A UNITARY SPACE-TIME CODING SCHEME FOR UWB SYSTEMS AND ITS APPLICATION IN WIRELESS SECURE COMMUNICATIONS

Yanbing Zhang and Huaiyu Dai
Department of Electrical and Computer Engineering
NC State University
Raleigh, N.C., USA
{yzhang, Huaiyu_Dai}@ncsu.edu

ABSTRACT

Recent research reveals that information security and information-hiding capabilities can be enhanced by proper exploitation of space-time techniques. Meanwhile, intrinsic properties of ultra wideband (UWB) signals make it an outstanding candidate for secure applications. In this paper, we propose a unitary space-time coding scheme for impulse radio UWB systems. Its transmission secrecy, including low probability of intercept (LPI), low probability of detection (LPD) and anti-jamming performance, is analyzed. Theoretical and simulation results show its superiority in wireless secure communications over other concurrent schemes.

1. INTRODUCTION

The boost in the amount of information conveyed by wireless links, especially for military and business uses has been prompting a corresponding increasing demand for the transmission security. Currently, chief among the methods of information security is cryptography. Working at the network or higher layers mostly, cryptography aims to deny the unintended attempt on the information content by making various transformations of the original message. Protection against unintended disclosure of the information, however, might also be enhanced at the physical layer. Three features are generally desired for transmission secrecy - low probability of intercept (LPI), low probability of detection (LPD), and anti-jamming protection. LPI, LPD and anti-jamming properties can be regarded as the counterparts of the three most important objectives in cryptography: integrity, secrecy, and availability.

A recent breakthrough in wireless communications, multi-input multi-output (MIMO) techniques, vastly expands the capacity and range of communications. An information-theoretic framework for investigating communication security in wireless MIMO links is proposed in [1]. One of the principal conclusions there is that proper exploitation of space–time diversity at the transmitter can enhance information security and information-hiding capabilities.

Research interests in ultra wide band (UWB) wireless communications have also been proliferated in both industry and academia recently [2]. Besides many other advantages, UWB also offers salient features, like ultra-short pulse and noise-like power density, for secure communications [3][4].

Intent to jointly exploit the advantages of MIMO and UWB has also been initiated. In particular, UWB-MIMO systems which employ space-time block coding have been proposed in [5][6]. These work show performance improvement over the conventional single-input single-output UWB systems for commonly adopted modulation and multiple-access techniques, in both single-user and multi-user scenarios. But to the best of our knowledge, there is no formal discussion on security issues when multiple antennas are introduced to UWB systems.

It is found in [1] that unitary space time codes with constant spatial inner product may achieve perfect secrecy in certain circumstances. This motivates us to investigate a unitary space-time coding for UWB systems, coined as USTC-UWB. Based on performance analysis of USTC-UWB in a multi-path channel, we demonstrate that USTC-UWB can achieve superior LPI, LPD and anti-jamming performances, making it an outstanding candidate for wireless secure communications. The rest of the paper is organized as follows. Section 2 presents the proposed USTC-UWB scheme, together with its BER performance analysis. Security metrics for USTC-UWB, including LPI, anti-jamming and LPD properties, are analyzed in Section 3. The trade-off between anti-jamming and LPD performance is also addressed. Section 4 concludes the paper.

2. UNITARY SPACE-TIME CODING FOR UWB SYSTEMS

2.1. Construction of Uniatry Space-Time codes for UWB

One of the motivations for unitary space-time coding [7] is that it doesn't require the receiver to know the channel. Typically an M-element transmitter antenna array sends a $T \times M$ signal matrix S over T time samples to N receive antennas. S is chosen from a transmit constellation matrix set $\{\Phi_l, l = 1,2,...2^{TR}\}$, where Φ_i satisfies $\Phi_l^* \Phi_l = I$ and R is desired transmission rate.

For UWB signals, if we constrain $M = T$ (without loss of generality), the transmit signal matrix can be formed as

$$S = \begin{bmatrix} \phi_{11}p(t) & \phi_{12}p(t) & \cdots & \phi_{1M}p(t) \\ \phi_{21}p(t-T_f) & \phi_{22}p(t-T_f) & \cdots & \phi_{2M}p(t-T_f) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{M1}p(t-MT_f) & \phi_{M2}p(t-MT_f) & \cdots & \phi_{MM}p(t-MT_f) \end{bmatrix}. \quad (1)$$

where $\Phi = \{\phi_{ij}\}$ is an unitary matrix to be designed, $p(t)$ is the fundamental transmit pulse, and T_f represents the frame interval (corresponding to one symbol transmission). In this paper the second derivative of a Gaussian pulse is chosen for $p(t)$ as

$$p(t) = A_c\left[1 - \left(4t/T_p\right)^2\right] e^{-\left(4t/T_p\right)^2} \quad (2)$$

with T_p denoting the pulse interval and A_c chosen such that the pulse has unit energy.

This work was supported in part by the National Science Foundation under Grant CCF-0515164.

Since UWB systems employ baseband transmission, it is convenient to set $\{\Phi_{ij}\}$ to be real. In the following, we propose novel real orthogonal constellation group codes based on Hadamard transform. For $n = 2^p$, with p an integer, a Hadamard matrix is generated by a simple recursion

$$H_n = \begin{bmatrix} H_{n/2} & H_{n/2} \\ -H_{n/2} & H_{n/2} \end{bmatrix} \tag{3}$$

with $H_1 = 1$. So our group codes can be defined by

$$\left\{\Phi_0, \Phi_1, ...\Phi_{2^{TR}-1}\right\} = \left\{\Omega_M(0), \Omega_M(1), ..., \Omega_M(2^{TR}-1)\right\},$$

where the $M \times M$ matrix $\Omega_M(i)$ is recursively generated as

$$\Omega_M(i) = \frac{1}{\sqrt{2}} \begin{bmatrix} \Omega_{M/2}(i) & \Omega_{M/2}(i) \\ -\Omega_{M/2}(i) & \Omega_{M/2}(i) \end{bmatrix}, \tag{4}$$

with the initial matrix given by

$$\Omega_2(i) = \begin{bmatrix} \cos(\pi \cdot i / 2^{TR}) & \sin(\pi \cdot i / 2^{TR}) \\ -\sin(\pi \cdot i / 2^{TR}) & \cos(\pi \cdot i / 2^{TR}) \end{bmatrix}. \tag{5}$$

Since $\Omega_M(i)\Omega_M(i)^T = \Omega_M(i)^T \Omega_M(i) = I_M$, these group codes fall into the category of real orthogonal design. Also note that the squared L_2 norm for every column and row of matrices so generated (corresponding to the total transmit power in space and time, respectively) is equal to 1. This design works well for any transmission rate R and $M = 2^p$ transmit antennas (as shown in 2.2). For other values of M, a design based on cyclic group codes can be employed [8], with some performance loss, whose discussion is omitted due to space limitations.

We consider an L-path frequency-selective channel, for which the impulse response from the ith transmit antenna to the jth receive antenna can be described as

$$h_{ij}(t) = \sum_{l=0}^{L-1} h_{ij}^l \delta(t - \tau_l), \tag{6}$$

with τ_l representing the delay and h_{ij}^l the complex amplitude of the lth path, respectively. At the receiver, we employ an L-finger Rake receiver, each adopting the delayed versions of the received monocycle as the reference waveform. It is shown in [6] that if $\tau_l - \tau_{l-1} \geq T_p$, $\forall \tau$, and the autocorrelation function of the pulse $\gamma(\tau) = 0$ for $|\tau| \geq T_p$, all L correlators' outputs at the jth receive antenna can be collected in a $T \times L$ (equivalently $M \times L$) matrix

$$Y_j = \sqrt{E_0 / M} S H_j + W_j, \tag{7}$$

where E_0 is the average transmit energy per symbol, W_j is the circularly symmetric complex Gaussian background noise with spectral height $N_0/2$, and the $M \times L$ matrix H_j collects the multipath gain as

$$H_j = \begin{pmatrix} h_{0j}^0 & h_{0j}^1 & \cdots & h_{0j}^{L-1} \\ h_{1j}^0 & h_{1j}^1 & \cdots & h_{1j}^{L-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{(M-1)j}^0 & h_{(M-1)j}^1 & \cdots & h_{(M-1)j}^{L-1} \end{pmatrix}. \tag{8}$$

The decision rule for the ML decoder can be stated as

$$\hat{\Phi}_{ML,CSI} = \arg \min_{\Phi \in \{\Phi_1, \Phi_1, ... \Phi_{2^{TR}}\}} \sum_{j=1}^{N} \left\| Y_j - \sqrt{E_0 / M} \Phi H_j \right\|^2. \tag{9}$$

2.2. Performance of USTC-UWB System

Let $\Psi(l) = E[|h_{ij}^l|^2]$, then the pair-wise error probability is given by

$$P(\Phi \to \Phi') \leq \left(\prod_{m=1}^{r} \prod_{l=0}^{L-1} \lambda_m \frac{\Psi(l)}{4M} \frac{E_0}{N_0} \right)^{-N}, \tag{10}$$

where r is the rank of $\Phi - \Phi'$ and λ_m, $m = 1, ..., r$ are the non-zero eigen-values of $(\Phi - \Phi')(\Phi - \Phi')^*$. For the group codes we design above, it can be shown that $\Omega_M(i) - \Omega_M(j), \quad \forall i \neq j$ has full rank, i.e. $r = M$ (thus full diversity is achieved), and all the eigenvalues are identical, given by

$$\lambda_m = 4 \sin^2 \left(\frac{\pi (i-j)}{2^{TR}} \right), \; m = 1, 2, ..., M. \tag{11}$$

Therefore

$$P_e \leq \left(\prod_{l=0}^{L-1} \left(\sin^2 \left(\frac{\pi}{2^{TR}} \right) \frac{\Psi(l)}{M} \frac{E_0}{N_0} \right) \right)^{-MN}. \tag{12}$$

Figure 1. presents the simulation BER and upper bound (12) for our proposed USTC-UWB scheme. We can see that the analytical bounds match the exact BER at high SNR region, which testifies the validity of our analysis.

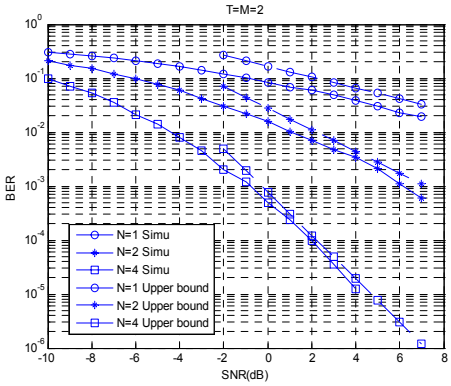

Figure 1. BER performance of USTC-UWB and its upper bound.

3. SECURITY PERFORMANCE ANALYSIS

3.1. Low Probability of Intercept (LPI)

As we discussed in 2.1, the group codes we design have constant spatial inner product. When the channel is unknown to the receiver, the maximum-likelihood (ML) decoding is given by [7]

$$\hat{\Phi}_{ML,NCSI} = \arg \max_{\Phi \in \{\Phi_1, ..., \Phi_{2^{TR}}\}} \sum_{j=1}^{N} \left\| Y_j^* \Phi \right\|^2 = \arg \max_{\Phi} \sum_{j=1}^{N} trace\left\{ Y_j^* \Phi \Phi^* Y_j \right\} \tag{13}$$

and when the channel is known to the receiver, the ML decision rule is given by (9). So if we can keep the desired user informed, but the eavesdropper uninformed, then the later will be absolutely blind to the transmitted information (see (13)). Thus a perfect secrecy can be achieved.

To reach this objective, we can use a reverse-channel estimation method motivated by [9]. That is, let the desired receiver transmit

pilot signals periodically, by which the transmitter can estimate the channel state information (CSI). Once the transmitter gets the CSI, it can precode the transmit signal to compensate for the effect of the forward channel and make the composite channel effectively constant. Thus, the desired user can be regarded as equivalently informed, while the eavesdropper is still kept uninformed, assuming the independence of the channels between the transmitter and the desired user, and the eavesdropper. This approach is valid when channel reciprocity holds. Otherwise, some secured feedback can be adopted for this purpose [10].

Denote the received signals for the desired user and the eavesdropper as Y and Z respectively, given S transmitted. With the constant spatial inner product property of S, we have $P(Z \mid S) = P(Z)$. So the mutual information

$$I(Z;S) = E\left\{\log \frac{P(Z \mid S)}{P(Z)}\right\} = 0 . \quad (14)$$

The secrecy capacity defined in [11] is then given by

$$C_s \geq I(Y;S) - I(Z;S) = \log_2 \det\left(I_N + \frac{E_0}{MN_0} HW^* WH^* \right). \quad (15)$$

Where W is the precoding weight matrix and H represent the channel between the transmitter and the desired receiver, which is a $MN \times LN$ block diagonal matrix with H_j (see(8)) as the block diagonal elements [12]. It is easy to see that the secrecy capacity is maximized by choosing $W = H^* / \|H\|$ under the constraints of $WH = c$ and $\|W\| = 1$.

3.2. Anti-Jamming

Consider a passband jamming signal $J(t)$ with central frequency f_J, modeled as a continuous-time wide-sense stationary zero-mean random process with bandwidth B_J and the power spectral density

$$S_J(f) = \begin{cases} J_0/2, & |f - f_J| \leq B_J \\ 0, & o.w. \end{cases} . \quad (16)$$

Then the received signal at receive antenna j can be modeled as

$$r_j(t) = \sum_{i=0}^{M-1} \sum_{k=0}^{T-1} \sum_{l=0}^{L-1} h_{ij}^l s_i^k (t - \tau(l)) + J(t) + n_j(t) . \quad (17)$$

with $s_i^k(t-\tau(l)) = \phi_{ik} p(t - kT_f)$ denoting the transmit signal from ith transmit antenna at kth time interval as defined in (1).

Through a single correlator, the output jamming signal is given by

$$J_{out,UWB}(t) = \int_0^{T_f} J(t) p(t) dt , \quad (18)$$

with a power of

$$\begin{aligned} N_{J,UWB} &= E(J_{out,UWB}^2) = E\left(\int_0^{T_f} \int_0^{T_f} J(t_1) J(t_2) p(t_1) p(t_2) dt_1 dt_2 \right) \\ &= \int_0^{T_f} \int_0^{T_f} R_J(t_1 - t_2) p(t_1) p(t_2) dt_1 dt_2 \\ &= \int_0^{T_f} \int_0^{T_f} \int_{-\infty}^{\infty} S_J(f) df\, p(t_1) e^{j2\pi f t_1} p(t_2) e^{-j2\pi f t_2} dt_1 dt_2 \\ &= \frac{J_0}{2} \int_{f_J - B_J}^{f_J + B_J} |P(f)|^2 df \approx J_0 B_J / 2B_{UWB} \end{aligned} \quad (19)$$

where $P(f)$ is the frequency response of $p(t)$ and B_{UWB} is the bandwidth of UWB pulse . Note that in the last line, we use the fact that the pulse has unit energy. We also assume $P(f)$ remains constant in the range of $[f_J - B_J, f_J + B_J]$ and approximately takes the average value of $1/\sqrt{2B_{UWB}}$. Consider all L correlators, the symbol error rate is bounded by

$$P_{e,UWB} \leq \left(\prod_{l=0}^{L-1} \left(\sin^2\left(\frac{\pi}{2^{TR}}\right) \frac{\Psi(l)}{M} \frac{E_0}{N_0 + LJ_0 B_J / 2B_{UWB}} \right) \right)^{-MN} . \quad (20)$$

3.3. Low Probability of Detection (LPD)

When the channel is unknown, a common detecting approach for the eavesdropper is to use radiometer [3][4], which measures the energy in a bandwidth B over a time interval T_s. If the captured energy is greater than a certain threshold, the presence of a signal is claimed.

In this subsection, we investigate the asymptotic behavior of a radiometer by considering the exponent of the detection error probability. When the product of the observation interval and the bandwidth $T_s B >> 1$, the output statistics of the radiometer can then be assumed as Gaussian [4]. That is,

$$f_{H_0}(y) = \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left\{ \frac{-(y - \mu_n)^2}{2\sigma_n^2} \right\}, \quad (21)$$

$$f_{H_1}(y) = \frac{1}{\sqrt{2\pi}\sigma_{sn}} \exp\left\{ \frac{-(y - \mu_{sn})^2}{2\sigma_{sn}^2} \right\}, \quad (22)$$

where the mean and the variance are given by $\mu_n = 2T_s B$, $\sigma_n^2 = 4T_s B$, $\mu_{sn} = 2T_s B + 2\gamma$, $\sigma_{sn}^2 = 4T_s B + 4\gamma$ and $\gamma = E_0 / N_0$ denotes SNR.

To study the asymptotic behavior, we keep the observation interval T_s fixed, and assume the number of the observations N_s goes to infinity. The Chernoff error exponent is defined as the exponentially decreasing rate of the detection error probability

$$\rho = \liminf_{N_s \to \infty} \frac{1}{N_s} \ln P_{\text{det\_err}} . \quad (23)$$

As a negative value, ρ is required to be as large as possible (close to 0) for LPD. By the large deviation technique ([1])

$$\begin{aligned} \rho &= \inf_{\alpha \in [0,1]} \liminf_{N_s \to \infty} \frac{1}{N_s} \ln \int f_{H_1}^{1-\alpha}(y_1, ..., y_{N_s}) f_{H_0}^{\alpha}(y_1, ..., y_{N_s}) dy_1, ..., dy_{N_s} \\ &= \min_{\alpha \in [0,1]} \left\{ (1-\alpha) \ln \sigma_n + \alpha \ln \sigma_{sn} - \frac{1}{2} \ln\left[(1-\alpha)\sigma_n^2 + \alpha \sigma_{sn}^2 \right] \right. \\ &\quad \left. - \frac{(1-\alpha)\alpha(\mu_{sn} - \mu_n)^2}{2((1-\alpha)\sigma_n^2 + \alpha \sigma_{sn}^2)} \right\}. \end{aligned} \quad (24)$$

In general, it is very hard to get an explicit expression for ρ from (24). But in secure communication scenarios, we can assume $T_s B >> \gamma$ (which generally holds for UWB signals). This assumption implies $\sigma_n^2 \approx \sigma_{sn}^2$, and ρ is obtained by taking $\alpha = 1/2$ as

$$\rho \approx -\frac{\gamma^2}{2T_s B} . \quad (25)$$

This nice and simple relationship coincides with the intuition that a system with larger time-bandwidth product owns better secure properties. It also explicitly illuminates the trade-off between anti-jamming and LPD performance: while the performance of the desired user in the presence of jamming (see (20)) will certainly

benefit from a larger transmit power, such an SNR increase inevitably leads to a higher probability of being detected by the eavesdropper. Figure 2. gives a schematic demonstration of this tradeoff, which also advocates the advantages of employing multiple antennas.

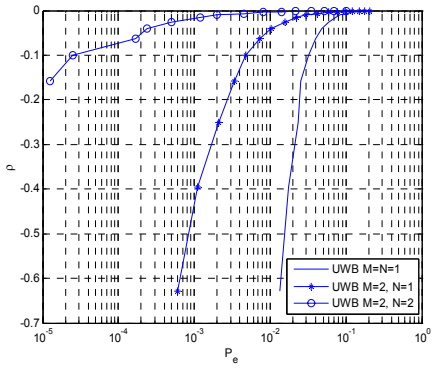

Figure 2. Tradeoff between LPD and anti-jamming

3.4. Comparison with Direct-Sequence Spread Spectrum (DS-SS) Techniques

Direct-sequence spread spectrum (DS-SS) signals are also widely used as a secure communications technique. Due to its much larger bandwidth, UWB is expected to outperform DS-SS for transmission secrecy. An immediate conclusion from (25) is that UWB has a better asymptotic LPD performance than DS-SS due to larger bandwidth and lower SNR, given the same observation interval T_s. This conforms to earlier observations in [3] and [4]. In the following, we further examine the anti-jamming performance.

Let $\{c_n\}$ denote the pseudo-random code sequence of the DS-SS scheme (i.i.d. Bernoulli), $p_c(t)$ the chip waveform, T_b the bit interval, T_c the chip interval, and $L_c = T_b / T_c$ the spreading ratio. Then the output jamming signal of the DS-SS receiver is

$$J_{out,DSSS}(t) = \int_0^{T_b} J(t) \sum_{n=0}^{L_c-1} c_n p_c(t - nT_c) dt \,. \qquad (26)$$

For fair comparison with UWB, we assume $p_c(t)$ also takes the form of (2), and has the energy of $1/L_c$. Then following a similar procedure as in the UWB case, it is not difficult to get

$$N_{J,DSSS} = E(J^2_{out,DSSS}) = \frac{L_c J_0}{2} \int_{f_J - B_J}^{f_J + B_J} |P_c(f)|^2 df \approx J_0 B_J / 2B_{DSSS} \,. \qquad (27)$$

where $P_c(f)$ is the frequency response of $p_c(t)$ and B_{DSSS} is the bandwidth of DS-SS signal .

Comparing (19) and (27), it is observed that the output jamming power for DS-SS is larger than that for UWB as long as $B_{UWB} > B_{DSSS}$, which means UWB provides a better anti-jamming protection than DS-SS. In Figure 3. we compare the performance of unitary space-time coding for UWB and DS-SS signals. The simulation parameters are set as $B_{UWB} = 500MHz$, $B_{DSSS} = 5MHz$ and $L_c = 16$ .We can see UWB and DS-SS systems possess the same diversity gain at high SNR. But UWB steadily outperforms DS-SS due to better anti-jamming properties.

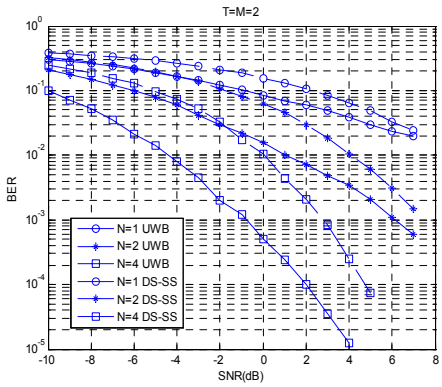

Figure 3. Anti-jamming performance comparison of UWB and CDMA

4. CONCLUSIONS

Motivated by some recent research progress on applying MIMO in UWB and secure communications, we propose a new unitary space time coding scheme for impulse radio UWB systems. Analysis and numerical results demonstrate that it not only improves the performance of conventional single-antenna UWB systems, but also offers prominent benefits on LPI, LPD and anti-jamming protection, which makes it an ideal candidate for wireless secure communications, especially for short-distance applications.

5. REFERENCES

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

[2] L. Yang and G. B. Giannakis, "Ultra-wideband communications-An idea whose time has come," *IEEE Signal Processing Magazine*, vol. 21, no. 6, pp. 26-54, Nov. 2004.

[3] A. Bharadwaj and J. K. Townsend, "Evaluation of the covertness of time-hopping impulse radio using a multi-radiometer detection system," *Proc. of IEEE MILCOM 2001*, vol. 1, pp. 128-134, 2001.

[4] D. R. McKinstry and R. M. Buehrer, "Issues in the performance and covertness of UWB communications systems", *IEEE Midwest Symposium on Circuits and Systems*, pp. 601-604, Tulsa, Oklahoma, August 2002.

[5] L. Yang and G. B. Giannakis, "Analog space-time coding for multi-antenna ultra-wideband transmissions," *IEEE Trans. on Communications*, vol. 52, no. 3, pp. 507-517, March 2004.

[6] W. P. Siriwongpairat, M. Olfat, and K. J. R. Liu, "Performance analysis and comparison of time-hopping and direct-sequence UWB-MIMO systems," *EURASIP Journal on Applied Signal Processing Special Issue on UWB - State of the Art,* vol. 2005, no. 3, pp. 328-345, Mar. 2005.

[7] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat fading," *IEEE Trans. Inform. Theory*, vol. 46, no.2, pp. 543–564, Mar. 2000.

[8] B. L. Hughes, "Optimal space-time constellations from groups," *IEEE Trans. Information Theory*, vol. 49, no. 2, pp. 401-410, Feb. 2003.

[9] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Comm. Letters*, vol. 4, no. 2, pp. 52-55, Feb. 2000.

[10] X. Li, M. Chen and E. P. Ratazzi, "A randomized space-time transmission scheme for secret-key agreement," *the 39th Annual Conference on Information Sciences and Systems* (CISS'2005), Johns Hopkins University, Mar. 16-18, 2005.

[11] I. Csiszar, J. Korner, "Broadcast channel with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp.339-348, May 1978.

[12] A. J. Paulraj, R. Nabar and D. Gore, *Introduction to Space-Time Wireless Communications*, Cambridge, UK: Cambridge University Press,2003.