Anti-Eavesdropping Space-Time Network Coding for Cooperative Communications

Zhenzhen Gao, *Student Member, IEEE*, Yu-Han Yang, *Student Member, IEEE*, and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*—Due to the broadcast nature of wireless medium, wireless transmissions can be overheard by any undesired receivers with eavesdropping capability within source transmission range. A novel physical layer approach for secure wireless cooperative communications against eavesdropping is proposed in this paper. For an asynchronous cooperative communication network with a cluster of user nodes transmitting to a common destination, we propose an anti-eavesdropping space-time network coding (AE-STNC) scheme to prevent eavesdropping and overcome the problem of imperfect synchronization. In the proposed scheme, training symbols are first transmitted by the destination (D). Owing to channel reciprocity, each user node can obtain the channel state information (CSI) between itself and D, which is unavailable to the eavesdroppers. By exploiting such CSI, anti-eavesdropping encoding is designed for each user node to create high decoding error rate at the eavesdroppers and ensure successful decoding at D. Furthermore, the AE-STNC is designed to achieve full diversity at D. Power allocation subject to average power constraint is considered and the secure region against eavesdroppers is also investigated. Based on the proposed AE-STNC scheme, an anti-eavesdropping space-time-frequency coding (AE-STFNC) scheme is proposed for broadband asynchronous cooperative communications. Simulations are provided to verify the performance and security of the proposed transmission schemes.**

***Index Terms*—Physical layer security, cooperative communication, synchronization, eavesdropping, space-time network codes.**

I. Introduction

SECURITY is a critical concern in wireless networks due to the open wireless medium. Any receiver within the range of a wireless transmission can potentially overhear the transmitted information. Security against eavesdropping can be achieved by using cryptographic algorithms. However, there are difficulties and vulnerabilities associated with key distribution and management [1] [2]. Physical (PHY) layer security, which exploits the physical characteristics of wireless channels for secure transmission, has attracted much attention recently. The maximum achievable secrecy rate is referred to as secrecy capacity, which is developed in [3], which shows that as long as the eavesdropper's channel is a degraded version of the receiver's channel, perfect secrecy can be achieved without any key. The scenario considered in [3] is generalized in [4], which shows that when the receiver and the eavesdropper have separate channels, secret communication is possible if the eavesdropper's channel has a smaller capacity than the receiver's. However, if the eavesdropper's channel happens to be better than the receiver's, e.g., the eavesdropper is closer to the transmitter than the receiver, secrecy cannot be guaranteed.

In this paper, we consider PHY layer security for a cooperative communication network with multiple eavesdroppers. A cluster of user nodes in the considered network tries to communicate to a common destination (D) via cooperation. The user nodes are geographically separated, which means the cooperative communication is asynchronous in nature [5]. It is challenging for D to receive all relaying signals simultaneously due to different propagation times, processing times, and time estimation errors. Assuming some passive eavesdroppers are present, the user nodes should provide secure transmissions without any knowledge about the eavesdroppers.

As in [3] and [4], mutual information is used in many papers as performance metric to design secure scheme for cooperative communications. Cooperative protocols based on amplify-and-forward (AF) and decode-and-forward (DF) are proposed in [6] and [7] for PHY layer wireless security in synchronized cooperative communications. System design that maximizes secrecy capacity or minimizes transmit power is considered based on the assumption that global channel state information (CSI) is available, where global CSI includes both channels between the user nodes and D and channels between the user nodes and the eavesdroppers. A scheme which enables an opportunistic selection of two relay nodes to increase security against eavesdroppers is proposed in [8]. The first relay assists the source to deliver its data to D via DF strategy, while the second relay is used to create intentional interference at the eavesdroppers. These studies using mutual information are based on the assumption that the eavesdropper's channel state information (CSI) is available. However in practice, the user nodes do not know if an eavesdropper is present or not, not to mention whether the eavesdropper would like to share his/her CSI. Such approaches by using mutual information are to understand the fundamental limits from information theory point of view, but not to mean to offer a practical solution.

Considering the practical problems of unawareness of eavesdroppers' CSI and imperfect synchronization, a distributed differentially encoded OFDM transmission scheme with deliberate signal randomization is proposed in [9] to achieve low probability of interception (LPI) as well as available diversities in asynchronous cooperative communications.

Manuscript received February 19, 2011; revised June 24, 2011; accepted August 15, 2011. The associate editor coordinating the review of this paper and approving it for publication was M. Valenti.

Z. Gao is with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China (e-mail: ygggzhen@umd.edu). This work was done during her visit at the University of Maryland.

Y. H. Yang and K. J. Ray Liu are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, 20742, USA (e-mail: {yhyang, kjrliu}@umd.edu).

Digital Object Identifier 10.1109/TWC.2011.100611.110320

The signal randomization in [9] is based on the structure of differential encoding which uses half of the useful subcarriers as reference. Therefore, the proposed scheme in [9] sacrifices much bandwidth efficiency.

LPI is one of the practical and important objectives of PHY layer security design. A goal of this paper is to devise a practical scheme to thwart eavesdropping. Therefore, the performance of interception of each bit (or symbol) of the transmitted information, similar to [9], is considered in this paper, where an anti-eavesdropping space-time network coding (AE-STNC) scheme to create LPI for each bit (or symbol) is proposed for asynchronous cooperative communication systems under the condition that the eavesdroppers' CSI is unavailable. Compared with the secure scheme in [9], the proposed scheme does not sacrifices transmission efficiency.

To overcome the problem of imperfect synchronization, we use the idea of space-time network coding (STNC) in [10]. TDMA is used by the STNC to overcome the imperfect synchronization issues. Existing TDMA-based cooperation schemes result in large transmission delay [11]. To reduce the transmission delay caused by TDMA, CDMA or FDMA is used at each user node in [10] to combine its decoded symbols. Compared with traditional TDMA-based cooperative communications, where N^2 time slots are needed for the transmission of N packets from N user nodes [11], only $2N$ time slots are required by the STNC scheme in [10]. Although the transmission delay is reduced in [10], more bandwith is required due to the use of CDMA or FDMA. Different from the STNC scheme in [10], the proposed AE-STNC scheme can reduce the transmission delay caused by TDMA without using extra bandwidth. A complex network coding vector is designed in this paper for the user nodes to combine their information symbols and the same frequency band is used by all the nodes. The proposed AE-STNC scheme can guarantee full diversity at D while preventing eavesdropping.

To prevent eavesdropping, the received signals at the eavesdroppers are randomized to create LPI for each bit (or symbol). At the beginning of each channel coherence time, D transmits training symbols on the same frequency band used by the user nodes, so that each user node can get its own CSI from D, named local CSI. The local CSI is location-specific and unavailable to the eavesdroppers. Based on the assumption of channel reciprocity, an anti-eavesdropping encoding is designed for each user node by exploiting the local CSI to randomize the received signals at the eavesdroppers without influencing the decoding at D. We analyze the pairwise error probability (PEP) performance of the AE-STNC scheme at D and derive the design criteria of the coding scheme.

We also extend the proposed AE-STNC scheme to frequency-selective channels. For broadband cooperative networks with multiple eavesdroppers, an anti-eavesdropping space-time-frequency network code (AE-STFNC), which provides security and flexible diversity, is proposed through mapping from the proposed AE-STNC scheme. Simulation results are provided to validate the performance of the proposed schemes. The simulations verify that by using the anti-eavesdropping coding schemes, full diversity can be achieved at the destination while high bit error rate (BER) is generated at the eavesdroppers to achieve LPI. It can be seen from the simulation results that the eavesdropper's BER can be around 0.5, which means he/she cannot decode better than guessing.

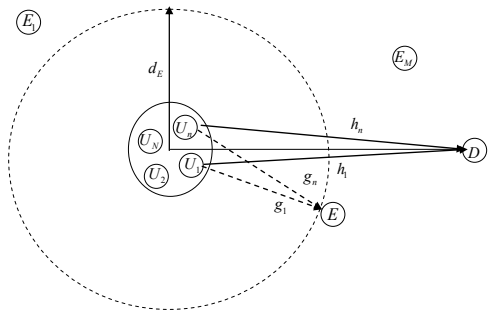


Fig. 1. System model of cooperative communications with multiple eavesdroppers.

The paper is organized as follows. In Section II, the system model and transmission protocol are introduced. In Section III, the design of the AE-STNC scheme for narrowband cooperative communications is discussed to guarantee full diversity at D and provide security in Phase II. Power allocation under average power constraint of each user node is investigated. In Section IV, the security and performance requirements of the considered network in Phase I is considered, and the secure region in which a certain security requirement is satisfied is given. In Section V, the anti-eavesdropping coding scheme is extended to frequency-selective channels. Simulation results are presented in Section VI. Finally, conclusions are drawn in Section VII.

Notations: Upper (Lower) case boldface letters stand for matrices (vectors). $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ denote transposition and conjugate transposition of a vector, respectively. $\mathrm{E}[\cdot]$ stands for expectation. $\circ$ denotes Hadamard product. $\mathrm{diag}[d_1, \ldots, d_N]$ denotes a diagonal matrix with d_n as its nth diagonal entry.

II. System Model and Transmission Protocol

A. System Model

Consider a wireless cooperative communication network consisting of N user nodes, a destination node D and K passive eavesdroppers, as shown in Fig. 1. Each node is equipped with single antenna. We assume the user nodes are located within the same cluster, and D is faraway from the cluster. Assume that the eavesdroppers are also at some faraway locations outside the cluster, which are unknown to the user nodes. These eavesdroppers are assumed to be independent and unable to collude. The user nodes in the cluster help one another to transmit to D and the transmissions should be kept secret from the unknown eavesdroppers. Since the user nodes are unaware of the eavesdroppers, without loss of generality, we consider from one particular eavesdropper's perspective, but of course the proposed PHY layer security scheme can prevent eavesdropping from any of the eavesdroppers.

Assume the channels between any two nodes in the system are independent and each channel is modeled as narrow-band Rayleigh fading with additive white Gaussian noise (AWGN). Let h_n denote the channel gain from D to the nth user U_n, and g_n denote the channel gain from the considered eavesdropper

(E) to U_n, where $n \in [1, N]$. They are modeled as independent zero-mean, complex Gaussian random variables. Since the cluster is far from D, the channel variance between U_n and D is assumed to be the same as that between U_m and D, where $m, n \in [1, N]$ and $n \neq m$. The same assumption is made on the channel variances between the user nodes and E. Denote the variances as $\mathrm{E}|h_n|^2 = \sigma_h^2$ and $\mathrm{E}|g_n|^2 = \sigma_g^2$, where $\sigma_h^2 = \kappa d_D^{-\alpha}$ and $\sigma_g^2 = \kappa d_E^{-\alpha}$, where κ is a constant whose value depends on the propagation environment, d_D and d_E are the distances from the cluster to D and E, respectively, and α is the path loss exponent, whose value is usually in the range of 2 and 4. We denote the radius of the cluster as d, and $d < \min(d_D, d_E)$. The distance between U_m and U_n is d_{mn}, and $\max\{d_{mn}, m, n \in [1, N]\} \leq 2d$. The AWGN is assumed to be zero-mean and the variance is σ^2.

B. Transmission Protocol

At the beginning of each channel coherence time, D transmits training symbols on the same frequency band used by the user nodes to initialize the transmission. Based on the assumption of channel reciprocity, each user node can estimate its local CSI between itself and D, which is location-specific. Although E can also receive the training symbols from D, E cannot get any useful information about the other nodes. Assume that frame synchronization has been established in the TDMA transmissions. There are two phases in each transmission, the broadcasting phase (Phase I) and the encoding/relaying phase (Phase II). The N user nodes transmit their packets to D in their allocated time slots during Phase I and Phase II. Assume there are N_s information symbols in each packet. Denote the ith 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., the average symbol energy of $\mathcal{A}$ is normalized to be 1. Fig. 2 illustrates the structure of AE-STNC with the ith symbols of the N packets.

In Phase I, each node $U_n, n \in [1, N]$ broadcasts its packet in its allocated time slot, where $s_n(i)$ is the ith symbol of U_n's packet. The transmit power is chosen so that the signal can be decoded successfully by the other nodes in the cluster. Compared with the distance from D, the nodes in the cluster are close to each other. Thus only a small amount of power is required in this phase. Assume that neither D nor E can receive the transmit signals in Phase I due to attenuation. In this paper, we first focus on the secure transmission problem in Phase II. Our purpose is to design a secure encoding scheme which guarantees full diversity at D and LPI at E regardless of E's location. Then we give the secure region for Phase I in which eavesdropping is not possible.

In Phase II, the user nodes in the cluster help one another to accomplish the secure transmission. First, each node linearly combines the decoded symbols obtained in Phase I as $x(i) = \boldsymbol{\theta}\mathbf{s}(i)$ for $\forall i \in [1, N_s]$, 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 vector. Since E can overhear the transmitted signals, to prevent E from eavesdropping, each user node encodes its transmit symbol with an anti-eavesdropping coefficient to randomize the received signal at E. Therefore, the ith symbol of the new packet transmitted by U_n is $x_n(i) = w_{n,i}x(i)$, where $w_{n,i}$ is the anti-eavesdropping coding coefficient at U_n for the ith transmit symbol. The AE-STNC with the ith symbols of the new packets can be written as a diagonal matrix $\mathbf{X}_i = \mathrm{diag}[x_1(i), \ldots, x_n(i), \ldots, x_N(i)]$, as shown in Fig. 2.

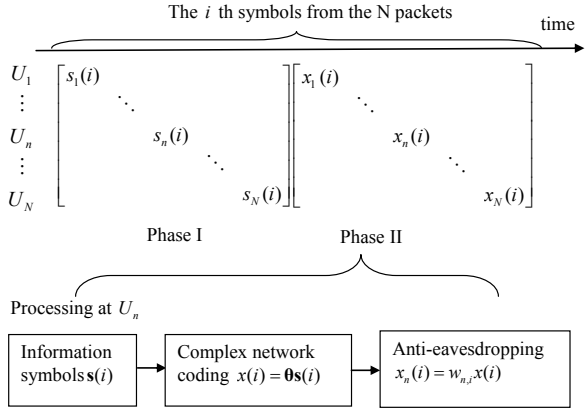


Fig. 2. Cooperative transmission and the structure of AE-STNC with the ith symbols of the N packets.

The ith signal received at D from U_n is

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

where P_t is the transmit power, $h_{n,i} = h_n w_{n,i}$, and $z_{n,i}$ is the AWGN. The ith received signal at E from U_n can be written as

$$r_{n,i} = \sqrt{P_t}g_n x_n(i) + v_{n,i} = \sqrt{P_t}g_{n,i}x(i) + v_{n,i}, \quad (2)$$

where $g_{n,i} = g_n w_{n,i}$ and $v_{n,i}$ is the AWGN. Since D transmits training symbols at the beginning of each channel coherence time, U_n can estimate h_n and obtain the CSI between itself and D due to channel reciprocity. The user nodes can not transmit training symbols because E can use the training symbols to estimate $g_n, \forall n \in [1, N]$, and decode the information symbols. However, when channels change slowly, E can use blind channel estimation to decode the information symbols. Therefore, the anti-eavesdropping encoding should be designed to prevent E from eavesdropping even when E can blindly estimate his/her channels.

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

In this section, we focus on the transmission in Phase II. An AE-STNC scheme is designed to prevent E from eavesdropping and to allow the user nodes to communicate to D effectively without perfect synchronization.

After Phase I, each user node has received the transmitted packets, and the vector of the ith transmitted symbols from the N packets is $\mathbf{s}(i)$. In Phase II, each user node transmits its new packet in its allocated time slot. The ith symbol of U_n's new packet is generated as $x_n(i) = w_{n,i}\boldsymbol{\theta}\mathbf{s}(i)$. The ith received signals from U_n at D and E are given by (1) and (2), respectively. After summing up the received copies of the

ith symbols from all the users, the received signal at D can be written as

$$y_i = \sqrt{P_t} h_i x(i) + z_i, \tag{3}$$

where the equivalent channel is $h_i = \sum_{n=1}^{N} h_{n,i}$, and the equivalent noise is $z_i = \sum_{n=1}^{N} z_{n,i}$. During the channel coherence time, we want the equivalent channel at D to be a deterministic constant $h_i = h$, while the channels $g_{n,i}, \forall n \in [1, N]$ change randomly at E for every transmit symbol so that E can not decode the transmitted symbols.

A. Anti-Eavesdropping Design

To prevent eavesdropping, each signal received at E is randomized by an anti-eavesdropping encoding. The idea of randomization is motivated by [12], which exploits the redundancy of transmit antenna arrays for deliberate signal randomization to randomize E's signal and secure the MIMO transmission. Different from [12], the user nodes in cooperative communications do not have multiple antennas, and they are geographically separated. The anti-eavesdropping design here is different from that in [12] in two aspects: 1) Each user node can only know its own local CSI to the destination; 2) each user node is unaware of the randomness generated by other user nodes. Assume that the user nodes and D share no additional information beforehand and know nothing about E. In this subsection, an anti-eavesdropping encoding is designed for each user node based on its local CSI and transmit information. This anti-eavesdropping encoding makes h a constant during the channel coherence time, while $g_{n,i}$ changes randomly at different time.

Denote the binary bits of $s_n(i)$ as $\mathbf{b}_{n,i} = [b_{n,i}(1), b_{n,i}(2), \ldots, b_{n,i}(log_2 M)]$. Then the available 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 for different i can be generated as

$$t_i = \sum_{m=1}^{Nlog_2 M} 2^{-m} \mathbf{b}_i(m). \tag{4}$$

Assume that $U_n, \forall n \in [1, N]$ knows the number of user nodes in the cluster and its index n. Based on t_i and the local CSI h_n, we can design the anti-eavesdropping encoding coefficient for U_n as

$$w_{n,i} = \frac{\beta_x |h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n} \tag{5}$$

where $u_1, \cdots, u_N$ are the Nth roots of unity satisfying $|u_n| = 1, \forall n \in [1, N]$. β_x and β_t will be chosen later to satisfy the average power constraint. Because $\mathbf{b}_i$ is the information bits to be transmitted, neither D nor E can know $\mathbf{b}_i$ in advance. From the perspective of the destination and eavesdroppers, the information bits change independently from one symbol to another. Therefore, $e^{j2\pi t_i}$ is a random variable changing independently for D and E. Because of the property of the roots, $\sum_{n=1}^{N} u_n = 0$, the equivalent channel at D becomes

$$h = \beta_x \sum_{n=1}^{N} |h_n| + \beta_t e^{j2\pi t_i} \sum_{n=1}^{N} u_n = \beta_x \sum_{n=1}^{N} |h_n|. \tag{6}$$

From (6) we can see that the equivalent channel h is constant during the channel coherent time. D can easily estimate $\sqrt{P_t} h$ as $\frac{\sum_{i=1}^{L} |y_i|}{L\overline{|x|}}$ from the received information signals, where L is the number of received signals used for estimation, and $\overline{|x|}$ represents the average amplitude of the transmit symbol $x(i)$. $\overline{|x|}$ can be estimated as long as the signal constellation is given. Thus, the maximum likelihood (ML) detection for $\mathbf{s}(i)$ at D is

$$\hat{\mathbf{s}}(i) = \arg \min_{\mathbf{s} \in \mathcal{A}^N} |y_i - \sqrt{P_t} h \boldsymbol{\theta} \mathbf{s}|^2, \tag{7}$$

where $\mathbf{s} = [s_1, s_2, \ldots, s_N]^{\mathrm{T}}$. The decoding complexity of the ML decoder increases exponentially with the number of user nodes, but sphere decoding method [13] [14] can be used to reduce the complexity. For a dense cluster of user nodes, the user nodes can be divided into groups and each group can use an AE-STNC of smaller size to reduce the decoding complexity while sacrificing some diversity.

As for the channels at E, $g_{n,i}$ in (2) can be written as $g_{n,i} = \beta_x \frac{g_n |h_n|}{h_n} + \beta_t u_n \frac{g_n}{h_n} e^{j2\pi t_i}$, which changes randomly because of the random changes of t_i at E. In fact, E can also use the similar processing at D to try to mitigate the influence of the randomness. After summing up the received copies, the received signal at E can be written as

$$r_i = \sqrt{P_t} g_i x(i) + v_i, \tag{8}$$

where the equivalent noise is $v_i = \sum_{n=1}^{N} v_{n,i}$, and the equivalent channel becomes

$$g_i = \beta_x \sum_{n=1}^{N} \frac{g_n |h_n|}{h_n} + \beta_t e^{j2\pi t_i} \sum_{n=1}^{N} \frac{g_n u_n}{h_n}. \tag{9}$$

Since h_n and g_n are independent for any $n \in [1, N]$, the second part of g_i is not zero and changes independently for different i because of t_i. Due to the random changes in the second parts of $g_{n,i}$ and g_i for different i, it is hard for E to get an accurate channel estimation of $g_{n,i}$ or g_i even if the channels h_n and g_n for all $n \in [1, N]$ change slowly. It is shown later in the simulations that, the decoder at E can not do better than guessing if E estimates the channels as D does. Considering the best case for E that E can blindly estimate the deterministic parts of $g_{n,i}$ and g_i without error, the decoding at E is still influenced by the random interference caused by the second parts of $g_{n,i}$ and g_i. Increasing β_t can increase the influence of the random interference at E, and thus provide better security. However, due to the average power constraint that will be discussed later, larger β_t results in smaller β_x, which means the transmit power for information decreases and the performance at D is degraded. Therefore, there is a tradeoff between performance and security. In this case, we can adjust $\{\beta_x, \beta_t\}$ based on the average power constraint to achieve different performance and security requirements. Since the anti-eavesdropping encoding is designed by utilizing local CSIs as well as the transmit information, which are independent with the eavesdroppers, the received signal at any of the eavesdroppers will be randomized according to the analysis above.

So far, the anti-eavesdropping encoding has been designed to fulfill two functions: randomization of E's signals and

inphase combining of the received signals at D. We can see from the simulation results that, the randomness will not influence the decoding at D when there are some decoding errors at the user nodes in Phase I. The user nodes can also use a common pseudorandom number generator (PRNG) to generate random numbers. In this case, secure coordination to share the PRNG is needed among the user nodes.

B. Design Criteria of STNC

In the previous subsection, an anti-eavesdropping encoding is designed for each user node to randomize the received signal at E without influencing the decoding at D. In this subsection, we design a complex network coding to achieve full diversity at D. The PEP performance of the AE-STNC at D is analyzed, based on which the design criteria are derived. From the signal detection at D in (7), we can derive the probability of transmitting $x(i)$ and deciding in favor of $\hat{x}(i)$, where $x(i) = \boldsymbol{\theta}\mathbf{s}$ with $\mathbf{s} = [s_1, \cdots, s_n, \cdots, s_N]^{\mathrm{T}}$, and $\hat{x}(i) = \boldsymbol{\theta}\mathbf{c}$ with $\mathbf{c} = [c_1, \cdots, c_n, \cdots, c_N]^{\mathrm{T}}$. Conditioned on the channel state h, the Chernoff bound [15] of PEP is given by

$$P(\mathbf{s} \to \mathbf{c}|h) \leq \exp\Big(-\frac{P_t h^2 |\sum_{n=1}^{N} \theta_n(s_n - c_n)|^2}{4N\sigma^2}\Big). \quad (10)$$

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

$$P(\mathbf{s} \to \mathbf{c}|h_D) \leq \exp\Big(-\frac{P_t \beta_x^2 h_D^2 |\sum_{n=1}^{N} \theta_n(s_n - c_n)|^2}{4N\sigma^2}\Big), \quad (11)$$

where $h_D^2 = \sum_{n=1}^{N} |h_n|^2$. Let $h_n = h_{Rn} + jh_{In}$, $n \in [1, N]$. Since the channels are independent and $h_n \sim CN(0, \sigma_h^2)$, then $\frac{2}{\sigma_h^2} h_D^2 \sim \chi^2(2N)$. The probability density function (pdf) of h_D^2 is $f(\chi) = \frac{1}{(\sigma_h^2)^N \Gamma(N)} \chi^{N-1} \exp(-\frac{\chi}{\sigma_h^2}), \chi > 0$ with $\chi = h_D^2$ and $\Gamma(N) = (N-1)!$. Thus, the average PEP is bounded by

$$\begin{aligned} P(\mathbf{s} \to \mathbf{c}) &\leq \mathrm{E}_\chi \exp\Big(-\frac{P_t \beta_x^2 \chi |\sum_{n=1}^{N} \theta_n(s_n - c_n)|^2}{4N\sigma^2}\Big) \\ &= \Big(1 + \frac{\sigma_h^2 \beta_x^2 P_t |\sum_{n=1}^{N} \theta_n(s_n - c_n)|^2}{4N\sigma^2}\Big)^{-N}, \end{aligned} \quad (12)$$

where the equation is derived according to [16, pp.377, 3.351]. When $|\sum_{n=1}^{N} \theta_n(s_n - c_n)| \neq 0$, and the 1 in (12) can be ignored for high SNR, the PEP bound becomes

$$P(\mathbf{s} \to \mathbf{c}) \leq \Big(\frac{4N}{\sigma_h^2 \beta_x^2 |\sum_{n=1}^{N} \theta_n(s_n - c_n)|^2}\Big)^N \Big(\frac{P_t}{\sigma^2}\Big)^{-N}, \quad (13)$$

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

$$|\sum_{n=1}^{N} \theta_n(s_n - c_n)| \neq 0, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N, \mathbf{s} \neq \mathbf{c}. \quad (14)$$

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

From (13), we can see that, given β_x, N, signal constellation and channel condition, the PEP depends on the design of the network coding. 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,

$$\arg\max_{\boldsymbol{\theta}} \min_{\mathbf{s} \neq \mathbf{c}, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N} |\sum_{n=1}^{N} \theta_n(s_n - c_n)|. \quad (15)$$

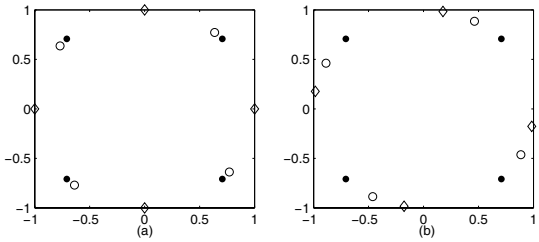


Fig. 3. Constellations with different $\boldsymbol{\theta}$ where • represents the constellation points for U_1, ◦ for U_2 and ⋄ for U_3.

Besides, from the ML detector in (7), D should be able to differentiate the 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 different the better. Take the case in Fig. 3 (a) for example. If $\theta_1 \approx \theta_2$, 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, the received symbols from U_1 can be confused with the received symbols from U_2 with high probability, which results in the failure of detection at D. In fact, we want the difference between any two rotated constellations from two distinct user nodes to be large so that different users' symbols will not be confusing to D. Therefore, as shown in Fig. 3 (b), we assume that the rotation angles are of equal distance for simplicity, and the problem is to find an optimal distance to satisfy the product criterion. Denote the equal distance as $\phi = \phi_{n+1} - \phi_n, \forall n \in [1, N-1]$. The product criterion becomes

$$\arg\max_{\phi} \min_{\mathbf{s} \neq \mathbf{c}, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N} |\sum_{n=1}^{N} e^{j((n-1)\phi + \phi_1)}(s_n - c_n)|. \quad (16)$$

The theoretic optimal solution for (16) of any N and any constellation is intractable. However, because there's only one parameter to be optimized, it is easy to find the optimal angle ϕ by an exhaustive computer search. Define the coding gain as

$$c_g = \min_{\mathbf{s} \neq \mathbf{c}, \forall \mathbf{s}, \mathbf{c} \in \mathcal{A}^N} |\sum_{n=1}^{N} e^{j((n-1)\phi + \phi_1)}(s_n - c_n)|, \quad (17)$$

and the step-length for computer search as $\triangle$. The number of steps for searching is $N_\triangle = 2\pi/\triangle$. Table 1 lists the optimal angles, coding gains and search complexity 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. Therefore, when the influence of coding gain prevails that of diversity order in the SNR region of

TABLE I
ROTATION ANGLES FOR DIFFERENT N AND CONSTELLATIONS

N	constellation	c_g	ϕ	complexity (number of loops)
2	BPSK	2	0.5π	$3^2 N_\triangle$
2	4QAM	1.0353	0.1667π	$9^2 N_\triangle$
2	8QAM	0.8828	0.3583π	$21^2 N_\triangle$
2	16QAM	0.5359	0.1667π	$49^2 N_\triangle$
3	BPSK	1.2361	0.6283π	$3^3 N_\triangle$
3	4QAM	0.6050	0.4033π	$9^3 N_\triangle$
3	8QAM	0.2599	0.1911π	$21^3 N_\triangle$
4	BPSK	1.0353	0.1667π	$3^4 N_\triangle$
4	4QAM	0.2520	0.4192π	$9^4 N_\triangle$

interest, we can divide a dense cluster of user nodes into several subclusters. Please note that, there may be more than one angle that have the same maximum coding gain. In that case, we can choose the one whose transmit constellation has the minimum peak to average power ratio (PAPR), where the transmit constellation includes the rotated constellations of all users. For example, when $N = 2$ and BPSK is used by the user nodes, both $\phi = \frac{\pi}{2}$ and $\frac{\pi}{3}$ have the same maximum coding gain of 2. Apparently, the transmit constellation has smaller PAPR when $\phi = \frac{\pi}{2}$.

C. Power Allocation

In this subsection, we will choose β_x and β_t to satisfy the average power constraint. The ith transmit symbol of U_n's packet in Phase II can be denoted as

$$x_{t,n}(i) = \sqrt{P_t}\frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}x(i). \tag{18}$$

Since the network coding vector is normalized as $\boldsymbol{\theta}\boldsymbol{\theta}^H = 1$, we have $\mathrm{E}[|x(i)|^2] = 1$. The average transmit power is

$$\bar{P}_t = \mathrm{E}\Big(P_t|\frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}|^2\Big), \tag{19}$$

which should not exceed the power constraint P_t. Thus $\mathrm{E}|\frac{\beta_x|h_n|+\beta_t u_n e^{j2\pi t_i}}{h_n}|^2 \le 1$. Because

$$\mathrm{E}|\frac{\beta_x|h_n| + \beta_t u_n e^{j2\pi t_i}}{h_n}|^2 \le \mathrm{E}\Big(\beta_x + \frac{\beta_t}{|h_n|}\Big)^2, \tag{20}$$

we can approximate the power constraint by setting $\mathrm{E}\Big(\beta_x + \frac{\beta_t}{|h_n|}\Big)^2 = 1$. Let $u = 1/|h_n|$ and $v = 1/|h_n|^2$, the pdf of u and v can be derived as $f_u(u) = \frac{2}{\sigma_h^2}u^{-3}e^{-\frac{1}{\sigma_h^2 u^2}}$ and $f_v(v) = \frac{1}{\sigma_h^2}v^{-2}e^{-\frac{1}{\sigma_h^2 v}}$, respectively. Therefore, $\mathrm{E}(\frac{1}{|h_n|}) = \sqrt{\frac{\pi}{\sigma_h^2}}$, and $\mathrm{E}(\frac{1}{|h_n|^2})$ is

$$\mathrm{E}(\frac{1}{|h_n|^2}) = \frac{1}{\sigma_h^2}\int_0^\infty \frac{1}{v}e^{-\frac{v}{\sigma_h^2}}dv \approx 3.3182/\sigma_h^2. \tag{21}$$

The approximation in (21) is obtained by using Laguerre integral formula [17, pp.923]. Then the power constraint becomes

$$\beta_x^2 + \frac{3.3182\beta_t^2}{\sigma_h^2} + 2\sqrt{\frac{\pi}{\sigma_h^2}}\beta_x\beta_t = 1. \tag{22}$$

Subject to the average power constraint, β_x and β_t can be chosen according to (22) to satisfy some desired performance-security requirement.

IV. SECURE REGION AGAINST EAVESDROPPERS

In the previous section, AE-STNC scheme is proposed to secure the transmission in Phase II. In Phase I, we assume that E can not hear the transmission due to attenuation. One question may be asked is how far is far enough to prevent E from eavesdropping? In this section, the secure region is discussed according to the requirements of performance and security.

Since the user nodes do not want E to get the transmit information, assume that the tolerable SER of E for the cooperative network is $P_{E,th}$. A secure region is defined as an area in which the SER of E is worse than $P_{E,th}$. Denote the transmit power in Phase I as P_I. Since the nodes in the cluster are very close to each other compared with their distance to D, P_I is only a small part of P_t. The average received SNR at U_n from U_m, $\forall n, m \in [1, N], m \ne n$, is $\rho_{mn} = \sigma_{mn}^2 P_I/\sigma^2$, where $\sigma_{mn}^2 = \kappa d_{mn}^{-\alpha}$. Assume that U_m and U_n are the farthest nodes in the cluster, then $d_{mn} = 2d$, and the received SNR at U_n is $\rho_{mn} = \kappa(2d)^{-\alpha}P_I/\sigma^2$. The average received SNR at E is $\rho_E = \sigma_g^2 P_I/\sigma^2$, where $\sigma_g^2 = \kappa d_E^{-\alpha}$.

After averaging with respect to Rayleigh fading channels, the average SER for M-QAM modulation can be expressed as [18, pp.199] $P_S = F_2\Big(1 + \frac{b_2\rho}{sin^2\theta}\Big)$, where ρ is the average received SNR, $b_2 = \frac{3}{2(M-1)}$ and $F_2(\cdot)$ is defined as

$$F_2(x(\theta)) = \frac{4K}{\pi}\int_0^{\frac{\pi}{2}}\frac{1}{x(\theta)}d\theta - \frac{4K^2}{\pi}\int_0^{\frac{\pi}{4}}\frac{1}{x(\theta)}d\theta, \tag{23}$$

with $K = 1 - 1/\sqrt{M}$. By applying symbolic integration, the average SER can be derived as a function of the average received SNR, i.e., $P_S = f(\rho)$, where

$$\begin{aligned} f(\rho) = &-2K\Big(\sqrt{\frac{b_2\rho}{1+b_2\rho}} - 1\Big) \\ &+ \frac{K^2}{\pi}\Big(4\sqrt{\frac{b_2\rho}{1+b_2\rho}}\arctan\sqrt{\frac{1+b_2\rho}{b_2\rho}} - \pi\Big) \end{aligned} \tag{24}$$

Denote $f^{-1}(\cdot)$ as the inverse function of $f(\cdot)$, the required SNR for a certain SER can be written as $\rho = f^{-1}(P_S)$. $f(\cdot)$ and $f^{-1}(\cdot)$ are decreasing on their own domains. Assume that the SER requirements of the user nodes in Phase I is $P_{U,th}$. U_n is the farthest node in the cluster to U_m, the transmit power P_I should be adjusted such that the received SNR at U_n from U_m satisfies $\rho_{mn} \ge f^{-1}(P_{U,th})$. On the other hand, due to the security requirement, the SER of the eavesdropped signals at E should be worse than $P_{E,th}$. Thus

TABLE II
NORMALIZED SECURE RADIUS γ_s FOR DIFFERENT SER REQUIREMENTS WITH BPSK MODULATION

	$P_{U,th}=10^{-3}$	$P_{U,th}=10^{-4}$	$P_{U,th}=10^{-5}$	$P_{U,th}=10^{-6}$
$P_{E,th}=0.1$	10.32	22	48	103.2
$P_{E,th}=0.4$	35	75.4	162.6	350.4

the received SNR at E should be $\rho_E \leq f^{-1}(P_{E,th})$, and $\frac{\rho_E}{\rho_{mn}} \leq \frac{f^{-1}(P_{E,th})}{f^{-1}(P_{U,th})}$. The distance from E to the cluster when E's SER is worse than $P_{E,th}$ is $d_E \geq 2d\left(\frac{f^{-1}(P_{U,th})}{f^{-1}(P_{E,th})}\right)^{\frac{1}{\alpha}}$. Define $\gamma_s = 2\left(\frac{f^{-1}(P_{U,th})}{f^{-1}(P_{E,th})}\right)^{\frac{1}{\alpha}}$ as normalized secure radius, then for any eavesdropper whose distance from the cluster is larger than $\gamma_s d$ is in the secure region. The analysis for M-PSK is similar and is omitted here. Table II gives the normalized secure radius for different requirements of security and performance when BPSK is used in the network. From Table I we can see that, for a fixed performance requirement, a higher desired security results in a smaller security region, which means larger γ_s. For a fixed security requirement, better performance at D requires larger γ_s to guarantee security. The proposed AE-STNC scheme can provide secure transmission to D in Phase II regardless of the eavesdroppers' location, while the security in Phase I is achieved as long as the eavesdroppers are in the secure region.

V. ANTI-EAVESDROPPING CODING OVER FREQUENCY-SELECTIVE CHANNELS

For broadband cooperative communications, orthogonal frequency-division multiplexing (OFDM) is adopted at each user node to overcome the intersymbol interference caused by multipath propagation. Each user node employs an OFDM modulator with N_c subcarriers. TDMA is used in Phase I and Phase II to overcome the issue of imperfect synchronization. In this section, we extend the proposed AE-STNC scheme and propose an anti-eavesdropping space-time-frequency coding (AE-STFNC) scheme for broadband cooperative communications by using the idea of mapping in [19].

Assume the channel between any two nodes in the network is independent. Denote the number of multipaths between the user nodes and D as L_1 and the number of multipaths between the user nodes and E as L_2. The channel frequency response from U_n to D is $H_n(q)=\sum_{l=0}^{L_1-1} h_n(l)e^{-j\frac{2\pi q \tau_{h,n}(l)}{T}}$, where $q \in [0, N_c-1]$ is the subcarrier index, $h_n(l)$ and $\tau_{h,n}(l)$ are the complex amplitude and delay of the lth path, respectively, and T is the OFDM symbol period. The channel taps $h_n(l)$ are assumed to be independent for different indices $l \in [1, L_1]$, and the delays are rounded to the nearest sampling position. The channel frequency response from U_n to E is $G_n(q)=\sum_{l=0}^{L_2-1} g_n(l)e^{-j\frac{2\pi q \tau_{g,n}(l)}{T}}$, where $g_n(l)$ and $\tau_{g,n}(l)$ are the complex amplitude and delay of the lth path, respectively. The channel coefficients $h_n(l)$ and $g_n(l)$ are modeled as independent zero-mean complex Gaussian variables with variances $\mathrm{E}|h_n(l)|^2=\eta_{n,l}^2$ and $\mathrm{E}|g_n(l)|^2=\varepsilon_{n,l}^2$, respectively. The total power of the multipath channels are $\sum_{l=0}^{L_1-1}\eta_{n,l}^2=\sigma_h^2$ and $\sum_{l=0}^{L_2-1}\varepsilon_{n,l}^2=\sigma_g^2$ with $n \in [1, N]$.

As in the narrowband scenario, the training signals are transmitted by D at the beginning of each channel coherence time. Each user node obtains the CSI between itself and D due to channel reciprocity, while E cannot get any useful information by these training symbols. Assume that the user nodes have decoded the transmit information in Phase I. In Phase II, each user node generates new symbols from the information symbols and N_f OFDM symbols construct a new packet, which is transmitted in its allocated time slot. The transmission for broadband asynchronous cooperative communications is given in Fig. 4. The subcarriers of each OFDM block are divided into P groups, and each group has Γ symbols, where $1 \leq \Gamma \leq L_1$ and $P=\lfloor \frac{N_c}{\Gamma} \rfloor$, i.e., the largest integer not greater than $\frac{N_c}{\Gamma}$. If N_c is not an integer multiple of Γ, $N_c - P\Gamma$ zeros are added at the end of each OFDM symbol. The integer Γ is adjustable for different desirable diversities. The pth group of the n_sth OFDM symbol at U_n is

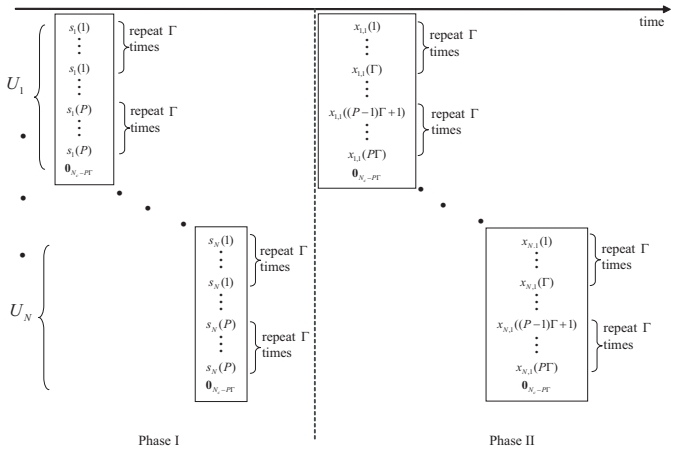


Fig. 4. cooperative transmission model for broadband asynchronous cooperative communications with $n_s = 1$ as an example.

$$\mathbf{x}_{n,n_s,p} = \mathbf{w}_{n,n_s,p} x_{n_s,p}, \tag{25}$$

where $p \in [1, P]$ and $n_s \in [1, N_f]$, $\mathbf{x}_{n,n_s,p} = [x_{n,n_s}((p-1)\Gamma+1), x_{n,n_s}((p-1)\Gamma+2), \cdots, x_{n,n_s}(p\Gamma)]^{\mathrm{T}}$ is the pth group of symbols to be transmitted, $\mathbf{w}_{n,n_s,p} = [w_{n,n_s,p}(1), w_{n,n_s,p}(2), \cdots, w_{n,n_s,p}(\Gamma)]^{\mathrm{T}}$ is the anti-eavesdropping encoding vector to randomize the received signal at E, and $x_{n_s,p} = \boldsymbol{\theta}\mathbf{s}_{n_s,p}$ with $\mathbf{s}_{n_s,p} = [s_1((n_s-1)P+p), s_2((n_s-1)P+p), ..., s_N((n_s-1)P+p)]^{\mathrm{T}}$ being the $(n_s-1)P+p$ th information symbols of the N users and $\boldsymbol{\theta}$ being the complex network coding vector introduced in Section III. Assume that the information symbol $s_n((n_s-1)P+p)$ is from normalized M-QAM (or M-PSK) constellation $\mathcal{A}$, and the bits in $s_n((n_s-1)P+p)$ is $\mathbf{b}_{n,n_s,p} = [b_{n,n_s,p}(1), b_{n,n_s,p}(2), \cdots, b_{n,n_s,p}(log_2 M)]$. Then the available information bits at the user nodes after Phase I can be written as $\mathbf{b}_{n_s,p} = [b_{1,n_s,p}(1), \cdots, b_{N,n_s,p}(1), b_{1,n_s,p}(2), \cdots, b_{N,n_s,p}(log_2 M)]$.

The n_sth OFDM symbol for U_n can then be written as

$$\mathbf{x}_{n,n_s} = [\mathbf{x}^{\mathrm{T}}_{n,n_s,1}, \cdots, \mathbf{x}^{\mathrm{T}}_{n,n_s,p}, \cdots, \mathbf{x}^{\mathrm{T}}_{n,n_s,P}, \mathbf{0}], \tag{26}$$

where $\mathbf{0}$ is an all zero matrix of size $1 \times (N_c - P\Gamma)$. When power-delay profile is known at the transmitter, the symbols in one OFDM block can be interleaved for better performance. The pth group of the OFDM block is analyzed as follows, and the analysis for other groups is similar.

After the transmission in Phase II, the pth group of the n_sth OFDM symbol from U_n received at D and E respectively are

$$\begin{aligned} \mathbf{y}_{n,n_s,p} &= \sqrt{P_t}\mathbf{H}_{n,p} \circ \mathbf{x}_{n,n_s,p} + \mathbf{z}_{n,n_s,p} \\ \mathbf{r}_{n,n_s,p} &= \sqrt{P_t}\mathbf{G}_{n,p} \circ \mathbf{x}_{n,n_s,p} + \mathbf{v}_{n,n_s,p}, \end{aligned} \tag{27}$$

where $\mathbf{H}_{n,p} = [H_n((p-1)\Gamma+1), \cdots, H_n((p-1)\Gamma+\gamma), \cdots, H_n((p-1)\Gamma+\Gamma)]^{\mathrm{T}}$ and $\mathbf{G}_{n,p} = [G_n((p-1)\Gamma+1), \cdots, G_n((p-1)\Gamma+\gamma), \cdots, G_n((p-1)\Gamma+\Gamma)]^{\mathrm{T}}$ are the pth group of channel frequency responses from U_n to D and E, respectively. $\mathbf{z}_{n,n_s,p} = [z_{n,n_s}((p-1)\Gamma+1), \cdots, z_{n,n_s}((p-1)\Gamma+\Gamma)]^{\mathrm{T}}$ and $\mathbf{v}_{n,n_s,p} = [v_{n,n_s}((p-1)\Gamma+1), \cdots, v_{n,n_s}((p-1)\Gamma+\Gamma)]^{\mathrm{T}}$ are the received AWGN of the pth group at D and E from U_n, respectively. Summing up the signals in the pth groups from the N users, D and E can get

$$\begin{aligned} y_{n_s,p} &= \sqrt{P_t}\sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} H_n((p-1)\Gamma+\gamma)w_{n,n_s,p}(\gamma)x_{n_s,p} + z_{n_s,p} \\ r_{n_s,p} &= \sqrt{P_t}\sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} G_n((p-1)\Gamma+\gamma)w_{n,n_s,p}(\gamma)x_{n_s,p} + v_{n_s,p}, \end{aligned} \tag{28}$$

where $z_{n_s,p} = \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} z_{n,n_s}((p-1)\Gamma+\gamma)$ and $v_{n_s,p} = \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} v_{n,n_s}((p-1)\Gamma+\gamma)$. Let $H_{n_s,p} = \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} H_n((p-1)\Gamma+\gamma)w_{n,n_s,p}(\gamma)$ and $G_{n_s,p} = \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} G_n((p-1)\Gamma+\gamma)w_{n,n_s,p}(\gamma)$ be the equivalent channels at D and E, respectively. During the channel coherence time, we want the equivalent channel at D to be a deterministic constant, while the channels at E change randomly from one transmitted OFDM symbol to another. Assume that no additional information is shared beforehand among the user nodes and D. Using the same idea of randomization in Section III A, the anti-eavesdropping encoding coefficient at U_n is designed by exploiting its local CSI and transmitted information bits as follows

$$w_{n,n_s,p}(\gamma) = \frac{\beta_x|H_n((p-1)\Gamma+\gamma)| + \beta_t u_n e^{j2\pi t_{n_s,p}}}{H_n((p-1)\Gamma+\gamma)}, \tag{29}$$

where u_n is defined in Section III A, and

$$t_{n_s,p} = \sum_{m=1}^{Nlog_2M} 2^{-m}\mathbf{b}_{n_s,p}(m), \tag{30}$$

which changes randomly to D and E since the transmitted information bits change randomly from the perspective of D and E. Substituting (29) and (30) into (28), the equivalent channels become

$$\begin{aligned} H_{n_s,p} =& \beta_x \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} |H_n((p-1)\Gamma+\gamma)| \\ G_{n_s,p} =& \beta_x \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} \frac{G_n((p-1)\Gamma+\gamma)|H_n((p-1)\Gamma+\gamma)|}{H_n((p-1)\Gamma+\gamma)} \\ &+ \beta_t e^{j2\pi t_{n_s,p}} \sum_{n=1}^{N}\sum_{\gamma=1}^{\Gamma} \frac{G_n((p-1)\Gamma+\gamma)u_n}{H_n((p-1)\Gamma+\gamma)}. \end{aligned} \tag{31}$$

Therefore, the equivalent channel $H_{n_s,p}$ for D is constant during the channel coherence time. Due to the change of $t_{n_s,p}$, the equivalent channel $G_{n_s,p}$ for E changes randomly from one OFDM symbol to another. Then (28) becomes

$$\begin{aligned} y_{n_s,p} &= \sqrt{P_t}H_{n_s,p}x_{n_s,p} + z_{n_s,p} \\ r_{n_s,p} &= \sqrt{P_t}G_{n_s,p}x_{n_s,p} + v_{n_s,p}. \end{aligned} \tag{32}$$

D can estimate $\sqrt{P_t}H_{n_s,p}$ from the received information signals as $\frac{\sum_{i=1}^{L}|y_{i,p}|}{L\overline{|x|}}$, where L is the number of received OFDM symbols used for estmiation, and $\overline{|x|}$ represents the average amplitude of the combined symbol $x_{n_s,p}$. $\overline{|x|}$ can be estimated as long as the signal constellation is given. The detector at D for $\mathbf{s}_{n_s,p}$ can be written as

$$\hat{\mathbf{s}}(n_s,p) = \arg\min_{\mathbf{s}\in\mathcal{A}^N} |y_{n_s,p} - \sqrt{P_t}H_{n_s,p}\boldsymbol{\theta}\mathbf{s}|^2, \tag{33}$$

where $\mathbf{s} = [s_1, \cdots, s_n, \cdots, s_N]^{\mathrm{T}}$ with $s_n \in \mathcal{A}$.

Since $h_n(l)$ for $l \in [0, L_1-1]$ are independent zero-mean complex Gaussian variables with variances $\mathrm{E}|h_n(l)|^2 = \eta^2_{n,l}$ and $\sum_{l=0}^{L_1-1}\eta^2_{n,l} = \sigma^2_h$, $H_n(q) = \sum_{l=0}^{L_1-1} h_n(l)e^{-j\frac{2\pi q\tau_n(l)}{T}}$ is complex Gaussian variable with zero-mean and variance σ^2_h. The $(p-1)\Gamma+\gamma$th signal transmitted from U_n is

$$x_{n,n_s}((p-1)\Gamma+\gamma) = \sqrt{P_t}w_{n,n_s,p}(\gamma)x_{n_s,p}, \tag{34}$$

and the average transmit power is

$$\bar{P}_t = P_t\mathrm{E}|\frac{\beta_x|H_n((p-1)\Gamma+\gamma)| + \beta_t u_n e^{j2\pi t_{n_s,p}}}{H_n((p-1)\Gamma+\gamma)}|^2 \tag{35}$$

Subject to the average power constraint P_t, the power allocation can be decided by a similar processing in Section III C, and $\{\beta_x, \beta_t\}$ can be chosen based on the same constraint in (22).

VI. Simulation Results

In this section, we show some simulation results of the proposed schemes for asynchronous cooperative networks with multiple eavesdroppers. Since the construction of the anti-eavesdropping encoding is independent with the eavesdroppers, and the eavesdroppers can not collude, similar performance can be obtained at the eavesdroppers. In the simulations, clusters of 2 and 3 user nodes are adopted, and one of the eavesdroppers E is considered. 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 $\frac{1}{\sqrt{N}}e^{j(n-1)\phi}$. Unless specified otherwise, $\beta_x = 0.9$ is used throughout, the channel variances are $\sigma^2_h = 1$ and

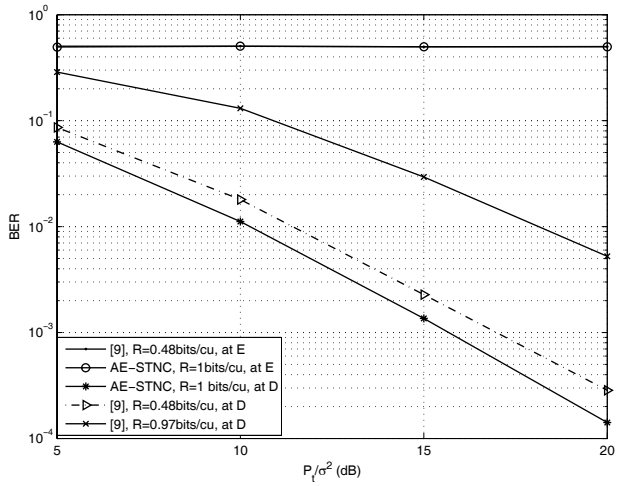


Fig. 5. BER performance of the AE-STNC scheme and the scheme in [9] with $N = 2$.

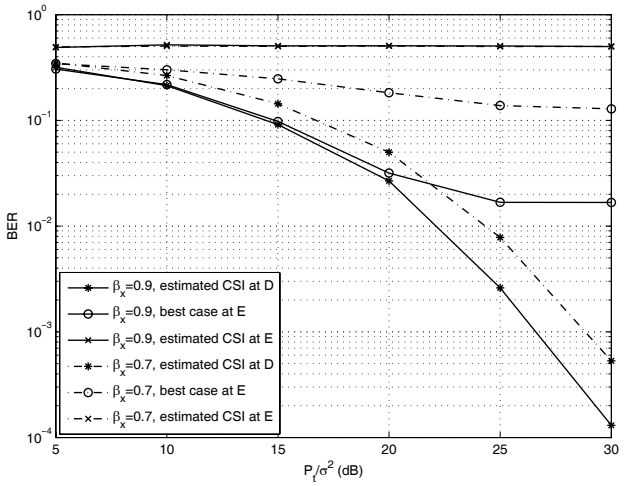


Fig. 7. BER performance of AE-STNC for different power ratios with $N = 3$.

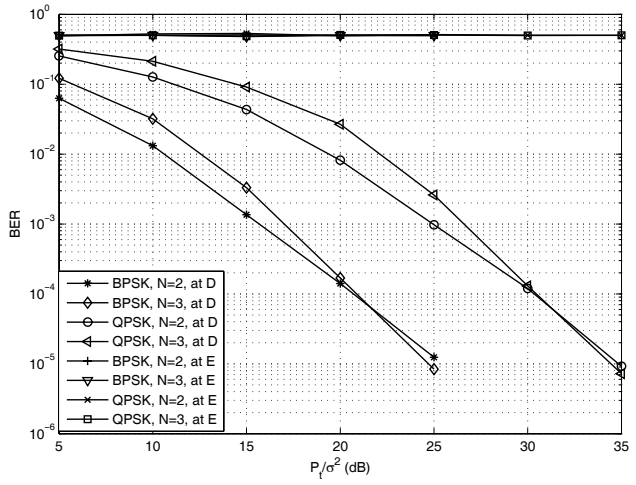


Fig. 6. BER performance of AE-STNC for different modulations with $N = 2, 3$.

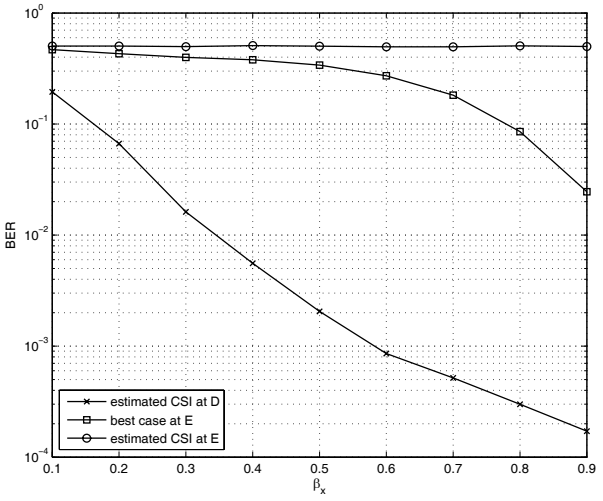


Fig. 8. Performance-security tradeoff for different choices of $\{\beta_x, \beta_t\}$.

$\sigma_g^2 = 1$, and E estimates the CSI based on received signals as D does.

In Fig. 5, we compare the proposed scheme with the differentially encoded OFDM scheme with LPI in [9]. $N = 2$ is adopted. Cyclic group codes $G_{2,4} = (2, 4, [1, 1])$ and $G_{2,16} = (2, 16, [1, 7])$ are used for the scheme in [9]. The transmission rates in Phase II for the scheme in [9] with $G_{2,4}$ and $G_{2,16}$ are 0.48 bits/channel use (cu) and 0.97 bits/cu, respectively. BPSK is used in our proposed scheme, and the transmission rate in Phase II is 1 bits/cu. It can be seen from Fig. 5 that, the BER of E is always around 0.5 for both schemes, which means E can not do better than guessing. However, the BER performance of the scheme in [9] is worse than that of the AE-STNC scheme, even when the rate of [9] 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 AE-STNC scheme.

The BER performances with different modulations for $N = 2$ and 3 are compared in Fig. 6. From the curves we can see that full diversity is always achieved when SNR is high enough. It can be seen from Fig. 6 that, for a fixed N, higher modulation results in worse BER performance due to smaller coding gain. 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 AE-STNC of small size. We can also observe from Fig. 6 that the BER at E is always around 0.5 for different N and modulations. That means E can not intercept the transmitted information.

Fig. 7 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 by using the received signals as D does, the BER for E is always around 0.5, which means

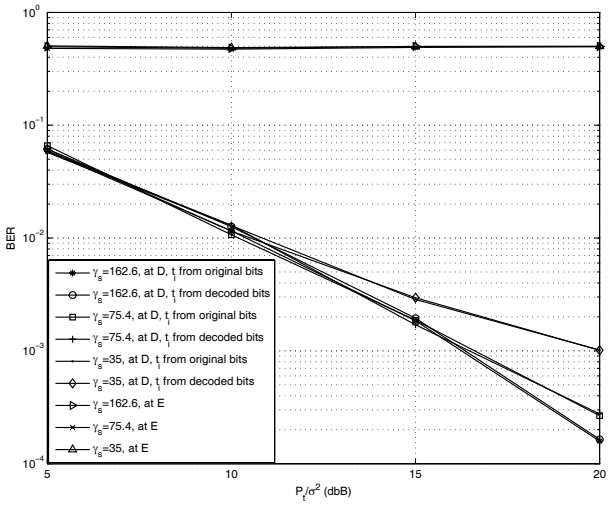


Fig. 9. The influence of decoding errors at the user nodes and BER performance of the AE-STNC scheme for different secure radius.

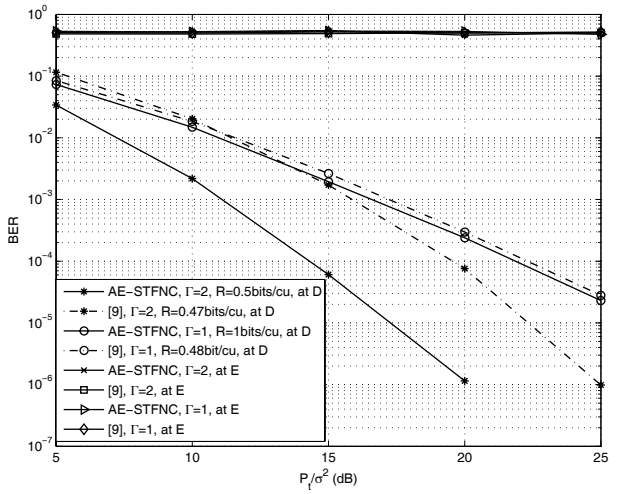


Fig. 10. BER performance for the AE-STFNC scheme and the scheme in [9] with $N = 2$.

E can not get the transmitted information even most of the power is used for signal transmission. When the best case for E is considered, which assumes E can blindly estimate the deterministic part of $g_{n,i}, \forall n \in [1, N]$, without estimation error, the BER at E is also given in Fig. 7 as a lower bound of E's BER performance. The decoding of the information signals at E is affected by the random interference, and error floor occurs as SNR increases. For the best case of E, error floor appears when SNR increases to $25dB$. When $\beta_x = 0.9$, the interference power is quite low, and the BER at E arrives at a floor around 2×10^{-2}. Higher error floor at E can be generated by decreasing β_x. It can be seen from Fig. 7 that the error floor at E is above 0.1 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. For the worst case of the cooperative system when E can blindly estimate the deterministic parts of its channels during the channel coherence time, the choice of $\{\beta_x, \beta_t\}$ is a tradeoff between performance and security in terms of LPI.

The tradeoff of $\{\beta_x, \beta_t\}$ is shown in Fig. 8. For a cooperative network of $N = 3$ user nodes using 4QAM, the BER performances for D and E are illustrated in Fig. 8 for $P_t/\sigma^2 = 30$dB when β_x changes from 0.1 to 0.9. First we can see that when E estimates the channels using the same channel estimation as D, the BER at E is always around 0.5. That means E can not intercept any information regardless of power allocation. When the best case for E is considered, the BER curves show the tradeoff between performance and security. As β_x increases, the BER performance at D gets better, while the probability for E to correctly decode a bit increases. Based on desired security or performance requirement, $\{\beta_x, \beta_t\}$ can be chosen.

Fig. 9 first shows the influence of decoding errors at the user nodes on the BER performance at D. BPSK is used in the simulation. There are 2 users in the cluster and the path loss exponent is $\alpha = 3$. The distance between D and the cluster is normalized as $d_D = 1$, and the distance between the user nodes is assumed to be $2d = d_D/100$. E is randomly located in the secure region and its distance from the cluster is uniformly distributed between $\gamma_s d$ and d_D. The transmit SNR in Phase I is less than -20dB. From Fig. 9 we can see that, when t_i is generated from the original information bits and from the decoded bits by the users, the performance curves are almost the same. That means the remaining randomness in (6) caused by the decoding errors at the user nodes does not cause performance degradation. This is because the user nodes are in the same cluster and close to each other, they can decode each other's information with high probability. Second, when the security requirement in Phase I is $P_{E,th} = 0.4$, the BER performance at D for different secure radius γ_s is shown in Fig. 9. The smaller γ_s is, the larger the security region is. According to Table II, for a fixed $P_{E,th}$, as γ_s decreases from 162.6 to 35, the SER at the users in Phase I increases. We can see from Fig. 9 that, when E is in the secure region, the BER performance at E is around 0.5 by combining its received signals in Phase I and Phase II. Thus E can not intercept the transmitted information. By decreasing P_I, the performance of the cooperative communication degrades, and the secure region can be extended. When γ_s decreases from 162.6 to 35, the eavesdropper becomes close to the cluster. The transmit power in Phase I is decreased to satisfy the security requirement, and the decoding errors at the users in Phase I increase. The increasing decoding errors in Phase I result in worse performance at D in Phase II, and this performance degradation can be seen from Fig. 9.

Fig. 10 shows the BER performance of the AE-STFNC scheme. In the simulation, $N_c = 128$ and the total bandwidth is 1 MHz. A simple two-ray equal power delay profile ($L_1 = L_2 = 2$) with a delay of $\tau = 20\mu s$ between the two rays as in [9] is considered. Assume that the cluster has $N = 2$ user nodes. For the scheme proposed in [9], $\Gamma = 2$ and $G_{4,16} = (4, 16, [1, 3, 5, 7])$ is used. Therefore, the transmission rate in Phase II is 0.47 bits/cu. To compare with the same diversity and a similar rate, BPSK is used in the proposed scheme and the rate in Phase II is 0.5 bits/cu when $\Gamma = 2$. From the curves, we verify that a full diversity order of $N\Gamma$ is

achieved by the proposed AE-STFNC scheme. Moreover, the BER performance of the proposed scheme is much better than that of the scheme in [9] under the same diversity and similar transmission rate. When $\Gamma = 1$ is used for both schemes, $G_{2,4}$ is used for the scheme in [9] and the transmission rate in Phase II is 0.48 bits/cu. In this case, the proposed scheme with BPSK outperforms the scheme in [9] slightly but achieves double transmission rate. We can see from the figure that the BER performances of the eavesdropper are both around 0.5 for the AE-STFNC scheme and the scheme in [9].

VII. Conclusion

In this paper, PHY layer secure transmission schemes for asynchronous cooperative communication networks with passive eavesdroppers over frequency-flat and frequency-selective channels are proposed. By utilizing local information at separated user nodes, AE-STNC is first proposed to prevent eavesdropping and achieve full diversity without sacrificing transmission efficiency. Without requiring any information about the eavesdroppers, the proposed scheme randomizes the received signals at the eavesdroppers, so that they can not intercept the transmitted information even when they have better channel quality. By extending the AE-STNC scheme to frequency-selective channels, AE-STFNC, which prevents eavesdropping and provides flexible diversity, is proposed for broadband asynchronous cooperative communications. Simulation results validate our analysis. Compared with the secure scheme proposed in [9], the proposed schemes can achieve better performance while generating LPI. Secure region is investigated according to different requirements of security and performance in Phase I. The secure transmission in Phase I regardless of the eavesdroppers' locations is an interesting problem but left for future work.

References

[1] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Comput.*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[2] Y. Sun, W. Trappe, and K. J. R. Liu, *Network-Aware Security for Group Communications*. Springer, 2007.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technical J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] I. Csiszar and J. Korner, "Broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 451–456, July 1978.

[5] Y. Li and X. G. Xia, "A family of distributed space-time trellis codes with asynchronous cooperative diversity," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 790–800, Apr. 2007.

[6] L. Dong, A. P. Petropulu, and H. V. Poor, "Amplify and forward based cooperation for secure wireless communications," in *Proc. IEEE ICASSP*, May 2009, pp. 2613–2616.

[7] L. Dong, H. Zhu, A. P. Petropulu, and H. V. Poor, "Secure wireless communication via cooperation," in *Proc. 46th Annual Allerton Conf. Commun. Control, Comput.*, 2008.

[8] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[9] Z. Li and X. G. Xia, "A distributed differential encoded OFDM scheme for asynchronous cooperative systems with low probability of interception," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3372–3379, July 2009.

[10] H. Q. Lai and K. J. R. Liu, "Space-time network coding," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1706–1718, 2011.

[11] A. K. Sadek, W. Su, and K. J. R. Liu, "Multinode cooperative communications in wireless networks," *IEEE Trans. Signal Process.*, vol. 55, no. 1, pp. 341–355, Jan. 2007.

[12] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *J. Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[13] M. Damen, A. Chkeif, and J. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.

[14] Z. Safar, W. Su, and K. J. R. Liu, "A fast sphere decoding algorithm for space-frequency block codes," *EURASIP J. Appl. Signal Process.*, vol. 2006, pp. 1–14, AID 97676, 2006.

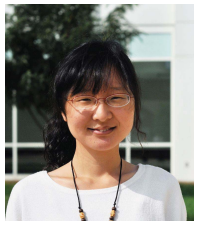
[15] H. Jafarkhani, *Space-Time Coding: Theory and Practice*. Cambridge University Press, 2005.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integral, Series, and Products*, 5th edition. Academic Press, 1994.

[17] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. National Bureau of Standards, Applied Mathematics Series, 1964.

[18] K. J. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative Communications and Networking*. Cambridge University Press, 2008.

[19] W. Su, Z. Safar, M. Olfat, and K. J. R. Liu, "Obtaining full-diversity space-frequency codes from space-time codes via mapping," *IEEE Trans. Signal Process.*, vol. 51, no. 11, pp. 2905–2916, Nov. 2003.



Zhenzhen Gao (S'10) received the B.S. in Communication Engineering in 2005 from Lanzhou University, Lanzhou, China. Now she is a Ph.D. student in the Department of Information and Communication Engineering, Xi'an Jiaotong University, Xi'an, China. She received a scholarship from China Scholarship Council (CSC) in 2009. From September 2009 to August 2011, she was a visiting student in the Department of Electrical and Computer Engineering at the University of Maryland, College Park, MD, USA. Her current research interests are in the areas of wireless communications and networks, including cooperative communications, space-time coding and network coding.

Y u-Han Yang (S'06) received his B.S. in electrical engineering in 2004, and two M.S. degrees in computer science and communication engineering in 2007, from National Taiwan University, Taipei, Taiwan. He is currently pursuing the Ph.D. degree at the University of Maryland, College Park. His research interests include wireless communication and signal processing. He received Class A Scholarship from National Taiwan University in Fall 2005 and Spring 2006. He is a recipient of Study Abroad Scholarship from Taiwan (R.O.C.) Government in 2009 and 2010.

K. J. Ray Liu (F'03) is named a Distinguished Scholar-Teacher of University of Maryland, College Park, in 2007, where he is Christine Kim Eminent Professor of Information Technology. He serves as Associate Chair of Graduate Studies and Research of Electrical and Computer Engineering Department and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of wireless communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering.

Dr. Liu is the recipient of numerous honors and awards including IEEE Signal Processing Society Technical Achievement Award and Distinguished Lecturer. He also received various teaching and research recognitions from University of Maryland including university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. An ISI Highly Cited Author in Computer Science, Dr. Liu is a Fellow of IEEE and AAAS.

Dr. Liu is President-Elect and was Vice President - Publications of IEEE Signal Processing Society. He was the Editor-in-Chief of *IEEE Signal Processing Magazine* and the founding Editor-in-Chief of *EURASIP Journal on Advances in Signal Processing*.