SECURE SPACE-TIME BLOCK CODING VIA ARTIFICIAL NOISE ALIGNMENT

S. Ali. A. Fakoorian, Hamid Jafarkhani, A. Lee Swindlehurst

Center for Pervasive Communications and Computing
University of California Irvine
afakoori, hamidj, swindle@uci.edu

ABSTRACT

In this work, we present a secure space time block code (STBC) for MIMO Gaussian wiretap channels. It is assumed that the transmitter has the receiver's channel state information, but not that of the eavesdropper. We first propose a full-rate STBC that provides separate decoding complexity (rather than pairwise) at the intended receiver, while requiring an exhaustive search for Maximum Likelihood (ML) decoding at the eavesdropper. Next we make the code more secure by including artificial noise symbols which (for the asymptotically high SNR regime) are aligned with each other and subtracted from the information symbols at the intended receiver, but which can not be cancelled at the eavesdropper. Simulations demonstrate the enhanced physical-layer security that results.

***Index Terms*—** MIMO, space-time block codes, physical-layer secrecy, wiretap channel.

1. INTRODUCTION

Wireless communications are inherently insecure due to the broadcast nature of the wireless medium. A passive eavesdropper in the vicinity of a wireless transmission has the ability to obtain information about the transmitted signal without risk of detection, since it never transmits itself. While encryption at the network layer can be used to ensure confidential wireless communications, its computational cost may be prohibitive and there are difficulties and vulnerabilities associated with key distribution and management. Even when encryption is available, it is often still desirable to augment the security of the link and prevent its detection or interception. As a result, recent information-theoretic research on secure communication has focused on enhancing security at the physical layer.

The wiretap channel, first introduced and studied by Wyner [1], is the most basic physical layer model that captures the problem of communication security. This work led to the development of the notion of perfect secrecy capacity, which quantifies the maximum rate at which a transmitter can reliably send a secret message to its intended recipient, without it being decoded by an eavesdropper. The secrecy capacity of a Gaussian wiretap channel, in which the outputs of the legitimate receiver and the eavesdropper are corrupted by additive white Gaussian noise, has been addressed and solved for in [2]-[4]. Note that much of this information theoretic work is based on the assumption that the eavesdropper's channel is known to the transmitter, which is hard to justify if the eavesdropper is truly passive.

In this paper we present a secure space time block code (STBC) that improves confidentiality in a MIMO Gaussian wiretap channel. The transmitter is assumed to have channel state information (CSI) for the intended receiver, but knows nothing about the CSI of the eavesdropper. We first propose a rate-one STBC [5] scheme that allows for separable decoding at the intended receiver but not at the eavesdropper, who must perform an exhaustive search to achieve Maximum Likelihood (ML) decoding. Next we make the code more secure by including artificial noise symbols that are asymptotically (for high SNR) aligned with each other and subtracted from the information symbols at the intended receiver. On the other hand, the eavesdropper is unable to cancel the effect of the noise symbols, and they further degrade her ability to decode the information symbols.

Notation: Throughout the paper, we use boldface uppercase and lowercase letters to denote matrices and column vectors, respectively. Scalar variables are written with non-boldface (lowercase or uppercase) letters. We use $(.)^T$ to denote transposition, $(.)^H$ to denote the Hermitian (i.e., conjugate) transpose, and $\mathcal{CN}(0, \sigma^2)$ to denote the complex circularly symmetric Gaussian distribution with zero mean and variance σ^2. Also, we denote the jth column of a matrix $\mathbf{A}$ by $\mathbf{A}(:, j)$.

2. SYSTEM MODEL

We consider a MIMO wiretap channel where there exists a transmitter, a legitimate receiver, and an eavesdropper. The transmitter and receiver each have two antennas, while the number of antennas at the eavesdropper is arbitrary. The transmitter sends confidential messages to its intended receiver,

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318, and by the National Science Foundation under grant CCF-1117983.

978-1-4673-0323-1/11/$26.00 ©2011 IEEE

while attempting to keep them as secret as possible from the eavesdropper. At each time slot, the signals present at the receiver and eavesdropper are respectively given by:

$$\mathbf{y}_r = \mathbf{H}_r\mathbf{x} + \mathbf{z}_r \tag{1}$$

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{x} + \mathbf{z}_e \tag{2}$$

where $\mathbf{x}$ is the 2×1 transmitted signal vector, and $\mathbf{z}_r$, $\mathbf{z}_e \in \mathbb{C}^{2\times 1}$ represent background noise with i.i.d. entries distributed as $\mathcal{CN}(0,1)$. The channel matrices $\mathbf{H}_r$ and $\mathbf{H}_e \in \mathbb{C}^{2\times 2}$ are assumed to be independent of each other. They have i.i.d. entries distributed as $\mathcal{CN}(0,1)$, which are assumed to be fixed during the transmission of one block (two time slots). We assume that the transmitter and the legitimate receiver both know $\mathbf{H}_r$, but neither is aware of $\mathbf{H}_e$. Furthermore we make the worst-case assumption that the eavesdropper knows both $\mathbf{H}_r$ and $\mathbf{H}_e$.

Assuming an average transmit power of P_s at the transmitter, the signals transmitted in the first and second time slots of each block are respectively given by

$$\mathbf{x}^1 = \sqrt{P_s}\mathbf{A}^1 \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} + \sqrt{P_s}\mathbf{B}^1 \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} \tag{3}$$

$$\mathbf{x}^2 = \sqrt{P_s}\mathbf{A}^2 \begin{bmatrix} -c_2^* \\ c_1^* \end{bmatrix} + \sqrt{P_s}\mathbf{B}^2 \begin{bmatrix} -c_4^* \\ c_3^* \end{bmatrix} \tag{4}$$

where $\mathbf{A}^1$, $\mathbf{A}^2$, $\mathbf{B}^1$, and $\mathbf{B}^2$ are precoding matrices that will be specified later, and where at this point we assume that c_1, c_2, c_3, and c_4 are all information symbols corresponding to the confidential message, with $|c_i| = 1$.

Our first goal is to design precoders to realize low-complexity decoding for the intended receiver. Using the channel model in Eqs. (1) and (2), the received signals at the intended receiver over the first and second time slots can be written as

$$\mathbf{y}_r^1 = \sqrt{P_s}\mathbf{H}_r\mathbf{A}^1 \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} + \sqrt{P_s}\mathbf{H}_r\mathbf{B}^1 \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} + \mathbf{z}_r^1 \tag{5}$$

$$\mathbf{y}_r^2 = \sqrt{P_s}\mathbf{H}_r\mathbf{A}^2 \begin{bmatrix} -c_2^* \\ c_1^* \end{bmatrix} + \sqrt{P_s}\mathbf{H}_r\mathbf{B}^2 \begin{bmatrix} -c_4^* \\ c_3^* \end{bmatrix} + \mathbf{z}_r^2 \tag{6}$$

By combining Eqs. (5) and (6), we have

$$\begin{bmatrix} \mathbf{y}_r^1 \\ \left(\mathbf{y}_r^2\right)^* \end{bmatrix} = \sqrt{P_s}\,\widehat{\mathbf{H}}_r \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} + \begin{bmatrix} \mathbf{z}_r^1 \\ \mathbf{z}_r^{2*} \end{bmatrix} \tag{7}$$

where

$$\widehat{\mathbf{H}}_r = \begin{bmatrix} \mathbf{H}_r\mathbf{a}_1^1 & \mathbf{H}_r\mathbf{a}_2^1 & \mathbf{H}_r\mathbf{b}_1^1 & \mathbf{H}_r\mathbf{b}_2^1 \\ \mathbf{H}_r^*\mathbf{a}_2^{2*} & -\mathbf{H}_r^*\mathbf{a}_1^{2*} & \mathbf{H}_r^*\mathbf{b}_2^{2*} & -\mathbf{H}_r^*\mathbf{b}_1^{2*} \end{bmatrix} \tag{8}$$

and $\mathbf{a}_i^j$ represents the ith column of the matrix $\mathbf{A}^j$, $i,\, j \in \{1,\, 2\}$. A similar description exists for the $\mathbf{b}_i^j$ vectors.

In [6], the precoders are designed such that $\widehat{\mathbf{H}}_r$ has a quasi-orthogonal structure [7]. More precisely, the subspace created by the first two columns of $\widehat{\mathbf{H}}_r$ is orthogonal to the subspace created by the second two columns. Hence, at the receiver, the pairs $(c_1,\, c_2)$ and $(c_3,\, c_4)$ can be decoded separately, although pairwise decoding is still required to determine each symbol. In the following, we design precoding matrices such that all columns of $\widehat{\mathbf{H}}_r$ are orthogonal to each other. Consequently, using this orthogonal design [8] the intended receiver can achieve symbol-by-symbol decoding rather than pairwise decoding for the quasi-orthogonal designs. Since the channel to the eavesdropper is different from $\mathbf{H}_r$, the orthogonalization will not hold at the eavesdropper and separable decoding will not be possible.

Suppose we want to design $\mathbf{A}^1$ and $\mathbf{A}^2$ such that the first two columns of $\widehat{\mathbf{H}}_r$ are orthogonal to each other. We must have

$$\mathbf{a}_1^{1^H}\, \mathbf{H}_r^H\mathbf{H}_r\,\mathbf{a}_2^1 - \mathbf{a}_2^{2^T}\left(\mathbf{H}_r^H\mathbf{H}_r\right)^*\mathbf{a}_1^{2*} = 0. \tag{9}$$

Define the eigenvalue decomposition of the 2×2 positive semi-definite matrix $\mathbf{H}_r^H\mathbf{H}_r$, i.e.,

$$\mathbf{H}_r^H\mathbf{H}_r = \mathbf{\Phi}\mathbf{\Lambda}\mathbf{\Phi}^H = \lambda_1\boldsymbol{\phi}_1\boldsymbol{\phi}_1^H + \lambda_2\boldsymbol{\phi}_2\boldsymbol{\phi}_2^H \tag{10}$$

where $\boldsymbol{\phi}_i$ represents the ith column of the unitary matrix $\mathbf{\Phi}$ and $\mathbf{\Lambda}$ is a diagonal matrix with real non-negative diagonal elements λ_1 and λ_2, for which we assume $\lambda_1 \geq \lambda_2$. Clearly, a solution for (9) is to let $\mathbf{a}_1^1 = \mathbf{a}_2^1 = \mathbf{a}_1^2 = \mathbf{a}_2^2 = \boldsymbol{\phi}_1$. In fact, it is easy to verify that all the columns of $\widehat{\mathbf{H}}_r$ are orthogonal to each other if we let

$$\mathbf{A}^1 = \mathbf{A}^2 = \frac{1}{2}\left[\boldsymbol{\phi}_1 \quad \boldsymbol{\phi}_1\right] \tag{11}$$

$$\mathbf{B}^1 = \mathbf{B}^2 = \frac{1}{2}\left[\boldsymbol{\phi}_2 \quad \boldsymbol{\phi}_2\right] \tag{12}$$

where the coefficient $\frac{1}{2}$ comes from the normalization conditions on the precoders.

Using Eqs. (11) and (12) in Eq. (8) and multiplying both sides of Eq. (7) with $\widehat{\mathbf{H}}_r^H$, we have

$$\overline{\mathbf{y}}_r = \frac{\sqrt{P_s}}{2}\begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} + \overline{\mathbf{z}}_r \tag{13}$$

where

$$\overline{\mathbf{y}}_r = \widehat{\mathbf{H}}_r^H \begin{bmatrix} \mathbf{y}_r^1 \\ \left(\mathbf{y}_r^2\right)^* \end{bmatrix} \quad \text{and} \quad \overline{\mathbf{z}}_r = \widehat{\mathbf{H}}_r^H \begin{bmatrix} \mathbf{z}_r^1 \\ \mathbf{z}_r^{2*} \end{bmatrix}.$$

Note that the noise elements of $\overline{\mathbf{z}}_r$ are uncorrelated due to the orthogonal structure of $\widehat{\mathbf{H}}_r$. Thus, at the intended receiver, the symbols can be decoded separately using the maximum likelihood (ML) method. For example, we can detect c_1 by

$$\widehat{c}_1 = \arg\min_{c_1}\left|\overline{\mathbf{y}}_r(1) - \frac{\sqrt{P_s}}{2}\lambda_1\, c_1\right|^2 \tag{14}$$

where $\overline{\mathbf{y}}_r(1)$ represents the first element of the vector $\overline{\mathbf{y}}_r$. Such separability will not occur for the eavesdropper, even if the eavesdropper is aware of the precoder.

3. ARTIFICIAL NOISE ALIGNMENT

While the precoder described above does not allow for symbol-by-symbol decoding at the eavesdropper, a further improvement in security can be obtained if the transmitter broadcasts artificial noise symbols that are detectable at the intended receiver but not the eavesdropper. The price paid for the inclusion of such symbols is a reduction in rate or coding gain. A simple approach would be to convert one of the symbols to noise; for example, we could set $c_i \sim \mathcal{CN}(0,1)$. Due to the separable decoding provided by the precoder of the previous section, the noise symbol does not impact the decoding of the other three information symbols at the intended receiver, but it will degrade the decoding ability of the eavesdropper. We will examine the performance of this simple scheme in Section 4.

In the following, we propose a different method in which artificial noise (AN) symbols are added to the information symbols such that at the intended receiver, the AN symbols are "aligned" and can be subtracted from the information symbols. The method is derived below by ignoring the background noise; its performance with background noise will be illustrated via simulation.

For the precoders given by Eqs. (11) and (12), the transmitted signals at each block can be written as

$$\mathbf{X} = \left[\mathbf{x}^1 \; \mathbf{x}^2\right] = \frac{\sqrt{P_s}}{2}\mathbf{\Phi} \left[\begin{array}{cc} c_1 + c_2 & c_1^* - c_2^* \\ c_3 + c_4 & c_3^* - c_4^* \end{array} \right] . \qquad (15)$$

Defining

$$\widetilde{\mathbf{H}}_r = \frac{\sqrt{P_s}}{2}\mathbf{H}_r\mathbf{\Phi} = \left[\begin{array}{cc} a & b \\ d & f \end{array} \right]$$

the received signal at the legitimate receiver in the noiseless case is given by

$$\mathbf{Y} = \widetilde{\mathbf{H}}_r\,\mathbf{X} = \left[\begin{array}{cc} a & b \\ d & f \end{array} \right] \left[\begin{array}{cc} c_1 + c_2 & c_1^* - c_2^* \\ c_3 + c_4 & c_3^* - c_4^* \end{array} \right] \qquad (16)$$

where each element $\mathbf{Y}(i,j)$ of matrix $\mathbf{Y}$ represents the received signal at antenna i and time slot j, for $i,\, j \in \{1,\, 2\}$.

In Section II, we showed that for the structure in (15), the legitimate receiver can decode c_1, c_2, c_3 and c_4 separately and independently of each other. If we now add artificial noise symbols m and n as follows

$$\mathbf{X}_n = \frac{\sqrt{P_s}}{2}\mathbf{\Phi} \left[\begin{array}{cc} c_1 + c_2 + m & c_1^* - c_2^* \\ c_3 + c_4 + n & c_3^* - c_4^* \end{array} \right] , \qquad (17)$$

separable decoding is in general no longer possible. With the embedded noise symbols, the received signal at the intended receiver is

$$\mathbf{Y}_n = \widetilde{\mathbf{H}}_r\,\mathbf{X}_n = \left[\begin{array}{cc} a & b \\ d & f \end{array} \right] \left[\begin{array}{cc} c_1 + c_2 + m & c_1^* - c_2^* \\ c_3 + c_4 + n & c_3^* - c_4^* \end{array} \right] . \qquad (18)$$

Our goal is to design m and n such that the effect of the noise symbols are removed; in particular, we will design m and n such that a simple transformation converts $\mathbf{Y}_n$ into $\mathbf{Y}$, so that the separable decoding method of the previous section can be directly employed.

Because of the structure of (18), it is clear that $\mathbf{Y}_n(:,2) = \mathbf{Y}(:,2)$ already. Furthermore, $\mathbf{Y}_n(2,1) = \mathbf{Y}(2,1)$ can be achieved if we design m and n such that

$$d\,m + f\,n = 0\,. \qquad (19)$$

Now, define the parameter η via the equation

$$a\,m + b\,n = \eta\,(a\,(c_1^* - c_2^*) + b\,(c_3^* - c_4^*))\ , \qquad (20)$$

where η must be chosen to satisfy the given power constraint. We can recover $\mathbf{Y}(1,1)$ via the simple transformation

$$\mathbf{Y}(1,1) = \mathbf{Y}_n(1,1) - \eta\mathbf{Y}_n(1,2)\ ,$$

and thus the entire matrix $\mathbf{Y}$ that allows for separable decoding can be reconstructed. Putting the above definitions together, the artificial noise symbols are constructed as

$$\begin{aligned} m &= \frac{\eta f}{af - bd}\,(a\,(c_1^* - c_2^*) + b\,(c_3^* - c_4^*)) \\ &= \eta z_1\,(c_1^* - c_2^*) + \eta z_2\,(c_3^* - c_4^*) \qquad (21) \\ n &= -\frac{\eta d}{af - bd}\,(a\,(c_1^* - c_2^*) + b\,(c_3^* - c_4^*)) \\ &= \eta z_3\,(c_1^* - c_2^*) + \eta z_4\,(c_3^* - c_4^*) \qquad (22) \end{aligned}$$

where the z_i coefficients are implicitly defined.

It should be noted that the parameter η depends on the equivalent channel coefficients (a, b, f, d) and the power assigned to the information symbols, but not the exact values of the information symbols. Thus, the intended receiver is aware of the value of η in advance. For example, assuming QPSK symbols with $|c_i| = p$, $i = 1, ..., 4$ and $p \leq 1$, the average transmit power is satisfied when η is given by

$$\eta = -\frac{-b + \sqrt{b^2 - 4a\,c}}{2\,a} \qquad (23)$$

where

$$\begin{aligned} a &= |z_1|^2 + |z_2|^2 + |z_3|^2 + |z_4|^2 \\ b &= |\mathrm{Re}(z_1)| + |\mathrm{Re}(z_2)| + |\mathrm{Re}(z_3)| + |\mathrm{Re}(z_4)| \\ c &= -2\,\frac{1-p}{p}\ , \end{aligned}$$

assuming that the fraction of power allocated to each information symbol is $\frac{p}{4}$. Clearly with this assumption the total transmit power at the second time slot is less than that of the first time slot. However this does not affect the decoding performance of the intended receiver, as we will observe in the next section.

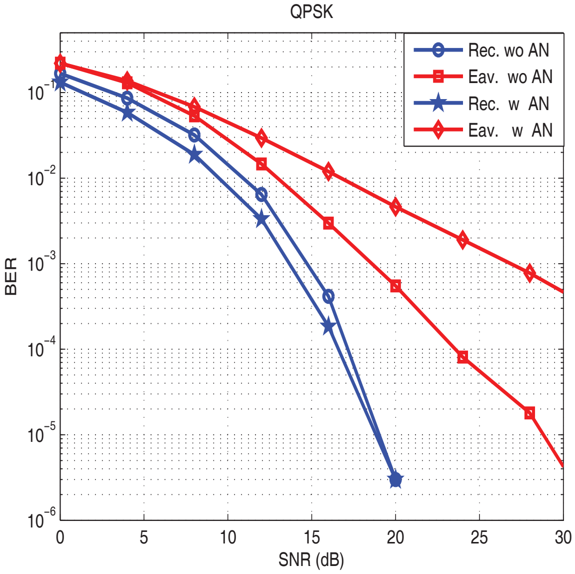

Fig. 1. BER performance for the proposed STBC with QPSK information symbols, with and without artificial noise.

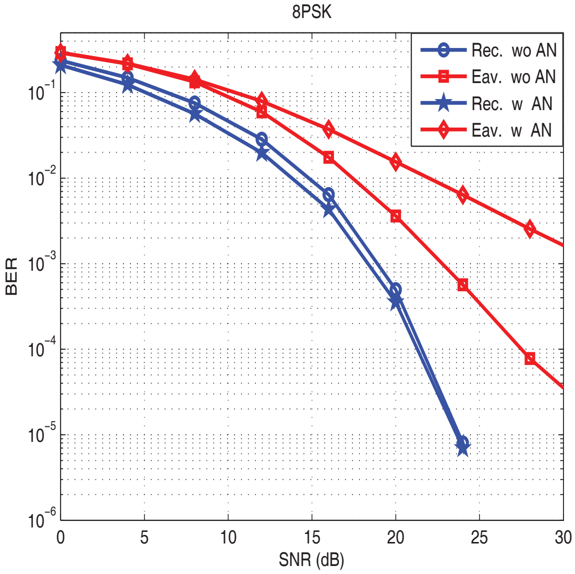

Fig. 2. BER performance for the proposed STBC with 8PSK information symbols, with and without artificial noise.

4. NUMERICAL RESULTS

In the following, we present simulation results for the proposed transmission schemes by evaluating the bit error rate (BER) of the intended receiver and the eavesdropper. In all the following examples, it is assumed that the number of antennas at each node is two. Furthermore, while the cross channel $\mathbf{H}_e$ is generated completely randomly, we consider only those direct channels $\mathbf{H}_r$ for which $\lambda_1 \times \lambda_2 \geq 1.8$, where λ_1 and λ_2 are the eigenvalues of $\mathbf{H}_r^H \mathbf{H}_r$, as given by (10). In all the following examples, we assume the eavesdropper knows $\mathbf{H}_r$ and $\mathbf{H}_e$ and implements an exhaustive ML decoder.

Fig. 1 compares the BER of the intended receiver and the eavesdropper when the information symbols are QPSK. This comparison is done for two cases: 1) when no artificial noise symbols are transmitted and 2) when the fourth symbol c_4 is an artificial noise symbol with a complex Gaussian distribution. The figure shows that for the QPSK constellation, transmitting artificial noise reduces both the diversity and coding gain at the eavesdropper, while due to the separable decoding at the intended receiver, the BER for the intended receiver is nearly the same as before. The price paid for this improvement in secrecy is a 25% rate loss (only three instead of four symbols are transmitted in each block), and a slight loss in coding gain.

Fig. 2 gives the same comparison as Fig. 1, but for the case that the information symbols are 8PSK. Again we have a similar observation, i.e., transmitting artificial noise considerably degrades the decoding ability at the eavesdropper, while the BER at the intended receiver is nearly unchanged.

In Fig. 3, we consider the performance of our secure STBC with artificial noise alignment assuming QPSK information symbols. The BER at the intended receiver is similar for $p = \frac{1}{2}$ and $p = \frac{5}{6}$, and these curves are also close to what is achieved by the intended receiver when no artificial noise is transmitted. This shows that the artificial noise symbols m and n are well aligned at the intended receiver even for low-to-medium SNR values. Comparison between the BER curves in this example with those of Fig. 1 shows that the decoding ability at the eavesdropper is better with the artificial noise alignment scheme than when transmitting c_4 as a Gaussian artificial noise symbol. This is due to the fact that we have made the worst-case assumption that the eavesdropper knows the direct channel $\mathbf{H}_r$ and can calculate the η and z_i coefficients.

5. CONCLUSIONS

A secure STBC was proposed that enables the intended receiver to perform separable decoding, while requiring an exhaustive ML search for any eavesdropper that is present. Two artificial noise transmission schemes were also considered. One of the schemes simply replaced one of the information symbols with an artificial noise symbol. In the other, it was shown that because of the separable decoding property of the STBC, the intended receiver can "align" or cancel the effect of the artificial noise symbols, while such an alignment is not possible at an eavesdropper. The artificial noise methods in effect trade off code rate or coding gain for improved secrecy, as illustrated by our simulation results.

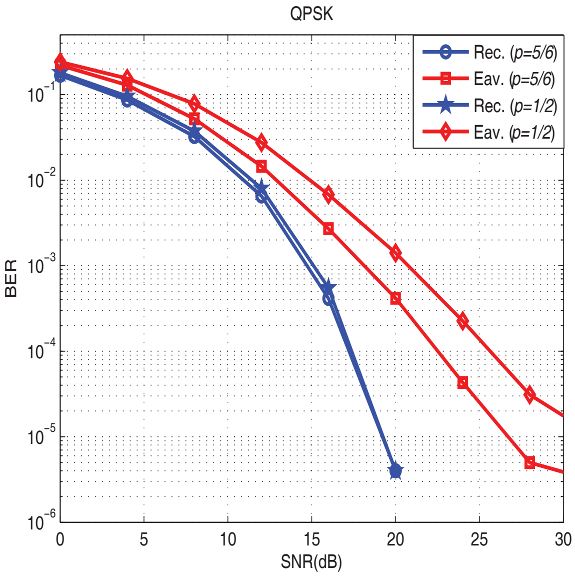

Fig. 3. BER performance of the receivers for the secure STBC with artificial noise alignment.

6. REFERENCES

[1] A. Wyner, “The wire-tap channel,” *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.

[2] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, 2010.

[3] T. Liu and S. Shamai (Shitz), “A note on secrecy capacity of the multi-antenna wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, 2009.

[4] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), “A MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009.

[5] H. Jafarkhani, Space-Time Coding: Theory and Practice. CambridgeUniversity Press, 2005.

[6] F. Li and H. Jafarkhani, “Multiple-Antenna Interference Cancellation and Detection for Two Users Using Precoders,” *IEEE J. Select. Topics in Signal Proc.*, vol. 3, no 6, pp. 1066-1078, Dec. 2009.

[7] H. Jafarkhani, “A quasi-orthogonal space-time block code,” *IEEE Trans. Commun.*, vol 49, no. 1, pp. 14, Jan. 2001.

[8] 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 1999.

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

[10] H. Wen, G. Gong and P. H. Ho, “MIMO Cross-Layer Secure Communication Architecture Based on STBC,” *in Proc. IEEE GLOBECOM 2010*.