SECURITY AND BER PERFORMANCE TRADE-OFF IN WIRELESS COMMUNICATION SYSTEMS APPLICATIONS

L. ARNONE†, C. GONZÁLEZ†, C. GAYOSO†, J. CASTIÑEIRA MOREIRA‡ and M. LIBERATORI‡

†Laboratorio de Componentes, U.N.M.D.P., J. B. Justo 4302, Mar del Plata, Argentina
learno@fi.mdp.edu.ar

‡Laboratorio de Comunicaciones, U.N.M.D.P., J. B. Justo 4302, Mar del Plata, Argentina
casti@fi.mdp.edu.ar

Abstract—There is nowadays a strong need of designing communications systems with excellent BER performance and high levels of privacy, specially in wireless networking and mobile communications.

The transmission of encrypted information over a noisy channel presents an error propagation effect, which degrades the BER performance of the system.

In this paper, we present combined error-control coding and encryption schemes based on iteratively decoded error-control codes like LDPC and turbo codes and AES algorithm. We show that the proposed schemes strongly reduce this degradation effect.

The increase of the level of privacy is obtained by using procedures of pseudo random nature over the encoders and decoders of the error-control code.

Thus, the proposed schemes provide a given communication system with excellent BER performance and encryption capabilities.

Keywords—Iteratively decoded error-control codes, AES algorithm.

I INTRODUCTION

In most of the modern communication applications, like wireless LAN, privacy and reliability of the transmission are both important aims of the design. Thus, most of the channels of practical interest are those for which good encryption properties and BER performance are joint important objectives to be achieved.

Regarding encryption and security properties, it is well known the reported attacks over the encryption technique implemented in the standard 802.11 for wireless LAN, called WEP (Wired Equivalent Privacy) protocol (Brown, 2003). This requires of the implementation of a better encryption technique. In this paper we propose a combined error control coding and encryption technique. For the encryption block, we have selected AES, witch is one of the most robust encryption techniques known nowadays (Daemen and Rijmen, 1999). However, this encryption technique produces an error propagation effect, so that, efficient error control coding techniques should be also applied to counteract this effect. We have found convenient to combine this encryption algorithm with some well known efficient error control techniques, like LDPC (Gallager, 1962; MacKay and Neal, 1997) and turbo codes (Berrou et al., 1993). The final result is the design of schemes with both good privacy capability and excellent BER performance.

In Section II we show that, depending on the value of the average bit energy-to-noise power spectral density ratio \( E_b/N_0 \) at which it is measured, the BER performance loss of the uncoded encrypted information transmission is from 1 to 5 dB, with respect to the uncoded and unencrypted transmission.

In Section III LDPC codes with parity check matrices \( H \) of size 128 \( \times \) 256 and 1280 \( \times \) 2560 are combined with the AES algorithm to show the improvement of the BER performance. In this Section we also propose some modifications based on pseudo random permutations over the structure of an LDPC code, to obtain an increase in the encryption capability of the scheme without degrading its BER performance. Section IV analyses the use of a turbo code combined with the AES algorithm. Section V presents a comparison of combined AES and efficient error control codes with respect to equivalent proposed schemes without AES. Finally, Section VI is devoted to the conclusions.

II AES ENCRYPTED UNCODED INFORMATION TRANSMISSION OVER THE AWGN CHANNEL

AES-128 (Daemen and Rijmen, 1999) is an iterative private-key symmetric block cipher that operates on a block of size \( L = 128 \) bits. The operations performed in the AES algorithm result into a non-linear transformation of the plaintext. In the case of the transmission over a noisy channel, this strong non-linearity produces an error propagation effect. Thus, few errors in a ciphered block of 128 bits result into a burst error event whose size is approximately equal to half of the