Adaptive secure channel coding based on punctured turbo codes

A. Payandeh, M. Ahmadian and M. Reza Aref

Abstract: Both security and error control coding are very extensive subjects, each with a variety of sub-disciplines. A secure channel coding (joint encryption-channel coding) scheme provides both data secrecy and data reliability in one process to combat problems in an insecure and unreliable channel. In this paper, an adaptive secure channel coding scheme based on serial or parallel concatenated turbo codes is developed. Recent results indicate that the turbo principle delivers near-to-optimal strategies for the channel coding. Reliability and security are achieved by adapting the pseudo-random puncturing strategy to the conditions of the noisy channel. Simulation results show the relevance and superior performance of the proposed scheme at all signal-to-noise ratio levels.

1 Introduction

Error control and security are both important aspects of modern digital communications. The demand for reliable, secure and efficient digital data transmission systems has been accelerated by the emergence of large-scale and high-speed communication networks. In 1948, Shannon [1, 2] demonstrated that errors induced by a noisy channel can be reduced to a desirable level by proper encoding of the information. Since Shannon's work, a great many developments have contributed towards achieving data reliability and the use of coding for error control has become an integral part in the design of modern communication systems and digital computers.

Forney [3] studied concatenated coding schemes as a class of codes whose probability of error decreased exponentially at the rate less than the capacity, while decoding complexity increased linearly. The process consists of a combination of two or more simple constituent encoders and interleavers. The parallel-concatenated convolutional code (PCCC) introduced in [4] has been shown to yield a remarkable coding gain close to the theoretical bound, yet admitting a relatively simple iterative decoding technique. The recently proposed serial concatenation of interleaved codes may offer superior performance to that of parallel concatenated codes [5]. In both coding schemes, the core of the iterative decoding structure is a soft-input soft-output (SISO) *a posteriori* probability (APP) module [6].

Merging security and channel coding processes is an attractive idea since it may reduce the overall processing cost of providing secure reliable data. A secret channel coding scheme is one that provides both data secrecy and data reliability in one process to combat with problems in an insecure and unreliable channel. Using error-correcting codes as cryptosystems was first introduced by McEliece [7], who suggested the use of a Goppa code as the underlying basis of an ingenious public-key scheme. The security of this scheme is based on the well known NP-completeness of the decoding problem for general linear codes [8] and the existence of a huge number of different Goppa codes with the same parameters. Some other public-key cryptosystems based on algebraic linear codes are proposed in [9–12]. It is well known that public-key cryptosystems can be used as private-key cryptosystems. Therefore, Rao and Nam [13] proposed to modify the McEliece scheme and subsequently introduced a new approach to the private-key algebraic coded cryptosystems requiring simple error-correcting codes. Hwang and Rao [14] then devised a class of private-key cryptosystems, called secret error-correcting codes. However, the problems of requiring large keys for security and existing doubts about the strength of the security in current schemes of combining security and error-correcting codes have not been solved yet.

In this paper, we propose a new adaptive secure channel coding scheme based on secret puncturing of a (parallel or serial) concatenated turbo code and adaptation with channel noise conditions. The advantages of our scheme are achieving good security without requiring a large size key, and improving the efficiency of a data transmission system by adaptation of coding rate with channel noise conditions.

2 Proposed scheme structure

A secure channel coding scheme is one that provides both data secrecy and data reliability in one process. Combining these two functions may give faster and more efficient implementation.

As a powerful coding technique, (parallel or serial) concatenated turbo codes have been proposed for any communication system where a significant energy saving is required or the operating signal-to-noise ratio is very low, such as in deep space and satellite communication systems. Performance of a turbo code depends on the selection of its component codes in addition to the interleaver structure.

IEE Proceedings online no. 20050086

doi:10.1049/ip-com:20050086

Paper first received 21st February and in final revised form 1st August 2005

A. Payandeh is with Department of Electrical Engineering, K.N. Toosi University of Technology and Applied Science Research Association (ASRA), Tehran, Iran

M. Ahmadian is with K.N. Toosi University of Technology, Tehran, Iran

M. Reza Aref is with Sharif University of Technology, Tehran, Iran

E-mail: a_payandeh@yahoo.com

The criteria for selection of component codes have been discussed in [5, 15] and several interleaver structures have been presented in [4, 16, 17]. A union bound to bit error probability for turbo codes was obtained in [18]. Since the 'error-floor' portion of the bit error probability curves is very time consuming in computer simulation, an estimated error-floor bound (free-distance asymptote) for the bit error probability over the additive white Gaussian noise (AWGN) channel may be considered as follows [19]

$$P_b(e) \geq \frac{N_{free} W_{free}}{K} Q\left(\sqrt{2 d_{free} R \frac{E_b}{N_0}}\right) \qquad (1)$$

where d_{free} is the free distance of the code, N_{free} is the number of code words with output weight d_{free}, W_{free} represents the weight of input sequence associated with output weight d_{free}, K is the input block length and R is the code rate.

As observed from (1), the bit error probability for a specific concatenated turbo code depends on code rate, transmission power and channel noise conditions. Therefore, for access to a given bit error probability with constant transmission power, the code rate must be varied in accordance with the channel noise level. We use an adaptive secure punctured turbo code whose puncturing rate can be varied in accordance with the channel noise level, so that the bit error probability is kept less than a pre-specified value.

Figure 1 displays our secure channel coding scheme. Each symbol of source output is first mapped to a binary sequence. A turbo encoder then takes a block U^K of information bits and delivers a block P^M of code bits, which are punctured to achieve the transmitted codeword X^N. The channel noise level is measured at the receiver and fed back to the transmitter synchronously. The transmitter uses this information to adjust its appropriate puncturing rate block-by-block. When the channel state is bad, the transmitter picks more redundant bits for protection. Therefore, the overall throughput is low. As the channel condition gets better, less redundancy is needed for protection. Hence, a higher throughput is achieved. The error rate of the channel will depend on the instantaneous receiver signal-to-noise ratio (SNR), the code rate, and the complexity of the channel code. The proposed puncturing scheme is based on the pseudo-random numbers generator algorithm for selecting N bits from M turbo encoded bits.

To study the security of the system, we need to determine, essentially, how difficult it will be for an eavesdropper who does not know the key of the pseudo-random numbers generator and intercepts X^N to detemine U^K. It appears that an eavesdropper has two basic attacks to try; first, to try to recover the key of the pseudo-random numbers generator from chosen known U^K and X^N pairs (chosen-plaintext attack). Second, they might recover U^K from X^N without knowing the key (ciphertext-only attack).

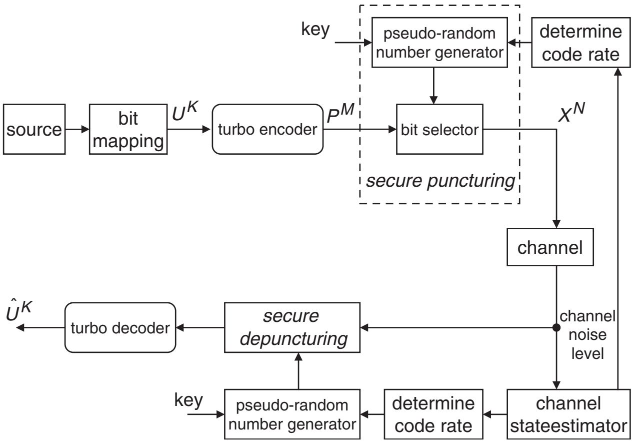

Fig. 1 *The proposed secure channel coding scheme*

The first attack seems to be hopeless if the structure of the pseudo-random numbers generator is nonlinear with a sufficiently large period, because there are so many possibilities for the key. In particular, suppose we choose a nonlinear feedback shift register of length $n = 100$, then there will be about $2^{2^n} = 2^{2^{100}}$ possible keys.

The second attack seems to be more promising but turbo decoding of a compressed block without knowing the puncturing pattern is the basic problem to be solved. This problem is NP-complete, hence it is expected that if the length of turbo encoded block P^M is sufficiently large, then this attack will also be unfeasible. Suppose we choose $M = 1000$ and $N = 400$, then there will be about $\begin{pmatrix} M \\ N \end{pmatrix} \cong \frac{\sqrt{2\pi M} M^M}{2\pi\sqrt{N(M-N)} N^N (M-N)^{M-N}} \cong 10^{292}$ possible puncturing patterns. For longer block lengths, the decoding process without knowing the puncturing pattern is even more complex.

3 Simulation results

To underline the effectiveness of the proposed secure channel coding scheme, we present a set of numerical results in this Section. A source block of a binary memoryless source is encoded using a rate 1/3 serially concatenated turbo code consisting of an outer 4-state recursive systematic convolutional code with $G_{outer}(D) = \left[1 \;\; \frac{1+D^2}{1+D+D^2}\right]$ and an inner 4-state recursive systematic convolutional code with $G_{inner}(D) = \begin{bmatrix} 1 & 0 & \frac{1+D^2}{1+D+D^2} \\ 0 & 1 & \frac{1+D}{1+D+D^2} \end{bmatrix}$ (Fig. 2). This serially concatenated turbo code has $d_{free} = 5$, $W_{free} = 2$ and $N_{free} = 3$ [4].

We processed 250 sequences, each sequence contains 2^{16} bits, from an i.i.d. source with uniform distribution. For simplicity, we use a 100-stage linear feedback shift register (LFSR) for the pseudo-random numbers generator. The BPSK-modulated punctured codeword with a fixed power is transmitted through an AWGN channel with variable noise variance. At the receiver, the depuncturing process is done with permutation of the symbols in the received block based on a secure key and substitution of zero values for punctured bits. Details of serially concatenated turbo decoding are explained in [5, 20].

Figure 3 shows the performance (code rate against E_b/N_0) of this secure serial concatenated turbo code for two pre-specified bit error probabilities $P_b(e) \cong 10^{-5}$ and $P_b(e) \cong 10^{-6}$. These curves have been obtained with a uniform interleaver of length 2048. Since the interleaver operates on coded sequences produced by the outer rate 1/2 encoder, its length of 2048 bits corresponds to a delay of $K = 1024$ information bits. It can be observed that the maximum code rate is about 0.84. As we can see from Fig. 4, the simulated bit error rate (BER) is approximately constant for different noise levels. We can change the BER value with changing the puncturing rate.

We demonstrate in Fig. 5 the results obtained for this secure punctured turbo code with different interleaving lengths 2×10^3, 2×10^4, 2×10^5 and 2×10^6 ($K = 10^3$, 10^{-4}, 10^5, 10^6), in terms of code rate against E_b/N_0 for a pre-

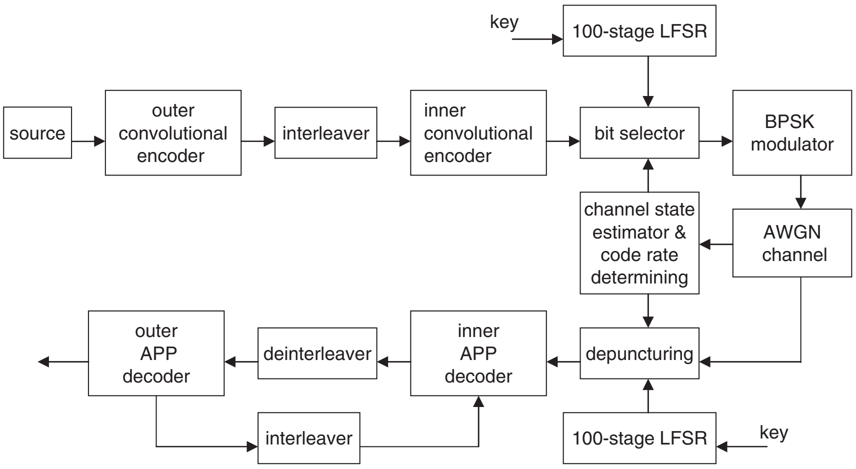

Fig. 2 *The simulated secure concatenated turbo coding system*

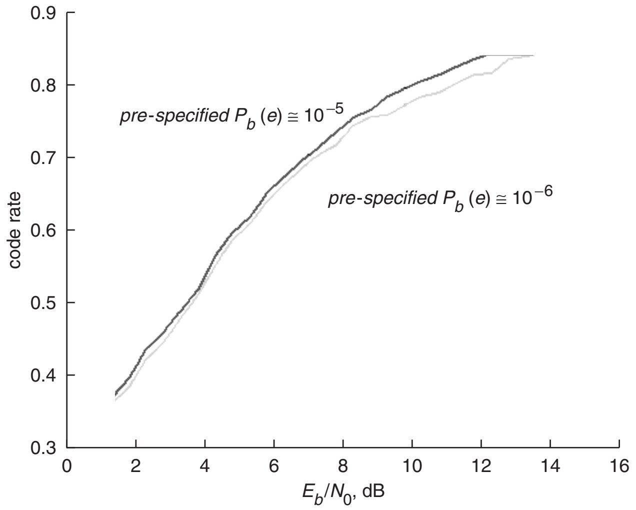

Fig. 3 *Code rate against E_b/N_0 for simulated secure serial concatenated code with interleaving length 2048*

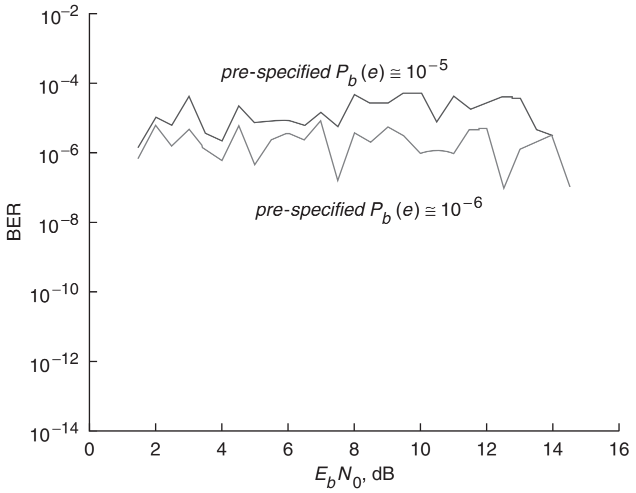

Fig. 4 *Performance (BER against E_b/N_0) obtained for simulated secure serial concatenated code with interleaving length 2048*

specified bit error probability $P_b(e) \cong 10^{-5}$. It is obvious that increasing the interleaving (input block) length results in a better performance. It is seen in Fig. 5 that for a fixed and sufficiently large E_b/N_0 (>12 dB), the code rate does not considerably change, when K increases from 10^4 to 10^6.

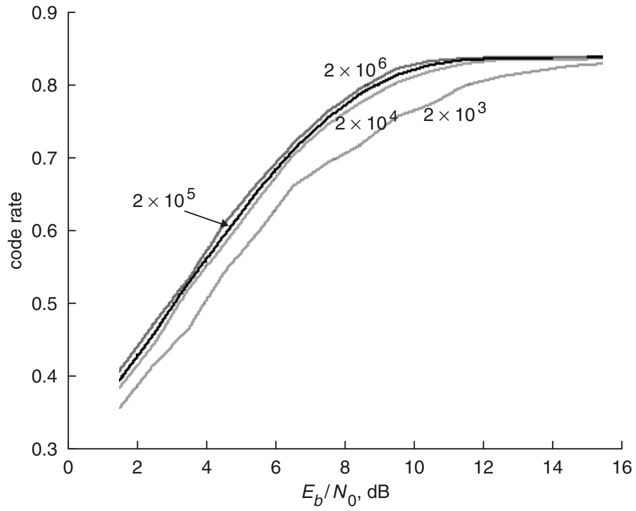

Fig. 5 *Code rate against E_b/N_0 for simulated secure serial concatenated code with different interleaving lengths and a pre-specified bit error probability $P_b(e) \cong 10^{-5}$*

4 Conclusion

A secure channel coding scheme combines data encoding with data encryption into one process. In this paper, an adaptive secure channel coding algorithm based on adaptive and pseudo-random puncturing of the concatenated turbo encoded block is presented. We investigated various crypto-analytical attacks against this scheme. Simulation results showed that we could obtain an efficient data transmission system with good reliability and security using this algorithm.

5 References

1 Shannon, C.E.: 'A mathematical theory of communication', *Bell Syst. Tech. J.*, 1948, **7**, pp. 379–423
2 Shannon, C.E.: 'A mathematical theory of communication', *Bell System Tech. J.*, 1948, **7**, pp. 623–656
3 Forney, G.D. Jr.: 'Concatenated Codes' (MIT Press, Cambridge, MA, 1966)
4 Berrou, C., Glavieux, A., and Thitimajshima, P.: 'Near Shannon limit error-correcting coding and decoding: turbo-codes'. Proc. ICC'93, Geneva, Switzerland, May 1993, pp. 1064–1070
5 Benedetto, S., Divsalar, D., Montorsi, G., and Pollara, F.: 'Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding', *IEEE Trans. Inf. Theory*, 1998, **44**, (3), pp. 909–926

6 Bahl, L.R., Cocke, J., Jelinek, F., and Raviv, J.: 'Optimal decoding of linear codes for minimizing symbol error rate', *IEEE Trans. Inf. Theory*, 1974, **IT-20**, pp. 284–287

7 McEliece, R.J.: 'A public-key cryptosystem based on algebraic coding theory'. JPL DSN Progress Rep., 1978, 42–44, pp. 114–116

8 Berlekamp, E.R., McEliece, R.J., and Van Tilborg, H.C.A.: 'On inherent intractability of certain coding problems', *IEEE Trans. Inf. Theory*, 1978, **IT-24**, pp. 384–386

9 Niederreiter, H.: 'Knapsack-type cryptosystems and algebraic coding theory', *Probl. Control Inf. Theory*, 1986, **15**, (2), pp. 159–166

10 Gabidulin, E.M.: 'Ideals over a non-commutative ring and their applications in cryptography', *Lect. Notes Comput. Sci.*, 1991, **547**, pp. 482–489

11 Gabidulin, E.M.: 'On public-key cryptosystems based on linear codes: efficiency and weakness' in 'codes and ciphers, Proc. 4th IMA Conference on cryptography and coding, 1993' (IMA Press, 1995)

12 Sidelnikov, V.M.: 'A public-key cryptosystem based on binary Reed-Muller codes', *Discrete Math. Appl.*, 1994, **4**, (3), pp. 191–207

13 Rao, T.R.N., and Nam, K.H.: 'A private-key algebraic-coded cryptosystem'. Proc. Crypto'86, Santa Barbara, California, USA, 1986, pp. 35–48

14 Hwang, T., and Rao, T.R.N.: 'Secret error-correcting codes (SECC)'. Proc. Crypto'88, Santa Barbara, California, USA, 1988, pp. 540–563

15 Divsalar, D., and Pollara, F.: 'On the design of turbo codes'. The Telecommunication and Data Acquisition Progress Report Jet Propulsion Laboratory, Nov. 1995, pp. 99–121

16 Berrou, C., and Glavieux, A.: 'Near optimum error correcting coding and decoding: turbo codes', *IEEE Trans. Commun.*, 1996, **44**, (10), pp. 1261–1271

17 Divsalar, D., and Pollara, F.: 'Multiple turbo codes for deep-space communication'. The Telecommunication and Data Acquisition Progress Report, Jet Propulsion Laboratory, May 1995, pp. 66–77

18 Divsalar, D., Dolinar, S., and McEliece, R.J.: 'Transfer function bounds on the performance of turbo codes'. Proc. IEEE Milcom'95, Aug. 1995, pp. 44–55

19 Perez, L.: 'Turbo codes' in Schlegel, C. (Ed.): 'Trellis coding' (IEEE Press, New York, 1997)

20 Benedetto, S., and Montorsi, G.: 'Iterative decoding of serially concatenated convolutional codes', *Electron. Lett.*, 1996, **32**, (13), pp. 1186–1187