Scientia Iranica, Vol. 13, No. 4, pp 373 378

SCIENTIA IRANICA

Research Note

An Adaptive Secure Channel Coding Scheme for Data Transmission over LEO Satellite Channels

A. Payandeh*, M. Ahmadian[1] and M.R. Aref[2]

Both secure 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, a joint encryption-channel coding scheme is developed, based on concatenated turbo codes for more efficient and secure transmission of LEO satellite data. Reliability and security are achieved by adapting the pseudo-random puncturing strategy with a change of distance between satellites and ground stations in the communication séance, an issue further burdened by reducing energy consumption or increasing bit rate of data transmission. Simulation results show the relevance and superior performance of the proposed scheme compared with the traditional data transmission system.

INTRODUCTION

Error control and security are both important aspects of modern digital communications and are often used together in one application. The demand for a reliable, secure and efficient digital data transmission system has been accelerated by the emergence of large-scale and high speed communication networks. In recent years, the use of small satellites in Low Earth Orbit (LEO) for remote sensing imagery has been extensive. Remote sensing imagery produces large amounts of data that often need to be secretly and reliably transmitted over a band-limited channel.

In 1948, Shannon [1] demonstrated that errors induced by a noisy channel can be reduced to a desired level by proper encoding of the information. Since Shannon's work, a great deal of developments have contributed toward achieving data transmission reliability, so that the use of error control coding has become an integral part in the design of modern communication systems and digital computers. Forney [2] studied concatenated coding schemes as a class of codes whose probability of error decreased exponentially at rates less than the capacity, while decoding complexity increased only algebraically. Parallel-concatenated convolutional codes (turbo codes) introduced in [3] obtained remarkable coding gains close to theoretical limits, yet admitting a relatively simple iterative decoding technique. The recently proposed serial concatenation of interleaved codes may offer a superior performance to that of parallel concatenated codes [4]. In both schemes, the core of the iterative decoding structure is a Soft-Input Soft-Output (SISO) A Posteriori Probability (APP) module [5].

Adding security to channel coding is an attractive topic, as it could reduce the overall processing cost of providing secure encoded data. A secret channel coding scheme is one that provides both data secrecy and data reliability in one process, to deal with problems in an insecure and unreliable channel. Using error-correcting codes as cryptosystems was introduced by McEliece [6]. The McEliece proposal was to use 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 [7] and the fact that there are a huge number of equivalent Goppa codes with a given set of parameters. Some other public-key cryptosystems, based on algebraic linear codes, are proposed in [8-11]. It is well-known that public-key cryptosystems can be used as private-key cryptosystems. Therefore, Rao and Nam [12] proposed a modification of the McEliece scheme and, subsequently, introduced

*. *Corresponding Author, Department of Electrical Engineering, K.N. Toosi University of Technology and Applied Science Research Association (ASRA), Tehran, I.R. Iran.*

1. *Department of Electrical Engineering, K.N. Toosi University of Technology, Tehran, I.R. Iran.*
2. *Department of Electrical Engineering, Sharif University of Technology, Tehran, I.R. Iran.*

a new approach to the private-key algebraic coded cryptosystems requiring simple error-correcting codes. Hwang and Rao [13] 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 security, in current schemes of combining security and error-correcting codes, have not yet been solved.

During data transmission between the LEO satellite and ground station, the distance may change. The LEO satellite data transmitting systems are normally designed for a pre-specified bit error probability, which leads to the worst case of a communications channel (maximum distance and worst environmental conditions). This pre-specified bit error probability is a requirement to achieve a desired image quality. The consequence of such design is a wasteful use of system resources. To overcome this problem, one can either save power by reducing the transmission level during favorable channel conditions or increasing the information throughput by transmitting at a higher rate. While adaptive power control is, at least conceptually, straightforward, adaptive rate control can be achieved by varying the bit rate, the coding rate, the modulation level, or any combination thereof. More advanced schemes were subsequently proposed, based on adaptation of the data transmission system, in accordance to environmental condition variations [14-17]. In [18], one method was presented, based on an adaptation of channel coding, with the distance between satellite and ground station in the communication zone.

In this paper, an adaptive secure channel coding (adaptive joint encryption-channel coding) scheme is proposed, based on secret puncturing of a (parallel or serial) concatenated code and adaptation with change of distance, to keep the bit error rate at a pre-specified level in the communication zone. The advantages of this scheme are: Achieving good security without requiring a large key and improving the efficiency of the data transmission system by adaptation of the coding rate with a change of distance.

The paper is organized as follows. In the following section, after a description of the problem statement, an adaptive joint encryption-channel coding algorithm for secure and efficient data transmission over LEO satellite channels, is proposed and its security level is discussed. Then, computer simulation results of the proposed scheme are given and finally, conclusions are drawn.

PROPOSED SCHEME STRUCTURE

Any communication link design between a satellite and a ground station must account for all power losses between transmitting and receiving nodes. Signal-to-Noise Ratio (SNR) in a ground receiver's input is calculated by [18]:

$$\mathrm{SNR} \cong P_{\mathrm{ST}_{dB}} + A + 20\log(\sin\beta) \quad \frac{B}{\sin\beta} \quad 10\log(\mathrm{BR}), \tag{1}$$

where P_{ST} is the satellite transmitter power, BR is the transmission bit rate, β is the elevation angle and A and B are constants, which depend on the environmental conditions and receiver specifications. Therefore, the received SNR for a specified communications system depends on the bit rate, transmission power, environmental conditions and distance (elevation angle). Let A and B be determined for the worst environmental conditions and assume that transmission rate and power are constants in the whole communication séance.

One can see from Equation 1, the distance between the satellite and ground station has a considerable effect on the performance (bit error rate) of the communication systems. In other words, the distance in LEO satellite configuration changes continuously. To access a desired image quality, a pre-specified bit error probability is enough. If bit error rate is less than a pre-specified value, the quality of the received image will improve, but this quality improvement, in practice, is not used. Therefore, designing the on-board data transmission system for the worst case of a channel, leads to a wasteful use of communication system resources. On the other hand, data confidentiality in satellite systems is usually an important issue. To overcome these problems, it is useful to use a combination of adaptive channel coding and encryption. Combining these two steps into one may result in faster and more efficient implementation. A secure channel coding scheme is one that provides both data secrecy and data reliability in one process.

As a powerful coding technique, (parallel or serial) concatenated codes have been proposed for any communication system where a significant power saving is required or the operating signal to noise ratio is very low, such as in deep space and satellite communication systems. Performance of turbo codes depends on the selection of component codes, as well as the interleaver structure. The criteria for selection of component codes have been discussed in [4,19] and several interleaver structures have been presented in [3,20,21]. A union bound of bit error probability for turbo codes was obtained in [22]. Since the "error-floor" portion of the Bit Error Rate (BER) curves is very time consuming to simulate, an estimated error-floor bound (free-distance asymptote) for the BER, over Additive White Gaussian Noise (AWGN) channels, is given by:

$$P_b(e) \cong \frac{N_{\mathrm{free}} W_{\mathrm{free}}}{K} Q\left(\sqrt{2 d_{\mathrm{free}} R \frac{E_b}{N_0}}\right), \tag{2}$$

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.

From Equation 2, it is observed that the BER for a specific concatenated code depends on code rate, transmission power and channel conditions. By substituting Equation 1 into Equation 2, one obtains the following:

$$P_b(e) \cong \frac{N_{\text{free}} W_{\text{free}}}{K} Q \left(\sqrt{2 d_{\text{free}} \frac{P_{\text{ST}} \times \text{BW}}{\text{BR}^2} 10^{\frac{A}{10}} \left[R(\beta) \times \sin^2(\beta) \times 10^{\frac{B}{10 \sin(\beta)}} \right]} \right), \quad (3)$$

where BW is the transmission bandwidth. For access to a given bit error probability in the whole communication séance with constant transmission power, the code rate must be varied, in accordance with the elevation angle (distance). The distance between the satellite and the ground station varies continuously. Therefore, one will need an error-correcting code with a continuous code rate variation. One method can be realized by using a lookup table of many nearly optimal codes with various code rates, and selecting a suitable code, according to the distance. The implementation cost of this method is very high. Hence, an adaptive secure punctured turbo coding scheme is proposed, whose puncturing rate can be changed with distance, so that the bit error probability is kept at a predetermined value.

Figure 1 displays the adaptive secure channel coding scheme. Each symbol of the source 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 is punctured to achieve the transmitted code word, X^N. The distance between the LEO satellite and the ground station is measured at the receiver and the transmitter instantaneously. The transmitter uses this information to adjust its appropriate puncturing rate block-by-block. When the distance is longer, the transmitter picks more redundant bits for protection. Therefore, the overall throughput is low. As the distance gets shorter, less redundancy is needed for protection. Hence, a higher throughput is achieved. The error rate of the channel will depend on the SNR at the receiver, the code rate and the complexity of the channel code.

The puncturing device selects N bits from M turbo-encoded bits, using N independent pseudo-random numbers over $[1, M]$. Therefore, it punctures each encoded bit independently, with probability $\lambda = 1 \quad \frac{N}{M}$. If a codeword of weight d enters the puncturing device, the codeword at the output will have a weight, h, with probability $\binom{c}{d} (1 \quad \lambda)^h \lambda^{d \quad h}$. The expected number of punctured codewords of weight, h, is given by:

$$\overline{A}_h^{C_P} = \sum_{d \geq h} \overline{A}_d^C \binom{d}{h} (1 \quad \lambda)^h \lambda^{d \quad h}, \quad (4)$$

where $\overline{A}_d^C$ is the average number of unpunctured code words of weight d. For an (N, K) binary linear code, C, with the weight enumerator, A_h^C, one has the well known union-Bhattacharyya bound on the Maximum Likelihood (ML) decoder word error probability [23]:

$$P_w(e) \leq \sum_{h=1}^{N} A_h^C \gamma^h, \quad (5)$$

where γ is the Bhattacharyya noise parameter. By applying Equation 4 in the above bound in Expression 5, one has:

$$\overline{P}_w(e) \leq \sum_{h=1}^{N} \overline{A}_d^C \binom{d}{h} (1 \quad \lambda)^h \lambda^{d \quad h} \gamma^h. \quad (6)$$

It was shown in [23] that for a turbo code, $A_0 = \limsup_{N \to \infty} \max_{d_{\text{free}} < h \leq N} \frac{\log \overline{A}_h^C}{h}$ is a finite positive number. Therefore, it can be seen that on a memoryless channel with Bhattacharyya parameter $\gamma <$ exp $A_0 + \log \frac{1 \quad \lambda}{\lambda}))$, $\overline{P}_w(e)$ goes to zero as N increases.

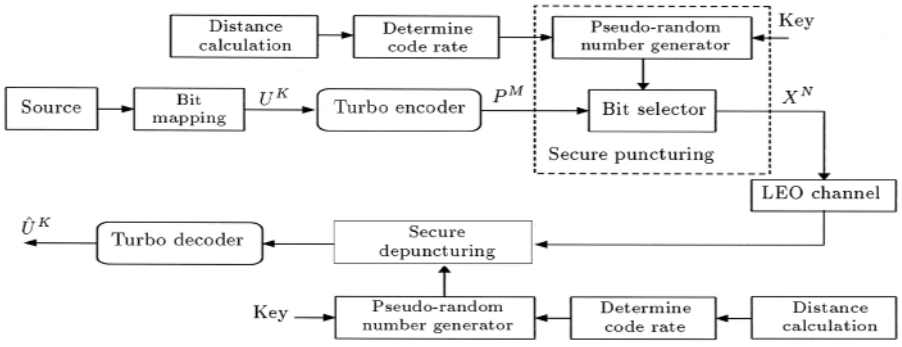

Figure 1. A proposed secure channel coding scheme for LEO satellite data transmission system.

In order to study the security of the system, one needs to determine, essentially, how difficult it is for an eavesdropper who doesn't know the key of the pseudo-random number generator and intercepts X^N to determine U^K. The security of this system is based on two computationally hard problems, which are an exhaustive search on the key space and the turbo decoding of a random punctured sequence. It appears that an eavesdropper uses two basic attacks: Decoding attacks and trapdoor attacks.

In decoding attacks, the attacker may try to recover the plaintext, U^K, directly from intercepted ciphertext X^N. In the case of a successful decoding attack, the plaintext is recovered but the cryptosystem remains intact. The basic problem to be solved is turbo decoding a punctured sequence without knowing the puncturing pattern. For each turbo-encoded sequence, one has a set of $(M)_N = \frac{M!}{(M-N)!}$ punctured sequences. If the length of the turbo-encoded block, (M), is sufficiently large, then, this attack will also be infeasible. Suppose $M = 1000$ and $N = 400$ are chosen, then, there will be about $\binom{M}{N} \cong \frac{\sqrt{2\pi M}M^M}{2\pi\sqrt{N(M-N)}N^N(M-N)^{M-N}} \cong 10^{292}$ possible puncturing patterns. For longer block lengths, the complexity of decoding without knowing the puncturing pattern is much greater.

In trapdoor attacks, the cryptanalyst may try to find the key of the pseudo-random number generator from an intercepted ciphertext (cipher text-only attack) or U^K and X^N pairs (known/chosen-plaintext attack). In a ciphertext-only attack, the attacker is assumed to have several ciphertexts and tries to guess the key by a brute-force search. In known/chosen-plaintext attacks, the attacker is assumed to have obtained several plaintext and ciphertext pairs (all of these pairs share a common key) and tries to analyze these pairs to obtain the common key. There are several types of cryptanalytic known/chosen-plaintext attacks against algebraic-code cryptosystems, discussed in [24,25]. These attacks are performed, based on the linearity of the system. They will not be applicable for nonlinear coding scheme. Therefore, the trapdoor attacks seem to be hopeless if the structure of the pseudo-random number generator is nonlinear and its period is sufficiently large, because there are so many possibilities for the key. In particular, suppose a nonlinear feedback shift register of length $n = 100$ is chosen, then, there will be about $2^{2^n} = 2^{2^{100}}$ possible keys.

These attacks are performed under the assumption that there is no occurrence of error in the channel. The presence of channel errors introduces an additional level of data security to this system.

Compared with the conventional methods, such as a combination of turbo coding and an Advanced Encryption Standard (AES) cryptosystem, this scheme has the advantages of: High-speed encryption and decryption with high security, smaller encoder and decoder size and greater efficiency. In a conventional method, if there is even a single error in the received ciphertext (after channel decoding), there will be a huge number of errors in the decrypted plaintext, whereas, in the proposed scheme, it is not so. Also, for an adaptation code rate, according to the distance in conventional methods, the appropriate puncturing patterns have to be saved. Therefore, a very high memory is needed.

SIMULATION RESULTS

To underline the effectiveness of the proposed secure channel coding scheme for a LEO satellite channel, an onboard data transmission system is designed for a practical example. The main parameters of the system are: $f = 1.7$ GHz, $G_{\mathrm{SA}} = 2$ dB (satellite transmitter antenna gain), $G_{\mathrm{EA}} = 29$ dB (ground station antenna gain), $T = 600$ sec (duration time), $H = 850$ km (orbital height), BPSK Modulation, $10^\circ \leq \beta \leq 170^\circ$ (elevation angle), $V_0 = 3.18 \times 10^9$ bit (total transmitted data in one communication séance), $P_b(e) \leq 10^{-6}$ and $\mathrm{SNR} \cong P_{\mathrm{ST}_{dB}} + 71.2 + 20\log(\sin\beta) + \frac{0.74}{\sin\beta} - 10\log(\mathrm{BR})$. The calculated values of the transmission rate and power for the basic data transmission system are:

$$\mathrm{BR}_0 = 5.3 \text{ Mbps}$$

$$P_b(e) \leq 10^{-6} \rightarrow \mathrm{SNR} \cong 10dB \rightarrow P_{\mathrm{ST}_0} \cong 49 \text{ w}.$$

Figure 2 displays a proposed coding scheme for the improved data transmission system. Each block of satellite data is encoded, using a serially concatenated turbo code, formed by an outer 4-state recursive systematic conventional code with:

$$G_{\mathrm{outer}}(D) = \left[1 \quad \frac{1+D^2}{1+D+D^2}\right],$$

and an inner 4-state recursive systematic conventional code with:

$$G_{\mathrm{inner}}(D) = \begin{bmatrix} 1 & 0 & \frac{1+D^2}{1+D+D^2} \\ 0 & 1 & \frac{1+D}{1+D+D^2} \end{bmatrix}.$$

The size of the source block for turbo coding is $K = 1024$. For simplicity, a 100-stage Linear Feedback Shift Register (LFSR) is used for a pseudo-random number generator. The BPSK-modulated punctured signals are transmitted through a LEO satellite channel. At the receiver, the depuncturing process is done with permuting symbols in the received block, based on a secure key and substituting zero values for punctured

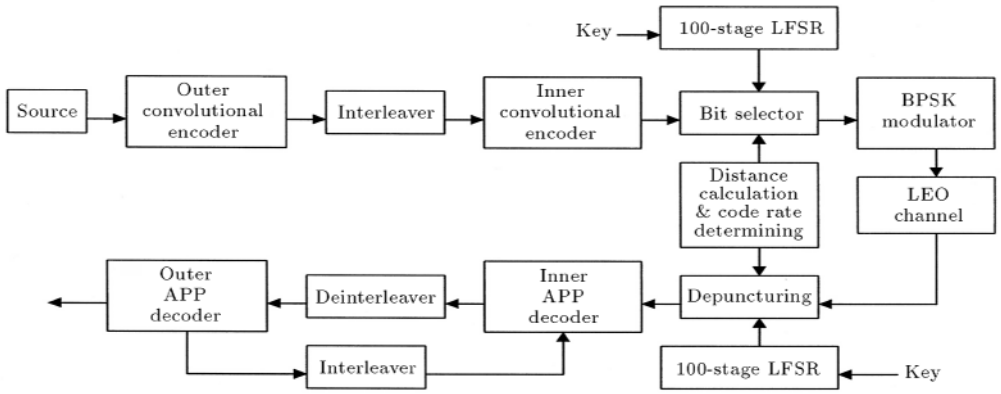

Figure 2. A simulated secure serially concatenated coding scheme for LEO satellite data transmission system.

bits. Details of serially concatenated turbo decoding are explained in [4,26,27]. The performance (puncturing rate allocation versus different SNRs) of this secure serially concatenated turbo code for $P_b(e) \cong 10^{-5}$ and $P_b(e) \cong 10^{-6}$ is given in Figure 3. It can be observed that the maximum code rate is about 0.84. The values of the transmission rate and power for the improved data transmission system can be calculated by knowing the total transmitted data, $V = V_0$:

$$V = \int_0^T \mathrm{BR} \times R(\beta) dt. \tag{7}$$

Therefore, for $V = 3.18 \times 10^9$ bits and $P_b(e) \cong 10^{-6}$, the calculated values for an improved data transmission system (Figure 2), based on this secure serially concatenated code, are:

$\mathrm{BR} \cong 8.93$ Mbps,

$P_{\mathrm{ST}} \cong 11.9$ w.

Figure 4 shows the bit error rates versus the elevation angle for basic and improved data transmission

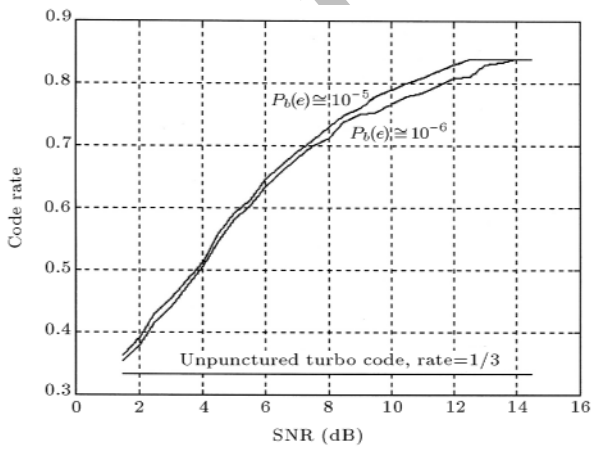

Figure 3. Code rate versus SNR for simulated secure serially concatenated code.

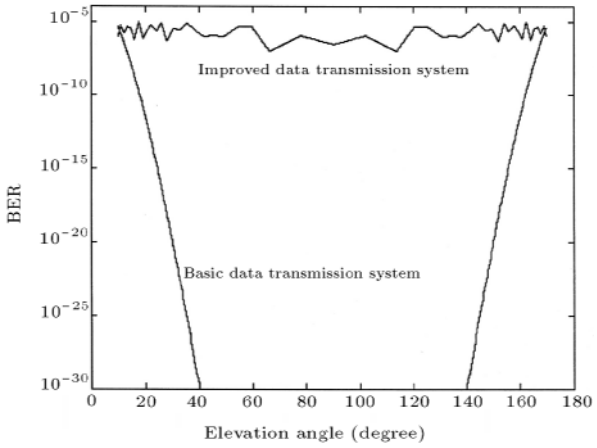

Figure 4. Bit error rates versus elevation angle for the basic and improved data transmission systems.

Table 1. Performance comparison of the basic and improved data transmission system.

Type	P_{ST} (w)	BR (Mbps)	V (bits)
Basic System	49	5.3	3.18×10^9
Improved System	11.9	8.93	3.19×10^9

systems. As one can see from Figure 4, the BER is approximately constant at different distances. A comparison of basic and improved systems is given in Table 1. For $V \cong V_0$, the improved system provides about 75.7% enhancement in onboard consumption energy, compared to the basic system. The BER value can be changed by changing the puncturing rate value.

CONCLUSION

A secure channel coding scheme combines data encoding and data encryption into one process. In this paper, an adaptive secure channel coding scheme for more efficient transmission data over the LEO satellite channels is presented. This scheme is based on adaptive and pseudo-random puncturing of the turbo-encoded

block. The puncturing rate in this scheme is selected in proportion to the distance between the LEO satellite and ground station.

Two cryptoanalytical attacks against this scheme are investigated. It would be a challenge, indeed, to find cryptoanalytic attacks that can break this system.

Simulation results show that one can obtain an efficient data transmission system, with good reliability and security, by using this scheme.

REFERENCES

1. Shannon, C.E. "A mathematical theory of communication", *Bell Systems Technical Journal*, **7**, pp 379-423 (Part I) and 623-656 (Part II) (1948).
2. Forney Jr., G.D., *Concatenated Codes*, MIT Press, Cambridge, MA, USA (1966).
3. Berrou, C., Glavieux, A. and Thitimajshima, P. "Near Shannon limit error-correcting coding and decoding: Turbo-codes", in *Proc. ICC'93*, Geneva, Switzerland, pp 1064-1070 (May 1993).
4. Bennedetto, S., Divsalar, D., Montorsi, G. and Pollara, F. "Serial concatenated of interleaved codes: Performance analysis, design, and iterative decoding", *IEEE Trans. on Information Theory*, **44**(3), pp 909-926 (May 1998).
5. Bahl, L.R., Cocke, J., Jelinek, F. and Raviv, J. "Optimal decoding of linear codes for minimizing symbol error rate", *IEEE Trans. Information Theory*, **IT-20**, pp 284-287 (1974).
6. McEliece, R.J. "A public-key cryptosystem based on algebraic coding theory", *JPL DSN Progress Rep. 42-44*, pp 114-116 (Jan.-Feb. 1978).
7. Berlekamp, E.R., McEliece, R.J. and Van Tilborg, H.C.A. "On inherent intractability of certain coding problems", *IEEE Trans. Information Theory*, **IT-24**, pp 384-386 (1978).
8. Niederreiter, H. "Knapsack-type cryptosystems and algebraic coding theory", *Problems of Control and Information Theory*, **15**(2) (1986).
9. Gabidulin, E.M. "Ideals over a non-commutative ring and their applications in cryptography", *Lecture Notes in Computer Science*, **547**, Proc. Eurocrypt 91, Springer Verlag (1991).
10. Gabidulin, E.M. "On public-key cryptosystems based on linear codes: Efficiency and weakness", *Codes and Ciphers, Proc. 4th IMA Conference on Cryptography and Coding* (1993).
11. Sidelnikov, V.M. "A public-key cryptosystem based on binary Reed-Muller codes", *Discrete Mathematics and Applications*, **4**(3) (1994).
12. Rao, T.R.N. and Nam, K.H. "A private-key algebraic-coded cryptosystem", *Proc. Crypto'86*, pp 35-48 (1986).
13. Hwang, T. and Rao, T.R.N. "Secret error-correcting codes (SECC)", *Proc. Crypto'88*, pp 540-563 (1988).
14. Ue, T., Sampei, S., Morinaga, N. and Hamaguchi, K. "Symbol rate and modulation level-controlled adaptive modulation/TDMA/TDD system for high bit rate wireless data transmission", *IEEE Trans. Vehicel Technology*, **47**, pp 1134-1147 (Nov. 1998).
15. Lim, C.H. and Cioffi, J. "Performance of the adaptive rate MQAM with on/off power control", *IEEE Communication Letters*, **5**, pp 16-18 (Jan. 2001).
16. Stojanovic, M. and Chan, V. "Adaptive power and rate control for satellite communications in Ka band", *IEEE International Conference on Communications (ICC'02)*, New York, USA (May 2002).
17. Mehta, M., Nunn, D. and Braithwaite, S. "Predictive action power control scheme for a land mobile satellite system", *Research Journal*, University of Southampton, pp 33-36 (1995/6).
18. Payandeh, A., Ahmadian, M. and Aref, M.R. "A novel joint source-channel coding scheme for image transmission over the LEO satellite channel", *2nd Asian Space Conference (ASC)*, Hanoi, Vietnam (8-11 Nov. 2005).
19. Divsalar, D. and Pollara, F. "On the design of turbo codes", *The Telecommunication and Data Acquisition Progress Report*, Jet Propulsion Laboratory, pp 99-121 (Nov. 1995).
20. Berrou, C. and Glavieux, A. "Near optimum error correcting coding and decoding: Turbo codes", *IEEE Trans. on Communications*, **44**(10), pp 1261-1271 (Oct. 1996).
21. Divsalar, D. and Pollara, F. "Multiple turbo codes for deep-space communication", *The Telecommunication and Data Acquisition Progress Report*, Jet Propulsion Laboratory, pp 66-77 (May 1995).
22. Divsalar, D., Dorlinar, S. and McEliece, R.J. "Transfer function bounds on the performance of turbo codes", *The Telecommunications and Data Acquisition Progress Report, TDA PR 42-122*, pp 44-55 (1995).
23. Jin, H. and McHliece, R.J. "Coding theorems for turbo code ensembles", *IEEE Trans. on Information Theory*, **48**, pp 1451-1461 (June 2002).
24. Nam, K.N. "Complexity analysis of algebraic-coded cryptosystems", PhD Dissertation, Tech Report NSA-1-85, The Center for Advanced Computer Studies, University of Southwestern (June 2006).
25. Chabaud, F. "On the security of some cryptosystems based on error-correcting codes", in *Advances in Cryptology (EUROCRYPT'94)*, 0950 of Lecture Notes in Computer Science, Springer-Verlag, USA (1994).
26. Benedetto, S. and Montorsi, G. "Iterative decoding of serially concatenated convolutional codes", *Electronic Letters*, **32**(13), pp 1186-1187 (June 1996).
27. Payandeh, H. "An improved secure and efficient coding system for remote sensing satellite", PhD Thesis, K.N. Toosi University of Technology, to be published.