Performance Analysis of Turbo Coding with AES for CCSDS Standard

Shajina.V
M.Tech student
Department of Electronics Engineering
Pondicherry University

P.Samundiswary
Assistant Professor
Department of Electronics Engineering
Pondicherry University

ABSTRACT
Turbo codes enable reliable communication over power-constrained communication channels at close to Shannon's limit. Further, the performance of the communication system is enhanced by incorporating security mechanism. Security is described as the process of minimizing the vulnerabilities of assets or resources. National Institute of Standards and Technology (NIST) chose Rijndael algorithm as Advanced Encryption Standard (AES) for security mechanism due to the enhanced security, performance efficiency, ease of implementation and flexibility. To ensure security and error correction together in the system, the encrypted data is given to the turbo encoder and at the receiver the data is decoded and decrypted back. Hence the system works well without much reduction in the bit error rate with the added advantage of security. In this paper, turbo coding with and without AES are simulated and Bit Error Rate (BER) analysis is done by varying SNR and number of iterations. The simulation is done using C.

General Terms
Channel coding, Turbo coding, Security, Algorithms

Key words
AES, Turbo coding, Max-log-MAP algorithm

1. INTRODUCTION
The purpose of a telemetry system is to convey measured information from a remotely located data generating source to users located in space or on Earth reliably and transparently. The task of channel coding is to encode the information sent over a communication channel in such a way that errors can be detected and/or corrected by the decoder while receiving the information in the presence of channel noise [1]. In addition, cryptography is the science of information and communication security, enabling the confidentiality of communication through an unsecured channel. It protects against unauthorized parties by preventing unauthorized alteration of use [2].

Turbo code is a very powerful error correcting technique, which enables reliable communication with BER close to Shannon limit [3]. It uses more bits of redundant data in order to achieve better reliability. The theoretical Maximum A posteriori Probability (MAP) algorithm is one of the decoding methods that is computationally complex and inaccurate estimation of the noise variance. The logarithmic version of the MAP algorithm [4] and the Soft Output Viterbi Algorithm (SOVA) are the practical decoding algorithms for implementation in real time systems. These algorithms are less sensitive to SNR mismatch and inaccurate estimation of the noise variance. SOVA has the least computational complexity and has the worst BER performance among these algorithms, while the Log- MAP algorithm [4] has the best BER performance equivalent to the MAP algorithm. However, it has the highest computational complexity.

Encryption uses a cryptographic system to transform a plaintext into a cipher text, using keys. The Advanced Encryption Standard (AES) is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard (DES) was found too weak because of its small key size and the technological advancements in processor power [5]. Fifteen algorithms were accepted in 1998 and based on public comments, the pool was reduced to five finalists in 1999. In October 2000, a slightly modified version of the Rijndael algorithm [6] is selected as the forthcoming standard out of these five algorithms. The algorithm is named as Rijndael based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen that is a Block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits [6].

In this paper, Max-Log-MAP algorithm is used for turbo decoding which is less complex than the Log-MAP algorithm but it performs very close to the Log-MAP algorithm. Further, AES is incorporated along with the turbo codes such that good error correction and security can be assured. Also BER performance is analysed. This paper is organized as follows; the block diagram is explained in section2.The turbo coding with optimized Max-Log-MAP decoding is explained in section 3. In Section 4, Rijndael algorithm for AES is explained. The analysis of the results is given in section 5. Finally, the work is concluded in section 6.

2. BLOCK DIAGRAM OF PROPOSED SYSTEM
Nowadays, there is a strong need of designing communication systems with excellent BER performance and high levels of privacy, especially in wireless communications. The transmission of encrypted information over a noisy channel presents an error propagation effect, which degrades the BER performance of the system. Here, combined error control coding and encryption schemes based on iteratively decoded error-control turbo codes and AES algorithm is developed. These make a given communication system with excellent BER performance and encryption capabilities. Figure 1 shows the basic block diagram of the work done in this paper.

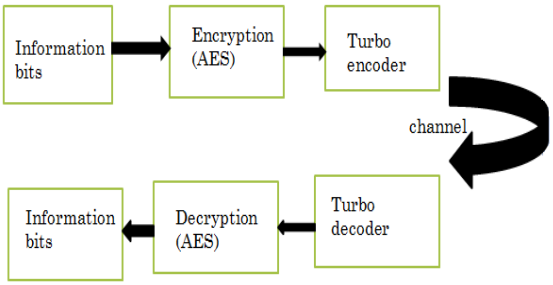

Figure 1: Block diagram

Information bits are generated according to the requirements. The data is taken as group of 128 bits and encrypted using a particular key as per AES specifying algorithm. The encrypted data is then given to the turbo encoder which generates parity bits for error correction purpose at the receiver. The encrypted information bits along with generated parity bits are transmitted under AWGN channel conditions. At the receiver, turbo decoder uses the memory optimized iterative max-log-MAP algorithm [7] for decoding .The decoded data is then decrypted using AES specified algorithm such that the information bits are recovered back correctly.

3. ADVANCED ENCRYPTION STANDARD

In 1998 Rijndael cipher is developed by the two Belgian cryptographers, John Daemen and Vincent Rijmen. This cipher was selected later on by the NIST as the Advanced Encryption Standard to supersede the old Data Encryption Standard. The NIST has published full details of AES under the Fedaral Institute of Publication Standard (FIPS) 197 [3]. The AES according to [5] has a constant block size of 128 bits (16 bytes) with 3 different key sizes of 128 bits, 192 bits and 256 bits, where 10, 12 and 14 encryption rounds will be applied for each key size, respectively. During the encryption and decryption processes, the 16 bytes of data will form a changeable (4*4) array called the state array. During the encryption process, the state array consists initially of the input data, this array will keep changing until reaching the final enciphered data. In the decryption process, the state array will start by the enciphered data and will keep changing until retrieving the original data. Each encryption round has 4 main steps, Shift Rows, Byte Substitution using the Substitution Box (S-BOX), Mix Columns, and Add Round Key. The decryption process consists of the inverse steps, where each decryption round consists of: Inverse Shift Rows, Byte Substitution using Inverse S-BOX, Add Round Key and Inverse Mix Columns[7]. The round keys will be generated using a unit called the key expansion unit. This unit will be generating 176,208 or 240 bytes of round keys depending on the size of the used key. Figure2 Shows the AES encryption and decryption processes.

As illustrated in Figure 2, the encryption and decryption processes start by adding the round key to the data. This round key is called the initial round key and it consists of the first 16 bytes of round keys in case of encryption and the last 16 bytes in case of decryption. The encryption iteration starts with the Shift Rows step, then the Bytes Substitution is applied, followed by the Mix Columns step, and finally the Round Key is added. In the decryption iteration the Round Key is obtained before the Inverse Mix Columns step. These iterations are repeated 9, 11 and 13 times for the key sizes 128,192 and 256 bits, respectively. The last encryption and decryption iterations exclude the Mix column and Inverse Mix column steps [8].

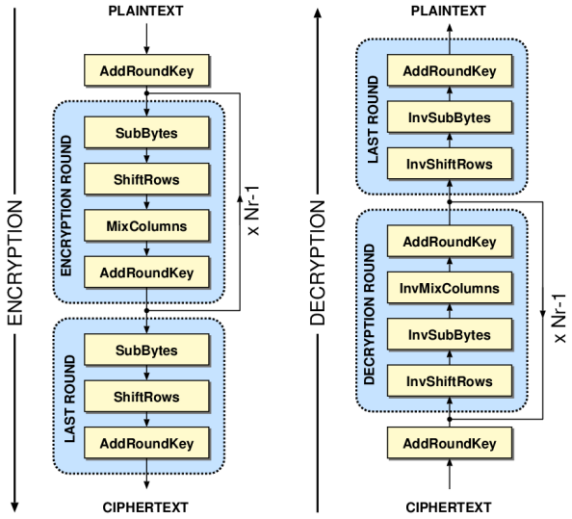

Figure 2: AES encryption and decryption process

4. TURBO CODING

A turbo encoder is a combination of two simple encoders. The input is a frame of K information bits. The two component encoders generate parity symbols from two simple recursive convolutional codes, each with a small number of states. The information bits are also sent uncoded. A key feature of turbo codes is an interleaver, which permutes bit-wise the original K information bits before input to the second encoder [9].Figure 3 shows the block diagram of CCSDS specified turbo encoder.

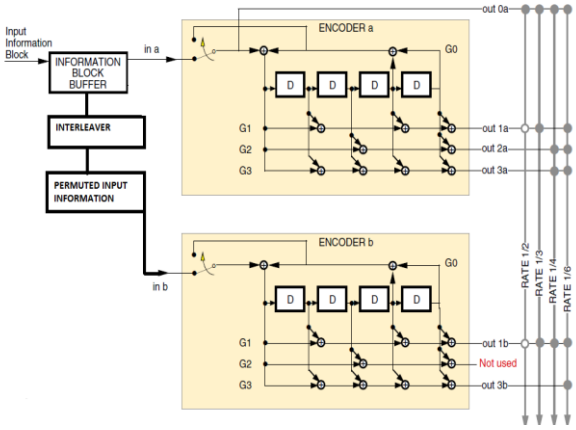

Figure 3: Turbo encoder block diagram

Turbo decoder uses an iterative decoding algorithm based on simple decoders individually matched to the two simple constituent codes. Each constituent decoder makes likelihood estimates derived initially without using any received parity symbols not encoded by its corresponding constituent encoder. Figure 4 shows the block diagram of turbo decoder.

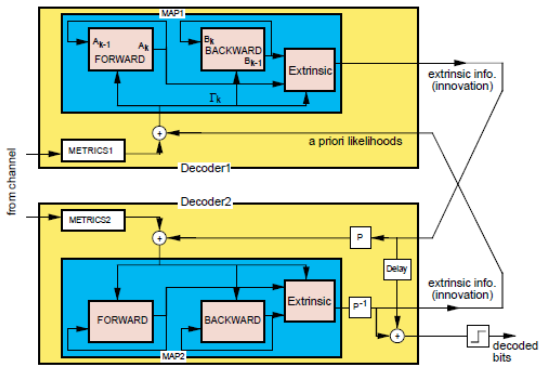

Figure 4: Turbo decoder block diagram

The received uncoded information symbols are available to both decoders for making these estimates. Each decoder sends its likelihood estimates to the other decoder, and uses the corresponding estimates from the other decoder to determine new likelihoods by extracting the 'extrinsic information' contained in the other decoder's estimates based on the parity symbols available only to it. The turbo decoder iterates between the outputs of the two constituent decoders until reaching satisfactory convergence. The final output is a hard quantized version of the likelihood estimates of either of the decoders [10].

Max-log-MAP algorithm is divided into four computational tasks;

- Branch matrix generation
- Forward matrix generation
- Backward matrix generation
- Generation of soft or hard bit estimate together with extrinsic information.

Here, it uses the memory optimized algorithm in which only forward matrices is stored; all the other matrices are calculated as and when required. This requires twice the calculation of branch matrices; even then memory requirement is less. For space application, memory requirement is one of the main constraints.

5. SIMULATION RESULTS

The encryption and turbo coding is applied to ensure security and error correction of the communication system. As specified by CCSDS standard, the turbo coder is simulated with a block size of 1784 and rate of 1/3. And 128 bit key is used for the encryption. The BER using turbo coding without encryption is calculated. Then it is compared with BER values obtained by appending AES with turbo coding.

Table 1 shows the number of bit positions with error and BER analysis of turbo coding only. Initially 13 bit positions were found to be error after single iteration. The error correction performance improves with the increase in number of iterations. After 9th iteration the complete errors are corrected.

Table 1: BER analysis using turbo coding only

No. of iterations	No. of bit positions with error	BER
1	13	0.007287
2	11	0.006166
3	10	0.005605
4	8	0.004484
5	6	0.003363
6	3	0.001682
7	2	0.001121
8	2	0.001121
9	0	0.000000

Table 2: BER performance with both AES and turbo Coding

No. of iterations	No. of bit positions with error	BER
1	494	0.276906
2	425	0.238229
3	408	0.228699
4	400	0.242152
5	327	0.183296
6	272	0.152466
7	139	0.077915
8	126	0.070628
9	0	0.000000

It is observed from table 2 that the number of bits with error is very high during initial iterations. But after 9th iteration it becomes zero.

BER performance is plotted against number of iterations which is illustrated in figure 5. It is inferred from the result that after 9th iteration, the BER is same for both the cases. i.e., there is no much degradation in BER performance even after appending encryption into turbo coded system.

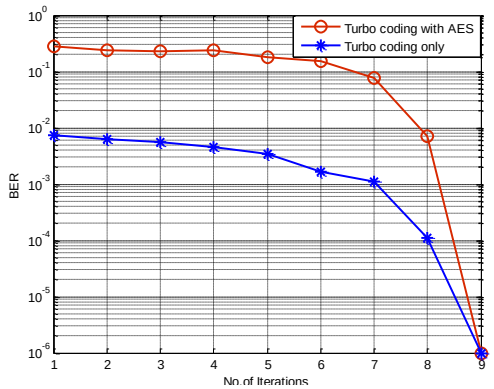

Figure 5: BER performance comparison with and without encryption for different iterations

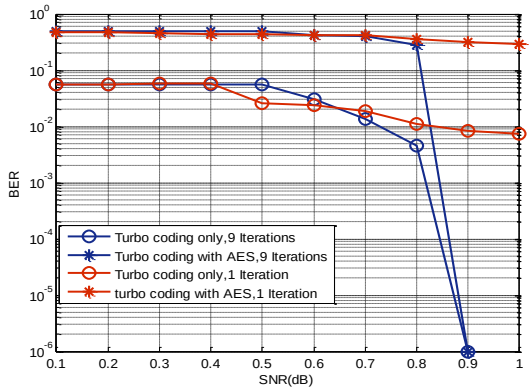

Figure 6: BER performance with different SNR and iterations

Further BER is calculated for different values of SNR by fixing the number of iterations and the plotted graph is shown in figure 6. It is inferred from the simulation results, when SNR is increased, BER is improved for both the cases. For low values of SNR, the BER performance of turbo coding without encryption is good, but when SNR is 0.9 dB, the BER performance converges for both the cases. It is also observed from figure 6 that during the first iteration, BER performance is not much good, but after 9^{th} iterations it performs well. A BER of 10^{-5}-10^{-6} is obtained at an SNR of 0.9 dB for 9^{th} iteration. Also it attains both security and error correcting capability by adding encryption along with the turbo coding.

6. CONCLUSION

A block length of 1784 bits is selected for incorporating AES with turbo coding for CCSDS standard. The encrypted data is given to turbo encoder and then the secured coded data is passed through the AWGN channel. Then the coded data is decoded and decrypted to retrieve the original data. Further, BER performance for different number of iterations and different SNR values are compared by using turbo coding only and turbo coding with AES. It is concluded from the results that turbo coding is performed well for the error correction using iterative decoding algorithm. Further, AES algorithm provides security without much degradation of BER performance.

7. REFERENCES

[1] Consultative Committee for Space Data Systems "Telemetry Channel Coding" Blue Book- 101.0-B-6., chapter 1, 2, 4, Oct.2002.

[2] Consultative Committee for Space Data Systems, "Encryption Algorithm-Trade Survey", Informational Report, CCSDS 350.2-g-1,Green book ,chapter 2,3,March 2008

[3] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes", Proceedings of International Conference on Communications, Geneve, pp. 1064–1070, May 1993.

[4] P. Robertson, P. Hoeher, and E. Villebrun, "Optimal and Sub-Optimal Maximum A Posteriori Algorithms Suitable for Turbo Decoding", European Transactions on Telecommunication, vol. 8, no. 2, pp. 1 19-126, March-April 1997.

[5] "Announcing the advanced encryption standard (AES), "Federal Information Processing Standards Publication 197", pp.5-47, November 2001.

[6] Joan Daemen, Vincent Rijmen, "AES proposal: Rijndael", AES proposal, pp.1-45, April 2003.

[7] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal, vol. 6, no. 2, pp.1-14, 2010.

[8] J. Nechvatal et al., "Report on the Development of the Advanced Encryption Standard (AES)," J. Research US Nat'l Inst. Standards and Technology, vol. 106, no. 3, pp. 511–576, 2001.

[9] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," IEEE Transactions on Information Theory, vol. 42, pp. 409–428, March 1996.

[10] R. Bahl and J. Cocke and F. Jelinek and J. Raviv, "Optimal Decoding of Linear Codes for Minimising Symbol Error Rate," IEEE Transactions on Information Theory, vol. 20, pp. 284–287, March 1974.