Research Article

A Real Orthogonal Space-Time Coded UWB Scheme for Wireless Secure Communications

Yanbing Zhang and Huaiyu Dai

Department of Electrical and Computer Engineering, NC State University, Raleigh, NC 27695, USA

Correspondence should be addressed to Huaiyu Dai, hdai@ncsu.edu

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 space-time coding scheme for impulse radio UWB systems. A novel real orthogonal group code is designed for multi-antenna UWB signals to exploit the full spatial diversity gain and achieve the perfect communication secrecy. Its performance in a frequency-selective fading channel is analyzed. The transmission secrecy, including low probability of detection (LPD), low probability of intercept (LPI), and anti-jamming performance, is investigated, and some fundamental tradeoffs between these secrecy metrics are also addressed. A comparison of the proposed scheme with the direct sequence spread spectrum (DSSS) technique is carried out, which demonstrates that proper combination of UWB and space-time coding can provide substantial enhancement to wireless secure communications over other concurrent systems.

1. Introduction

The rapid expansion and proliferation of the wireless applications, especially in military and commercial use, have been prompting a corresponding increasing demand for 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, can also be enhanced at the physical layer. Three features are generally desired for transmission secrecy—low probability of detection (LPD), low probability of intercept (LPI), and anti-jamming protection [1]. LPD, LPI, and anti-jamming properties may be viewed as the counterparts of the three important objectives in cryptography: secrecy, integrity, and availability.

It is well known that code division multiple access (CDMA) systems can provide an inherent physical layer security solution to wireless communications. However, if an eavesdropper can intercept a $2n$-bit sequence segment generated from an n-stage linear feedback shift register, the characteristic polynomial and the entire spreading code can be reconstructed through certain algorithms [2]. This motivates researchers to study enhancing the physical layer built-in security of CDMA systems through secure scrambling [2] or random spreading codes [3]. In 1990s, chaos, a very universal phenomenon in many nonlinear systems, has also been found valuable in secure communication systems due to its extreme sensitivity to initial conditions and parameters [4]. As a hybrid approach, it was shown that CDMA systems employing time-varying pseudo-chaotic spreading sequences can provide improvements with respect to their conventional CDMA counterparts (employing binary-valued pseudo-noise spreading sequences) [5]. Techniques have also been proposed to use the characteristics of the radio channel itself to provide secure key distribution in a mobile radio environment, where the information bearing signal is modified to precompensate for the phase effects of the channel [6].

A recent breakthrough in wireless communications, multiple-input multiple-output (MIMO) technique, vastly expands the capacity and range of communications. An information-theoretic framework for investigating communication security in wireless MIMO links is proposed in

[7]. 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. Particularly, if a source with constant spatial inner products (see Section 3.1) is transmitted over an uninformed link, the cutoff rate of the channel will be equal to zero and the minimum probability of decoding error will be forced to one. There are many known signal constellations satisfying this perfect-secrecy property, like double unitary codes, square unitary codes, or space-time QPSK.

Reference [8] is an exemplary work of this principle, where the authors proposed a secure transmission scheme based on random space-time coding. The basic idea is multiplying a random coefficient to the symbol sequence to make the eavesdropper completely blind with the transmitted signal. However, this random space-time transmission scheme has some drawbacks as well. One is that since the weight should be randomly selected, it has to trade transmission power for secrecy. The other is that before the data transmission, a secure initialization method has to be adopted to set up the feedback channel.

Research interests in ultra-wideband (UWB) wireless communications have also proliferated in both industry and academia recently [9]. Besides many other advantages, UWB also offers salient features, like ultrashort pulse and noise-like power density, for secure communications [10, 11]. 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 [12–14]. More recently, cooperative schemes have also been considered for such systems [15]. These works show performance improvement over the conventional single-input single-output (SISO) UWB systems for commonly adopted modulation and multiple-access techniques, in both single-user and multiuser scenarios. But to the best of our knowledge, there is no formal discussion on security issues when multiple antennas are introduced to UWB systems.

This motivates us to investigate a unitary space-time coding scheme for UWB systems, coined as USTC-UWB, which can simultaneously exploit the information security and information-hiding capabilities of space-time coding and UWB. Compared with general approaches in [7], USTC-UWB employs real space-time codes suitable for UWB signals and can work at any transmission rate. Based on the performance analysis in a multipath fading channel, we demonstrate that USTC-UWB can achieve superior LPD, LPI, and anti-jamming performances, making it an outstanding candidate for wireless secure communications. In the analysis, some fundamental trade-offs between the secrecy metrics are also explicitly addressed. A comparison of USTC-UWB with the direct sequence spread spectrum (DSSS) technique is also carried out, which further demonstrates its advantages.

The rest of the paper is organized as follows. Section 2 describes the system model and assumptions. The proposed USTC-UWB scheme is presented in Section 3, together with its BER performance analysis. Security metrics for USTC-UWB, including LPD, LPI, and anti-jamming properties, are analyzed in Section 4. The trade-off between anti-jamming and LPD performance is also addressed. In Section 5 the simulation results are presented. And finally, some concluding remarks are given in Section 6.

2. System Model

Consider a peer-to-peer UWB communication system equipped with M transmit antennas and N receive antennas. The transmitted waveform at the ith transmit antenna during D time frames can be described as

$$x^{(i)}(t) = \sum_{d=0}^{D-1} \sqrt{\frac{E}{M}} \phi_{id} p\left(t - dT_f\right), \qquad (1)$$

where T_f represents the pulse repetition time (frame) interval corresponding to one symbol transmission. $p(t)$ is the transmitted monocycle with the pulse duration T_p, which is modulated by the (real) space-time code ϕ_{id}. Typically, the duration T_p is between 0.2–2 nanoseconds, resulting in a transmitted signal of ultra-wideband, while T_f is hundred or thousand times longer than T_p [9, 13]. The factor $\sqrt{E/M}$ ensures that the total transmitted power is E. For simplicity, the random time-hopping (TH) codes for multiple access are omitted ([13]).

A class of unitary space-time signals is proposed in [16] for flat-fading channels where neither the transmitter nor the receiver necessarily knows the fading coefficients. Suppose that signals are transmitted in blocks of T time samples, over which interval the fading coefficients are approximately constant. Then, this space-time coding design admits a constellation of $K = 2^{RT}$ (R is the data rate in bits per channel use) signals $\mathbf{S}_k = \sqrt{T}\mathbf{\Phi}_k$, $k = 1,\ldots,K$, with the property that $\mathbf{\Phi}_1,\ldots,\mathbf{\Phi}_K$ are $T \times M$ complex-valued matrices obeying $\mathbf{\Phi}_1^H\mathbf{\Phi}_1 = \cdots = \mathbf{\Phi}_K^H\mathbf{\Phi}_K = \mathbf{I}$ (We use superscripts T and H in this paper to respectively denote the transpose and conjugate transpose operations.).

Extending this discussion to UWB systems, and assuming $M = T$ (without loss of generality), the transmit signal matrix can be formed as

$$\mathbf{S}$$

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

$$(2)$$

where $\mathbf{\Phi} = \{\phi_{ij}\}$ is a unitary matrix to be designed.

Due to its large bandwidth, the channel observed by UWB signals is usually subject to frequency selective fading. So an L-path tapped-delay line model is adopted in the discussion, for which the impulse response from the ith transmit antenna to the jth receive antenna can be described as

$$h_{ij}(t) = \sum_{l=0}^{L-1} h_{ij}^l \delta(t - \tau_l), \qquad (3)$$

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 to exploit the multipath diversity inherent in UWB systems, each adopting the delayed versions of the received monocycle as the reference waveform. It can be shown that if $\tau_l - \tau_{l-1} \geq T_p$, $l = 1,\ldots,L-1$, 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 into a $T \times L$ (equivalently $M \times L$) matrix

$$\mathbf{Y}_j = \sqrt{\frac{E}{M}}\mathbf{SH}_j + \mathbf{W}_j, \qquad (4)$$

where $\mathbf{W}_j$ is the circularly symmetric complex Gaussian background noise with spectral height $N_0/2$, and the $M \times L$ matrix $\mathbf{H}_j$ collects the multipath gain as

$$\mathbf{H}_j = \begin{pmatrix} h_{1j}^1 & h_{1j}^2 & \cdots & h_{1j}^L \\ h_{2j}^1 & h_{2j}^2 & \cdots & h_{2j}^L \\ \vdots & \vdots & \ddots & \vdots \\ h_{Mj}^1 & h_{Mj}^2 & \cdots & h_{Mj}^L \end{pmatrix}. \qquad (5)$$

The decision rule for the ML decoder with channel state information (CSI) can be stated as ([17, Chapter 7])

$$\hat{\mathbf{\Phi}}_{\text{ML,CSI}} = \arg \min_{\mathbf{\Phi} \in \{\mathbf{\Phi}_1, \cdots \mathbf{\Phi}_{2^{TR}}\}} \sum_{j=1}^{N} \left\| \mathbf{Y}_j - \sqrt{\frac{E}{M}}\mathbf{\Phi}\mathbf{H}_j \right\|^2. \qquad (6)$$

3. Unitary Space-Time Coding for UWB Systems

Conveying information with ultrashort pulses, UWB signals can resolve many paths and thus are rich in multipath diversity. This has motivated research toward using Rake receivers to collect the available diversity and thus enhance the performance of UWB communication systems. On the other hand, multi-antenna-based space-time systems offer an effective means of enabling space diversity, which has the potential to improve not only error performance but also capacity. In this section, we consider the construction of space-time codes for UWB systems. A novel unitary space-time code is designed, which can exploit the full spatial diversity and fulfill the purpose of secure communications. In Section 3.1, we first elaborate the design of this space-time code, and then its performance is characterized by a union bound on the block error probability in Section 3.2.

3.1. Construction of Unitary Space-Time Codes for UWB. Rank and determinant criteria are proposed in [18] for space-time code design. That is, in order to achieve the maximum diversity, the matrix $\mathbf{\Phi} - \mathbf{\Phi}'$ has to be full rank for any different codewords $\mathbf{\Phi}$ and $\mathbf{\Phi}'$. It is shown in [19] that all optimal (full-rank) space-time group codes are unitary, which coincide with the secure space-time code structure found in [7].

A family of complex-valued space-time codes is devised in [20] by use of rotated constellation and the Hadamard transform, which can achieve full-rate and full diversity. However, since UWB systems employ baseband transmission, it is necessary to set $\{\phi_{ij}\}$ to be real. In the following, we propose a class of real orthogonal group codes for UWB signals based on Hadamard transform and rotation matrices, which also admit more general transmit antenna settings. For $n = 2^m$, with m an integer, a Hadamard matrix is generated by a simple recursion

$$\mathbf{\Theta}_n = \begin{bmatrix} \mathbf{\Theta}_{n/2} & \mathbf{\Theta}_{n/2} \\ -\mathbf{\Theta}_{n/2} & \mathbf{\Theta}_{n/2} \end{bmatrix} \qquad (7)$$

with $\mathbf{\Theta}_1 = 1$. So our group codes can be defined by

$$\begin{aligned} \mathbf{\Phi} &= \{\mathbf{\Phi}_0, \mathbf{\Phi}_1, \cdots \mathbf{\Phi}_{2^{TR}-1}\} \\ &= \{\mathbf{\Omega}_M(0), \mathbf{\Omega}_M(1), \ldots, \mathbf{\Omega}_M(2^{TR}-1)\}, \end{aligned} \qquad (8)$$

where the $M \times M$ matrix $\mathbf{\Omega}_M(i)$ is recursively generated as

$$\mathbf{\Omega}_M(i) = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{\Omega}_{M/2}(i) & \mathbf{\Omega}_{M/2}(i) \\ -\mathbf{\Omega}_{M/2}(i) & \mathbf{\Omega}_{M/2}(i) \end{bmatrix}, \qquad (9)$$

with the initial rotation matrix given by

$$\mathbf{\Omega}_2(i) = \begin{bmatrix} \cos\left(\pi \cdot \dfrac{i}{2^{TR}}\right) & \sin\left(\pi \cdot \dfrac{i}{2^{TR}}\right) \\ -\sin\left(\pi \cdot \dfrac{i}{2^{TR}}\right) & \cos\left(\pi \cdot \dfrac{i}{2^{TR}}\right) \end{bmatrix}. \qquad (10)$$

Since $\mathbf{\Omega}_M(i)\mathbf{\Omega}_M(i)^T = \mathbf{\Omega}_M(i)^T\mathbf{\Omega}_M(i) = \mathbf{I}_M$, this group code falls into the category of real orthogonal design and admits the perfect-secrecy property (constant spatial inner product) as well (Following the definition in [7], we call $\mathbf{\Omega}_M(i)\mathbf{\Omega}_M(i)^T$ the spatial inner product of $\mathbf{\Omega}_M(i)$ in this paper.). Also note that the squared L_2 norm for every column and row of the matrices so generated (corresponding to the total transmit power in space and time, resp.) is equal to 1. This design works well for any transmission rate R and $M = 2^m$ transmit antennas. For odd values of M, a similar design can be applied for a few special cases with some performance loss. For example, for $M = 3$, a code based on 3-dimensional rotation matrix can be employed:

$$\mathbf{\Omega}_3(i) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\left(\pi \cdot \dfrac{i}{2^{TR}}\right) & \sin\left(\pi \cdot \dfrac{i}{2^{TR}}\right) \\ 0 & -\sin\left(\pi \cdot \dfrac{i}{2^{TR}}\right) & \cos\left(\pi \cdot \dfrac{i}{2^{TR}}\right) \end{bmatrix} \qquad (11)$$

with the group codes given by

$$\mathbf{\Phi} = \{\mathbf{\Omega}_3(0), \mathbf{\Omega}_3(1), \ldots, \mathbf{\Omega}_3(2^{TR}-1)\}. \qquad (12)$$

The code design for general odd M constitutes our future work. In the following, we give some performance analysis of this code for $M = 2^m$ cases.

3.2. Performance of USTC-UWB System. Suppose $\boldsymbol{\Phi}$ and $\boldsymbol{\Phi}'$ are two different transmitted ST codewords, then the pairwise error probability (PEP) conditioned on the channel matrix $\mathbf{H}_j, j = 1, \ldots, N$, is given by [20]

$$P\left(\boldsymbol{\Phi} \longrightarrow \boldsymbol{\Phi}' \mid \mathbf{H}_j, \, j = 1, \ldots, N\right) = Q\left(\sqrt{\frac{E}{4MN_0}d^2(\boldsymbol{\Phi}, \boldsymbol{\Phi}')}\right), \tag{13}$$

which is tightly upper bounded as

$$P\left(\boldsymbol{\Phi} \longrightarrow \boldsymbol{\Phi}' \mid \mathbf{H}_j, \, j = 1, \ldots, N\right)$$
$$\leq \frac{1}{2}\exp\left\{-\frac{E}{8MN_0}d^2(\boldsymbol{\Phi}, \boldsymbol{\Phi}')\right\}. \tag{14}$$

The square distance between $\boldsymbol{\Phi}$ and $\boldsymbol{\Phi}'$ is defined as

$$d^2(\boldsymbol{\Phi}, \boldsymbol{\Phi}') = \sum_{l=1}^{L}\sum_{j=1}^{N}\left(\mathbf{H}_j^{(l)}\right)^H (\boldsymbol{\Phi} - \boldsymbol{\Phi}')^T (\boldsymbol{\Phi} - \boldsymbol{\Phi}')\mathbf{H}_j^{(l)}, \tag{15}$$

where $\mathbf{H}_j^{(l)} = [h_{1j}^l \ h_{2j}^l \ \cdots \ h_{Mj}^l]^T$ is the lth column of $\mathbf{H}_j$ (cf., (5)).

Since $(\boldsymbol{\Phi} - \boldsymbol{\Phi}')^T(\boldsymbol{\Phi} - \boldsymbol{\Phi}')$ is real and symmetric, the eigenvalue decomposition leads to

$$(\boldsymbol{\Phi} - \boldsymbol{\Phi}')^T(\boldsymbol{\Phi} - \boldsymbol{\Phi}') = \mathbf{V}\boldsymbol{\Lambda}\mathbf{V}^T, \tag{16}$$

where the columns $\{v_1, \ldots, v_M\}$ of $\mathbf{V}$ are the orthogonal eigenvectors of $(\boldsymbol{\Phi} - \boldsymbol{\Phi}')^T(\boldsymbol{\Phi} - \boldsymbol{\Phi}')$, and the diagonal matrix $\boldsymbol{\Lambda}$ contains its eigenvalues $\lambda_m, m = 1, \ldots, M$. Using (16), the expression (14) can be written as

$$P\left(\boldsymbol{\Phi} \longrightarrow \boldsymbol{\Phi}' \mid \mathrm{H}_j, \, j = 1, \ldots, N\right)$$
$$\leq \frac{1}{2}\exp\left\{-\frac{E}{8MN_0}\sum_{l=1}^{L}\sum_{n=1}^{N}\sum_{m=1}^{M}\lambda_m\left\|\left(\mathbf{H}_j^{(l)}\right)^H v_m\right\|^2\right\}. \tag{17}$$

Let $\Psi(l) = \mathbf{E}\{\|(\mathbf{H}_j^{(l)})^H v_m\|^2\} = \mathbf{E}\{(\mathbf{H}_j^{(l)})^H v_m v_m^T(\mathbf{H}_j^{(l)})\} = \mathbf{E}\{\|\mathbf{H}_j^{(l)}\|^2\}$, the average pair-wise error probability can be calculated by

$$P(\boldsymbol{\Phi} \to \boldsymbol{\Phi}') = \mathbf{E}\left[P\left(\boldsymbol{\Phi} \longrightarrow \boldsymbol{\Phi}' \mid \mathbf{H}_j, \, j = 1, \ldots, N\right)\right]$$
$$\leq \frac{1}{2}\prod_{l=1}^{L}\prod_{n=1}^{N}\mathbf{E}\left[\exp\left\{-\frac{E}{8MN_0}\lambda_m\left\|\mathbf{H}_j^{(l)}\right\|^2\right\}\right] \tag{18}$$
$$= \frac{1}{2}\prod_{l=1}^{L}\prod_{n=1}^{N}\prod_{m=1}^{M}\left[1 + \frac{E}{8MN_0}\lambda_m\Psi(l)\right]^{-1},$$

where in the last line, we use the fact that the moment generation function for an exponential ranodm variable X with mean $\mathbf{E}(X)$ is $\mathbf{E}(e^{sX}) = (1 - \mathbf{E}(X)s)^{-1}$. Therefore, at the

high signal-to-noise ratio (SNR) region, this probability is upper-bounded by

$$P(\boldsymbol{\Phi} \longrightarrow \boldsymbol{\Phi}') \leq \frac{1}{2}\left(\prod_{m=1}^{r}\prod_{l=0}^{L-1}\lambda_m\frac{\Psi(l)}{8M}\frac{E}{N_0}\right)^{-N}, \tag{19}$$

where r is the rank of $\boldsymbol{\Phi} - \boldsymbol{\Phi}'$.

For the group code we design above, it can be shown that $\boldsymbol{\Omega}_M(i) - \boldsymbol{\Omega}_M(j), \ \forall i \neq j$ has full rank, that is, $r = M$ (thus full diversity is achieved). Following the similar approach in [19] we can get that all the eigenvalues are identical, given by

$$\lambda_m = 4\sin^2\left(\frac{\pi(i - j)}{2^{TR}}\right), \quad m = 1, 2, \ldots, M. \tag{20}$$

Without loss of generality, we can assume $\boldsymbol{\Phi}_0$ is transmitted, therefore the block probability of error could be bounded by

$$P_e \leq \sum_{i=1}^{2^{TR}-1}P(\boldsymbol{\Phi}_0 \longrightarrow \boldsymbol{\Phi}_i)$$
$$\leq \frac{2^{TR} - 2}{2}\left(\prod_{l=0}^{L-1}\left(\sin^2\left(\frac{\pi}{2^{TR}}\right)\frac{\Psi(l)}{2M}\frac{E}{N_0}\right)\right)^{-MN}. \tag{21}$$

4. Security Performance Analysis

There are a variety of metrics used to describe the security properties in a wireless communications system from different aspects. The most important of them is LPD, LPI, and anti-jamming capability. LPD is concerned with preventing adversaries from detecting a radio transmission. Low probability of being detected also means low probability of being jammed by hostile transmitters, which is especially preferable for military communications. Even after being detected, a good secure communication system is still expected to have a strong ability to prevent being intercepted and jammed; therefore these properties should be considered equally important. In this section, we analyze the LPD, LPI, and anti-jamming performance of the proposed USTC-UWB scheme.

4.1. Low Probability of Detection (LPD). When the channel is unknown, a common detecting approach for the eavesdropper is to use radiometer [10, 11], which measures the energy in a bandwidth B over a time interval T_s. The received signal is fed to a bandpass filter with bandwidth B, followed by the squaring device and the T_s-second integrator. The output of the integrator is sent to a comparator with a fixed threshold level. If the integrator output is higher than the threshold, the presence of a signal is declared.

Performance of the radiometer in practical systems has been well studied in [10, 11]. 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 $T_sB \gg 1$, the output statistics of the radiometer

can be modeled as Gaussian [11]. Assuming that H_0 and H_1 are two hypotheses that correspond to the absence and presence of the signal, respectively, then

$$f_{H_0}(y) = \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left\{\frac{-(y-\mu_n)^2}{2\sigma_n^2}\right\},$$
$$f_{H_1}(y) = \frac{1}{\sqrt{2\pi}\sigma_{sn}} \exp\left\{\frac{-(y-\mu_{sn})^2}{2\sigma_{sn}^2}\right\}, \quad (22)$$

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

To study the asymptotic behavior, we keep the observation interval T_s fixed, and assume that the number of the observations N_s goes to infinity as in [7]. The Chernoff error exponent is defined as the exponentially decreasing rate of the detection error probability $P_{\det\_err}$:

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

As a negative value, ρ is required to be as large as possible (close to 0) for LPD. By the large deviation technique [7]

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

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

$$\rho \approx -\frac{\gamma^2}{4T_sB}. \quad (25)$$

This nice and simple relationship coincides with the intuition that a system with larger time-bandwidth product owns better secure properties.

In a secure communications system, the intended communicators (transmitter/receiver) should avoid signal detection/interception, which implies that the minimum transmit power should be used at the transmitter end and the highest sensitive receiver employed at the receiver end. But the communications should also prevent signal jamming, in this regard the transmitter should use the maximum transmit power and employ the least sensitive receiver (see Section 4.3). Therefore, certain trade-off exists between these objectives. Equation (25) also explicitly illuminates the trade-off between anti-jamming and LPD performance: while the performance of the desired user in the presence of jamming will certainly benefit from a larger transmit power, such an SNR increase inevitably leads to a higher probability of being detected by the eavesdropper.

4.2. Low Probability of Intercept (LPI). As we discussed in Section 3.1, the group code we design has constant spatial inner product. When the channel is unknown to the receiver, the maximum-likelihood (ML) decoding is given by [16]

$$\hat{\mathbf{\Phi}}_{ML,NCSI} = \arg \max_{\mathbf{\Phi} \in \{\mathbf{\Phi}_1, \ldots, \mathbf{\Phi}_{2^{TR}}\}} \sum_{j=1}^{N} \left\| Y_j^H \mathbf{\Phi} \right\|^2$$
$$= \arg \max_{\mathbf{\Phi}} \sum_{j=1}^{N} \mathrm{tr}\left\{ \mathbf{Y}_j^H \mathbf{\Phi}\mathbf{\Phi}^H \mathbf{Y}_j \right\}, \quad (26)$$

where $\mathrm{tr}\{A\}$ denotes the trace of matrix A. When the channel is known to the receiver, the ML decision rule is given by (6). So if we can keep the desired user informed, but the eavesdropper uninformed, the later will be absolutely blind to the transmitted information (see (26)). Thus a perfect secrecy can be achieved.

To reach this objective, we can use a reverse-channel estimation method motivated by [6]. That is, let the desired receiver transmit pilot signals periodically, by which the transmitter can estimate the channel state information. 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 [8].

Denote the received signals for the desired user and the eavesdropper by $\mathbf{Y}$ and $\mathbf{Z}$, respectively, given $\mathbf{\Phi}$ transmitted. Since the conditional probability density $P(\mathbf{Z} \mid \mathbf{\Phi})$ depends on $\mathbf{\Phi}$ only through the matrix $\mathbf{\Phi}\mathbf{\Phi}^H$, with the constant spatial inner product property of $\mathbf{\Phi}$ (i.e., $P(\mathbf{Z} \mid \mathbf{\Phi})$ is independent with $\mathbf{\Phi}$), we have

$$P(\mathbf{Z}) = \sum_{\mathbf{\Phi}} P(\mathbf{Z} \mid \mathbf{\Phi})p(\mathbf{\Phi}) = P(\mathbf{Z} \mid \mathbf{\Phi})\sum_{\mathbf{\Phi}} p(\mathbf{\Phi}) = P(\mathbf{Z} \mid \mathbf{\Phi}). \quad (27)$$

So the mutual information is

$$I(\mathbf{Z}; \mathbf{\Phi}) = E\left\{ \log \frac{P(\mathbf{Z} \mid \mathbf{\Phi})}{P(\mathbf{Z})} \right\} = 0. \quad (28)$$

That is, the received signal of the eavesdropper Z does not contain any information of the transmitted signal $\mathbf{\Phi}$.

The secrecy capacity defined in [21] is then given by

$$C_s \geq I(Y; \mathbf{\Phi}) - I(Z; \mathbf{\Phi}) = \log_2 \det\left(\mathbf{I}_{MN} + \frac{E}{MN_0}\mathbf{H}\mathbf{\Sigma}\mathbf{\Sigma}^H\mathbf{H}^H \right), \quad (29)$$

where $\mathbf{\Sigma}$ is the precoding weight matrix and $\mathbf{H}$ represents the channel between the transmitter and the desired receiver, which is an $MN \times LN$ block diagonal matrix with $\mathbf{H}_j$ (see (5)) as the block diagonal elements. It is easy to see that the secrecy capacity is maximized by choosing $\mathbf{\Sigma} = \mathbf{H}^H/\|\mathbf{H}\|$ under the constraints of $\mathbf{\Sigma}\mathbf{H} = c\mathbf{I}_{LN}$ and $\|\mathbf{\Sigma}\| = 1$.

4.3. Anti-Jamming Performance. 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

$$S_J(f) = \begin{cases} \dfrac{J_0}{2}, & |f - f_J| \leq B_J, \\ 0, & \text{otherwise.} \end{cases} \tag{30}$$

It follows that the autocorrelation of $J(t)$ is

$$R_J(\tau) = J_0 \frac{\sin(\pi B_J \tau)}{\pi \tau} \cos(2\pi f_J \tau). \tag{31}$$

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

$$r_j(t) = \sum_{i=0}^{M-1} \sum_{k=0}^{T-1} \sum_{l=0}^{L-1} h_{ij}^l s_i^k(t - \tau(l)) + J(t) + n_j(t) \tag{32}$$

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 (2).

The jamming signal appears at the output of a single correlator as

$$J_{\text{out,UWB}}(t) = \int_0^{T_f} J(t)p(t)dt \tag{33}$$

with a power of

$$\begin{aligned} N_{J,\text{UWB}} &= \mathbf{E}\left(J_{\text{out,UWB}}^2\right) \\ &= \mathbf{E}\left(\int_0^{T_f} \int_0^{T_f} J(t_1)J(t_2)p(t_1)p(t_2)dt_1 dt_2\right) \\ &= \int_0^{T_f} \int_0^{T_f} R_J(t_1 - t_2)p(t_1)p(t_2)dt_1 dt_2 \\ &= \int_0^{T_f} \int_0^{T_f} \int_{-\infty}^{\infty} S_J(f)df \, p(t_1)e^{j2\pi f t_1} p(t_2)e^{-j2\pi f t_2} dt_1 dt_2 \\ &= \frac{J_0}{2} \int_{f_J - B_J}^{f_J + B_J} |P(f)|^2 df \approx \frac{J_0 B_J}{2B_{\text{UWB}}}, \end{aligned} \tag{34}$$

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 that $P(f)$ remains constant in the range of $[f_J - B_J, f_J + B_J]$ and approximately takes the average value of $1/\sqrt{2B_{\text{UWB}}}$. Consider all L correlators, the block error rate is bounded by (cf., (21))

$$P_{e,\text{UWB}}$$

$$\leq \frac{2^{TR} - 2}{2} \left(\prod_{l=0}^{L-1}\left(\sin^2\left(\frac{\pi}{2^{TR}}\right)\frac{\Psi(l)}{2M}\frac{E_0}{N_0 + LJ_0 B_J/2B_{\text{UWB}}}\right)\right)^{-MN}. \tag{35}$$

Direct-sequence spread spectrum signals are also widely used as a secure communications technique. With much larger bandwidth, UWB is expected to outperform DSSS for transmission secrecy [22]. An immediate conclusion from (25) is that UWB has a better asymptotic LPD performance than DSSS due to larger bandwidth and lower SNR, given the same observation interval T_s. This conforms to earlier observations in [10, 11]. In the following, we further examine the anti-jamming performance.

Let $\{c_n\}$ denote the pseudo-random code sequence of the DSSS scheme (independent and identically distributed 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 [22]. Then the jamming signal at the output of the DSSS receiver is

$$J_{\text{out,DSSS}}(t) = \int_0^{T_b} J(t) \sum_{n=0}^{L_c - 1} c_n p_c(t - nT_c)dt. \tag{36}$$

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

$$N_{J,\text{DSSS}} = \mathbf{E}\left(J_{\text{out,DSSS}}^2\right) = \frac{L_c J_0}{2} \int_{f_J - B_J}^{f_J + B_J} |P_c(f)|^2 df \approx \frac{J_0 B_J}{2B_{\text{DSSS}}}, \tag{37}$$

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

Comparing (34) and (37), it is observed that the output jamming power for DSSS is larger than that for UWB as long as $B_{\text{UWB}} > B_{\text{DSSS}}$, which means that UWB provides a better anti-jamming protection than DSSS.

5. Numerical Results

In this section, some numerical examples are provided to better illustrate our main results in the previous sections. We employ UWB signals with frame interval $T_f = 25$ nanoseconds and pulse duration $T_p = 0.2$ nanoseconds The second derivative of a Gaussian pulse is adopted as the transmit pulse

$$p(t) = A_c \left[1 - \left(\frac{4t}{T_p}\right)^2\right] e^{-(4t/T_p)^2} \tag{38}$$

with A_c chosen such that the pulse has unit energy.

First, the simulation BER and upper bound (21) for our proposed USTC-UWB scheme is presented in Figure 1. We can see that employing multiple antennas for UWB signals dramatically improves the BER performance and analytical bounds match the exact BER at the high SNR region, which testifies the validity of our analysis.

Figure 2 gives a schematic demonstration of the tradeoff between LPD and anti-jamming performance, where the relationship between the asymptotic detection error probability and the BER is visualized. Note that although an
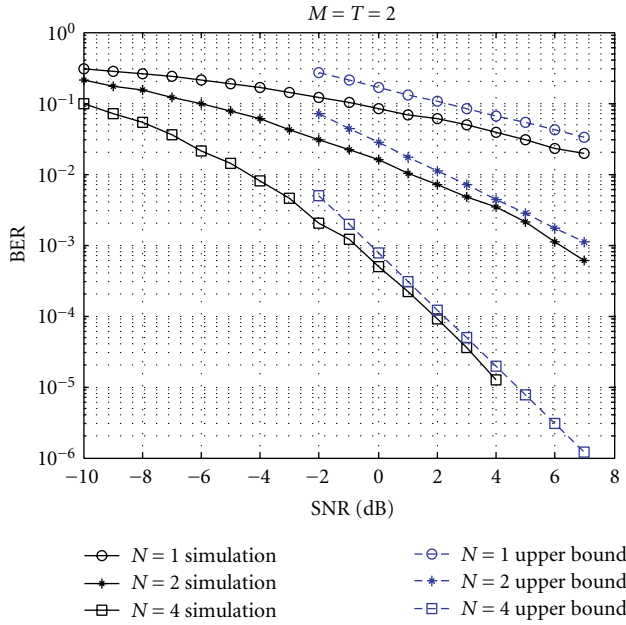
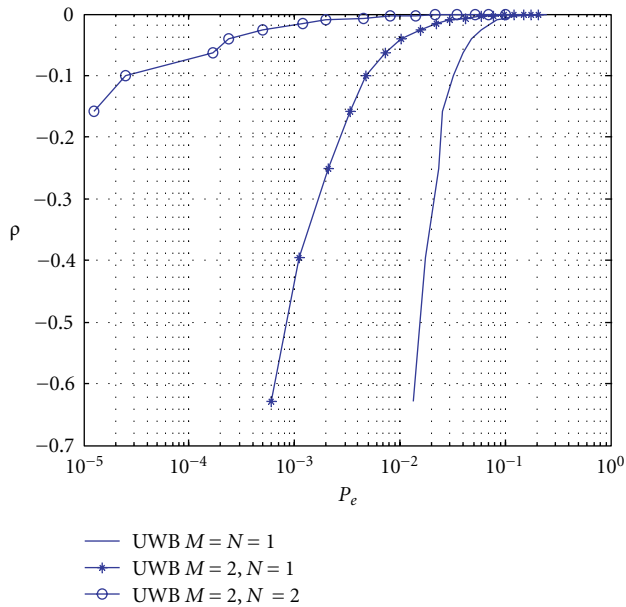FIGURE 1: BER performance of USTC-UWB and its upper bound.

FIGURE 3: Anti-jamming performance comparison of UWB and CDMA.

FIGURE 2: Tradeoff between LPD and anti-jamming.
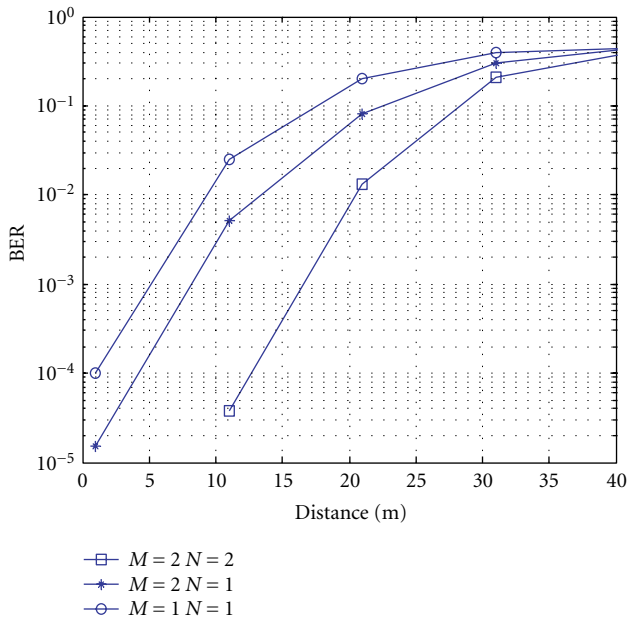
FIGURE 4: BER performance versus coverage range of SISO, MISO, and MIMO UWB system.

increase of SNR corresponds a lower BER, it also inevitably leads to a higher probability of being detected. However, a MIMO system can significantly reduce this probability compared with multiple-input single-output (MISO) or SISO systems.

Figure 3. compares the performance of unitary space-time coding for UWB and DSSS signals. The simulation parameters are set as $B_{DSSS} = 5$ MHz and $L_c = 16$ as in [23]. We can see that UWB and DSSS systems possess the same diversity gain at high SNR. But UWB steadily outperforms
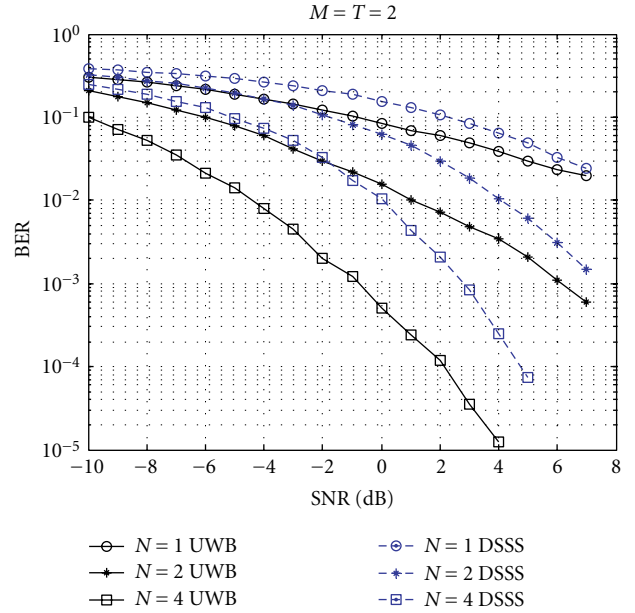
DSSS due to better interference suppression (anti-jamming) capability.

Finally, the coverage range extension advantage of employing multiple antennas in UWB transmission is examined in Figure 4. A path link model in [24] is used in the simulation. We can see that compared to conventional SISO, MISO and MIMO schemes significantly increase the transmission distance of UWB system. For instance, at the target BER of 10^{-4}, SISO is able to cover a range of 1 m, while with 2 transmit antennas MISO can cover about 5 m.

By using 2 antennas also at receiver end, the range can be extended to almost 12 m. It is also observed that since the path loss increases dramatically with the distance, the BER of all three schemes becomes very large after a certain distance. Note that this comparison assumes that the same power is used at transmit side; that is, for a certain transmission distance, multiple antennas result in a lower transmit power, thus reducing the probability of detection.

6. Conclusions

Motivated by some recent research progress on applying MIMO technique in UWB and secure communications, we propose a new unitary space-time coding scheme for impulse radio UWB systems. Its error rate and various transmission secrecy metrics are analyzed. The tradeoff between low probability of detection and anti-jamming is revealed, which indicates that any of these security features could not be solely enhanced without sacrificing another. Our work demonstrates that introducing properly designed space-time codes into UWB systems not only improves the performance of conventional single-antenna schemes but also offers prominent benefits on physical-layer transmission covertness, making it a strong candidate for wireless secure communications, especially for short-distance applications.

Acknowledgment

References

[1] M.-K. Tsay, C.-H. Liao, C.-S. Shyn, and T.-Y. Yang, "Simultaneous AJ and LPD evaluations for secure communication," in *Proceedings of IEEE Military Communications Conference (MILCOM '07)*, Orlando, Fla, USA, October 2007.

[2] Q. Ling, T. Li, and J. Ren, "Physical layer built-in security enhancement of DS-CDMA systems using secure block interleaving," in *Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers*, Pricenton, NJ, USA, March 2004.

[3] L. Nguyen, "Self-encoded spread spectrum communications," in *Proceedings of IEEE Military Communications Conference (MILCOM '99)*, vol. 1, pp. 182–186, Atlantic City, NJ, USA, October 1999.

[4] T. Yang and L. O. Chua, "Secure communication via chaotic parameter modulation," *IEEE Transactions on Circuits and Systems I*, vol. 43, no. 9, pp. 817–819, 1996.

[5] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2637–2649, 2004.

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

[7] A. O. Hero III, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[8] X. Li, M. Chen, and E. P. Ratazzi, "A randomized space-time transmission scheme for secret-key agreement," in *Proceedings of the 39th Annual Conference on Information Sciences and Systems (CISS '05)*, Baltimore, Md, USA, March 2005.

[9] 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, 2004.

[10] A. Bharadwaj and J. K. Townsend, "Evaluation of the covertness of time-hopping impulse radio using a multi-radiometer detection system," in *Proceedings of IEEE Military Communications Conference (MILCOM '01)*, vol. 1, pp. 128–134, Washington, DC, USA, November 2001.

[11] D. R. McKinstry and R. M. Buehrer, "Issues in the performance and covertness of UWB communications systems," in *Proceedings of IEEE Midwest Symposium on Circuits and Systems*, vol. 3, pp. 601–604, Tulsa, Okla, USA, August 2002.

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

[13] 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*, vol. 2005, no. 3, pp. 328–345, 2005.

[14] A. Tyago and R. Bose, "M-PAM space-time trellis codes for ultra-wideband multi-input multi-output communications," *IET Communications*, vol. 2, no. 4, pp. 514–522, 2008.

[15] C. Abou-Rjeily, N. Daniele, and J.-C. Belfiore, "On the amplify-and-forward cooperative diversity with time-hopping ultra-wideband communications," *IEEE Transactions on Communications*, vol. 56, no. 4, pp. 630–641, 2008.

[16] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 543–564, 2000.

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

[18] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744–765, 1998.

[19] B. L. Hughes, "Optimal space-time constellations from groups," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 401–410, 2003.

[20] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 628–636, 2002.

[21] I. Csiszar and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[22] B. M. Sadler and A. Swami, "On the performance of episodic UWB and direct-sequence communication systems," *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 2246–2255, 2004.

[23] Y. Zhang and H. Dai, "A unitary space-time coding scheme for UWB systems and its application in wireless secure communications," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '06)*, vol. 4, pp. 485–488, Toulouse, France, May 2006.

[24] K. Siwiak and A. Petroff, "A path link model for ultra wide band pulse transmissions," in *Proceedings of the 53rd IEEE Vehicular Technology Conference (VTC '01)*, vol. 2, pp. 1173–1175, Rhodes, Greece, May 2001.