16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

JOINT SECURITY AND CHANNEL CODING FOR OFDM COMMUNICATIONS

Alessandro Neri, Daniele Blasi, Luca Gizzi, and Patrizio Campisi

Department of Applied Electronics, University of ROMA TRE
Via della vasca navale 84, 00146, ROMA, ITALY
phone: + (39) 57337017, fax: + (39) 57337026, email: (neri, campisi)@uniroma3.it
web: www.comlab.uniroma3.it

ABSTRACT

In this paper we propose an algorithm for joint authentication, integrity verification and channel coding, optimized for OFDM based communication systems. Joint security and channel coding is performed by means of a Shannon's substitution-permutation scheme and a pseudo-random punctured Turbo Code, whose actual parameters are set in accordance to a private session key. User authenticity and message integrity are verified comparing the log-likelihood of the decoded ciphertext with a threshold, adapted to actual channel condition.

1. GENERAL INFORMATION

The demand for secure digital communications, assuring privacy, as well as data integrity and authenticity is dramatically increasing day by day, pushed by the diffusion of mobile and nomadic multimedia services. Therefore, modern wireless access networks should guarantee that the transmitted data can not be understood/used by unauthorized users, still maintaining a strong error resilience even in severe conditions, like those involved by indoor and outdoor scenarios affected by multipath. In the meanwhile the receiver should be capable of authenticating the transmitter to avoid man in the middle attacks.

Often, to isolate the security mechanisms from the characteristics of the technologies adopted at the physical layer, security services are implemented at higher levels of the ISO OSI stack. Usually, source authenticity and message integrity are verified by means of a *message authentication code*, often denoted as message hash, characterized by two functionally distinct parameters, a message input and a secret key $\mathbf{k}_A$. For every fixed allowable value of the secret key $\mathbf{k}_A$ (supposed unknown to an adversary), given zero or more (ciphertext, hash) pairs it should be computationally infeasible to recover the unknown key and to compute the message authentication code for any new input. Data authenticity and integrity are verified by controlling the coincidence between the received hash and the hash evaluated on the received text. Since the control fails in presence of communication errors, strong forward error correction (FEC) codes and ARQ protocols have to be adopted in severe environments.

However, implementation of security mechanisms at physical and link levels allows to reduce the overhead produced by encryption, mutual authentication, and data integrity, then, increasing the overall spectral efficiency, and to deploy more effective countermeasures facing denial of service or hijacking attacks.

Thus, recently, several authors have investigated the use of FEC codes with authentication codes, [1]-[10]. A theoretical analysis on the relationships between authentication codes and FECs can be found in [1]. An asymmetric authentication system based on the McEliece public-key cryptosystem, that makes use of Goppa codes is proposed in [2]. Digital signature schemes based on the McEliece systems have been investigated in [3] and [4]. A more efficient approach, from a computational complexity point of view, has been proposed by Rao and Nam, that keep the public generator matrix used in the McEliece technique as private [9]-[12].

A security framework for OFDM systems that combines data encryption and authentication at physical layer with channel coding, has been proposed, by the authors, in [14]. In essence, encryption of the plaintext message is performed by means of a pseudo-random phase-hopping (PH), acting as a generalized Vernam Stream cipher, encrypting individual sub-carrier symbols one at a time, using an encryption transformation which varies with sub-carrier index and time. Joint authentication and error resilience are based on a 128 bit Message Digest (MD-2) encrypted-hash algorithm. Although simulations demonstrated its effectiveness, this method has some lack of flexibility in adapting the amount of redundancy introduced by channel coding to the actual environment.

Concatenated turbo coders whose puncturing element is selected on the basis of a secret session key have been proposed in [13], for joint FEC and security.

Here we propose a soft authentication verification procedures that replaces the hard decision about authenticity and integrity with the likelihood of the received text-hash pair.

The joint message authentication and FEC is based on a parallel turbo code whose interleavers, recursive convolutional coders, and puncturing blocks are pseudo-randomly selected from a predefined dictionary, based on the secret session key.

The paper is organized as follows. In Sect. II the scheme of the joint security and channel coding is presented. In Sect. III the results of the performance assessment based on Montecarlo simulations are evaluated. Finally, conclusions are drawn in Sect. IV.

2. MATHEMATICAL FRAMEWORK

As illustrated in Fig.1, the proposed scheme, to jointly provide security services and channel coding for OFDM based communications, consists of two-stages. In the first stage, following the Shannon's substitution-permutation paradigm, for each OFDM symbol interval, we XOR the binary plain text **m** with a (pseudo-random) binary i.i.d. sequence. Then we dissipate the remaining statistical structure by permuting the XORed sequence by means of a pseudo-random interleaver Π_c , selected from an interleaver dictionary on the basis of the session key $\mathbf{k}_C$. We note that this part of the scheme is not affected by error propagation, since modification of a ciphertext digit during transmission does not affect decryption of other digits.

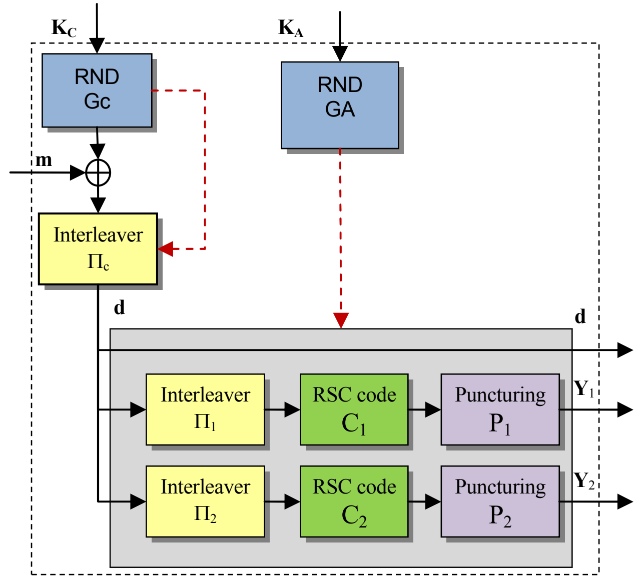

Fig.1. Authentication and FEC coder.

The second stage is a parallel turbo code consisting of 2 interleavers Π_1, Π_2, cascaded with 2 recursive convolutional coders C_1, C_2, and two puncturing blocks P_1, P_2. Π_1, Π_2, C_1, C_2, P_1, and P_2 are pseudo-randomly selected from a predefined dictionary, based on the output of a pseudo-random generator driven by the secret key $\mathbf{k}_A$. To reduce the amount of memory required to store the dictionary, while keeping low the probability of use of coders with poor performance, a gray-list of poor elements is employed.

The input to the OFDM modulator is therefore constituted by the ciphertext **d**, that represents the systematic part of the turbo encoder, and the punctured parity/hash sequences $\mathbf{Y}_1$ and $\mathbf{Y}_2$.

The pair ($\mathbf{k}_C$, $\mathbf{k}_A$) constitutes the session key and is periodically updated. Moreover **p** is the pilot sequence carried on the pilot OFDM subcarriers.

With reference to Fig.2, the receiver is constituted by a turbo decoder, [15], cascaded with a block that computes the likelihood of the (ciphertext, hash) pair, thus providing a soft authentication verification indicator. Hard decision can still be performed by thresholding the likelihood functional.

Let **X** be the noisy ciphertext and $\mathbf{R}_1$ and $\mathbf{R}_2$ the noisy parity hash sequences at the output of the OFDM demodulator. Due to the OFDM properties, for AWGN channels, denoting with μ(.) the mapping from the OFDM binary input to the constellation points, we have

$$\mu(\mathbf{X})=\mu(\mathbf{d})+\mathbf{n},$$

$$\mu(\mathbf{R}_1)= \mu(\mathbf{Y}_1)+\mathbf{n}_1,$$

$$\mu(\mathbf{R}_2)=\mu(\mathbf{Y}_2)+\mathbf{n}_2$$

where **n**, $\mathbf{n}_1$, and $\mathbf{n}_2$ are White Gaussian Noise samples.

Let $\hat{\mathbf{d}}$ be the cipher-text estimated by the turbo decoder. Then, denoting with H_0 the hypothesis that the message has been altered or forged and with H_1 the hypothesis that the received signal is the noisy version of the authentic original message, to decide about integrity and authenticity of the received data we should evaluate the ratio between the posterior probabilities of the two hypotheses, namely,

$$\frac{\Pr\left\{\hat{\mathbf{d}}/\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2\right\}}{\sum\limits_{\mathbf{d}_i\in\mathcal{D}}\Pr\left\{\mathbf{d}_i/\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2\right\}},$$

where $\mathcal{D}$ is the set of all forged/altered messages. Since this procedure appears to be unfeasible, due to the computational burden, we employ the log-likelihood $\log\Lambda(\hat{\mathbf{d}};\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2)$ of the decoded ciphertext, given the received signal.

It can be easily verified that, for AWGN channels, this quantity can be written as follows:

$$\begin{aligned}\log\Lambda\left(\hat{\mathbf{d}};\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2\right)&=\log\Pr\left\{\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2/\hat{\mathbf{d}}\right\}=-M\log 2\pi\sigma_N^2\\&-\frac{1}{2\sigma_N^2}\left[\mu(\mathbf{X})-\mu(\hat{\mathbf{d}})\right]^{\dagger}\left[\mu(\mathbf{X})-\mu(\hat{\mathbf{d}})\right]\\&-\frac{1}{2\sigma_N^2}\left[\mu(\mathbf{R}_1)-\mu(\hat{\mathbf{Y}}_1)\right]^{\dagger}\left[\mu(\mathbf{R}_1)-\mu(\hat{\mathbf{Y}}_1)\right]\\&-\frac{1}{2\sigma_N^2}\left[\mu(\mathbf{R}_2)-\mu(\hat{\mathbf{Y}}_2)\right]^{\dagger}\left[\mu(\mathbf{R}_2)-\mu(\hat{\mathbf{Y}}_2)\right],\quad(1)\end{aligned}$$

where † denotes the Hermitian operator, σ_N^2 is the noise variance, M is the number of OFDM subcarriers used for transmitting **X**, $\mathbf{Y}_1$ and $\mathbf{Y}_2$, and $\hat{\mathbf{Y}}_1$ and $\hat{\mathbf{Y}}_2$ are hash/parity, eventually punctured, sequences corresponding to $\hat{\mathbf{d}}$.

The log-likelihood given by Eq. (1) can be directly employed for soft authentication and data integrity verification. As expected the maximum corresponds to the noiseless reception of the original message and the original hash/parity controls.

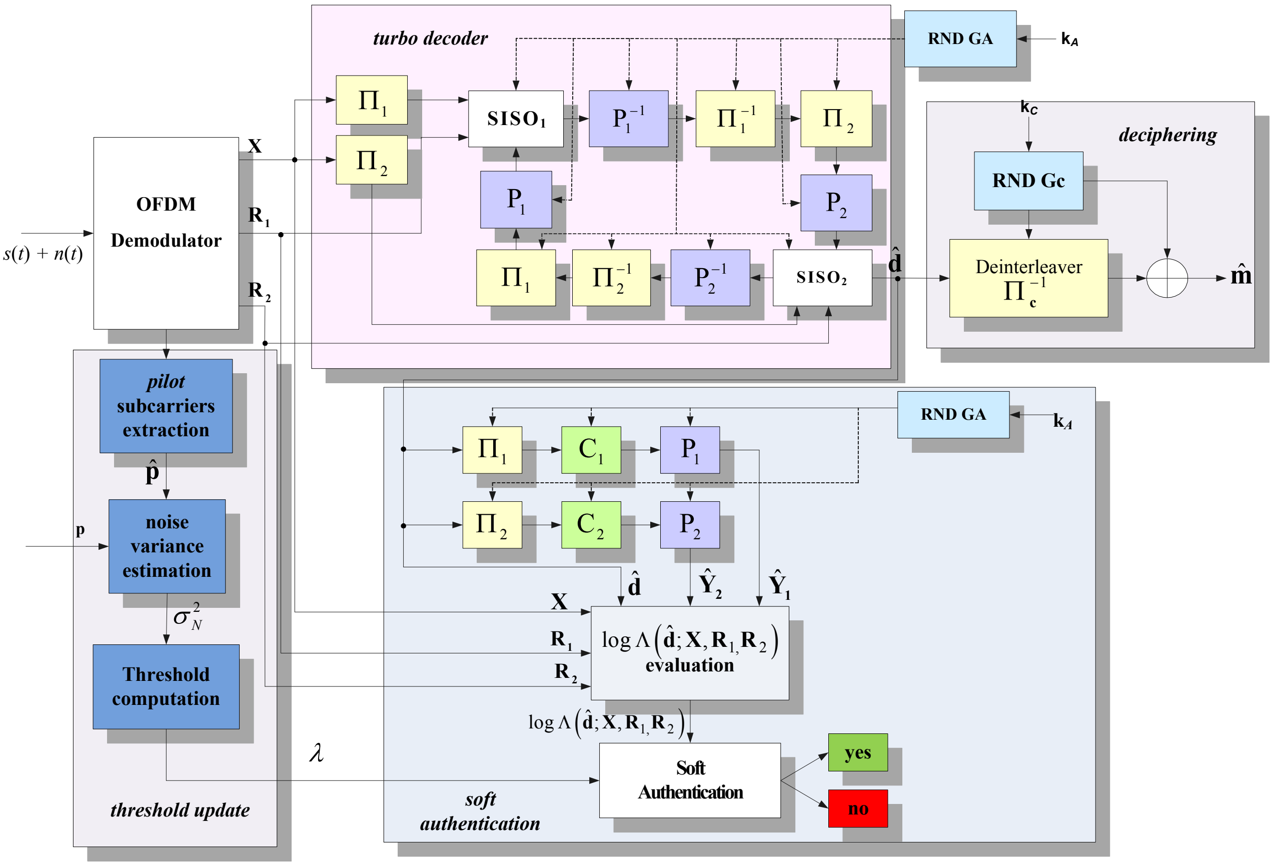

Fig.2. Soft Authentication and FEC decoder.

Moreover, classical hard decision about authenticity and integrity can be performed by comparing this quantity with a threshold. Then, the authenticity and integrity verification test becomes

$$\log\Lambda\left(\hat{\mathbf{d}};\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2\right)\underset{H_0}{\overset{H_1}{\gtrless}}\lambda .$$

Here, we propose to set the threshold λ in accordance to the Neyman-Pearson lemma. The choice of this criterion has been inspired to the radar context, and is motivated by the fact that, even in our case, it is quite difficult to attribute a value to the a priori probability of being attacked by an intruder. Thus, defining as *false alarm* the event of rejecting an authentic message because of the noise, we set the threshold in accordance to the maximum acceptable level of probability of false alarm. Obviously this value is application dependent and has to be intended as a requirement.

Having set the threshold to meet the false alarm probability requirements, we may choose the remaining parameters (e.g. turbo code rate, transmitting power, number of subcarriers), in order to maximize the probability of detecting any security attack. Obviously a trade off to meet additional constraints on maximum transmitting power, bit rate, hardware and software complexity, etc., may be required.

To evaluate the false alarm probability P_{fa}, we observe that, when the bit error rate at the output of the decoder is small, $\hat{\mathbf{d}}\cong\mathbf{d}$, and thus, under the hypothesis H_1, the log-likelihood functional (1), can be well approximated as follows:

$$\log\Lambda\left(\hat{\mathbf{d}};\mathbf{X},\mathbf{R}_{1,}\mathbf{R}_2/H_1\right)\cong -M\log 2\pi\sigma_N^2-\frac{\nu}{2}$$

where M is defined as in (1) and

$$\nu=\frac{1}{\sigma_N^2}\sum_{i=1}^{M}\left(n_{I_k}^2+n_{Q_k}^2\right),$$

is a random variate with a chi-square distribution with $2M$ degrees of freedom. Therefore, for the false alarm probability we obtain:

$$P_{fa}=\int_{-2\lambda-2M\log 2\pi\sigma_N^2}^{\infty}p_{\chi_{2M}^2}(x)dx=\frac{\gamma\left(M,-\lambda-M\log 2\pi\sigma_N^2\right)}{(M-1)!} \qquad (2)$$

where $\gamma(k,z)$ is the upper incomplete Gamma function:

$$\gamma(a,x)=\int_x^{\infty}t^{a-1}e^{-t}dt .$$

Thus, the authenticity and integrity test threshold can be computed by numerical inversion of Eq. (2).

Threshold adaptivity requires the on line estimation of the noise power spectrum density. However, this task can be accomplished by resorting to the statistics extracted from the pilot subcarriers.

It is worthy to observe that, to increase the strength of the security mechanism, even the position of the pilot subcarriers can be randomly varied in accordance to an additional session key k_P. Obviously, since pilot subcarriers should be undistinguishable from data subcarriers, their complex amplitude should be pseudorandomly generated using the same constellation employed to transmit data.

For an effective identification of the channel behavior, only small hops around nominal values designed for a regular sampling of the frequency response will be allowed.

Nevertheless, when the number N_{pilot} of pilot sub-carrier is relatively high, even small fluctuations can prevent brute force attacks. In fact, if for each nominal pilot subcarrier, 2^H hops are allowed, the total number of different pilot signals is $2^{HN_{pilot}}$, and the average number of brute force attacks is $2^{HN_{pilot}-1}$ (obviously, the length of the session key k_P should be set accordingly to HN_{pilot}). Thus, for $HN_{pilot} \geq 128$, we can assume a brute force attack as unfeasible.

3. SIMULATIONS

The entire communication system was simulated referring to a wideband OFDM signal transmission over an AWGN channel. The bandwidth of this signal and the turbo code constraint length are respectively 500Mhz and 192 bits in every simulation.

Fig.3 shows the FRR (False Rejection Rate) versus the cardinality L of the QAM constellation employed on every OFDM carrier. In the simulation, the total number of orthogonal sub-bands is N = 8192, the number of pilot sub-carrier is N_{pilot} = 256, the turbo-code rate R is equal to 1/7, while the desired false-alarm probability P_{fa} is 10^{-3}.

As expected, for a given SNR, the increase in the constellation cardinality produces an increase in the BER. Consequently becomes harder and harder to detect real security attacks, and the FRR increases.

Fig.4 depicts the FRR versus the turbo-code rate R, for the 4-QAM constellation; the number of orthogonal sub-bands N is 8192, the number of pilot sub-carrier N_{pilot} equals 256, and the desired false-alarm probability P_{fa} is 10^{-3}. Once more, decreasing the turbo code redundancy reflects into a corresponding decrease in the ability in the correction of the channel errors and in the detection of intrusions, tampering, etc.

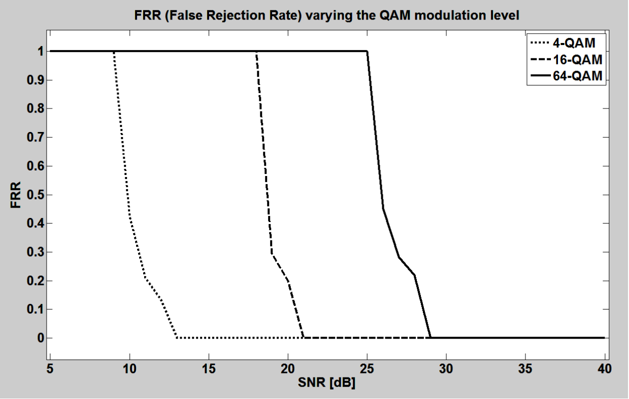

Fig.3: system FRR versus the QAM modulation order.

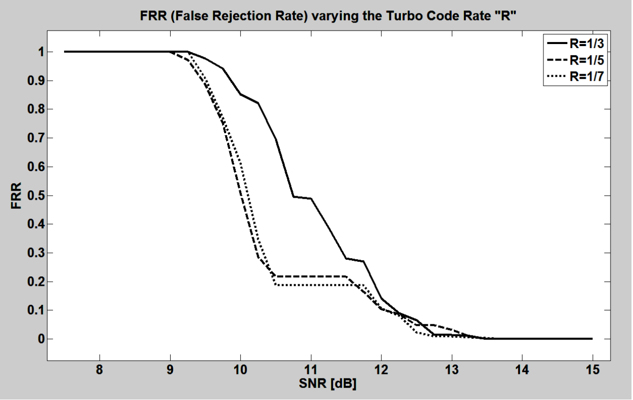

Fig.4: system FRR versus turbo-code rate for 4-QAM modulation.

Fig.5 shows the impact of the number of OFDM carriers on the FRR. Indeed, since the authentication word length is approximately given by Nlog2(L), it is clear that, at constant B.E.R., the FRR increases with N. In this simulation, a turbo-code with rate R equal to 1/7 has been employed, while the false alarm probability P_{fa} has been set equal to 10^{-3}.

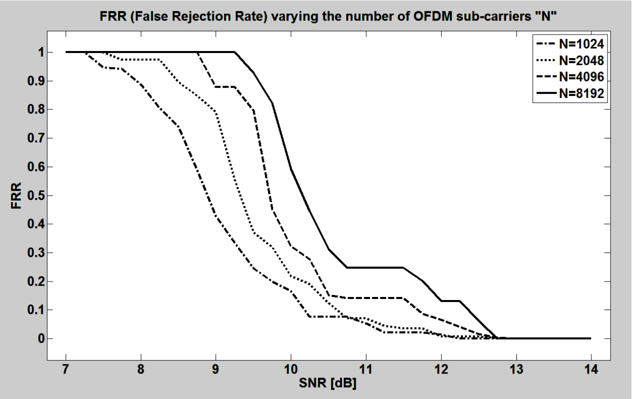

Fig.5: system FRR varying the number of OFDM sub-carriers.

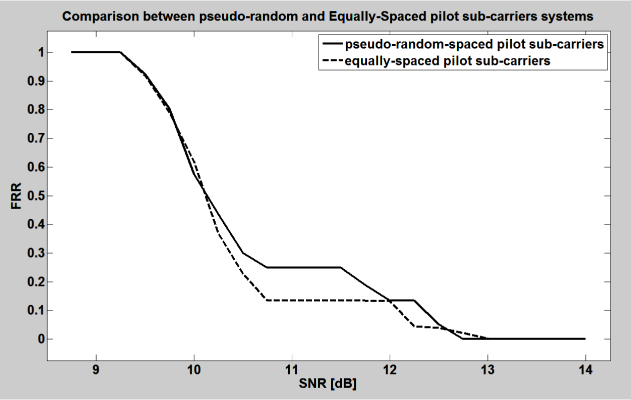

Fig.6: Random vs. equally-spaced pilot sub-carrier systems.

All previous simulations were carried out using random-spaced pilot sub-carriers. However, as illustrated in Fig.6, the differences in performance between such a system and a system with equally-spaced pilot sub-carrier are quite small. Nevertheless, as previously discussed, random selection of pilot sub-carriers can increase the security level. We observe that we evaluated only the impact of pseudorandom pilot sub-carrier hopping on security and error correction capabilities. Impact on channel state estimation would require more sophisticated indoor and outdoor channel models. However, we remark that even very small hops can produce tangible benefits from the security viewpoint.

4. CONCLUSIONS

Simulation results have demonstrated the feasibility of joint authentication, integrity verification and channel coding, optimized for OFDM based communication systems. In particular, use of a pseudo-random punctured Turbo Code, whose actual parameters are set in accordance to a private session key, simplifies the computation of the log-likelihood of the decoded ciphertext.

While this quantity can be directly employed for soft authentication and data integrity verification, classical hard decision about authenticity and integrity can be performed by comparing this quantity with an adaptive threshold.

REFERENCES

[1] G. A. Kabatianskii, B. Smeets, and T. Johansson, "On the cardinality of systematic authentication codes via error-correcting codes," *IEEE Transactions on Information Theory*, vol. 42, pp. 566–578, March 1996.

[2] R. S. Safavi-Naini and J. R. Seberry, "Error-correcting codes for authentication and subliminal channels," *IEEE Transactions on Information Theory*, vol. 37, pp. 13–17, January 1991.

[3] W. Xinmei, "Digital signature scheme based on error-correcting codes," *Electronics Letters*, vol. 26, pp. 898–899, June 1990. 21st June 1990.

[4] L. Harn and D.-C. Wang, "Cryptanalysis and modification of digital signature scheme based on error-correcting code," *Electronics Letters*, vol. 28, pp. 157–159, January 1992.

[5] W. Godoy J´unior and D. Pereira J´unior, "A proposal of a cryptography algorithm with techniques of error correction," *Computer Communications*, vol. 20, no. 15, pp. 1374 – 1380, 1997.

[6] K. Zeng, C.-H. Yang, and T. R. N. Rao, "Cryptanalysis of the Hwang-Rao secret errorcorrecting code schemes," in *Information and Communications Security, Third International Conference, ICICS 2001*, Xian, China (S. Qing, T. Okamoto, and J. Zhou, eds.), vol. 2229 of Lecture Notes in Computer Science, pp. 419–428, Springer-Verlag, 2001. Obtained online at http://crypto.nknu.edu.tw/publications/icics2001.pdf.

[7] N. V. Patsei and P. P. Urbanovich, "On the design of error detection and correction cryptography schemes," in *EUROCOMM 2000: Information Systems for Enhanced Public Safety and Security, IEEE, AFCEA, IEEE Communications Society, IEEE*, 2000. Munich, Germany, 2000.

[8] Y. Aumann and M. O. Rabin, "Authentication, enhanced security and error correcting codes (extended abstract)," in Advances in Cryptology - Crypto '98 (H. Krawczyk, ed.), vol. 1462 of Lecture Notes in Computer Science, Springer-Verlag, 1998, *18th Annual International Cryptology Conference*, Santa Barbara, California, USA, August 1998.

[9] T.R.N. Rao, "Joint encryption and Error Correction Schemes", ACM SIGARCH Computer Architecture News, Vol.12, Issue 3, pp. 240-241, june 1984.

[10] T.R.N. Rao, "Cryptosystems using Algebraic codes", *Intl. Conf. On Computer Systems and Signal Proc*. Bangalore, India, Dec. 1984.

[11] T. R. N. Rao, Kil-Hyun Nam, "Private-Key Algebraic-Coded Cryptosystems", *Advances in Cryptology - CRYPTO '86: Proceedings*, Volume 263/1987, pp. 35-48, Springer Berlin / Heidelberg, 1987.

[12] T. Hwang and T. R. N. Rao, "Secret error-correcting codes (SECC)," in *Advances in Cryptology - CRYPTO '88* (S. Goldwasser, ed.), vol. 403 of Lecture Notes in Computer Science, pp. 540–563, Springer-Verlag, 1988.

[13] A. Payandeh, M. Ahmadian and M. Reza Aref, "Adaptive secure channel coding based on punctured turbo codes", *IEE Proc.-Commun*., Vol. 153, No. 2, pp. 313-316, April 2006.

[14] A. Neri, D. Blasi, P. Campisi "Secure OFDM-UWB communication based on phase hopping", *SPIE Proceedings Vol. 6579, Mobile Multimedia/Image Processing for Military and Security Applications 2007,* Sos S. Agaian; Sabah A. Jassim, Editors, 2 May 2007.

[15] C. Berrou and A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo-codes", *IEEE Trans. Commun*., vol. 44, no. 10, Oct. 1996, pp. 1261–71.

[16] N. Yamamoto and T. Ohtsuki, "Adaptive Internally Turbo Coded Ultra-Wide-Band Impulse Radio (AITC-UWB-IR) system" *IEEE International Conference on Communications (ICC 2003)*, pp. 3535-3539, Alaska, U.S.A. May 2003

[17] M. C. Chiu, W. D. Wu and C. C. Chao, "Frequency diversity OFDM (FD-OFDM) for ultra-wideband systems with reduced sampling rate receiver", in Proc. Int. Symp. Inform. Theory and its App., Parma, Italy, Oct. 2004, pp. 212-217.