TRANSMISSION OF ENCRYPTED MESSAGES OVER COMPOUND-ERROR CHANNELS

Ahmed Elosmany*

ABSTRACT

When transmitting encrypted messages over a noisy insecure communication channel, they are influenced by the existence of both random and burst errors so that an unacceptable incorrect text is obtained after decryption. To combat the effects of these compound errors, both error-control coding and interleaving are applied. System performance is calculated to evaluate the improvement obtained when applying these techniques.

I. INTRODUCTION

Cryptography is applied for protecting information transmitted through ground communications networks, communication satellites, and microwave facilities [1]. Its two principal objectives are *secrecy* (to prevent unauthorized disclosure of data) and *authenticity* (to prevent unauthorized modification of data) [2].

The transmission path (insecure communication channel) is assumed error-free [1] or may be represented by an additive white Gaussian noise (AWGN) channel [3]. When transmitting the encrypted messages over such a channel, the bit error rate is determined by the signal energy per bit-to-noise power density ratio, (E_b/N_o). For a fixed value of E_b/N_o, it is not possible to provide acceptable data quality (i.e., low enough error performance), and the practical solution available is to use *error-control coding*, also known as *channel coding* [4].

Error-control coding is accomplished by a channel encoder and a channel decoder. The channel encoder adds digits to the transmitted message digits [5]. These additional digits make it possible for the channel decoder to detect and correct errors. Thus, the error detection and/or correction lowers the overall probability of error. A linear block code with minimum distance d_{min} can correct up to R errors if

* Department of ACG, M. T. C

$$R \le [(d_{min}-1)/2]$$

where [x] denotes the largest integer not greater than x.

Many real communication channels exhibit a mixture of independent and burst errors. Such channels are called *compound-error channels*. In *telephone channels*, for example, bursts of errors result from impulse noise on circuits due to lightning, and transients in central office switching equipment [4]. In *radio channels*, bursts of errors are produced by atmospherics, multipath fading, and interference from other users of the frequency band.

An effective method to apply coding on a burst-error channel is to use *interleaving*. With this method, the channel is effectively transformed into an independent-error channel for which many forward-error correction coding techniques are applicable. In the transmitter, an encoder is followed by an *interleaver* which scrambles the encoded data stream in a deterministic manner such that successive bits (or symbols) transmitted over the channel are separated as widely as possible. In the receiver, a *deinterleaver* unscrambles the received data so that the decoding operation may proceed properly. Whereas the original data passes through both interleaving and deinterleaving, the error bursts are processed by the deinterleaver only. Accordingly, after deinterleaving, error bursts that occur in the channel are spread out in the data sequence to be decoded, thereby spanning many code words. The combination of interleaving and forward-error correction thus provides an effective means of combating the effect of error bursts [4].

This paper is arranged as follows. In section II, we introduce the model of the system under discussion and present the mathematical analysis required for evaluating the system performance. Results are given and interpreted in section III. Finally, section IV summarizes the conclusions.

II. SYSTEM MODEL AND ANALYSIS

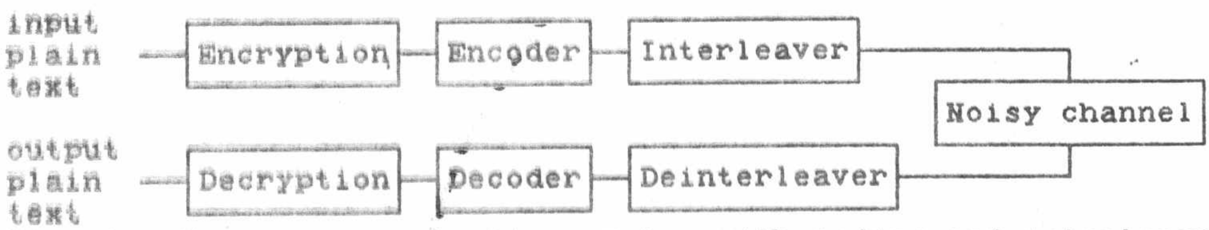

Fig. 1. Secure communication system with coding and interleaving

Consider the secure communication system of Fig. 1. In the transmitter part of this system, the input plaintext message is divided into blocks each of *M* bits. Each block is ciphered into an *M*-bit cipher using block encryption. The error-control encoder replaces each cipher block by its corresponding codeword of length *L* bits. We assume that the applied code is capable of correcting up to *R* errors.

Let us first transmit the encoder output directly through the noisy channel without any further processing. The plaintext message can be obtained *completely error-free* at the destination if not more than R errors occur in any of the transmitted blocks. If just one received block contains more than R errors, then the output plaintext message will not be an exact replica of the original plaintext message.

Let us now supply the encoder output to the interleaver before transmission through the noisy channel. The interleaver waits till the total message (consisting of K blocks) is stored, then starts its operation of rearranging the message bits in a specific way. The interleaver input can be viewed as a KxL matrix in which the i-th row (i = 1, 2, ..., K) stores the i-th codeword. The interleaver output, similarly, may be considered as an LxK matrix in which the j-th row (j = 1, 2, ..., L) contains only one bit from each row of the input matrix. Thus, each input block contributes to only one bit of each output block in the group of K blocks.

Let the output of the interleaver be sent through the noisy channel. The plaintext message will also be obtained *completely error-free* at the destination if not more than R errors occur in any block. However, in this case, we can get an error-free copy of the original message when having not more than R received blocks each with more than R erroneous bits. The reason is that the deinterleaver in the receiver will rearrange the group of L received blocks in a manner inverse to that done in the transmitter such that, in our case, each codeword at the output of the deinterleaver will contain not more than R bits in error. These errors will be corrected in the decoder. Thus, the decrypter receives *completely error-free* M-bit cipher blocks, and consequently produces the corresponding error-free plaintext message.

What about the quantitative improvement introduced by the encoder and the interleaver? Let P_{eb} denote the probability of a bit error during transmission due to channel noise. An L-bit block at the decoder input will be decoded correctly if it contains not more than R errors. Thus, the probability P_{ck} of correct decoding of an L-bit block is given by

$$P_{ck} = \sum_{i=0}^{R} \binom{L}{i} (1-P_{eb})^{L-i} (P_{eb})^{i}$$

where

$$\binom{L}{i} = L! \;/\; \{i! \;(L-i)!\}$$

The probability P_{ek} of erroneous decoding of an L-bit block (*i.e.*, more than R errors) is

$$P_{ek} = 1 - P_{ck}$$

As stated previously, the complete message (consisting of K blocks) will be obtained correctly when having not more than R blocks each with more than R bits in error. Thus, the probability

P_{cm} of correct reception of the message is given by

$$P_{cm} = \sum_{i=0}^{R} \binom{K}{i} (1-P_{eK})^{K-i} (P_{eK})^{i}$$

The probability P_{em} of erroneous reception of the message is

$$P_{em} = 1 - P_{cm}$$

What is the probability of erroneous reception of the message if we did not use coding and interleaving? This can be calculated as follows. The probability of having a correct block at the input of the decrypter is

$$P_{cK0} = (1-P_{eb})^{M}$$

and the probability that this block will be in error is

$$P_{eK0} = 1 - P_{cK0}$$

For a message with K blocks, the probability of correct message reception is

$$P_{cm0} = (1-P_{eK0})^{K}$$

and the probability of message error is

$$P_{em0} = 1 - P_{cm0}$$

III. RESULTS AND DISCUSSION

To evaluate the performance of the secure communication system shown in Fig. 1, we consider a message composed of K blocks each of M bits such that the total message length (KxM) is fixed. When plotting the logarithm of the message error probability versus the channel bit error probability for different block lengths, we get the graphs shown in Figs. 2-4. Fig. 2 shows the results for a system with encryption only, while Fig. 3 demonstrates the results when the system comprises encryption, coding (single-error correction), and interleaving. Fig. 4 depicts the results when the system has encryption, coding (double-error correction) and interleaving.

From Fig. 2, it can be seen that all graphs for M = 8, 16, 32, and 64 are coincident, thus, the performance is independent of block length. The message error probability P_{em} is higher than the bit error probability P_{eb} by at least 10 times over the considered range of values (10^{-6} to 10^{-1}) of P_{eb}. Decreasing the bit error probability by one order (for values in the range 10^{-6} to 10^{-3}) results in a decrease in the message error probability by only one order. At $P_{eb} = 10^{-3}$, we have $P_{em} = 0.4$. To get an acceptable value of the message error probability we need a very low value of the bit error probability (possibly can not be realized).

The influence of single-error correction coding and interleaving is evident from Fig. 3. A lower value of the block length gives a lower value of the message error probability. Decreasing the bit error probability by one order (for values in the range 10^{-6} to 10^{-2}) is seen to result in a decrease of the message error probability by four orders. At $P_{eb} = 10^{-3}$, we have $P_{em} = 10^{-4}$ to $6x10^{-6}$ depending on the block length.

When using a more powerful (double-error correcting) code we get the results shown in Fig. 4. As before, a lower value of the message error probability is obtained at a lower value of the block length. Decreasing the bit error probability by one order (for values in the range 10^{-6} to 10^{-2}) results in a decrease of the message error probability by at least eight orders (for block length $M = 16$ and higher). At $P_{eb} = 10^{-3}$ we have $P_{em} = 7x10^{-12}$ to $9x10^{-16}$ depending on the block length.

In Figs. 3 and 4, some curves appear incomplete for the lower values of the bit error probability . The reason is that the calculation of the message error probability at these values gave a zero value.

IV. CONCLUSIONS

Encryption is used to secure confidential data and messages from being exposed to or changed by unauthorized parties. When sending a ciphertext through a noisy channel, the probability of obtaining a message error after decryption at the receiver is so high (0.4 at $P_{eb} = 10^{-3}$).

Applying both error-correction coding and interleaving can improve the situation dramatically. Using a single-error correction coding and interleaving decreases the message error probability to 10^{-4} or less (at $P_{eb} = 10^{-3}$ for the considered message length) depending on the block length. A double-error correction code and interleaver can make the message error probability drop further to $7x10^{-12}$ or less depending on the block length (at $P_{eb} = 10^{-3}$ for the considered message length). The price paid for this advantage is the more complex circuitry and the lower information rate due to the added redundancy.

REFERENCES

[1] C.H. Meyer and S.M. Matyas, *Cryptography: A New Dimension in Computer Data Security*, John Wiley & Sons, Inc., 1982, ch. 1.

[2] D. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, 1982, ch. 1.

[3] G.B. Agnew, "Cryptographic Systems Using Redundancy," *IEEE Trans. Inf. Th.*, vol. 36, no. 1, pp. 31-39, Jan. 1990.

[4] S. Haykin, *Digital Communications*, John Wiley & Sons, Inc., 1988, ch. 8.

[5] K.S. Shanmugam, *Digital and Analog Communication Systems*, John Wiley & Sons, Inc., 1979, ch. 9.

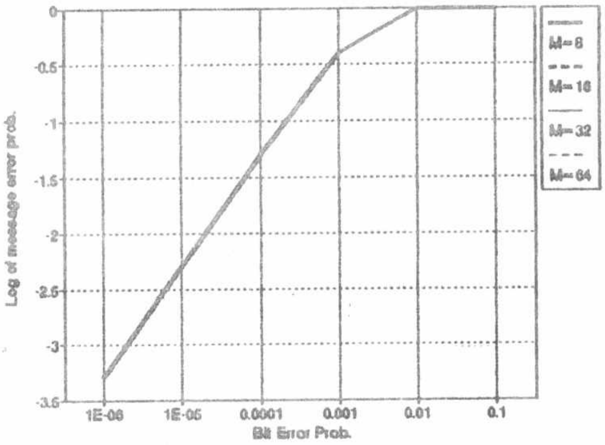

Fig. 2. Performance of a system with encryption only.

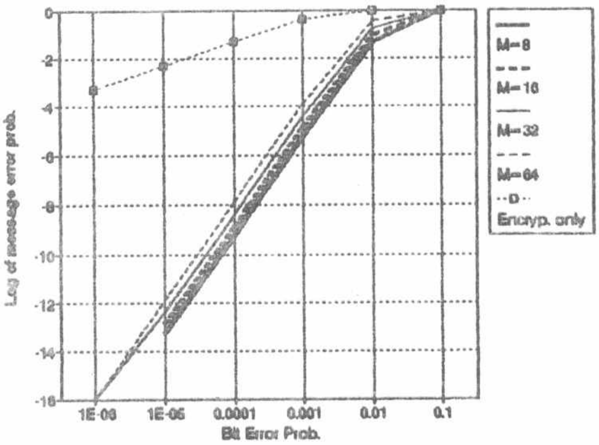

Fig. 3. Performance of a system with single-error correction.

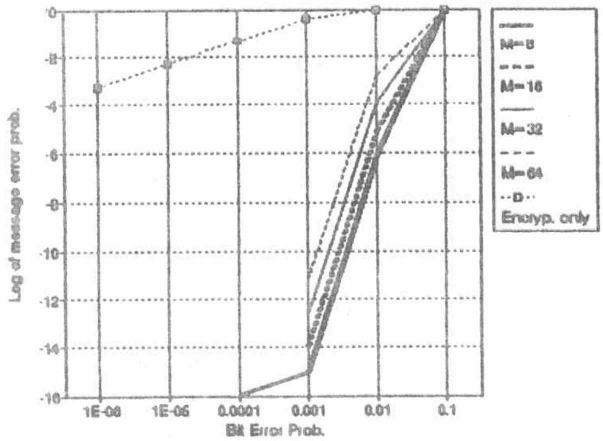

Fig. 4. Performance of a system with double-error correction.