Space-Time Encoded Secure Chaos Communications with Transmit Beamforming

Yuu-Seng Lau, Kevin H. Lin, and Zahir M. Hussain

School of Electrical and Computer Engineering, RMIT University, Melbourne, Victoria 3000, Australia
Emails: s9701549@student.rmit.edu.au; s9510490@student.rmit.edu.au; zmhussain@ieee.org

***Abstract*— It is shown that the use of chaos shift keying (CSK) with a transmit diversity technique such as beamforming and space-time coding can provide a secure communication link with improvement in the system error performance. Spreading sequences that are used to scramble data in spread spectrum (SS) systems can be generated using a single mathematical relationship of a chaotic generator. These chaotic sequences are very difficult to predict over long-term chaotic pattern unless the exact initial condition of the chaotic generator is known, providing security. On the other hand, beamforming and orthogonal space-time block coding (OSTBC) transmit diversity techniques are known to provide optimal transmitting structures for communication systems, especially if combined. Based on the signal angle-of-arrival (AoA) estimates, the channel correlation matrix can be constructed, and it is shown that signal transmission of OSTBC codes in the eigen-modes of this matrix gives an effective array weighting gain which improves system error performance without sacrificing any diversity and coding gain. A performance study of CSK with beamforming and space-time encoded is carried out in this paper.**

I. Introduction

A high secure physical communication link with an optimum bit-error-rate (BER) performance is required due to the increased criminal activities that attack privacy in both wired and wireless communication systems. Conventionally, spread spectrum (SS) communication is produced by directly multiplying the information bits (in the time domain) with a known spreading sequence running at a much higher rate, to spread the information over the bandwidth of the transmitted signal. The spreading sequence can be generated using a pseudo-random noise generator or some specially-designed code generator. However, these generators produce repeating sequences and lead to a very predictable fashion which reduces the system capacity and security. Recent research suggested the use of chaos generator to target the security drawback for spread spectrum communication. [1], [2].

To provide a secure communication channel, a chaos generator can be used to generate chaos shift keying (CSK) sequences [1], where different sequences can be generated using the same generator but with different initial conditions. These sequences have the auto- and cross- correlation properties requested by spread spectrum systems. The beauty of chaos generator bifurcation behavior can provide a security aspect to the system, where the chaotic sequence is very sensitive to the initial condition chosen. An exact value must be known in the receiver side to be able to demodulate the transmitted CSK signal.

In order to enhance the error-rate performance of this secure chaos communication, the adaptive transmission scheme proposed in [3] is used. To combine CSK with the adaptive transmission scheme in [3], we first encode the chaos chip-symbols into orthogonal space-time block codewords and transmit these codewords in the eigen-directions of the wireless channel to provide diversity in the spatial domain. In this work, we also investigate the performance improvement from such combination over a macrocell channel model that is originally proposed in [4] and proved to be a realistic model.

This paper is organized as follows. Section II describes the general CSK modulation and demodulation technique. Section III explains the process of OSTBC encoding of chaos chip sequences. Section IV describes the wideband frequency-selective channel and the spatial correlation model that is used in our simulation. Section V provides an overview of eigen-beamforming technique. Section VI shows the overall system, received signal model, maximum likelihood decoding rule for OSTBC matrices, and simulation results. Conclusion is then delivered in Section VII.

Notation used: $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ are complex conjugate, vector transposition, and Hermitian transposition, respectively. $\|\cdot\|_F$ is the Frobenius norm; $\sqrt{\mathcal{A}}$ stands for Hermitian square root of matrix $\mathcal{A}$; finally, capital (small) bold letters represent matrices (vectors).

II. Chaos Shift Keying

The simplest chaos shift keying modulation technique is to transmit a one-bit information using a pair of chaotic generated sequences (g_1 and g_2) [5]. For the data bit ($\alpha_l = +1$) during the l^{th} bit period, g_1 sequence is radiated from the transmitter , and for ($\alpha_l = -1$), g_2 sequence is transmitted. The spreading factor (SF) is the length of a chaotic sequence to be transmitted for one chaotic symbol. The output of the CSK transmitter is $c_k = \alpha_l g_{v,k}$, v decides which chaos sequence to be send. In this work, the chaotic sequences for CSK (i.e., g_1 and g_2) are generated using the same chaotic generator with the same initial condition but multiplied by two different constants. The two chaotic sequences are related as $g_1 = -g_2$. Other methods such as using two different chaotic generator or using two different initial conditions for the same

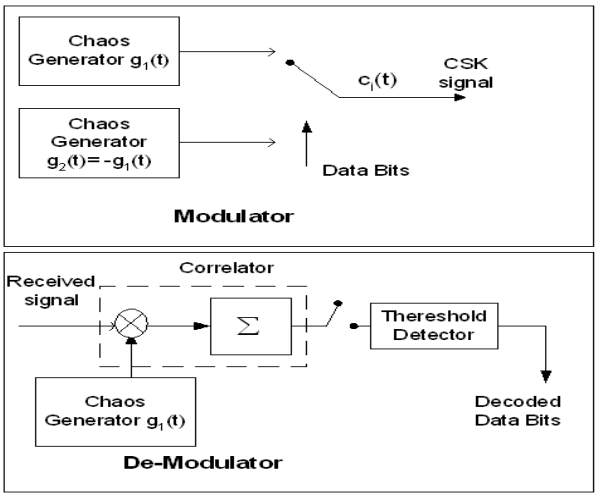

Fig. 1. Modulator and demodulator block diagrams for chaos shift keying.

chaotic generator are not used in here. The demodulation process for CSK is a simple coherent correlator at the receiver as shown in Fig. 1.

We use the simplest chaotic logistic maps for generation of chaotic sequences as in [6]

$$g_{n+1} = 1 - 2g_n^2 \tag{1}$$

which has the invariant probability density function [6], [7]

$$\rho(g) = \begin{cases} \frac{1}{\pi\sqrt{1-g^2}} & \text{, if } \mid g \mid < 1 \\ 0 & \text{, otherwise} \end{cases} \tag{2}$$

III. OSTBC Encoding

At the output of CSK modulator, a series of N_s chip sequences are first converted into parallel streams before the OSTBC encoding process, each stream containing SF chip-symbols, where SF is the spreading factor in the CSK modulation function. In this paper we made the choice of N_s streams dependent on the OSTBC encoding matrix used. The OSTBC encoding of these streams of chip-symbols is done by taking one chip-symbol in each stream as the input symbol and then format these chips into a codeword matrix. Thus, the SF codeword matrices are constructed from these N_s input streams.

Denote the p^{th} output codeword matrix as $\mathbf{C}_p \in \mathbb{C}^{N_t \times N}$, which has N_t spatial dimensions and spans across N chip-symbol intervals. Since the number of baseband constellation points is finite, there is a limited number of possible OSTBC codeword matrices that can be generated; we denote this finite set as $\boldsymbol{\Upsilon}_p \ni \mathbf{C}_p$. Suppose that N_s input chip-symbols, which we collect into a row vector $\mathbf{s}_p = [c_{1,p}, \cdots, c_{m,p}, \cdots, c_{N_s,p}]$, are used to generate $\mathbf{C}_p$ by formatting $\mathbf{s}_p$ with an encoding matrix $\boldsymbol{\mathcal{G}}_p$ such that $\boldsymbol{\mathcal{G}}_p : \mathbf{s}_p \rightarrow \mathbf{C}_p$. According to [8], such encoding process can be mathematically expressed as

$$\mathbf{C}_p = \sum_{m=1}^{N_s} [c_{m,p}\mathbf{A}_m + c_{m,p}^*\mathbf{B}_m] \tag{3}$$

which are then split into a set of N_t parallel symbol sequences and transmitted during N chip intervals. The $\{\mathbf{A}_m, \mathbf{B}_m\}$ are matrices designed to satisfy the orthogonality condition that is well documented in both [8] and [9] as

$$\mathbf{C}_p\mathbf{C}_p^* = \sum_{m=1}^{N_s} \mid c_{m,p} \mid^2 \cdot \mathbf{I}_N, \tag{4}$$

where $(.)^*$ denotes the complex conjugate and $\mathbf{I}_N$ is an identity matrix of size N.

Since data symbols are ST block encoded in the proposed transmission structure, we regard all signal transmissions under consideration here as block transmissions. In the well-known STBC of [10], a different ST block encoding matrix requires different number of input chip symbols for different number of transmit antennas. The OSTBC encoding matrix $\boldsymbol{\mathcal{G}}4$ that we used for our system simulation is given by [10]

$$\boldsymbol{\mathcal{G}}4 = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2 & s_1 & -s_4 & s_3 \\ -s_3 & s_4 & s_1 & -s_2 \\ -s_4 & -s_3 & s_2 & s_1 \\ s_1^* & s_2^* & s_3^* & s_4^* \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ -s_3^* & s_4^* & s_1^* & -s_2^* \\ -s_4^* & -s_3^* & s_2^* & s_1^* \end{pmatrix} \tag{5}$$

which is employed for systems with $N_t = 4$.

IV. Channel Model

Assume that the system operates in a typical cellular communication scenario where the base station (BS) antennas are placed at the building roof-top in an unobstructed environment and the mobile station (MS) is located at the street level surrounded by dense distribution of local scatterers. It is stated in [11] that signal transmission in such an environment over a multipath channel leads to uncorrelated signal paths arriving at the MS but there would be partial correlation in the spatial domain at the BS. These propagation assumptions are normally used to model macrocell operation. Assume that a uniform linear array (ULA) configuration is used for N_t BS antennas with a spacing of d meters. The transmit spatial correlation matrix is defined in [12] as

$$\mathbf{R}_t = \frac{1}{L}\sum_{\ell=1}^{L} \mathbf{a}(\theta_\ell)\mathbf{a}^H(\theta_\ell), \tag{6}$$

where L denotes the number of dominant resolvable paths and $\mathbf{a}(\theta_\ell) := [1, e^{j\beta}, e^{j2\beta}, \cdots, e^{j(N_t-1)\beta}]^T$ is the array propagation vector for the ℓ^{th} tap with an angle-of-arrival (AoA) of θ_ℓ impinging on the BS ULA. $\beta = [2\pi \cdot d \cdot \sin(\theta_\ell)]/\lambda$, λ being

the carrier frequency wavelength. In general, $\mathbf{R_t}$ is an non negative-definite Hermitian Toeplitz matrix of the form

$$\mathbf{R}_t = [R_{uv}]_{N_t \times N_t} = \text{toeplitz}([1\ R_{12}\ R_{13}\ ...\ R_{1N_t}]), \quad (7)$$

where R_{uv} is the spatial correlation between signals from u^{th} and v^{th} antennas. Eigenvalue-decomposition (EVD) of $\mathbf{R}_t$ can be expressed as $\mathbf{V}\mathbf{R}_t\mathbf{V}^H = \mathbf{\Lambda}$, where $\mathbf{V} = [\boldsymbol{\upsilon}_1, \cdots, \boldsymbol{\upsilon}_{N_t}]$ is a unitary matrix with columns that are the eigenvectors and $\mathbf{\Lambda} = \text{diag}[\omega_1, \cdots, \omega_n, \cdots, \omega_{N_t}]$ is a diagonal matrix contains the corresponding eigenvalues.

We consider multi-input multi-output (MIMO) frequency-selective channel between the transmitting and receiving antennas. Following [13], this underlying frequency-selective channel can be modelled as a tapped delay line that represents an L^{th}-order finite-impulse response (FIR) filter whose coefficients are τ-samples of the impulse response $\{h_{i,j}(\tau;t)\}$ of the channel corresponding to the $(i,j)^{\text{th}}$ receive-transmit antenna pair

$$h_{i,j}(\tau;t) = \sum_{\ell=1}^{L} \alpha_{i,j}(\ell;t)\delta(\tau - n_\ell), \quad (8)$$

where t represents time, τ is the time-delay, $\alpha_{i,j}(\ell;t)$ is the ℓ^{th} path complex fading coefficient, $\delta(\cdot)$ is the Dirac delta function, and $n_\ell = \ell/W$ is the delay of the ℓ^{th} path. Thus, the channel impulse response includes the channel fading effect and the relative delay spread of the multi-paths. Denote the discrete-time baseband equivalent impulse response vector as $\mathbf{h}_{i,j}[n] = [\alpha_{i,j}(1;nT), \cdots, \alpha_{i,j}(L;nT)]$ for the n^{th} chip interval, where T is the total time duration of one OSTBC codeword. In this paper, $\{\alpha_{i,j}(\ell;nT)\}$ are modelled as correlated circularly symmetric complex Gaussian random variables with zero mean.

Let us denote the correlated MIMO channel impulse response matrix for the p^{th} OSTBC codeword block as $\mathbf{H}[n;p] \in \mathbb{C}^{N_r \times N_t}$. The $(i,j)^{\text{th}}$ element, which represents the subchannel gain between the i^{th} receive antenna and the j^{th} transmit antenna, is defined as

$$h_{i,j}[n;p] := \sum_{\ell=1}^{L} \alpha_{i,j}(\ell;nT). \quad (9)$$

According to [11], we can also express the channel matrix as $\mathbf{H}[n;p] = \overline{\mathbf{H}}[n;p]\sqrt{\mathbf{R}_t}$, where $\overline{\mathbf{H}}[n;p]$ can be thought of as a *pre-whitened* channel matrix with independent circularly symmetric complex Gaussian random variables from $\mathcal{CN}(0,\sigma_h^2)$. Furthermore, quasi-static fading is assumed throughout the duration of one STBC codeword length (i.e., if N is the length of the p^{th} codeword, then $\mathbf{H}[1;p] = \mathbf{H}[n;p]\,|n = 1, \cdots, N)$, but fading may vary from one block to another. Therefore, the timing index n will be dropped and $\mathbf{H}[n;p]$ will hereafter be written as $\mathbf{H}_p$.

V. Adaptive Eigen Beamforming

In enhancing the received signal-to-noise ratio (SNR) and thus the probability for correct detections of transmitted

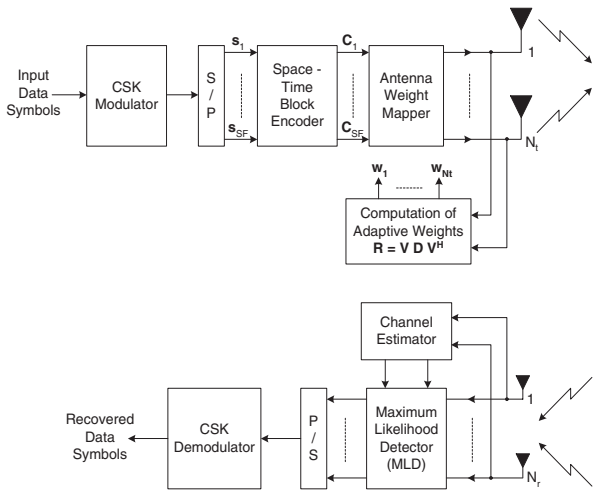

Fig. 2. General structure of the proposed system structure.

OSTBC codeword, signal transmission in the eigen-modes of the correlation matrix, eigen weight mapping is performed across the space dimension of the OSTBC codeword $\mathbf{C}_p$ prior to transmission as in [3]. Mathematically, it can be expressed as $\mathbf{W}^H\mathbf{C}_p$, where $\mathbf{W} = [\mathbf{w}_1, \cdots, \mathbf{w}_{N_t}]$ is the eigen weight mapping matrix and $\mathbf{w}_j = \boldsymbol{\upsilon}_j$. Then signal transmission on different eigenvectors of $\mathbf{R}_t$ amounts for transmitting N_t orthonormal beams in the direction of the dominant multipaths seen by the transmitter.

VI. System Simulation

The system diagram in Fig. 2 showed the proposed transceiver structure with CSL modulator, OSTBC encoder, and eigen weight mapper at the transmitter. The transmitted signal is corrupted by frequency selective rayleigh fading (for microcell wireless channel) before arriving at the receiver.

At the receiver, OSTBC codeword signals are received from N_r antennas. The discrete time baseband equivalent expression of the received signal has the form

$$\mathbf{Y}_p = \overline{\mathbf{H}}_p\sqrt{\mathbf{R}_t}\mathbf{W}^H\mathbf{C}_p + \mathbf{E}_p\ , \quad (10)$$

where $\mathbf{E}_p$ is the receiver noise matrix and its elements are modelled as uncorrelated white Gaussian random variables taken from $\mathcal{N}(0,\sigma_n^2)$.

In order to perform OSTBC codeword decoding, channel estimation is needed to be performed first by correlating the embedded pilot symbols sent with the data signal with a prior known sequence. The estimation results from N_r receive antennas are then fed into the maximum likelihood decoder (MLD) for the OSTBC codeword decoding. The general decision matrix for the evaluation of transmitted data can be written as

$$\widehat{\mathbf{C}}_p = \arg \min_{\mathbf{C}_p \in \mathbf{\Upsilon}_p} \|\mathbf{Y}_p - \overline{\mathbf{H}}_p\sqrt{\mathbf{R}_t}\mathbf{W}^H\mathbf{C}_p\|_F^2\ . \quad (11)$$

A more specific decoding algorithms can be found in [10] for various sizes of OSTBC encoding matrices. The final state to

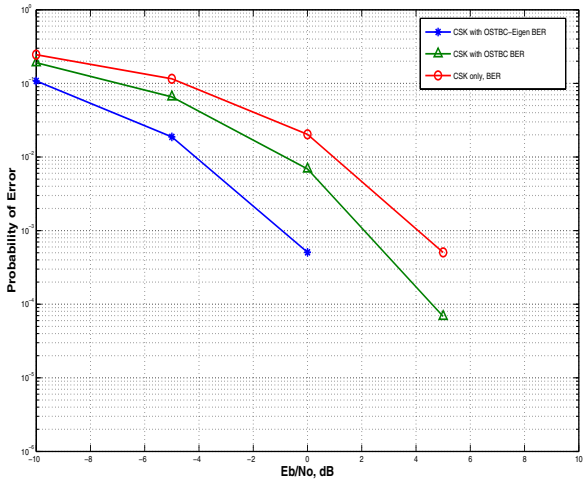

Fig. 3. BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 16$.

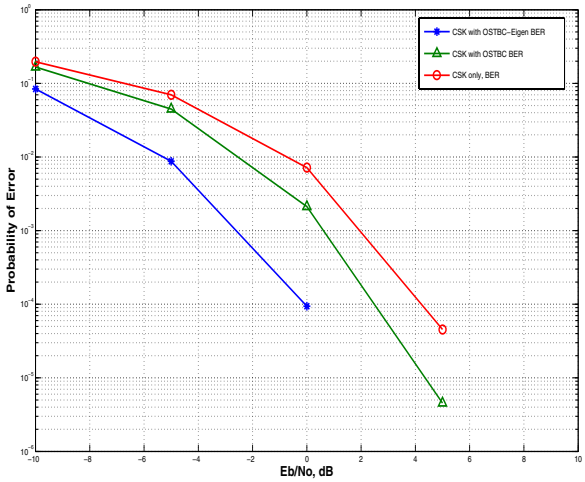

Fig. 5. BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 64$

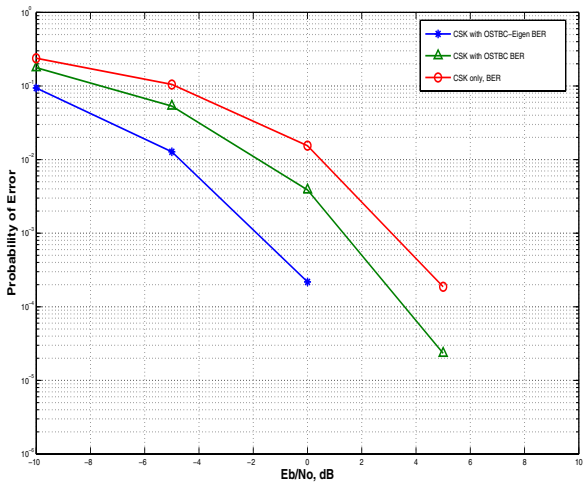

Fig. 4. BER vs Eb/No performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and $SF = 32$

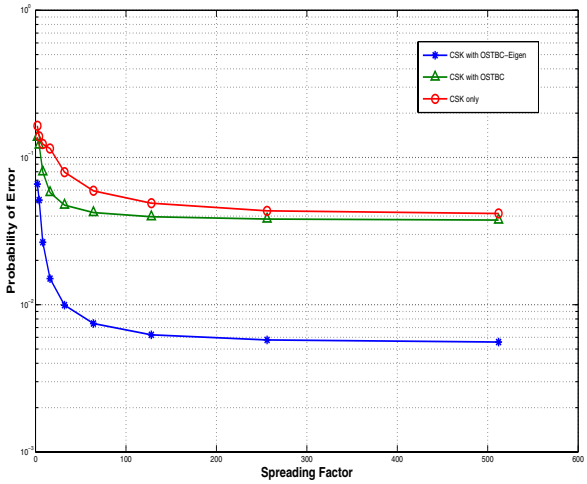

Fig. 6. BER vs SF performance for CSK with eigen-beamforming and OSTBC, Nr=1, 4-tap correlation, and Eb/No = -5 dB.

recover the original bit stream signal is only a simple parallel to series conversion on the $\widehat{\mathbf{C}}_p$ then passed thought a CSK demodulator (simple correlator) as described in Section II.

In order to simulate the proposed transmission structure in frequency-selective Rayleigh fading channels, the following parameters and simulation assumption were adopted: BPSK baseband modulation is used, the spatial channel correlation is modelled using the Macrocell GBHDS channel model in [4], $\mathcal{G}_4$ encoding matrix in [9] is utilized for OSTBC codeword construction, and hence $Nt = 4$, $N_r = 2$ were employed.

Figs. 3 - 5 show the BER performance of CSK with eigen-beamforming and OSTBC for different spreading factors. As expected, combining eigen-Beamforming with OSTBC in CSK will outperform those systems without any diversity technique, or systems with only OSTBC. Generally, at low Eb/No, the performance gain is more dependent on the coding gain of OSTBC, else at higher Eb/No, the gain is more dependent on the diversity gain. Comparing the BER ranges in Figs. 3 - 5, we can see that an increase in the spreading factor will lead to a better BER performance. However, Fig 6 does show that there is a convergence point where increasing SF will not provide much different performance gain. Hence, choosing the SF should be carefully considered, keeping in mind that increasing SF will increase the processing time. The optimum value in this case is around $SF = 100$. It is also noted that, a lower value for SF can be used when diversity technique is deployed.

VII. Conclusions

A secure communication with diversity technique is proposed in this paper. The use of a chaotic generator for spreading can provide a more secure communication than

using the conventional digital spreading. The scheme is combined with space-time coding and eigenbeamforming, giving a much lower bit error rate and hence, increased security. The proposed scheme can be used in wireless communication systems where security is the concern. To enhance the security performance, a larger spreading factor can be used, but it is shown that there is a threshold for this increase, after which no BER performance advantage can be obtained.

REFERENCES

[1] Y.-S. Lau and Z. M. Hussain, "A new approach in chaos shift keying for secure communication", in *Proc. IEEE International Conference on Information Technology and Applications 2005*, Sydney, Australia, July 2005.

[2] Y.-S. Lau, Z. M. Hussain, and R. J. Harris, "Chaotic-based CDMA versus PN-based CDMA for digital secure communications: A comparative study", *Australian Telecommunications Networks and Applications Conference 2004*, Sydney, Australia, Dec. 2004.

[3] K. H. Lin, Z. M. Hussain, and R. J. Harris, "Space-time OFDM with adaptive beamforming: Performance in spatially correlated channels," in *Proc. IEEE TENCON*, ChiangMai, Nov. 2004, pp. 617-620.

[4] S. S. Mahmoud, Z. M. Hussain, and P. O'Shea, "A space-time model for mobile radio channel with hyperbolically distributed scatterers," *IEEE Antennas Wireless Propagat. Lett*., vol. 1, pp. 211-214, 2002.

[5] M. P. Kennedy and G. Kolumban, "Digital communications using choas," *Elsevier Signal Processing Journal* , vol. 80, pp.1307-1320, 2000.

[6] F. C. M. Lau, C. K. Tse, M. Ye, and S. F. Hau, "Coexistence of chaos-based and conventional digital communication systems of equal bit rate," *IEEE Trans. Circuits and Systems*, vol. 51, pp. 391-408, Feb. 2004.

[7] T. Kohda and A. Tsuneda, "Even- and odd-correlation fucntions of chaotic chebyshev bit sequences for CDMA," in *Proc. IEEE Int. Symp. Spread Specturm Technology and Applications*, 1994, pp. 391-395.

[8] G. Ganesan, P. Stoica, and E. G. Larsson, "Diagonally weighted orthogonal space-time block codes," *Thirty-Sixth Asilomar Conference on Signals, Systems and Computers*, vol. 2, Nov. 2002, pp. 1147-1151.

[9] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456-1467, July 1998.

[10] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block coding for wireless communications:Performance results," *IEEE J. Select. Areas in Commun*., vol. 17, pp. 451-460, Mar. 1999.

[11] E. G. Larsson and P. Stoica, *Space-Time Block Coding for Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[12] Siemens, *Channel Model for Tx Diversity Simulations using Correlated Antennas*, 3GPP Document TSG-RAN WG1 #15, R1-00-1067, Berlin, Germany, Aug. 2000.

[13] J. G. Proakis, *Digital Communications*, New York, N.Y.: McGraw-Hill Inc., Fourth Edition, 2001.