Securing MIMO Space-Time Block Coding Technique over a Wireless Communication Links

Mahdi Nouri, Abolfazl Falahati

***Abstract*—A secure space-time block coding (i.e. a joint encryption and coding) scheme can provide both data secrecy and data reliability in one process to tackle problems in an insecure and unreliable communication channel. In this paper, an adaptive secure space-time block coding scheme based upon a normal Alamouti STBC codes is proposed. The crypto-analysis technique such as brute-force attacks over the proposed secure STBC indicates that the joint design can indeed provide both secrecy and data reliability very well. Such operations on Alamouti's STBC are achieved by adapting a pseudorandom sequence to control the key stream process over noisy channels. The analytical and simulation results indicate a superior performance of the proposed secure scheme for all adequate signal-to-noise ratios.**

Index Terms*— *Space-Time Block Codes, Cryptographic Pseudorandom Sequence Key, MIMO Channel Modeling, Changing Matrix.

I. Introduction

Channel coding and security are both imperative aspects of modern digital communication systems. 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, making the system an integral as well as necessary part in the design of modern communication systems and digital computers. Today, wireless devices have become increasingly pervasive and essential for the crypto-analysis attackers targets. It must be noted that the avalanche effect that makes a joint block cipher and channel coding also causes sensitivity to bit error rate performance. This results in a fundamental trade-off between security and throughput in encryption based wireless security. In a wireless network, the wireless communication medium is open to intruders so that an eavesdropper can intercept a communication by listening to the transmitted signal. Hence, encrypting the transmitted packets helps to achieve confidentiality. Merging security and channel coding processes is an attractive idea since it can reduce the overall processing cost too.

Security issues based on Shannon secrecy model are effective in terms of efficiency and link reliability [3]. Hero [4] and Koorapaty *et al.* [5] present an information security approach which uses channel state information (CSI) as the secret key in multiple-input multiple-output (MIMO) links. Unfortunately, attackers still can use the blind de-convolution algorithm [6], [7] to estimate channels, which decreases the strength of such approaches d. Li *et al.* [8] and Kim *et al.* [9] developed MIMO security schemes which use the attacker's blind identification capacity loss. Their schemes assume that the channels with intended receivers and attackers are neither identical and nor highly correlated. The security in classical cryptographic system is based on unproven assumptions regarding the complexity of certain computational tasks; therefore, commutation systems are insecure if the presumed assumptions are wrong or if efficient attacks are developed. Reference [10] presents a physical-layer security under the theoretic security information models. This procedure can amplify the system secrecy in theory if suitably long codes are deployed. The system can now be designed and tuned for a specific level of security.

Traditionally, the design of encryption algorithms and their parameters are used only against an adversary attack as the main criterions. To achieve this goal, the encrypted data or the cipher is made to satisfy several properties including the avalanche effect [11]. The avalanche criterion requires that a single bit change to the plain text or the key must result in significant and random-looking changes of the ciphertext. Typically, an average of one half of the decrypted bits should change whenever a single input bit to the decryption device is complemented. This guarantees that there will not be any noticeable resemblance between two ciphertexts obtained by applying two neighboring keys for encrypting the same plain text. Otherwise, there would be considerable reduction of the keyspace search by the cryptanalyst.

In the proposed scheme, a key stream set of an orthogonal code set is introduced for wireless networks based on space time block code (STBC) precoding technique [12, 13, 14]. The transmitter randomly rotates and changes the form of symbols in precryptocoding matrix to confuse the attacker and a pseudorandom sequence is employed to control the key stream process.

II. Channel Model And Security Measure

There are several methods in which one can quantify the strength of an encryption scheme [15]. One method is to

measure the work involved by breaking the cipher plaintext which is called the best known cryptanalysis splitting method (known as shortcut attack). In the absence of any shortcut attacks, the only way to crack the encryption key is to use the brute force technique. As a simple example, for an AES cipher with a key length of 128 bits, there are 2^{128} possible splitting of key sets. Assuming a certain complexity for testing one key (single decryption), the complexity involved in cracking a 128-bit AES cipher is 2^{128}. However, note that this is the worst-case complexity possible. This motivates a choice of a security measure to be $S(N) = log_2^N$, where N is the encryption block length. It must be stated that, in many practical encryption schemes, the block length and key length are equal. With the maximum block length of N_{max}, the normalized security level can be defined as $s(N) = \frac{log_2^N}{S_{max}}$, where $S_{max}(N) = log_2^{Nmax}$. Furthermore, in the following paragraph it is tried to understand the Alamouti basic phenomenon on STBC over MIMO channels and its application into a secure MIMO communication link

The space time block code (STBC) technique is a special form of diversity which is a complex combination of coding theory, matrix algebra and signal processing. Space-Time block coded multiple input-multiple output (MIMO) systems are capable of achieving maximum diversity over a frequency selective channel (FSC) [3]. However, acquiring knowledge of the channel state information (CSI) for an FSC with many taps is prohibitively complex. It is a technique which operates on a block of input symbols producing a matrix and outputs whose columns and rows represent time and antennas positions, respectively. A key feature of STBC is the provision of full diversity with extremely low encoder/decoder complexity [12], [14]. Therefore, STBC can be effectively used to exploit the advantage of MIMO systems.

To explain the Alamouti STBC basic idea, consider Fig. 1 with two transmitters and one receiver [12]. For explanation the basic idea, the Alamouti STBC is taken [12]. Alamouti code is shown in Fig. 1 with two transmitters and one receiver.

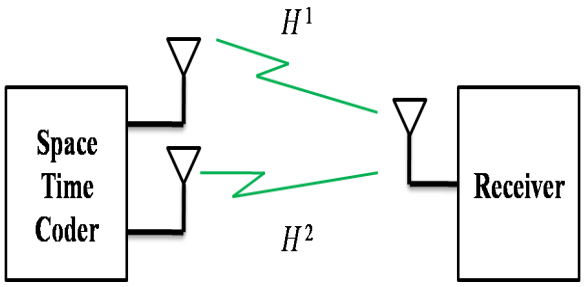

Fig. 1. Block diagram for Alamouti code

First, the transmitter picks two symbols from the input signal constellation, where the signal constellation set consists of $M = 2^m$. If s_1 and s_2 are the selected symbols, the transmitter sends s_1 by antenna one and $-s_2$ by antenna two at the time instant one. Then at the next time duration, it transmits s_2 and s_1 or their conjugated signal by antennas one and two, respectively. Therefore, the transmitted codeword is :

$$S = \begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \quad (1)$$

Where $*$ denotes the symbol conjugates. Let us assume that the path gains from transmit antennas one and two to the receive antenna are $h_1 = \alpha_1 e^{j\theta 1}$ and $h_2 = \alpha_1 e^{j\theta 2}$, respectively. Then the decoder receives signals r_1 and r_2 at times one and two, respectively as:

$$\begin{cases} r_1 = s_1 h_1 + s_1 h_2 + n_1 \\ r_2 = -s_2^* h_1 + s_1^* h_2 + n_2 \end{cases} \quad (2)$$

Where $n_1$and n_2 are zero-mean Gaussian noise processes. If the receiver knows the channel path gains h_1 and h_2, then $(\widetilde{s_1}, \widetilde{s_2})$ are the estimation value of the transmit signal pair (s_1, s_2).

$$\begin{cases} \widetilde{s_1} = r_1 h_1^* + r_2^* h_2 \\ \widetilde{s_2} = r_2 h_1^* - r_1^* h_2 \end{cases} \quad (3)$$

III. The Proposed Security Method

For the proofs of the proposed method, the following investigations are added. Instead of transmitting the signal in its original form given in (1), the transmit signal set is produced by changing the transmission symbols to provide ambiguity in receiver for confusion purposes. This act is fulfilled by the rotating the code matrix. This proposed method analysis is given by following subsections:

A. First key Matrix with 90^o symbols rotation

The first key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{90\ degrees\ rotates} \begin{pmatrix} s_1^* & -s_2^* \\ s_2 & s_1 \end{pmatrix} \quad (4)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) which seems like noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set as:

$$\begin{pmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{pmatrix} \xrightarrow{90\ degrees\ rotates} \begin{pmatrix} h_2^* & h_1^* \\ -h_1 & h_2 \end{pmatrix} \quad (5)$$

B. Second key Matrix with 180^o symbol rotation

The second key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{180\ degrees\ rotates} \begin{pmatrix} -s_2^* & s_1 \\ s_1^* & s_2 \end{pmatrix} \quad (6)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) which is $(s_1^*, -s_2^*)$ as noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set.

C. *Third key Matrix with 270^o symbol rotation*

The third key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{270\ degrees\ rotates} \begin{pmatrix} s_2 & s_1^* \\ s_1 & -s_2^* \end{pmatrix} \quad (7)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) as (s_2, s_1^*) which seems like noise again. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set as:

$$\begin{pmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{pmatrix} \xrightarrow{270\ degrees\ rotates} \begin{pmatrix} h_1^* & -h_2 \\ h_2^* & h_1 \end{pmatrix} \quad (8)$$

D. *Fourth key changing the main symbol diagonal Matrix*

The fourth key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{\text{main diagonal}} \begin{pmatrix} s_1^* & s_2 \\ -s_2^* & s_1 \end{pmatrix} \quad (9)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) as (s_1^*, s_2) which seems like noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set.

E. *Fifth key changing the minor symbol diagonal Matrix*

The fifth key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{\text{minor diagonal}} \begin{pmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{pmatrix} \quad (10)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) as $(s_1, -s_2^*)$ which seems like noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set.

F. *Sixth key multiplying a minus to main symbol diagonal Matrix*

The sixth key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{\text{The negetive main diagonal}} \begin{pmatrix} -s_1 & s_2 \\ -s_2^* & -s_1^* \end{pmatrix} \quad (11)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) as $(-s_1, s_2)$ which seems like noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set.

G. *Seventh key changing the minor and main diagonal Matrix in symbol*

The seventh key matrix rotation of (1) is:

$$\begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \xrightarrow{\text{The minor and main diagonal}} \begin{pmatrix} s_1^* & s_2^* \\ -s_2 & s_1 \end{pmatrix} \quad (12)$$

At the receiver, employing (3), the attacker is faced with the rotated estimation value of the transmit signal pair (s_1, s_2) as (s_1^*, s_2^*) which seems like noise. But the intended destination must rotate H matrix according to the known rotation given by the transmitter considering the given key set.

Therefore, the symbol changes by matrix rotation can enhance ambiguity at receiver for the attackers. For instance, to receive a single symbol like s_1, the corresponding set, namely, $\{s_1, -s_1, s_1^*, -s_1^*\}$ and for s_2, $\{s_2, -s_2, s_2^*, -s_2^*\}$ could be received. Indeed, the attacker is faced with a number of received symbols to detect but the intended receiver is faced with only one correct symbol pair bearing his key set.

IV. Simulation Results

A. *The Performance Properties*

In this section, the effectiveness of the proposed transmission scheme is simulated by evaluating the bit error rate (BER) of the intended receiver and the attacker. The channel is assumed to be a block Rayleigh fading channel, i.e., it is constant during the transmission of one packet, but randomly changes between packets so that the channel coefficients do not actually change during one hob transmission. BER performance of the intended receiver and the attacker are measured under the proposed scheme with two transmit and one receive antennas with BPSK, 4PSK

modulation techniques. The white Gaussian stream ciphers [16] are employed to generate the sequence key stream.

The first simulation results are obtained considering the transmitter to have perfect channel state information.

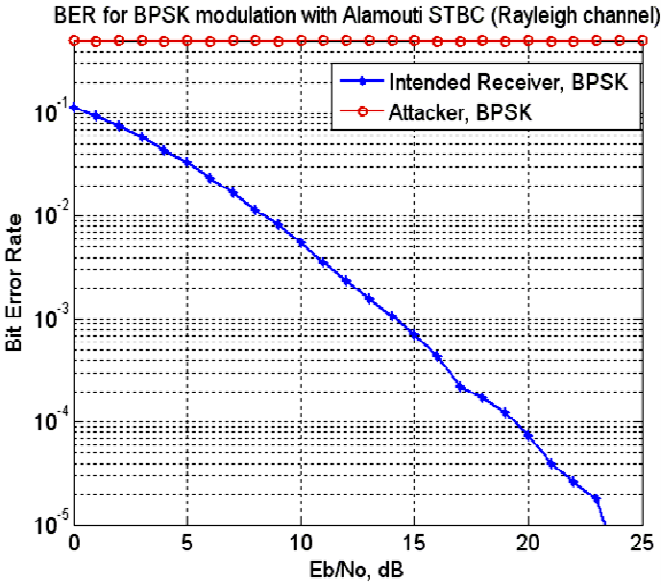

Fig. 3. BER performance of secure communication architecture for BPSK based on STBC

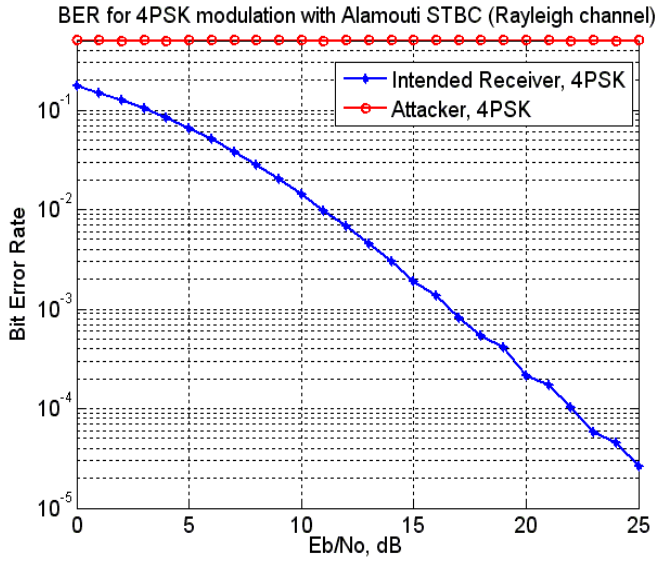

Fig. 4. BER performance of secure communication architecture for 4PSK based on STBC

The simulation results in Fig. 3 and Fig. 4 show that the attacker can only receive noise while the intended receiver receive signal with errors for a normal STBC system. The second set of simulation results is obtained considering the transmitter to have imperfect channel state information (i.e. partial channel state information at transmitter and receiver). The channel state information (CSI) is estimated by inserting pilot sequences in the transmitted signals. It is assumed that the channel is constant over the duration of a frame and independent between frames.

B. *The Secret Capacity*

In [17], the secrecy capacity C_s is defined as the maximum rate at which a transmitter can reliably send information to an intended receiver such that the rate at which the attacker obtains this information is arbitrarily small. In other words, the secrecy capacity is the maximal number of bits that a transmitter can send to an intended receiver in secrecy for every use of the channel. If the channel from the transmitter to the intended receiver and the channel from the transmitter to the attacker have different bit error probabilities (BER) ε and δ, respectively, the secret capacity C_s is [18].

$$C_s = \begin{cases} h(\delta) - h(\varepsilon), & if\ \ \delta > \varepsilon \\ 0\ , & otherwise \end{cases} \tag{13}$$

Where h denotes the binary entropy function defined by

$$h(p) = -plog_2^p - (1-p)log_2^{(1-p)} \tag{14}$$

The secrecy capacity of the multi-antenna system is introduced in [18]. This depends on the existence of the enhanced channel. This characterization is directly built through the optimal transmission strategy in the multi-antenna system. Our schemes are not built on this approach. Therefore, we still use the simple result in (13) to evaluate the secret capacity of the new schemes. Based on the BER results in Fig. 3 for the intended receiver and attacker, the secret capacity is calculated by (14) and shown in Fig. 5. It is assumed that the transmitter and the intended receiver can achieve the normal communication when the BER performance of the intended receiver is less than 10^{-2}. Therefore, the proposed method can achieve sufficiently good secret capacity within the corresponding SNR ranges.

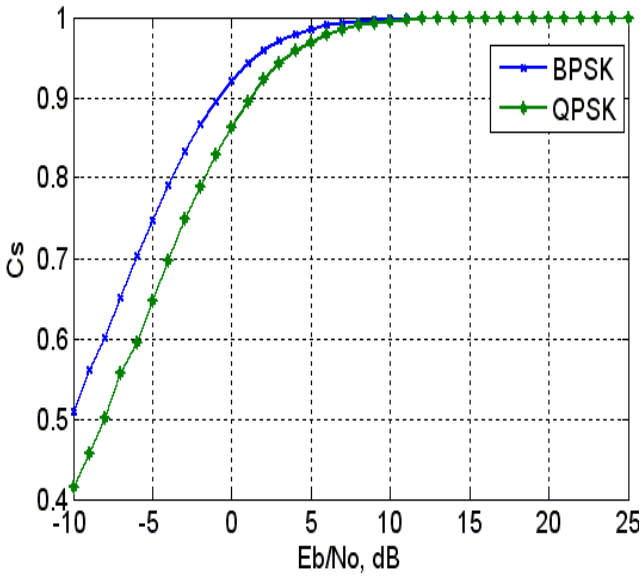

Fig. 5. The secret channel capacity from the BER performance results based on proposed scheme

V. CONCLUSION

A secure space-time block coding scheme joins channel encoding with encryption algorithms into one process. In this paper, an adaptive secure space-time block coding algorithm based on adaptive and pseudorandom sequence key of the STBC is presented. The various crypto analytical attacks against this scheme are then investigated. In the proposed method, the eavesdroppers can only receive the noisy signals, so they have to find the secret key in the noisy key stream. Therefore, these schemes provide stronger security for secure communication links. A more detailed study on the robustness of the scheme against attacks to find the secret key is left for future publications. Actually, this method can be extended to all kinds of space-time block codes schemes. Simulation results show that we can obtain an efficient data transmission system with good reliability as well as a good security.

REFERENCES

[1] Shannon, C.E.: 'A mathematical theory of communication', Bell Syst. Tech. J., 1948, 7, pp. 379–423 and pp. 623–656.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[3] A.O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[4] H. Koorapaty, A.A. Hassan, S. Chennakeshu, "Secure Information Transmission for Mobile Radio," *IEEE Trans. Wireless Communications*, pp. 52–55, July 2003.

[5] S.Hayking, *Blind Deconvolution*, Prentice Hall, Englewood Cliffs, NJ, 1994.

[6] Y. Hua, S. An and Y. Xiang, "Blind identification of FIR MIMO channels by decorrelation subchannels," *IEEE Trans. Signal Processing*, vol. 51, no. 5, pp. 1143-1155, May 2003.

[7] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, May 2007.

[8] H. Kim and J. D. Villasenor, "Secure MIMO communcications in a system with equal numbers of transmit and receive antennas," *IEEE Communications Letters*, vol. 12, no. 5, pp. 386–388, May 2008.

[9] C. H. Bennett, G. Brassard, C. Crpeau, and U. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915- 1923, Nov. 1995. no. 6, pp. 1426-1428, Nov. 1990.

[10] "Data encryption standard," FIPS PUB 46, National Bureau of Standards, Washington, D. C., Jan. 1997.

[11] S. Alamouti, "A simple transmitter diversity scheme for wireless communications," IEEE Journal on Selected Areas in Comm., Vol. 16, no. 8, pp. 1451-1458, Oct. 1998.

[12] V. Tarokh, N. Seshadri and A.R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communications: performance Criterion and Code Construction," IEEE Trans. on Inf. Theory, vol. 44, no. 2, pp. 744-765, 1998.

[13] V. Tarokh, H. Jafarkhani, A.R. Calderbank, "Space-time block codes from orthogonal designs," IEEE Trans. On Inf. Theory, vol. 45, no. 5, pp. 1456-1467, July 1999.

[14] J. Daemen and V. Rijmen, "AES Proposal: Rijndael, AES Algorithm submission," Sep. 1999.

[15] Y. Nawaz and G. Gong, "WG: A family of stream ciphers with designed randomness properties," Information Sciences, vol. 178, no. 7, pp. 1903-1916, April 1, 2008.

[16] A. D. Wyner, "The Wire-tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[17] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, Mar. 1993.

[18] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiantenna wiretap channel," IEEE Trans. Inf. Theory, to appear.

Mahdi Nouri (S'09–M'11) received the B.Sc and M.Sc degrees in communication secure system engineering from Tabriz University, Tabriz, Iran, in 2009, the M.S. degree in communication system engineering from Iran University of Science and Technology (IUST), Tehran, in 2011. From 2007 to 2009, he was a Research Engineer and then Assistant Scientist, working on signal processing and DSP and , at the Institute of DSP, Tabriz Academy of Sciences, Iran. Currently, His research interests are in the areas of Digital signal processing, Channel Coding and Cryptography.

Abolfazl Falahati was born in Tehran, Iran. He received the B.Sc. (Hons) degree in electronics engineering from Warwick University, U.K., in 1982, and the M.Sc. degree in digital communication systems and the Ph.D. degree in digital communication channel modeling from Loughborough University, U.K., in 1984 and 1988, respectively. In 1993, he was a Postdoctoral Researcher in HF channel signaling, Rotherford Appleton Laboratory, Oxford, U.K. Since 1994, he has been an Associate Professor and faculty member with Department of Electrical Engineering, Iran University of Science and Technology (IUST), Tehran. His research interests are ultrawideband communication systems and antenna designs, mimo channel modeling and relay networks, cognitive radio and wireless sensor networks, mimo relay network modeling and simulation, information theory and channel coding techniques, cryptography, secure communication system managements and applications, universal mobile for telecommunication system (UMTS) in adaptation with GSM mobile system and WiMAX systems.