ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Reduction of Bit Error Rate Using Secured LDPC Crypto Coding

Kottapalli Sushma
Department of Electronics and Communication Engineering,
G. Narayanamma Institute of Technology and Sciences,
Hyderabad, Telangana - 500008, India.

Dr. B. Venkateshulu
Department of Electronics and Communication Engineering,
G. Narayanamma Institute of Technology and Sciences,
Hyderabad, Telangana - 500008, India.

Abstract

For the past many years secure and error free transmission of data has been great challenge in conventional communication system. Particularly, the data security has always been a major concern and a huge challenge for governments and individuals throughout the world since the early times. Recent advances in technology, such as cloud computing make it even bigger challenge to keep data secure. Traditionally the error correction and the data encryption in communication networks have been addressed independently. Over 30 years discussion has been carried out to perform error correction and encryption together. This conventional approach for achieving this purpose is inefficient because of complexity in calculations [1], [2], [3]. In this paper, the data security is achieved through AES (Advanced Encryption Standard) encryption technique and the error correction through LDPC(Low-Density Parity-Check) Codes. Both the encryption and encoder techniques use the same matrix as s-box and parity check matrix respectively. Also the decoding is performed through an algorithm of BP (Belief Propagation).

Keywords: ***AES (Advanced Encryption Standard), LDPC (Low-Density Parity-Check) Codes, BP (Belief Propagation).***

1. INTRODUCTION

To implement a typical wireless communication scheme that provides security to the data through Advanced Encryption Standards and the error free transmission through LDPC codes. In other words, a Joint Security as well as Advanced Low-density parity-check Coding (JSALC) is proposed. Both the AES technique and LDPC coding scheme share the same matrix, as substitution box and parity-check matrix respectively. This averts the calculations involved in fetching the parity-check matrices and hence retains the power efficiency. This is an enhanced method utilized for crypto-coding. In this technique, the security is provided by Advanced Encryption Standards (AES) method and the error correction is achieved from LDPC codes [4], [5], [6], [7]. The information to be transmitted is provided to the AES encryption block for transforming the plain message to cipher. It is then encoded by using traditional LDPC encoder before passing it through a channel. Later the message is fed into LDPC decoder which decodes it by utilising belief propagation. Ultimately this decoded error free information is decrypted by the AES decrypter block as shown in figure 1.

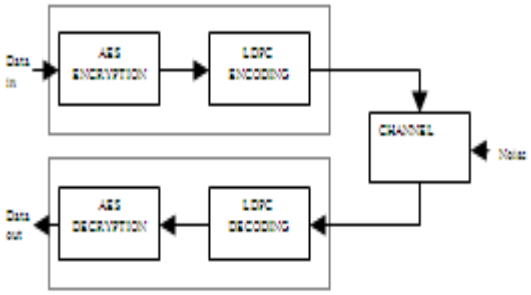

Figure 1 Conventional approach of encryption followed by encoding

Cite this article as: Kottapalli Sushma & Dr. B. Venkateshulu, "Reduction of Bit Error Rate Using Secured LDPC Crypto Coding", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 11, 2017, Page 76-79.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Every block in this process uses the same matrix as substitution box for encryption/decryption and as parity check matrix for encoding/decoding respectively. This will reduce the complexity involved in calculating separate matrices, because of which the power efficiency is retained if compared to the traditional systems.

The brief introduction of different important modules used in this project is discussed below:

i) AES

AES is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. AES does not use a Feistel structure. Instead, each full round consists of four separate functions: byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key.

The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST). AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. Evaluated to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is somewhat complex and cannot be explained as easily as many other cryptographic algorithms[8].

ii) LOW-DENSITY PARITY-CHECK

Low-density parity-check (LDPC) codes are forward error-correction codes, proposed in the 1962 PhD thesis of Gallager. At the time, their incredible potential remained undiscovered due to the computational demands of simulation in an era when vacumm tubes were only just being replaced by the first transistors. They remained largely neglected for over 35 years. In the mean time the field of forward error correction was dominated by highly structured algebraic block and convolutional codes. Despite the enormous practical success of these codes, their performance fell well short of the theoretically achievable limits set down by Shannon in his seminal 1948 paper. By the late 1980s, despite decades of attempts, researchers were largely resigned to this seemingly insurmountable theory–practice gap.

The relative quiescence of the coding field was utterly transformed by the introduction of "turbo codes," proposed by Berrou, Glavieux and Thitimajshima in 1993, wherein all the key ingredients of successful error correction codes were replaced: turbo codes involve very little algebra, employ iterative, distributed algorithms, focus on average (rather than worst-case) performance, and rely on soft (or probabilistic) information extracted from the channel. Overnight, the gap to the Shannon limit was all but eliminated, using decoders with manageable complexity.

As researchers struggled through the 1990s to understand just why turbo codes worked as well as they did, two researchers, McKay and Neal, introduced a new class of block codes designed to posses many of the features of the new turbo codes. It was soon recognized that these block codes were in fact a rediscovery of the LDPC codes developed years earlier by Gallager. Indeed, the algorithm used to decode turbo codes was subsequently shown to be a special case of the decoding algorithm for LDPC codes presented by Gallager so many years before.

New generalizations of Gallager's LDPC codes by a number of researchers including Luby, Mitzenmacher, Shokrollahi, Spielman, Richardson and Urbanke, produced new irregular LDPC codes which easily outperform the best turbo codes, as well as offering certain practical advantages and an arguably cleaner setup for theoretical results. Today, design techniques for LDPC codes exist which enable the construction of codes which approach the Shannon's capacity to within hundredths of a decibel.

So rapid has progress been in this area that coding theory today is in many ways unrecognizable from its state just a decade ago. In addition to the strong 3 theoretical interest in LDPC codes, such codes have already been adopted in satellite-based digital video broadcasting and long-haul optical communication standards, are highly likely to be adopted in the IEEE wireless local area network standard, and are under consideration for the long-term evolution of third generation mobile telephony[9].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

iii) Belief Propagation

The class of decoding algorithms used to decode LDPC codes are collectively termed message-passing algorithms since their operation can be explained by the passing of messages along the edges of a Tanner graph. Each Tanner graph node works in isolation, only having access to the information contained in the messages on the edges connected to it. The message-passing algorithms are also known as iterative decoding algorithms as the messages pass back and forward between the bit and check nodes iteratively until a result is achieved (or the process halted). Different message-passing algorithms are named for the type of messages passed or for the type of operation performed at the nodes.

In some algorithms, such as bit-flipping decoding, the messages are binary and in others, such as belief propagation decoding, the messages are probabilities which represent a level of belief about the value of the codeword bits. It is often convenient to represent probability values as log likelihood ratios, and when this is done belief propagation decoding is often called sum-product decoding since the use of log likelihood ratios allows the calculations at the bit and check nodes to be computed using sum and product operations[10].

2. IMPLEMENTATION:

The AES encryption is implemented by system simulation using MATLAB. Then the output is fed to the simulink block for error correction. Finally the error free output is decrypted using AES decryption using MATLAB. The figure 2 shows the implementation.

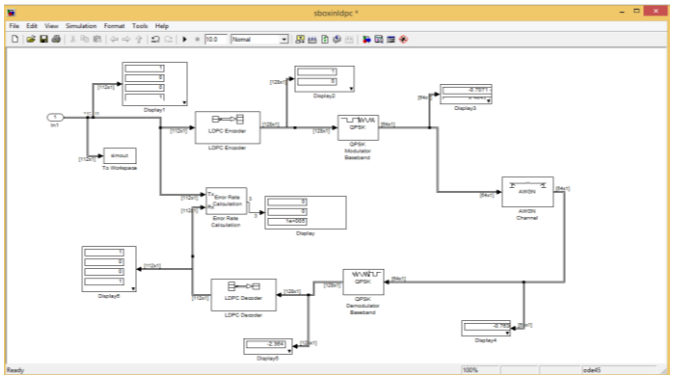

Figure 2 Implementation

This whole process is also be done by system simulation in MATLAB. The input to the encrypter will be an 128-bit binary data that is given in hexadecimal form. During the encryption the data is converted to decimal and binary at appropriate stages and finally encrypter outputs hexadecimal values. These hexadecimal value is converted to binary and fed to LDPC encoder. This binary data is encoded and transmitted over a channel and given to LDPC decoder. The decoder outputs the binary data which is converted to hexadecimal prior to the decryption. This hexadecimal value is again converted to decimal and binary at different stages of AES decryption. Ultimately the decrypted output will be in hexadecimal form.

3. RESULTS

SIMULINK RESULTS FOR 128 BIT INPUT DATA

Table 1 SNR values at zero errors for 128-bit input of joint AES and LDPC coding.

S.No.	Change in parameter (SNR value)	Error rate	Number of Errors
1.	SNR(dB) = 1	0.00023	23
2.	SNR(dB) = 2	3.999e-005	4
3.	SNR(dB) = 3	0	0
4.	SNR(dB) = 4	0	0
5.	SNR(dB) = 5	0	0

The tabulated values illustrates that, for a given 128 bit input data, the SNR value at which no error occurs is as low as 3dB. Hence the BER is reduced at low SNR value for a joint AES encryption and LDPC error correcting system.

MATLAB RESULTS FOR 128 BIT INPUT DATA

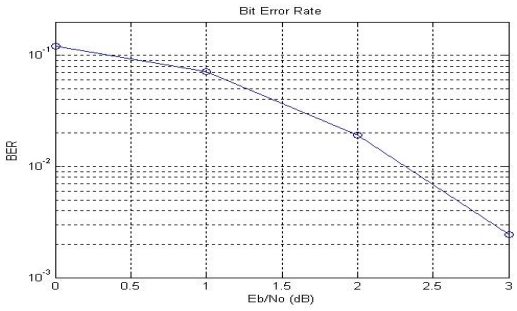

Figure 3 Graph showing change in Bit Error Rate

This graph is used to find out the bit error rate of the data frame after decoding is done. The bit error rate is measured with parameters signal to noise ratio versus the number of errors between the original data and the decoded data. After encoding and decoding the data with LDPC codes, the error rate reduces as the SNR value increases from three decibels.

4. ACKNOWLEDGEMENT

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

REFERENCES

[1] C P Gupta, S Gautam, "Joint AES Encryption and LDPC Coding," International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[2] Eran Pisek, Shadi Abu-Surra, Rakesh Taori, James Dunham, Dinesh Rajan, "Enhanced Cryptocoding: Joint Security and Advanced Dual-Step Quasi-Cyclic LDPC Coding," IEEE Global Communications Conference, GLOBECOM, pp.1-7, 2015.

[3] G. Forney and D. Costello, "Channel coding: The road to channel capacity," Proceedings of the IEEE, vol. 95, no. 6, pp. 1150–1177, 2007.

[4] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, vol. 42-44, pp. 114–116, 1978.

[5] S. Kak, "Encryption and error-correction coding using d sequences," IEEE Transactions on Computers, vol. 100, no. 9, pp. 803–809, 1985.

[6] T. Hwang and T. Rao, "Secret error-correcting codes (secc)," in Advances in Cryptology-CRYPTO'88. Springer, 1990, pp. 540–563.

[7] D. Gligoroski, S. Knapskog, and S. Andova, "Cryptcoding-encryption and error correction coding in a single step," in Proceed-ings of International Conference on Security and Management. Citeseer, pp.1–7, 2006. (Conference proceedings)

[8] W Stallings,Cryptography and Network Security: Principles and Practice, 4th ed. Prentice-Hall Press, 2006. (Book Style)

[9] R G Gallager, "Low-density parity-check codes," Cambridge MA: MIT Press, 1963.

[10] A. Boudaoud, M. El Haroussi, E. Abdelmounim, "VHDL Design and FPGA Implementation of LDPC Decoder for High Data Rate," International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, 2017