This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Eavesdropping-Resistant Space-Time Network Coding for Cooperative Communications

Zhenzhen Gao *†, Yu-Han Yang *, and K. J. Ray Liu *
*Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA
†Department of Information and Communication Engineering, Xi'an Jiaotong University, Xi'an, 710049, P. R. China
Email:{ygggzhen, yhyang, kjrliu}@umd.edu

***Abstract*—Due to the broadcast nature, wireless transmissions can be overheard by any receiver within the transmission range. A physical layer approach for secure wireless cooperative communications is proposed in this paper. Considering the asynchronous nature of cooperative communications, this paper proposes an eavesdropping-resistant space-time network coding (STNC) scheme for cooperative communications to prevent eavesdropping and overcome the problem of imperfect synchronization. In the proposed scheme, training symbols are transmitted by the destination D instead of the user nodes. Therefore, based on the assumption of channel reciprocity, each user node can obtain the channel state information (CSI) between itself and D, which is unavailable to the eavesdropper E. Weighting coefficient is designed by exploiting such CSI at each user node to prevent E from interception and ensure successful decoding at D. Based on the pairwise error probability (PEP) analysis, STNC is designed to achieve full diversity at D and improve the transmission efficiency of the asynchronous cooperative system. Simulation results are presented to verify the performance of the proposed eavesdropping-resistant STNC scheme.**

I. Introduction

Security is an important issue in wireless networks due to the open wireless medium. Security against eavesdroppers can be achieved by using cryptographic algorithms. However, there are difficulties and vulnerabilities associated with key distribution and management [1]. Physical (PHY) layer security, which exploits the physical characteristics of wireless channel to transmit securely, has attracted much attention [2].

User cooperation is an effective scheme to introduce spatial diversity in wireless networks without the cost of co-located multiple antennas. This paper focuses on the physical layer security issue in wireless cooperative communication systems with a passive eavesdropper. In [3] and [4], cooperative protocols based on amplify-and-forward (AF) and decode-and-forward (DF) are proposed for PHY layer wireless security. Optimal weights are designed in [3] and [4] to maximize secrecy capacity or minimize transmit power. The transmissions from all the nodes are assumed to be synchronized and global channel state information (CSI) is required for the design of weights. However, the eavesdropper's CSI is unavailable for systems with passive eavesdroppers. Besides, since the nodes in cooperative networks are geographically separated, it is challenging for the receiver to receive all relaying signals simultaneously due to different propagation time, processing time, and timing estimation errors. Different from [3] and [4], which are more from the perspective of information theory, [5] has proposed a distributed differentially encoded OFDM transmission scheme with deliberate signal randomization to achieve low probability of interception (LPI) as well as the available diversities in asynchronous cooperative systems. LPI is one of the practical and important objectives of physical-layer security design. However, the differential encoding adopted in [5] reduces the transmission rate of the proposed scheme. Based on the previous studies, we propose a PHY layer secure transmission scheme with LPI and full diversity for asynchronous cooperative communication systems without sacrificing the transmission efficiency.

To overcome the imperfect synchronization problems, we use the idea of space-time network coding (STNC) in [6]. In this paper, an eavesdropping-resistant STNC scheme is proposed for the cooperative network without the knowledge of eavesdropper's CSI. Different from the STNC in [6], which uses FDMA or CDMA to separate different users' signals and thus requires more bandwidth, the proposed scheme uses the same frequency band for the whole network. Assume that E knows all the transmission protocols. To prevent eavesdropping, high bit error rate (BER) must be introduced at E. D transmits the training symbols so that each user node can get its own CSI from D, named local CSI. Based on the assumption of channel reciprocity, the local CSI is used by each user node to design its eavesdropping-resistant weighting coefficient to randomize the received signals at E without influencing the decoding at D. We analyze the PEP performance of the eavesdropping-resistant STNC scheme at D and derive the design criteria of the complex network coding vector, which guarantee full diversity at D. Simulation is provided to validate the performance of the proposed scheme. It can be seen from the simulation that, by the eavesdropping-resistant STNC scheme, full diversity can be achieved at D while high bit error rate is generated at E.

II. System Model and Transmission Protocol

A. System Model

Consider a wireless multinode cooperative communication network consisting of N user nodes, a destination node D and a passive eavesdropper E. We assume the user nodes are located within the same cluster, and D is faraway from the cluster. Assume that E is also at a faraway location outside the cluster, which is unknown to the user nodes. Each node is equipped with single antenna except E. Here E has K antennas ($K \geq 2$) for better received signal quality. As in [6], TDMA is used in the network. Channel reciprocity is

978-1-61284-233-2/11/$26.00 ©2011 IEEE

assumed. The channels between any two nodes in the system are modeled as narrow-band Rayleigh fading with additive white Gaussian noise (AWGN). Let h_n denote the channel gain from the nth user U_n to D, and g_{nk} denote the channel gain from U_n to the kth antenna of E, where $n \in [1, N]$ and $k \in [1, K]$. They are modeled as independent zero-mean, complex Gaussian random variables with variances $\mathrm{E}|h_n|^2 = \sigma_h^2$ and $\mathrm{E}|g_{nk}|^2 = \sigma_g^2$, respectively. The AWGN is assumed to be zero-mean and the variance is σ^2.

B. Transmission Protocol

In the beginning of each channel coherence time, D will transmit training symbols to initialize the transmission. Each user node can estimate its CSI from D based on the training symbols. Specifically, each transmission comprises two phases, the broadcasting phase (Phase I) and the encoding/relaying phase (Phase II). Assume that frame synchronization has been established for the TDMA transmissions. Based on the assumption of channel reciprocity, each node can get the CSI between itself and D. The N user nodes transmit their packets to D in their allocated time slots during each transmission. Assume there are N_s information symbols in each packet. Denote the ith information symbols of the N packets as a vector $\mathbf{s}(i) = [s_1(i), s_2(i), ..., s_N(i)]^{\mathrm{T}}$ with $i \in [1, N_s]$. The information symbol $s_n(i)$ comes from a normalized M-QAM (or M-PSK) constellation $\mathcal{A}$, i.e., average symbol energy of $\mathcal{A}$ is normalized to be 1.

In Phase I, the transmit power is chosen so that the signal can be decoded successfully by other nodes in the cluster Compared to the distance from D to the cluster, the user nodes in the cluster are close to each other. Only a small amount of power is required in Phase I, and neither D nor E can receive the transmitted signals. In this paper, we consider the secure transmission of Phase II. In Phase II, the nodes in the cluster linearly combine the decoded symbols as $x(i) = \boldsymbol{\theta}\mathbf{s}(i)$, where $\boldsymbol{\theta} = [\theta_1, \cdots, \theta_n, \cdots, \theta_N]$ is the complex network coding vector with $\boldsymbol{\theta}\boldsymbol{\theta}^H = 1$. Assume that both D and E know the network coding coefficients. Since E can overhear the signals transmitted to D, each user node multiplies the ith transmit symbol $x(i)$ with a weighting coefficient to randomize the received signal at E and prevent it from interception. Therefore, the ith signal of the new packet transmitted by U_n is $x_n(i) = w_{n,i}x(i)$.

The ith received signal at D from U_n is

$$y_{n,i} = \sqrt{P_t}h_n x_n(i) + z_{n,i}, \tag{1}$$

where P_t is the average transmit power constraint, and $z_{n,i}$ is the AWGN. The received signal from U_n at the kth antenna of E can be written as

$$r_{n,k,i} = \sqrt{P_t}g_{n,k}x_n(i) + v_{n,k,i}, \tag{2}$$

where $v_{n,k,i}$ is the AWGN. Since D transmits the training symbols in the beginning, each user node can obtain the corresponding channel from itself to D due to channel reciprocity, while these training symbols contribute nothing to E. The user nodes can not transmit training symbols because E can use the training symbols to estimate the channel and decode the information symbols. However, when channels change slowly, E can use blind channel estimation to detect the information. Therefore, we want to design a physical-layer transmission scheme for cooperative communications with LPI so that D can decode the symbols with full diversity, while E can not decode the symbols even when E can use blind channel estimation.

III. Design of Eavesdropping-Resistant Space-Time Network Codes

In this section, an eavesdropping-resistant STNC scheme is designed to prevent E from interception and to make the user nodes communicate to D effectively and asynchronously.

After Phase I, each user node has the transmit packets. The ith signals received from U_n at D and E are given by (1) and (2), respectively. After summing up the received copies from all the users, the received signals at D and E are

$$\begin{aligned} y_i &= \sqrt{P_t}\sum_{n=1}^{N} h_n w_{n,i}x(i) + z_i = \sqrt{P_t}hx(i) + z_i, \\ r_i &= \sqrt{P_t}\sum_{k=1}^{K}\sum_{n=1}^{N} g_{n,k}w_{n,i}x(i) + v_i = \sqrt{P_t}g_i x(i) + v_i, \end{aligned} \tag{3}$$

respectively, where the equivalent noises are $z_i = \sum_{n=1}^{N} z_{n,i}$, $v_i = \sum_{k=1}^{K}\sum_{n=1}^{N} v_{n,k,i}$, and the equivalent channels are $h = \sum_{n=1}^{N} h_n w_{n,i}$ and $g_i = \sum_{k=1}^{K}\sum_{n=1}^{N} g_{n,k}w_{n,i}$. During the channel coherent time, we want h to be a deterministic constant while the equivalent channel at E changes randomly for every cooperative transmission.

A. Anti-Eavesdropping Design

To prevent eavesdropping, the signal received at E is randomized by weighting coefficients for each transmission. The idea of randomization is motivated by [7], which exploited the redundancy of transmit antenna arrays for deliberate signal randomization to randomize E's signal and secure the MIMO transmission. Different from [7], the user nodes in cooperative communications do not have multiple antennas, and they are geographically separated. Assume that the user nodes and D share no additional information beforehand and know nothing about E. In this subsection, weighting coefficients are designed based on local CSI and transmit information. These weights make h a constant while g_i changes randomly for different i.

Assume that $U_n, \forall n \in [1, N]$ knows the number of nodes in the cluster and its index n. Denote the information bits in $s_n(i)$ as $\mathbf{b}_{n,i} = [b_{n,i}(1),\ b_{n,i}(2),\ \ldots,\ b_{n,i}(log_2 M)]$. Then the information bits at the user nodes after Phase I can be written as $\mathbf{b}_i = [b_{1,i}(1),\ \ldots,\ b_{N,i}(1),\ b_{1,i}(2),\ \ldots,\ b_{N,i}(log_2 M)]$. Based on these information bits, a variable can be generated as $t_i = \sum_{m=1}^{Nlog_2 M} 2^{-m} b_i(m)$. From t_i and h_n, $w_{n,i}$ for U_n can be designed as $w_{n,i} = \frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}$, where $u_n, n = 1, 2, \ldots, N$, are the Nth roots of unity satisfying $|u_n| = 1$. β_x and β_t will be chosen later to satisfy the average power constraint.

Because $\mathbf{b}_i$ is the information to be transmitted, neither D nor E can know it in advance. For different cooperative transmissions, the transmit information changes independently for D and E. Therefore, $e^{j2\pi t_i}$ is a random variable changing independently for D and E. Because $\sum_{n=1}^{N} u_n = 0$, the equivalent channels at D and E become

$$\begin{aligned} h &= \beta_x \sum_{n=1}^{N} |h_n| + \beta_t e^{j2\pi t_i} \sum_{n=1}^{N} u_n = \beta_x \sum_{n=1}^{N} |h_n|, \\ g_i &= \beta_x \sum_{k=1}^{K} \sum_{n=1}^{N} \frac{g_{n,k}|h_n|}{h_n} + \beta_t e^{j2\pi t_i} \sum_{k=1}^{K} \sum_{n=1}^{N} \frac{g_{n,k} u_n}{h_n}, \end{aligned} \tag{4}$$

respectively. The equivalent channel h is constant during the channel coherent time, and D can easily estimate $\sqrt{P_t}h$ as $\frac{\sum_{i=1}^{L}|y_i|}{L|x|}$ from the received signals, where L is the number of received signals used for estimation, and $|x|^2$ represents the average signal power of the transmit symbol $x(i)$, which can be estimated as long as the signal constellation is given. Thus, the detection for $\mathbf{s}(i)$ at D is

$$\hat{\mathbf{s}}(i) = \arg \min_{\mathbf{s} \in \mathcal{A}^N} |y_i - \sqrt{P_t} h \boldsymbol{\theta} \mathbf{s}|^2, \tag{5}$$

where $\mathbf{s} = [s_1 \ s_2 \ \dots s_N]^{\mathrm{T}}$.

As for the equivalent channel at E, g_i can be divided into two parts $g_i = g_{c,i} + g_{r,i}$, where $g_{c,i} = \beta_x \sum_{k=1}^{K} \sum_{n=1}^{N} \frac{g_{n,k}|h_n|}{h_n}$, and $g_{r,i} = \beta_t e^{j2\pi t_i} \sum_{k=1}^{K} \sum_{n=1}^{N} \frac{g_{n,k}}{h_n} u_n$. Thus the received signal at E can be written as $r_i = g_{c,i}x(i) + g_{r,i}x(i) + v_i$. Since h_n and $g_{n,k}$ are independent for any $n \in [1, N]$ and $k \in [1, K]$, $g_{r,i} \neq 0$ and $g_{r,i}$ changes independently for different i because of t_i. Due to the independent changes in $g_{r,i}$ for each cooperative transmission, it is hard for E to get an accurate channel estimation of g_i even if the channels h_n and $g_{n,k}$ for all $n \in [1, N], k \in [1, K]$ change slowly. Considering the best case for E that E can blindly estimate $g_{c,i}$ without error when all the channels change slowly, the decoding at E is still influenced by the random interference caused by $g_{r,i}x(i)$. β_x and β_t can be adjusted to induce high BER at E. Increasing β_t can increase the transmit power for randomness but decrease the power for information. Therefore, there is a tradeoff between performance and security.

B. Design Criteria of STNC

In this subsection, we design a set of complex network coding coefficients optimized for conventional signal constellations. The design criteria are derived based on PEP analysis at D. From the received signal y_i in (3), we can derive the probability of transmitting $\mathbf{s}$ and deciding in favor of another $\mathbf{c} = [c_1 \ c_2 \ \dots \ c_N]^{\mathrm{T}}$ at D. Conditioned on the channel state h, the Chernoff bound [8] of PEP is given by

$$P(\mathbf{s} \to \mathbf{c}|h) \leq \exp\Big(-\frac{P_t h^2 |\sum_{n=1}^{N} \theta_n (s_n - c_n)|^2}{4N\sigma^2}\Big). \tag{6}$$

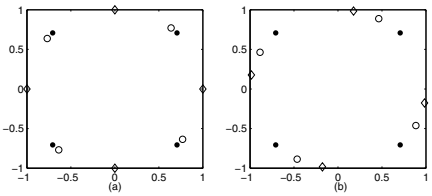

Fig. 1. Constellations with different $\boldsymbol{\theta}$ where $\bullet$ represents the constellation points for U_1, $\circ$ for U_2 and $\diamond$ for U_3.

Because $h^2 = \beta_x^2 (\sum_{n=1}^{N} |h_n|)^2 \geq \beta_x^2 h_D^2$ with $h_D^2 = \sum_{n=1}^{N} |h_n|^2$, the Chernoff bound can be written as

$$P(\mathbf{s} \to \mathbf{c}|h_D) \leq \exp\Big(-\frac{P_t \beta_x^2 h_D^2 |\sum_{n=1}^{N} \theta_n (s_n - c_n)|^2}{4N\sigma^2}\Big).$$

Let $h_n = h_{Rn} + j h_{In}$, $n \in [1, N]$. Since the channels are independent and $h_n \sim CN(0, \sigma_h^2)$, h_{Rn} and h_{In} are independent zero-mean real Gaussian random variables with variance $\frac{\sigma_h^2}{2}$. Then $\frac{2}{\sigma_h^2} h_D^2 \sim \chi^2(2N)$, and the probability density function (pdf) of h_D^2 is $f(\chi) = \frac{1}{(\sigma_h^2)^N \Gamma(N)} \chi^{N-1} \exp(-\frac{\chi}{\sigma_h^2})$ with $\chi = h_D^2, \chi > 0$ and $\Gamma(N) = (N-1)!$. Averaging with respect to χ, the PEP is bounded by

$$P(\mathbf{s} \to \mathbf{c}) \leq \Big(1 + \frac{\sigma_h^2 \beta_x^2 P_t |\sum_{n=1}^{N} \theta_n (s_n - c_n)|^2}{4N\sigma^2}\Big)^{-N}, \tag{7}$$

where the equation is derived according to ([9, pp.377, 3.351]). When SNR is high, 1 in (7) is neglectable. If $|\sum_{n=1}^{N} \theta_n (s_n - c_n)| \neq 0$, the PEP bound becomes

$$P(\mathbf{s} \to \mathbf{c}) \leq \Big(\frac{4N}{\sigma_h^2 \beta_x^2 |\sum_{n=1}^{N} \theta_n (s_n - c_n)|^2}\Big)^N \Big(\frac{P_t}{\sigma^2}\Big)^{-N}, \tag{8}$$

which means full diversity gain N can be achieved by D if the following maximum diversity condition holds true for any distinct pair $\{\mathbf{s}, \mathbf{c}\}$,

$$|\sum_{n=1}^{N} \theta_n (s_n - c_n)| \neq 0, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N, \mathbf{s} \neq \mathbf{c}. \tag{9}$$

Diversity is an important criterion since it determines the slope of the performance curve.

From (8), we can see that, given β_x, N, signal constellation and channel condition, the PEP depends on the design of the network coding coefficients. To get a better performance, the minimum value of $|\sum_{n=1}^{N} \theta_n (s_n - c_n)|$ over all distinct pairs of $\{\mathbf{s}, \mathbf{c}\}$ should be as large as possible. So we can get the product criterion as follows,

$$\arg \max_{\boldsymbol{\theta}} \min_{\mathbf{s} \neq \mathbf{c}, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N} |\sum_{n=1}^{N} \theta_n (s_n - c_n)|. \tag{10}$$

Besides, from the detection in (5), D should be able to differentiate different symbols from different user nodes based on the received signals. Assume that $\theta_n = \frac{1}{\sqrt{N}} e^{j\phi_n}$, and $\phi_1 < \phi_2 < \cdots < \phi_N$. Multiplying U_n's symbol by θ_n is equivalent to rotating the constellation at U_n by ϕ_n. To differentiate the symbols of U_n from that of U_m, U_n's rotated constellation should be different from U_m's, and the more

TABLE I
ROTATION ANGLES FOR DIFFERENT N AND CONSTELLATIONS

N	constellation	c_g	ϕ	complexity-number of loops
2	BPSK	2	0.3350π	3^2N_s
2	4QAM	1.0353	0.1667π	9^2N_s
2	8QAM	0.8828	0.3583π	21^2N_s
3	BPSK	1.2361	0.6283π	3^3N_s
3	4QAM	0.6050	0.4033π	9^3N_s
3	8QAM	0.2599	0.1911π	21^3N_s

different the better. Take the case in Fig. 1 (a) for example. When $\theta_1 \approx \theta_2$, there exist $s_1 \in \mathcal{A}$ from U_1 and $s_2 \in \mathcal{A}$ from U_2 to make $\theta_1 s_1 + \theta_2 s_2 \approx \theta_1 s_2 + \theta_2 s_1$. Due to the adjacency of the signal points from the rotated constellations of U_1 and U_2, D can be confused with the symbols from U_1 and U_2 with high probability, which results in the failure of detection. In fact, we want the difference between any two rotated constellations for two distinct user nodes to be large so that different users' symbols will not be confusing to D. Therefore, as show in Fig. 1 (b), we assume that the rotation angles are of equal distance for simplicity. The problem is to find an optimal distance to satisfy the product criterion. Denote the equal distance as $\phi = \phi_{n+1} - \phi_n, \forall n \in [1, N-1]$. Then the product criterion becomes

$$\arg\max_{\phi} \min_{\mathbf{s}\neq\mathbf{c},\forall \mathbf{s},\mathbf{c}\in\mathcal{A}^N} |\sum_{n=1}^{N} e^{j((n-1)\phi+\phi_1)}(s_n - c_n)|, \quad (11)$$

The optimal theoretic solution for (11) of any N and any constellation is untractable. However, because there's only one parameter to be optimized, it is easy to find the optimal angle ϕ by exhaustive computer search. Define the coding gain as

$$c_g = \min_{\mathbf{s}\neq\mathbf{c},\forall \mathbf{s},\mathbf{c}\in\mathcal{A}^N} |\sum_{n=1}^{N} e^{j((n-1)\phi+\phi_1)}(s_n - c_n)|, \quad (12)$$

and the step-length in computer search as $\triangle$. The number of steps for searching is $N_s = 2\pi/\triangle$. Table 1 lists the optimal angles, coding gains and search complexities for different N and constellations.

It can be seen from Table 1 that when the number of user nodes is fixed, coding gain decreases as constellation size increases. When a constellation is given, more cooperative users result in larger diversity gain but smaller coding gain.

C. Power Allocation

In this subsection, we will choose β_x and β_t to satisfy the average power constraint. The signal transmitted from U_n in the ith transmission can be denoted as

$$x_{t,n}(i) = \sqrt{P_t}\frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}x(i). \quad (13)$$

The average transmit power is $\bar{P}_t = \mathrm{E}\Big(P_t|\frac{\beta_x|h_n|+\beta_t u_n e^{j2\pi t_i}}{h_n}|^2\Big)$, which should not exceed the average power constraint P_t. Thus $\mathrm{E}|\frac{\beta_x|h_n|+\beta_t u_n e^{j2\pi t_i}}{h_n}|^2 \leq 1$. Because

$$\mathrm{E}|\frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}|^2 \leq \mathrm{E}\Big(\beta_x + \frac{\beta_t}{|h_n|}\Big)^2, \quad (14)$$

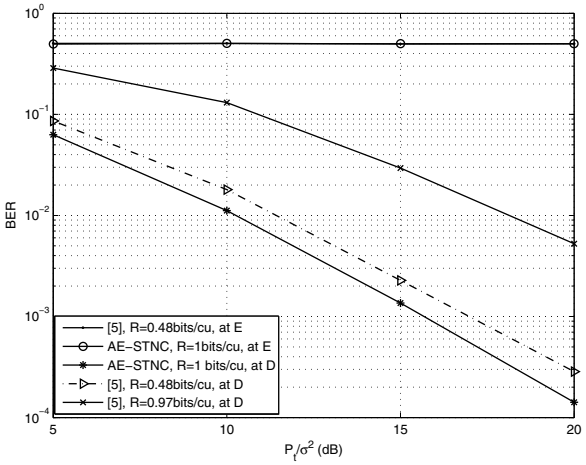

Fig. 2. BER performance for the eavesdropping-resistant STNC scheme and the scheme in [5] with $N = 2$

we can approximate the power constraint by setting $\mathrm{E}\Big(\beta_x + \frac{\beta_t}{|h_n|}\Big)^2 = 1$. Because $\mathrm{E}(\frac{1}{|h_n|}) = \sqrt{\frac{\pi}{\sigma_h^2}}$, and $\mathrm{E}(\frac{1}{|h_n|^2})$ is

$$\mathrm{E}(\frac{1}{|h_n|^2}) = \frac{1}{\sigma_h^2}\int_0^\infty \frac{1}{t}e^{-t}dt \approx 3.3182/\sigma_h^2, \quad (15)$$

where $t = |h_n|^2/(\sigma_h^2)$ and the approximation is obtained by using Laguerre integral formula [10, pp.923], the power constraint becomes

$$\beta_x^2 + \frac{3.3182\beta_t^2}{\sigma_h^2} + 2\sqrt{\frac{\pi}{\sigma_h^2}}\beta_x\beta_t = 1. \quad (16)$$

Subject to the average power constraint, β_x and β_t can be chosen according to (16). Different choice of $\{\beta_x, \beta_t\}$ represents the tradeoff between the performance of the cooperative system and transmission security.

IV. SIMULATION RESULTS

In this section, we show some simulation results of the proposed scheme for asynchronous cooperative communications by comparing the BER performances of D and E. In the simulations, clusters of 2 and 3 user nodes are adopted. Without loss of generality, we set $\phi_1 = 0$. Thus θ_1 for U_1 is $\frac{1}{\sqrt{N}}$, and θ_n for U_n is $\frac{1}{\sqrt{N}}e^{j(n-1)\phi}$. The channel variances are $\sigma_h^2 = 1$ and $\sigma_g^2 = 1$. The number of antennas for E is $K = 2$. Unless specified otherwise, $\beta_x = 0.9$ is used throughout, and E uses the same channel estimation based on the received signal energy as D.

In Fig. 2, we compare the proposed scheme with the differentially encoded OFDM scheme with LPI in [5]. $N = 2$ is adopted. The cyclic group codes $G_{2,4} = (2, 4, [1, 1])$ and $G_{2,16} = (2, 16, [1, 7])$ are used in [5]'s scheme with the corresponding rates of 0.24 bits/channel use (cu) and 0.48 bits/cu. BPSK is used in our proposed scheme, and the transmission rate is 0.5 bits/cu. It can be seen from Fig. 2 that, the BER of E is always around 0.5 for both schemes, which means E can not do better than guessing. However, the

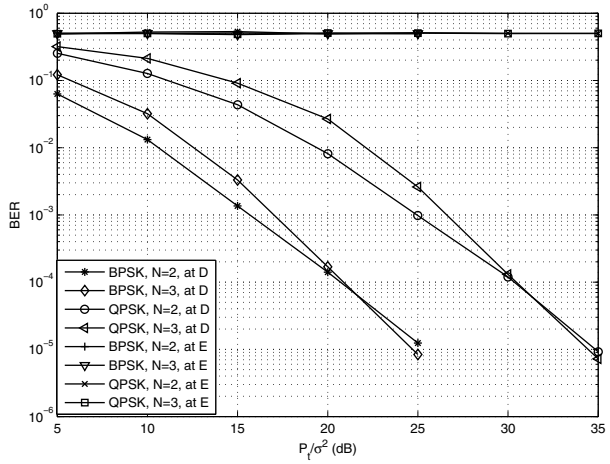

Fig. 3. BER performance for different modulations with $N = 2, 3$

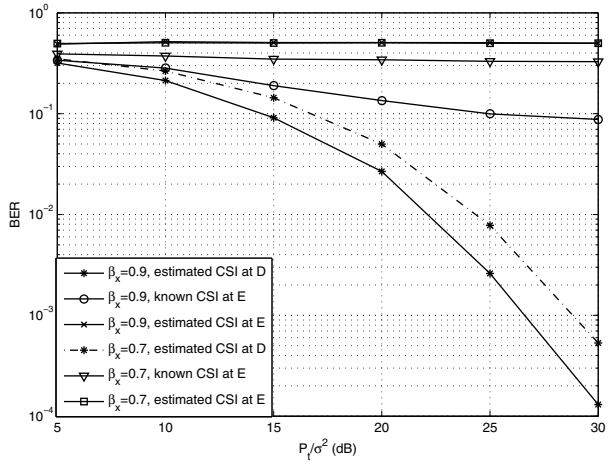

Fig. 4. BER performance for different power ratios

BER performance of the scheme in [5] is worse than that of the eavesdropping-resistant STNC scheme, even when the rate of [5] is a half of the proposed scheme. From the curves, we verify that the full diversity order, which is equal to the number of user nodes N, is achieved by the proposed eavesdropping-resistant STNC scheme.

The BER performances with different modulations for $N = 2$ and 3 are compared in Fig. 3. From the curves we can see that full diversity is always achieved when SNR is high enough. It can be seen from Fig. 3 that, for a fixed N, higher modulation results in worse BER performance due to smaller coding gain, and for a fixed constellation, more cooperative nodes can get higher diversity but lower coding gain. When SNR is sufficiently high, diversity gain dominates the performance and cooperative communications with more user nodes can have better performance. When moderate or low SNR region is considered for a dense cluster of user nodes, for better BER performance, the nodes can be divided into groups and each group uses an eavesdropping-resistant STNC of small size. We can also observe from Fig. 3 that the BER at E is always around 0.5 for different N and modulations.

Fig. 4 shows the BER performances of different power ratios for $N = 3$ user nodes with 4QAM modulation. From the figure we can see that, when E does not know the CSI and estimates the CSI using the same method as D, the BER for E is around 0.5, which means E can not decode the transmit information even most of the power is used for signal transmission. The BER performance when E can blindly estimate g_{ci} without estimation error is also given in Fig. 4 as a lower bound of E's BER performance, which is the worst case for the cooperative system. The decoding of the transmit information at E is affected by the random interference. When $\beta_x = 0.9$, the interference power is quite low, and the BER at E is around 0.1. Higher BER at E can be generated by increasing β_t. It can be seen from Fig. 4 that the BER at E is above 0.3 when β_x decreases to 0.7. Due to the decrease of β_x, the transmission power for information signals reduces, resulting in performance degradation at D. The choice of $\{\beta_x, \beta_t\}$ is a tradeoff between performance and security in terms of LPI.

V. Conclusion

In this paper, we propose an eavesdropping-resistant space-time network coding scheme for asynchronous multinode cooperative systems to prevent eavesdropping and achieve full diversity without sacrificing transmission efficiency. The eavesdropping-resistant STNC, which is designed based on local information at the separated user nodes, can guarantee full diversity at D and high BER at E. The PEP performance of eavesdropping-resistant STNC is analyzed, and the design criteria are derived. Simulation results validate our analysis. Compared with the differentially encoded OFDM scheme proposed in [5], the proposed eavesdropping-resistant STNC scheme can achieve better performance and higher transmission rate.

References

[1] B. Schneier, "cryptographic design vulnerabilities," *IEEE Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.
[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[3] L. Dong, A. P. Petropulu, and H. V. Poor, "Amplify and forward based cooperation for secure wireless communications," in *Proc. IEEE ICASSP*, Taipei, May 2009, pp. 2613–2616.
[4] L. Dong, H. Zhu, A. P. Petropulu, and H. V. Poor, "Secure wireless communication via cooperation," in *Proc. 46th Annual Allerton Conf. Commun. Control, and Computing*, Monticello, IL, 2008.
[5] Z. Li and X. G. Xia, "A family of distributed space-time trellis codes with asynchronous cooperative diversity," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3372–3379, Jul. 2009.
[6] H. Q. Lai and K. J. R. Liu, "Space-time network codes utilizing transform-based coding," in *Proc. IEEE ICASSP*, 2010, pp. 2878–2881.
[7] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.
[8] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal design," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1456–1467, Jul. 1999.
[9] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integral, Series, and Products, fifth edition*. Academic Press, 1994.
[10] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. National Bureau of Standards, Applied Mathematics Series, 1964.