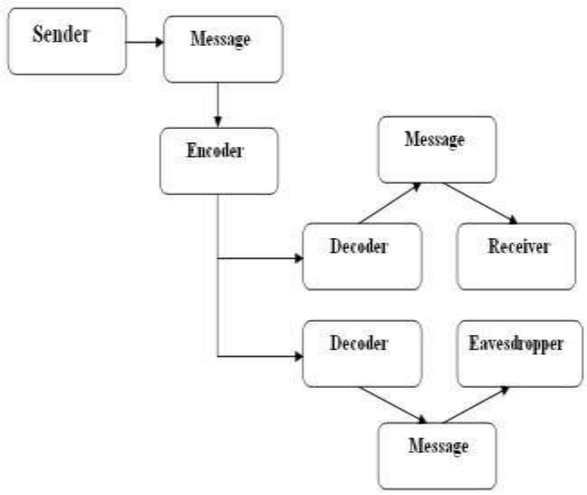
1. Start
2. Sending the message
3. Encode the message by LDPC encoder.
4. Transmit the message to the decoder.
5. if(message=error free) Message decode successfully ;Else
6. Acknowledgement to the sender
7. Transmit the message to receiver.
8. Repeat step 5.
9. Message hacked by the eavesdropper.
10. Captured message is in the form of binary.
11. LDPC cannot permit the eavesdropper.
12. Message transmitted successfully.
13. Stop

[6]IV. SYSTEM ARCHITECTURE



Sender send the message this message is given to the LDPC encoder. Bits of M(Message) are encoded using LDPC encoder. LDPC Encoder sends message to the puncture block. The error correction capabilities of the LDPC codes are restricted by intentional puncturing of encoded message. This message is stored in buffer memory. Message from encoded blocks are interleaved among several transmitted packets so that a single erased packet result in erasures in many encoded blocks of data. Deinterleaver will access the message stored in buffer. Deinterleaver is high speed compact design that is fully synchronous using a single clock. They decode the message. Then these message are mapped and these message are mapped according to the LDPC encoder. When the message is error free then it is received by the receiver.

[7]V.BLOCK DIAGRAM



SENDER:-Sender is used to send the message to the multiple clients. This message is passed to the multiple client .

ENCODER:- When the message is send by the sender then this message are encoded using encoder. Encoder use the LDPC algorithm to encode the message. LDPC is nothing but Lower Density Parity Check.

DECODER: - When the data is encoded then it is send to the multiple client but before the data is reached to the receiver it will be decoded using Stopping set algorithm by decoder.

RECEIVER:- When the data is encoded by the encoder then it will go to the multiple client. the receiver will accept this message & this message is decoded by the decoder. so the receiver will get the message in original format.

EAVESDROPPER:-When data is encoded by the encoder then it will send to the multiple client. The eavesdropper also try to hack this message but they will get the data in binary format. So they can not get the actual message & they do not understand what the actual message is.

5.1Defination and Assumptions

Let S be a system such that S be a encrypted communication channel where S= Message(M), Sender (X), Receiver (Y), Hacker (H), Key (K), Encrypted Message i.e. Ciphertext(C). Suppose sender(S) send message(M) to receiver (R) at that time attacker or hacker(H) modify the data due to that modification in the data there was security Problemis occurred or receiver do not receive original data or message. Therefore receiver not gets error free data. If sender sends data to receiver but in between communication attacker attack on data and loss the data, so sender not get acknowledgement not received at so we are have to implement concept of this acknowledgement technique. To solve security and confidentiality of message is achieve by using LDPC and stopping set.

IV. CONCLUSION

We have presented the process of secure data transmission from sender to receiver by using the two dynamic algorithm i.e. LDPC for encoder and STOPPING SET for decoder. These algorithm help us to establish a secure and error free communication between two entities. Also we have presented use of LDPC algorithm for error correction, and stopping set algorithm for decode the error free message. This process help us to keep the message content secret even if it is hack by the eavesdropper.

ACKNOWLEDGMENTS

We are thankful to SPCOE College for giving us an opportunity to complete the paper successfully. Also we are thankful to our guide prof. D.O.Shamkuwar for their kind co-operation in completion of this paper and giving us all possible help and suggestion to give our project a perfect shape.

Last but not least we have to express our feeling towards all staff members of SPCOE College (Otur) and special thanks to our college and friends for their moral support and help.

REFERENCES

[1] Stopping Set Distribution of LDPC Code Ensembles :Alon Orlitsky, Member, IEEE, Krishnamurthy Viswanathan, and Junan Zhang, Student Member,IEEE.March 2005

[2] Wireless Information-Theoretic Security. Matthieu Bloch, Student Member, IEEE, Joo Barros, Member, IEEE, Miguel R. D. Rodrigues, Member, IEEE, and Steven W. McLaughlin, Fellow, IEEE 2008.

[3] The Wiretap Channel with Feedback: Encryption over the Channel Lifeng Lai, Hesham El Gamal and H. Vincent Poor 2007.

[4] An Efficient Algorithm to Find All Small-Size Stopping Sets of Low-Density Parity-Check Matrices Eirik Rosnes, Member, IEEE, and yvind Ytrehus, Senior Member, IEEE 2009.

5]IRE TRANSACTIONS ON IFORMATION THEORY 21 Low-Density parity-Check Codes2005

6] Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes Hessam Mahdavifar, Student Member, IEEE, and Alexander Vardy, Fellow, IEEE 2011

7] Information-Theoretic Key Agreement: FromWeak to Strong Secrecy for Free Ueli Maurer and Stefan Wolf Computer Science Department, Swiss Federal Institute of Technology (ETH Zurich)

8]Physical-Layer security:Combining Error Control Coding and Cryptography Willie K Harrison and Steven W. McLaughlin IEEE 2008.

9] [Herbert Schild] The Complete Reference JAVA, Mc Graw Hill2007.

10] Jonathan Knudsen, Java Cryptography, Oreilly1998.

11] cryptography-network-security-5th-edition.