Method to Improve Channel Coding Using Cryptography

Ayyaz Mahmood

***Abstract*—**A new approach for the improvement of coding gain in channel coding using Advanced Encryption Standard (AES) and Maximum A Posteriori (MAP) algorithm is proposed. This new approach uses the avalanche effect of block cipher algorithm AES and soft output values of MAP decoding algorithm. The performance of proposed approach is evaluated in the presence of Additive White Gaussian Noise (AWGN). For the verification of proposed approach, computer simulation results are included.

***Keywords*—**Advanced Encryption Standard (AES), Avalanche Effect, Maximum A Posteriori (MAP), Soft Input Decryption (SID).

I. Introduction

THE need to minimize the effect of noise in our increasingly digital world on the entire digital communication system (i.e. transmission from source to destination) is becomingly increasingly pertinent. This effect can be mitigated by the use of error control coding [1]; the addition of redundancy that is utilized to correct or detect errors but to the extent delineated by the theoretical limit known as *Shannon limit*. Cryptography on the other hand is primarily used for secure communications. The main goals of modern cryptography are normally considered as data confidentiality, data authentication (data integrity and data origin authentication), user authentication and non-repudiation.

In this paper, cryptography is used to improve channel decoding and a new method is presented by using the avalanche effect [2] of block cipher algorithms and soft output of Maximum A Posteriori (MAP) decoding algorithm. The MAP [3] decoder initially received very little attention because of its increased complexity over alternative decoders. The reason was its minimal advantage in bit-error rate performance over other decoding algorithms. In the last few years, MAP decoder has enjoyed a new and greatly increased attention as an iterative soft-output decoder for turbo codes [4]. Other soft output algorithms have also been proposed notably Soft Output Viterbi Algorithm (SOVA) [5]. In [6], [7], it was shown that MAP can also be used for soft input decryption.

Fig. 1 shows block diagram of a typical communication system. The channel decoding using this type of arrangement is usually referred to as hard decision decoding.

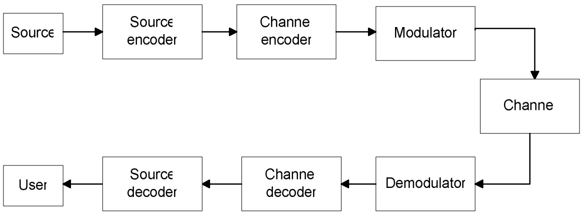

Fig. 1 Block diagram of a digital communication system

A more efficient decoding approach is to combine the demodulation and decoding functions, i.e. to pass the output of the channel directly to the decoder. In this scheme, called *soft decision decoding*, the decoder has access to more information about the transmitted data and, therefore better performance is achieved [8]. Soft decision decoding is used in the new proposed method, so the input of channel decoder is soft values.

The paper is organized as follows. In Section II, a digital error correction system based on convolutional encoder, binary phase shift keying (BPSK), Additive White Gaussian Noise (AWGN), and Maximum A Posteriori (MAP) algorithm is presented. In Section III, Advanced Encryption Standard (AES) is used to improve the bit-error rate performance of the digital system described in Section II and a new method is presented for this purpose. In Section IV, simulation results are presented and discussed. The paper ends with a brief conclusion in Section V.

II. Error Correction Using Maximum A Posteriori (Map) Algorithm

Fig. 2 shows a digital error correction system with Modulator (BPSK), Convolutional encoder, Demodulator and MAP decoder in the presence of Additive White Gaussian Noise (AWGN). In this chapter, an error correction system is presented using MAP decoding. The simulation results will be shown in Section IV considering a non-systematic (2, 1, 3) convolutional encoder and a non-systematic (4, 1, 3) convolutional encoder [1]. These two encoders were selected because they have the same coding gain and the similar structure, which enables fair comparison of decoding results. The convolutional encoder accepts data consisting of a block of 128 bits. The bit 0 is mapped into the signal “+1”, while the signal “-1” is sent for a binary value 1 [9].

Ayyaz Mahmood is with the Department of Electrical Engineering and Computer Science, The University of Siegen, Siegen, Germany (e-mail: mahmood.ayyaz@uni-siegen.de).

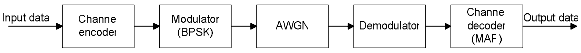

Fig. 2 Error correction system using MAP decoding

A. Selection of Noise Variance

In error control coding, k input bits yield n output bits, where $n > k$. If E_b is energy per bit of the uncoded bits, E_c energy per bit of the coded bits, $\gamma = E_b / N_0$ the desired signal to noise ratio and R a rate of the convolutional encoder. Then AWGN has variance $\sigma^2 = E_c / 2R\gamma$ and zero mean value [10].

B. MAP Decoder

In order to decode the data received from the channel, MAP decoder [10] is used. The object of MAP decoder is to calculate the probability information or "soft output". These soft output values are also known as L-values or reliability values which are used in the next chapter for improving the bit-error rate performance in combination with cryptography. The sign of L-value is the hard decision of the transmitted data and the magnitude of L-value is the reliability of this decision.

III. Error Correction Improvement Using MAP Algorithm and Cryptography

Fig. 3 shows the proposed error correction improvement scheme. The two blocks which are named as first block and second block are actually responsible for error correction improvement. The second block comes into operation in the case that first block is not able to do error correction.

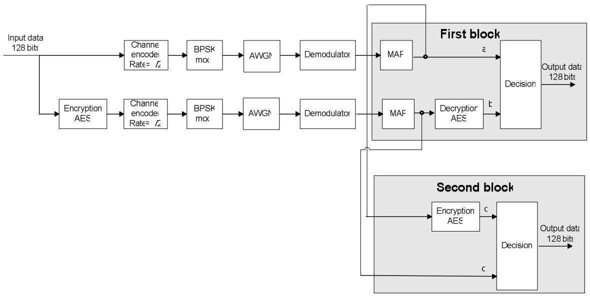

Fig. 3 A rate 1/4 error correction scheme using cryptography

Scheme in Fig. 3 (ignoring second block) includes 3 new blocks when it is compared with Fig. 2: encryption, decryption and decision. The decision block is included for taking decision between two inputs 'a' and 'b' applied to it. The decision block selects only one input which has the minimum number of errors.

In this paper, avalanche effect of block cipher algorithms and L-values of MAP decoder are used for error correction. First block and the second block receive data from both branches and perform error correction (if possible) to give the estimated output data. The new purposed technique has been developed using block cipher algorithm AES [11].

A. Advanced Encryption Standard (AES)

The AES is a symmetric key (uses same key for encryption and decryption) block encryption algorithm. It has been analyzed extensively and is used worldwide now as its predecessor, the Data Encryption Standard (DES) [12]. The AES block size is 128 bits and that is the reason for using a block of 128 input data bits in the simulations. The key sizes for AES can be either 128,192, or 256 bits. The key size is not important for this work because AES is used for error correction purpose instead of security. Every key defines a different codebook, mapping each plaintext value to a unique ciphertext values. The AES can be used in different modes of operation [13].

B. Modes of Operation

In cryptography, a block cipher operates on block of fixed length, often 64 or 128 bits. In order to encrypt a message of arbitrary length, several modes of operation have been invented with different secrecy and error recovery properties. Electronic codebook (ECB) mode is the simplest mode of operation and is used in our simulations. In ECB mode, message is split into fixed blocks and each is encrypted separately. Therefore one block of plaintext always produces the same block of ciphtertext. The disadvantage of ECB mode is that if cryptanalysts learn that the block "8d226acd" encrypts to the ciphertext block "1c7ed351", they can immediately decrypt that ciphertext whenever it appears in a message. The other commonly used modes are cipher block chaining (CBC), cipher feedback (CFB) mode, output feedback (OFB) mode, and counter (CTR) mode.

C. Description of Error Correction Improvement Technique

Fig. 3 shows that in case of first block, decryption is used in lower branch because the input data was encrypted. The decision block will compare the outputs 'a' and 'b' and will do error correction. If the first block is not able to perform error correction, second block comes into operation. In second block, the outputs 'c' and 'd' are encrypted data. These outputs 'c' and 'd' will also be compared to perform error correction in the case that upper block is not able to do it .

D. Error correction improvement considering first block

The two outputs 'a' and 'b' applied to decision block have the following possibilities:

1) Both are error free.
2) Both have errors.
3) The output 'a' applied to decision block is error free whereas the output 'b' applied to decision block has about 50% errors (avalanche effect).
4) The output 'b' is error free whereas the output 'a' has errors.

The decision block will be able to improve error correction considering all of the above possibilities. The output 'b' in lower branch exhibits avalanche effect because of the use of AES. It means that if MAP decoder in lower branch is not able to correct all errors, then the output ‘b’ will have about 50% errors. The output ‘a’ in upper branch will have significantly smaller number of errors as compared to the output ‘b’. Therefore decision block will always compare output ‘a’ and output ‘b’ to check if this difference is above a certain value. This value depends upon the signal to noise ratio and is named threshold. The decision block calculates a value which is called BER_compare for each iteration. It is calculated as a difference between BER of the output ‘a’ and BER of the output ‘b’. If BER_compare for each iteration is higher than the threshold, then the output ‘b’ in lower branch has about 50% errors. In this case SID [6], [7] is used for achieving error free output ‘b’ (if SID is successful). If BER_compare is lower than the threshold, then the output ‘b’ is error free; the decision block will select the output ‘b’.

E. Soft Input Decryption (SID)

The soft input decryption [6], [7] is a technique which is able to correct all errors occurring after decryption in lower branch. It uses soft output values of the channel decoder. The SID corrects all errors (if it is successful) in lower branch by taking the upper branch as reference. As the magnitude of L-value gives the reliability of the decision, it can be used to correct all erroneous bits in lower branch. First of all, absolute L-values of MAP decoder in lower branch are taken and arranged in ascending order because the L-value having lowest magnitude has more probability of being incorrect. Then first eight values are selected for error correction. The selection of eight values means SID will have 256 attempts for error correction. In each attempt, a bit or a combination of bits is flipped (0 to 1 or 1 to 0) and then decryption is performed. For each attempt BER_compare is calculated and compared with the threshold until it becomes less than the threshold. When BER_compare is less than the threshold, the errors at output ‘b’ in lower branch are totally corrected. The decision block will then select the output ‘b’ because it is error free. It can also happen that within 256 attempts, SID is not successful. In that case second block comes into operation.

F. Error Correction Improvement Considering Second Block

If soft input decryption is not able to correct errors in the first block, the second block attempts to achieve it. In the case of second block, upper branch is encrypted after MAP decoder, so avalanche effect will be present in upper branch at output ‘c’. The decision block will therefore treat output ‘c’ exactly like output ‘b’ and output ‘d’ exactly like output ‘a’ . The error correction can be done in the same way as it was performed for the first block. Instead of SID, second block performs soft input encryption. If BER_compare is higher than threshold, the lowest L-values will be flipped at the input of encryption block until all errors are corrected (if soft input encryption is successful).

IV. Simulation Results and Discussion

It is explained in the previous chapter that improvement in error correction can be achieved using soft input decryption which depends on the threshold. Therefore a curve is simulated in Matlab as shown in Fig. 4. It can be seen from this curve that threshold depends upon E_b / N_0. The curve shows that threshold decreases with the increase of E_b / N_0. The reason is that with the increase of E_b / N_0, the channel introduces lesser errors.

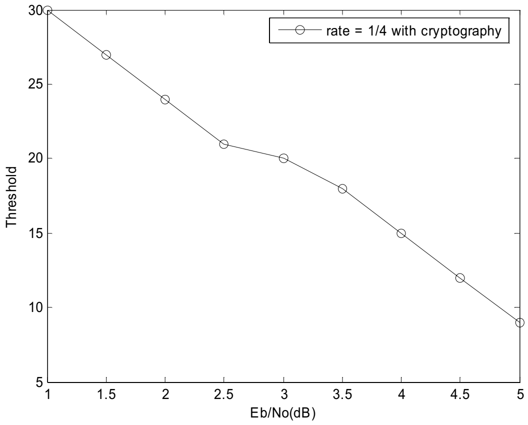

Fig. 4 Threshold versus E_b / N_0 for error correction system using cryptography

The error correction system described in Section II and error correction system using the new technique explained in Section III are simulated using Matlab. The signal to noise ratio is varied from 1dB to 5dB. The proposed system shown in Fig. 3 has an overall rate of 1/4 because both of the convolutional encoders used in this system are of rate 1/2. This system is then compared with an error correction system shown in Fig. 2 having a convolutional encoder of rate 1/2 and a convolutional encoder of rate 1/4. This comparison is shown in Fig. 4.

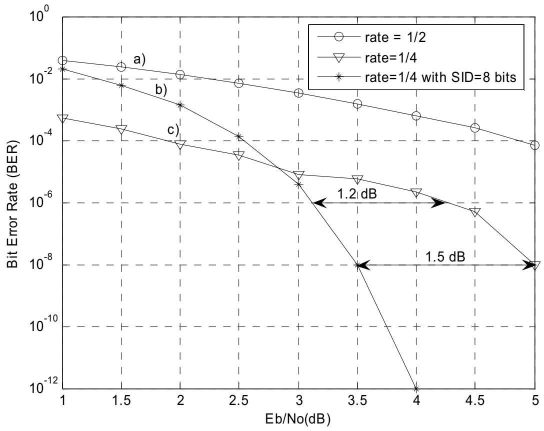

Fig. 5 BER versus E_b / N_0 for error correction systems with and without cryptography

a) Error correction system using rate 1/2 convolutional encoder for the system shown in Fig. 2.

b) Error correction system with improvement using two 1/2 rate convolutional encoders shown in Fig. 3.

c) Error correction system using a rate 1/4 convolutional encoder for the system shown in Fig. 2.

Fig. 5 shows that the error correction system using cryptography exhibits considerable coding gain of 1.5 dB and 1.2 dB over error correction system without cryptography. The reference points for these coding gains are at bit error rates of 10^{-8} and 10^{-6} respectively. Furthermore, it can be observed that the proposed system achieves better performance at about 3 dB and higher values of E_b / N_0.

V. Conclusion

A new decoding structure is purposed in this paper which uses cryptographic algorithm Advanced Encryption Standard (AES) for error correction purpose. The simulation results show that better performance in channel coding can be achieved using soft output of channel decoders and avalanche effect of block ciphers at about 3dB or higher values of signal to noise ratio. This improvement is done using eight soft output values of MAP decoder. The coding gain can be improved further if the number of soft output values for error correction is more than eight bits.

Acknowledgment

The author wishes to thank his colleague Zivic Natasa for providing simulation results for error correction system of rate 1/4 convolutional encoder without cryptography used in this paper. The author also gratefully acknowledges for the motivating discussion and suggestions provided by her.

References

[1] S. Lin and D. J. Costello, Jr., *Error Control Coding*. New Jersey: Prentice-Hall, 2004.

[2] Fernandez-Gomez. S, Rodriquez-Andina. J. J, Mandado. E, "Concurrent error detection in block ciphers," in *Proc. IEEE Int. Test Conf,* Atlantic City, NJ, pp. 979-984, 2000.

[3] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inf. Theory*, vol. 20, pp. 284-287, Mar. 1974.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. IEEE ICC'93*, Geneva, Switzerland, vol. 2, pp.1064-1070, May 1993.

[5] J. Hagenauer and P. Hoeher, "A Viterbi algorithm with soft-decision outputs and its applications," in *Conf. Rec. GLOBECOM 89*, Dallas, TX, vol. 3, Nov.1989, pp. 47.1.1- 47.1.7.

[6] N. Zivic, C. Ruland, "Soft input decryption," *4th Turbocode Conference, 6th Source and Channel Coding Conference, VDE/IEEE,* Munich, April , 2006.

[7] N. Zivic, C. Ruland, "Feedback in joint channel coding and cryptography," *7th Source and Channel Coding Conference, VDE/IEEE,* Ulm, Jan, 2008.

[8] M. R. Soleymani, Y. Gao and U. Vilaipornsawai, *Turbo Coding for Satellite and Wireless Commuications*. Boston: Kluwer Academic Publishers, 2002.

[9] S. Riedel, "MAP decoding of convolutional codes using reciprocal dual codes," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1176-1187, May 1998.

[10] T. K. Moon, *Error correcting coding.* New Jersey: Wiley, 2005.

[11] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing Standard FIPS PUB 197, November 26, 2001.

[12] FIPS 46, "Data Encryption Standard," Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

[13] FIPS 81, "Operational Modes of DES," Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.