IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VIII (Feb. 2014), PP 81-87
www.iosrjournals.org

Enhancement of Cryptographic Security using Stopping Sets

Preeti L Darade[1], Vanaja R Chirchi[2] ,IEEE Memeber
[1](*PG student of Computer Network Engineering, MBES's College of Engineering, Ambajogai, Maharashtra, INDIA)*
[2](*Assistant Professor, PG Department of Computer Science of Engg, MBES's College of Engineering, Ambajogai, Maharashtra, INDIA)*

Abstract : *In this paper, we have used channel codes in cryptographic secrecy**.** Main idea of this paper is to develop the notion of combined security due to cryptography and channel coding. Thus, it is providing a more complete security solution. To achieve this goal, we cast coding into a cryptographic enhancement role, and seek to prevent an attacker from obtaining a noise free cryptogram using channel coding. In this paper, we have used degrees of freedom to characterize security which analyzes combined cryptographic and physical-layer security in a practical coding. In this scheme was shown to inflict a passive eavesdropper using a message-passing decoder with stopping sets with very high probability when a legitimate receiver and an eavesdropper view transmitted data through statistically independent packet erasure channels (PEC). The scheme relies on a nonsystematic low-density parity-check (LDPC) code design, with puncturing and interleaving steps in the encoder.*

Keywords: *Automatic repeat-request (ARQ), low-density parity-check (LDPC) codes, packet erasure channels(PEC), physical-layer security, stopping sets.*

I. INTRODUCTION

Low-density parity-check (LDPC) codes are a class of linear block LDPC codes. This name comes from the characteristic of their parity-check matrix which contains only a few 1's in comparison to the amount of 0's. Their main advantage is that they provide a performance which is very close to the capacity for a lot of different channels and linear time complex algorithms for decoding. Furthermore they are suited for implementations that make heavy use of parallelism.

1.1 Representations for LDPC codes:

Basically there are two different methods to represent LDPC codes. Like all linear block codes they can be described via matrices. The second one is a graphical representation.

1.1.1 Matrix Representation:

Let's look at an example for a low-density parity-check matrix first. The matrix defined in fig 1 is a parity check matrix with dimension n × m for a (8, 4) code.

We can now define two numbers describing this matrix. W_r for the number of 1's in each row and W_c for the columns. For a matrix to be called low-density the two conditions $W_c << n$ and $W_r << m$ must be satisfied. In order to do this, the parity check matrix should usually be very large, so the example matrix can't be really called low-density.

1.1.2 Graphical Representation:

Tanner introduced an effective graphical representation for LDPC codes. It provides graphs as a complete representation of the code. Tanner graphs are bipartite graphs. That means that the nodes of the graph are separated into two distinctive sets and edges are only connecting nodes of two different types. The two types of nodes in a Tanner graph are called variable nodes (v-nodes) and check nodes (c-nodes).

Figure 1 is an example for such a Tanner graph and represents the same code as the matrix in 1. The creation of such a graph is rather straight forward. It consists of m check nodes (the number of parity bits) and n variable nodes (the number of bits in a codeword). Check node f_i is connected to variable node c_j if the element h_{ij} of H is a 1.

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

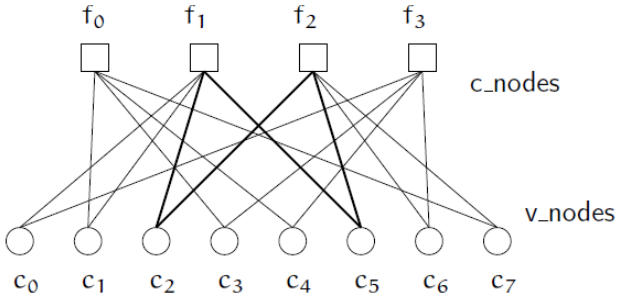

Fig 1. Tanner graph corresponding to the parity check matrix in H. The marked path c2 ->f1 -> c5 -> f2 -> c2 is an example for a short cycle. Those should usually be avoided since they are bad for decoding performance.

1.2 Cryptography and Physical-Layer Security:

Many cryptosystems in place today measure security computationally. If all known attacks are computationally intractable, then the system is deemed to be secure. The chief failings of this notion of security are the assumptions placed on the attacker. First, it is assumed that the attacker has limited resources to confront the problem, even if those resources are state-of-the-art. Second, it is assumed that the attacker uses attacks that are publicly known, even though a better attack may exist. Shannon addressed these shortcomings by defining the notion of perfect secrecy [1].

1.3 Stopping Set:

This system describes the security technique using Stopping Sets [1]. A stopping set is a subset S of the variable nodes such that every check node connected to S is connected to S at least twice. The empty set is a stopping set (trivially). The support set (i.e., the positions of 1's) of any codeword is a stopping set (parity condition). A stopping set need not be the support of a codeword.

1.3.1 Stopping Set Properties:

1. Every set of variable nodes contains a largest stopping set (since the union of stopping sets is also a stopping set).
2. The message-passing decoder needs a check node with at most one edge connected to an erasure to proceed.
3. So, if the remaining erasures form a stopping set, the decoder must stop.
4. Let *E* be the initial set of erasures. When the message-passing decoder stops, the remaining set of erasures is the largest stopping set *S* in *E*.
    - If S is empty, the codeword has been recovered.
    - If not, the decoder has failed.

II. SYSTEM MODEL

2.1 Existing System:

Practical designs maximizing the information-theoretic secrecy are not trivial. Most currently suffer from one or more of several drawbacks. Turbo codes were the early technique used for security, but it suffers from many drawbacks, to overcome all this drawbacks LDPC algorithm is used. Drawbacks decode complexity and relatively high latency, which make them unsuitable for some applications. For satellite use, this is not of great concern, since the transmission distance itself introduces latency due to the finite propagation speed. The decoding delay, the time it takes to decode the data, is a major drawback to turbo codes. The several iterations required by turbo decoding make the delay unacceptable for real-time voice communications and other applications that require instant data processing, like hard disk storage and optical transmission. It is affected by error floor. Most currently techniques suffer from one or more of several drawbacks. For instance, code designs are oftentimes a function of specific channel parameters (channel state information or CSI) seen by legitimate receivers and eavesdroppers. Without accurate CSI, the results of these systems are not guaranteed.

2.2 Proposed System:

This system describes the security technique using Stopping Sets [1]. Stopping sets are the misconceptions used to offer secrecy. The system provides with the three models one is the sender, receiver and hacker. When sender sends the message to receiver, firstly message is encoded in sender side using encoder i.e. LDPC encoder. Receiver must contain LDPC decoder to decrypt the valid message. In LDPC algorithm only three steps of security is provided. Messages are undergone by maximum likelihood, message passing and then by maximum likelihood Message is undergone firstly from puncturing and stopping sets is used to decrypt. Message passing is used to get the valid result but even after message passing original message in its valid form is not visible to the receiver. Maximum likelihood is used to retrieve the original message. Hacker cannot get the original message without LDPC algorithm. Maximum Likelihood does not provide high computation so maximum likelihood pivoting algorithm is used here. So the LDPC algorithm using Stopping sets provide complete security.

2.2.1 Modules:

1. LDPC codes and Stopping Sets.
2. Stopping Sets
3. Encode/decode Security Enhancements
4. Message-Passing Encoding/Decoding
5. Error-free cryptogram

2.2.2 Module Description:

1. LDPC codes and Stopping Sets:

Low-density parity-check (LDPC) codes and exploits the phenomenon of stopping sets to obtain security from the physical layer. This section provides limited background of LDPC codes and stopping sets in order to establish the foundation upon which to present our encoder. Decoding of an LDPC codeword over a BEC can be accomplished using maximum-likelihood (ML) decoding, by solving a system of equations. However, the iterative Message-passing (MP) decoder is commonly used due to its computational efficiency.

2. Stopping Sets

Our encoder makes use of fundamental practical design ideas which have been shown to offer secrecy. For example, our encoder employs nonsystematic LDPC codes in order to hide information bits and magnify coding errors. Secrecy properties of these codes have been studied in. We further employ intentional puncturing of encoded bits, a technique shown to offer security in. Our scheme punctures with the goal of inducing stopping sets in an eavesdropper's received data. As a result, every transmitted bit is crucial for decoding. Our intent is to punish an eavesdropper for every missing piece of information. Finally, in order to distribute erasures throughout the data set, the encoder interleaves coded bits among several transmitted packets.

3. Encode/decode Security Enhancements

Security analysis of the scheme given in by addressing the following points.

Encoder Description: End-to-end details of the encoder and decoder are provided, as well as simulation results which match theoretical expectations.
Optimization: Design criteria are specified to maximize the degrees of freedom in the maximum-likelihood attack as well as the message-passing attack. This involves comparison of irregular LDPC codes with regular LDPC codes.
Extensions: Security results are made general so as to apply to multiple receivers and multiple collaborative attackers. Ultimately, bounds on the increase in computational secrecy of an underlying cryptosystem are specified when the physical-layer encoding system is employed.

4. Message-Passing Encoding/Decoding

Encoder/decoder for legitimate users is simply the inverse of all encoder operations. A user can decode all data as long as every packet is received error-free. Legitimate users make use of the authenticated feedback channel to request retransmission of packets erased in the main channel during transmission.

5. Error-free cryptogram

The following principles are addressed in the design of this encoder.
1. Bits of M are hidden from immediate access in the decoded words using nonsystematic LDPC codes.
2. Scrambling prior to coding magnifies errors due to the physical layer of the communication system.

3. The error-correction capabilities of the LDPC code are restricted by intentional puncturing of encoded bits. (Bob obtains reliability through ARQ, rather than error correction.)

In this paper, we broaden the security analysis of the scheme from [7] by addressing the following points.

1) *Degrees of Freedom*: The system security is analyzed using the new metric. Computational secrecy is shown to grow exponentially with E[D] , which is also shown to be equal to H [X|Z] for the prescribed encoder.

2) *Encoder Description:* End-to-end details of the encoder and decoder are provided, as well as simulation results that match theoretical expectations.

3) *Optimization:* Design criteria are specified to maximize the degrees of freedom in maximum-likelihood (ML) and message-passing (MP) attacks over erasure channels.

4) *Extensions:* Security results aremade general so as to apply to multiple receivers and multiple collaborative attackers. Bounds on the expected increase in computational secrecy of an underlying cryptosystem are specified.

We begin by presenting the wiretap channel model with the addition of feedback in Figure 2. A user named Alice wishes to transmit an encrypted binary message $M=(m^1,m^2,\ldots m^L)$ to a legitimate receiver named Bob, where $m^i=(m^i1,m^i2\ldots,m^iK)$ belongs to M for i=1,2,…L. It will be helpful to think of M as being comprised of L blocks of length k, where k is the dimension of the encoder to follow. Let n be the block length of the encoder. Then the coding rate is k/n.

The fig. 2 explains how Alice sends the encrypted message to the Bob. Alice sends with the key to valid receiver i.e. is Bob. Bob sends Alice the feedback of message. This increases the security level of the message. Eavesdropper can receive only the invalid data.

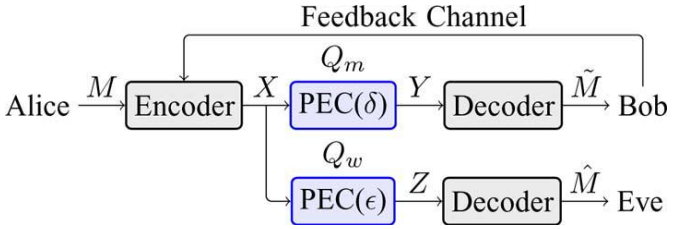

Fig 2. Wiretap channel model with feedback with PECs for both the main channel Q_m and the wiretap channel Q_w.

2.2.3 Message-passing decoding

The MP decoder is an iterative decoder based on the Tanner graph Gc. The decoder passes messages between U and V along the edges of Gc. One version of the decoder is given as Algorithm 1 The number of degrees of freedom in the MP decoder DMP is the cardinality of the smallest set of bit values that must be supplied to decode all remaining bits. If the decoder succeeds, then DMP=0. Clearly, this maintains the definition of degrees of freedom given in Definition 1 when restricted to this decoder, because any bit combination for these DMP bits decodes to a valid codeword, and each is equally likely to be correct. A bound on the decoder's correction capability is given by the following proposition.

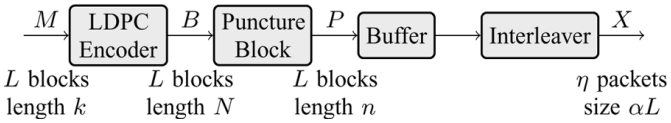

Fig 3. Detailed block diagram of the encoder. Number and size of blocks or packets are indicated at each step.

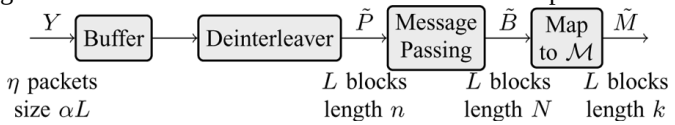

Fig 4. Detailed block diagram of Bob's decoder. Number and size of blocks or packets are indicated at each step.

III. ENCODER AND DECODER DESIGN

Each stage in the encoding or decoding process addresses one of the following principles.

1) Bits of M are hidden from immediate access in the decoded codewords using nonsystematic LDPC codes.

2) Scrambling before coding magnifies errors in the decoder.

3) The error-correction capabilities of the LDPC code are restricted by intentional puncturing of encoded bits. (Reliability for Bob is provided by ARQ rather than error correction.)

4) Bits from encoded blocks are interleaved throughout all packets so that an erased packet results in stopping sets in all codewords.

3.1 Encoding

1. Convert message into a character array
2. Embed Message into a dummy file
3. Create a byte array of length equal to size of input file
4. Open the input file read all bytes into byte Array
5. Convert the 32 bit input file size into 4 byte array
6. Embed 4 byte input File size array into the master file
7. Write the remaining bytes
8. Convert the 32 bit message size into 4 byte array
9. Embed 4 byte message size array into the master file
10. Embed the message
11. Data Sent to Receiver.

3.2 Decoding

1. Receive Data from Sender
2. Retrieve message size from data
3. Retrieve File size from data
4. Identify location of message
5. Retrieve message based on message size & file size from data.

3.3 Algorithm: - Message-Passing Decoder over the BEC

1: Initialize: For $y_i \neq e$, set $v_i = y_i$ and declare all such variable nodes as known.
2: if (No variable nodes are known and no check node has degree one) then
3: Output the (possibly partial) codeword and stop.
4: else
5: Delete all known variable nodes along with their adjacent edges.
6: end if
7: For each variable node vj connected to a degree one check node ui, declare vj as known and set vj = P k∈Ni,j vk.
Jump to 2.

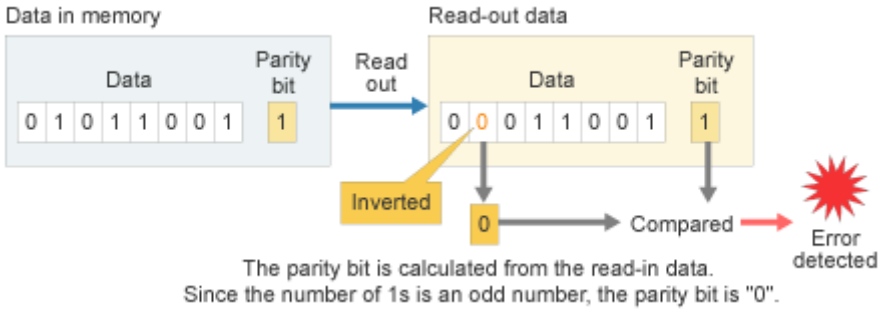

Fig. 5 Error correcting method

IV. RESULT

The final result of this system is complete security from eavesdropper. Message which are confidential are protected from their misuse. Final product gives complete privacy to messages or file transferred. If any eavesdropper attacks the messages still they won't b able to retrieve the original message. Hence complete safety of message and file is guaranteed. Feedback from the valid user is also given as the acknowledgment. Thus the product gives us complete survey of the security enhancement.

Simulations of the end-to-end encoder and decoder clearly indicate the expected bit-error rate of 0.5 in M^ for any incorrect guess in any of the D bits. The irregular LDPC code ensemble of Example with N=1000 and k=500 was used for these simulations. Puncturing patterns used were such that |R| >= 498 bits. Let be the number of the bits in Eve's guess that is incorrect. We offer simulation results for Y 1, 2, 3, 4, 5, 10, 15, 20, 25, 30, 40, 50, 60, 70, 80, 90, 100, 200, 300, and 400 in Fig. 6. Each Y value was tested 300 times on both theMP and ML decoder, while a new was generated every 10 experiments, and a new code from the ensemble was selected every 30 experiments. All tests produced error rates in between 0.414 and 0.578 in M^ , while the mean

depicted a 0.5002 bit-error rate with no noticeable difference between MP and ML decoders, or between values, as Fig. 6 indicates.

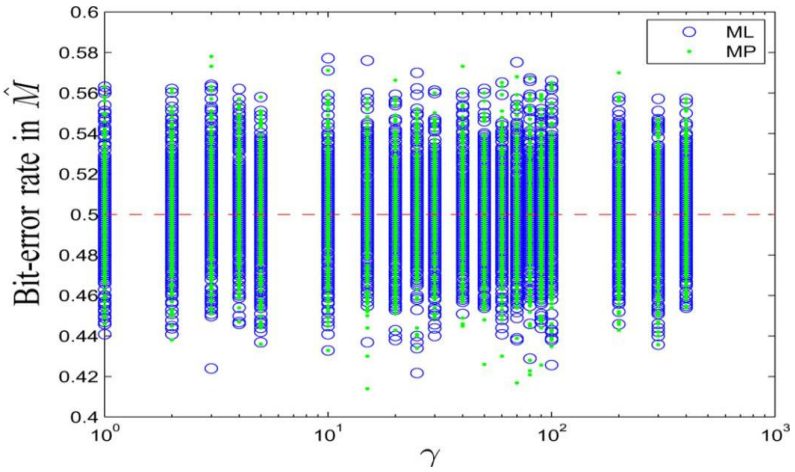

Fig. 6 Simulated bit-error rates in Eve's decoded cryptogram M when errors are made in guessing bit values for degrees of freedom in Eve's received codewords.

V. CONCLUSION AND FUTURE WORK

We have presented and analyzed a practical physical-layer coding scheme that provides cryptographic security enhancements using channel coding and ARQ. The system propagates errors to an expected bit-error rate of 0.5 in the cipher text.

As in this research study we investigated the best approach for improved cryptography. Both encryption and decryption is done with LDPC algorithm. It contains Channel state information .It gives Physical Level security. Provide security for data encryption. LDPC algorithm is the latest of all algorithms. It contains three level of data security so it overcomes the entire problem faced by existing encryption technique. Therefore the security metric of degrees of freedom D in an eavesdropper's received code words, and applied this metric to a physical-layer coding scheme to show cryptographic security enhancements due to channel coding. The iterative decoding approach is already used in turbo codes but the structure of LDPC codes give even better results. In many cases they allow a higher code rate and also a lower error floor rate. Furthermore they make it possible to implement parallelizable decoders. The main disadvantages are that encoders are somehow more complex and that the code length has to be rather long to yield good results.

ACKNOWLEDGEMENTS

I would like to thank to Prof. Mrs. Vanaja R Chirchi for giving me moral support to implement this paper and for providing all necessary help. Also I would like to thank Prof. Dr. Veeresh Kasabegoudar for their kind cooperation during this research work. I am thankful to MBES's College of Engineering, Ambajogai, Maharashtra for giving me an opportunity to complete the Paper successfully

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst.Tech. J., vol. 28, no. 4, pp. 656–715, 1949.
[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ.Press, Sep. 2011.
[5] W. Meier and O. Staffelbach, "*Fast correlation attacks on certain stream ciphers*," J. Cryptology, vol. 1, pp. 159–176, 1989.
[6] W. K. Harrison and S.W.McLaughlin, "*Physical-layer security: Combining error control coding and cryptography*," in Proc. IEEE Int. Conf. Communications (ICC), Dresden, Germany, Jun. 2009, pp. 1–5.
[7] W. K. Harrison, J. Almeida, D. Klinc, S.W. McLaughlin, and J. Barros, "*Stopping sets for physical-layer security*," in Proc. IEEE Information Theory Workshop (ITW), Dublin, Ireland, Aug.–Sep. 2010, pp. 1–5.
[8] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "*Applications of LDPC codes to the wiretap channel*," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[9] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "*Strong secrecy for erasure wiretap channels*," in Proc. IEEE Information Theory Workshop (ITW),Dublin, Ireland, Aug.–Sep. 2010, pp. 1–5.
[10] H. Mahdavifar and A. Vardy, "*Achieving the secrecy capacity of wiretap channels using polar codes*," IEEE Trans. Inf. Theory, submitted for publication.
[11] D. R. Stinson, Cryptography Theory and Practice, ser. Discrete Mathematics and Its Applications, K. H. Rosen, Ed., 3rd ed. Boca Raton, FL: Chapman & Hall/CRC Taylor & Francis Group, 2006.

[12] U. Maurer and S. Wolf, "*Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result*," IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 822–831, Apr. 2003.
[13] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
[14] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Hoboken, NJ: Wiley, 2005.
[15] T. Richardson and R. Urbanke, Modern Coding Theory. NewYork, NY: Cambridge Univ. Press, 2008.
[16] D. Burshtein and G. Miller, "*An efficient maximum-likelihood decoding of LDPC codes over the binary erasure channel*," IEEE Trans. Inf. Theory, vol. 50, no. 11, pp. 2837–2844, Nov. 2004.
[17] T. J. Richardson and R. L. Urbanke, "*Efficient encoding of low-density parity-check codes*," IEEE Trans. Inf. Theory, vol. 47, no. 2, pp. 638–656, Feb. 2001.
[18] T. K.Moon and W. C. Stirling, *Mathematical Methods and Algorithms for Signal Processing*. Upper Saddle River, NJ: Prentice-Hall, 2000, vol. 07458.

BIOGRAPHICAL NOTES

Preeti L Darade is pursuing M.E. in Computer Network Engineering from MBES's College of Engineering, Ambajogai, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. She has completed B.E. in Computer Science and Engineering from MBES's COE, Ambajogai, Dr. BAMU Universuty, Aurangabad, Maharashtra, India in 2010. Her research interest includes network-security and cryptography.

Vanaja R. Chirchi has received B.Tech & M.Tech in Computer Science & Engineering and pursuing Ph.D. from JNTU University, Hyderabad. Working as Assistant Professor , PG Department of CSE, MBES's College of Engineering, Ambajogai, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. Her research interest includes network-security, cryptography and Biometrics.