On the Application of Cooperative Transmission to Secrecy Communications

Zhiguo Ding, *Member, IEEE*, Kin K. Leung, *Fellow, IEEE*, Dennis L. Goeckel, *Fellow, IEEE*, and Don Towsley, *Fellow, IEEE*

***Abstract*—Information theoretic security has recently emerged as an effective physical layer approach to provide secure communications. The outage performance of such a secrecy communication system is considered in this paper, since it is an important criterion to measure whether users' predefined quality of service can be met. Provided that the legitimate receiver and eavesdropper have the same noise power, many existing secure schemes cannot achieve outage probability approaching zero, regardless of how large the transmission power is. By introducing cooperative transmission into secrecy communication systems, it will be shown here that outage probability approaching zero can be achieved. In particular, scenarios with single-antenna nodes and multiple-antenna nodes will both be addressed, and the optimal design of beamforming/precoding will be investigated. Explicit expressions of the achievable outage probability and diversity-multiplexing tradeoff will be developed to demonstrate the performance of the proposed cooperative secure transmission schemes, and numerical results are presented.**

***Index Terms*—Secrecy communications, optimization, cooperative diversity, beamforming and precoding**

I. Introduction

THE DYNAMIC nature of wireless channels due to the node mobility and multipath fading has offered opportunities which can be utilized by the legitimate transceiver to realize perfect secrecy communications without relying on traditional encryption techniques [1]. To keep the source messages from being intercepted by eavesdroppers, the secrecy capacity is typically much smaller than the Shannon capacity of the scenarios without eavesdroppers, and this motivates the use of multiple antennas for secrecy communications [2]–[5], where the focus of these works is the secrecy rates. Furthermore, the impact of cooperation on secrecy capacity has been studied in [6], [7] and a new way to use un-trusted relays, so called cooperative jamming, has been proposed in [8]. In general, the achievable secrecy capacity, such as the ones developed in [1], [2], [6], assume that the channel state information (CSI) is available at the transmitter, and the impact of different CSI assumptions on the secrecy capacity has been studied in [9].

A general principle for secrecy communications is that the source will transmit only if the legitimate receiver has a better channel condition than the eavesdropper; otherwise, it will keep silent. Obviously such an opportunistic transmission strategy cannot meet the users' predefined quality of service, and our focus in this paper is to study the outage performance of secrecy communications, which is defined as the probability that a targeted data rate cannot achieved. The design of secrecy transmission to satisfy users' predefined quality of service has been studied in [2], [10], but the impact of eavesdropping on the diversity and multiplexing gains is still not clear. The aim of this paper is to introduce cooperative diversity into secrecy communications and realize outage probability approaching zero given sufficiently large transmission power. Different to existing works, we specifically focus on the outage performance of secrecy transmissions for scenarios with and without multiple antennas. The design of beamforming and precoding has been studied, where their impact on reliability and throughput has been analyzed by using the diversity-multiplexing tradeoff.

Specifically we first focus on the secrecy communication scenario where all nodes are equipped with a single antenna. It is shown that a straightforward application of classical cooperative protocols in [11] cannot realize zero-approaching outage probability. Then we propose a simple cooperative secure transmission strategy, where the source only communicates with relays at the first stage and distributed beamforming is then adopted by asking the source and relays to act together. Dependent on the tolerable system overhead, there are two choice to use the available relays: one to use all available relays and the other to only use the best one. In the second part of the paper, the multiple-input multiple-output (MIMO) cooperative scheme is studied in the context of secrecy communications, whose motivation is to further increase secrecy capacity and improve reception reliability. The optimization problem for the design of source/relay precoders to maximize secrecy capacity is formulated and then a suboptimal solution based on orthogonal projection is proposed. One advantage of employing such a suboptimal solution is that the system overhead to coordinate the source and relay transmission can be reduced. Again the two choices of the use of available relays are studied and the explicit expressions for information theoretic metrics, such as diversity-multiplexing tradeoff

Manuscript received 14 April 2011; revised 20 July 2011. Z. Ding was supported by the UK EPSRC under grant number EP/I037423/1. K. Leung, D. L. Goeckel and D. Towsley were sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence under Agreement Number W911NF-06-3-0001. D. L. Goeckel and D. Towsley were also sponsored by the National Science Foundation under grants CNS-0721861, ECS-0725616, and CNS-1018464.

Z. Ding is with School of Electrical, Electronic, and Computer Engineering, Newcastle University, NE1 7RU, UK.

K. K. Leung is with Dept. of Electrical and Electronic Engineering, Imperial College, London, SW7 2BT, UK.

D. L. Goeckel is with Dept. of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, US. Don T. is with Dept. of Computer Science, University of Massachusetts, Amherst, MA, US.

Digital Object Identifier 10.1109/JSAC.2012.120215.

and outage probability [12], are developed. Different to the scenario with single antenna nodes, in the context of MIMO cases, the best relay scheme can achieve the same diversity gain as the one using all relays.

II. A Motivating Example Based on a Simple Four-node Scenario

Consider a simple four-node scenario with one source-destination pair, one relay and one eavesdropper, where all nodes are equipped with a single antenna. The classical decode-forward protocol can be straightforwardly applied to the addressed scenario [11]. The transmission will be divided into two stages. At the first stage the source broadcasts a symbol to all other nodes. At the second stage, the relay will forward the decoded message to the destination and the eavesdropper if it is capable; otherwise, no one transmits during the second stage. The achievable perfect secrecy rate can be written as

$$\mathcal{I}=\begin{cases} \frac{1}{2}\{\log[1+\rho\phi_M]-\log[1+\rho\phi_E]\}^+, & |h_R|^2\geq g(\rho) \\ \frac{1}{2}\{\log[1+\rho|h_M|^2]-\log[1+\rho|h_E|^2]\}^+, & |h_R|^2<g(\rho) \end{cases},$$

where h_M, h_E, h_R, g_M and g_E denote the i.i.d. Raleigh fading coefficients for the source-destination, source-eavesdropper, source-relay, relay-destination, and relay-eavesdropper channels respectively, ρ denotes the signal-noise ratio (SNR), the function $g(x)=\frac{2^{2R}-1}{x}$ describes the decoding capability of the relay, R is the targeted secrecy data rate and $\{x\}^+$ denotes $\max\{0,x\}$. Furthermore $\phi_M=|h_M|^2+|g_M|^2$ is defined as the channel gain for the legitimate user and $\phi_E=|h_E|^2+|g_E|^2$ for the eavesdropper. Quasi-static fading has been assumed throughout the paper, and it is assumed that the source has the perfect knowledge of all CSI as in [2], [3], [13]. Note that our focus in this paper is the analysis of the outage probability and the development of an achievable diversity-multiplexing tradeoff, where the used achievable rates are not necessarily the maximum and it is out of the scope of this paper to obtain the maximum achievable rates. Hence the outage probability for the targeted secrecy data rate R

$$\begin{aligned} P(\mathcal{I}\leq 2R)=&P\left(\frac{1+\rho\phi_M}{1+\rho\phi_E}<2^{2R}\,|\phi_M>\phi_E\right)P\left(\phi_M>\phi_E\right)\\ &\times P(|h_R|^2\geq g(\rho))+P\left(\phi_M<\phi_E\right)P(|h_R|^2\geq g(\rho))+\\ &P\left(\frac{1+\rho|h_M|^2}{1+\rho|h_E|^2}<2^{2R}\,\big||h_M|^2>|h_E|^2\right)P\left(|h_M|^2>|h_E|^2\right)\\ &\times P(|h_R|^2<g(\rho))+P\left(|h_M|^2<|h_E|^2\right)P(|h_R|^2<g(\rho)), \end{aligned}$$

By using the fact that ϕ_M and ϕ_E are i.i.d Chi-square distributed random variables with pdf $f(x)=xe^{-x}$, at high SNR and for a fixed targeted rate, the expression of the outage probability is simplified as

$$P(\mathcal{I}\leq 2R)\sim\frac{1}{2}\left[\frac{1}{2}-\frac{3\cdot 2^{2R}+1}{(2^{2R}+1)^3}\right]+\frac{1}{2}\geq\frac{1}{2}, \qquad (1)$$

where $x\sim y$ denotes that x is asymptotically equivalent to y. Hence provided a fixed secrecy data rate, the outage probability experienced in the symmetric eavesdropping system cannot be decreased to zero by straightforwardly applying the classical cooperative protocols in [11], no matter how large we increase the transmission power.

III. Cooperative Secrecy Transmission with Single-Antenna Nodes

In this section, consider a secrecy communication scenario with one source-destination pair, one eavesdropper and L relays, where all nodes are equipped with a single antenna. The proposed cooperative transmission can again be divided into two stages. At the first stage, the source broadcasts its messages, and all relaying nodes listen. At the second stage, the capable relays and the source will act together and perform distributed beamforming. In this section, we consider a topology where the source and the L trusted relay nodes form a virtual antenna array and perform distributed beamforming. So we assume that during the first phase, e.g. the initialization phase, the source talks to the surrounding relays with low power, whereas the destination and eavesdropper are far away from the source and relays and cannot hear such a transmission[1]. Such a scenario has applications in wireless sensor networks. For example, consider smart home wireless healthcare applications, where digital gadgets in the home form the virtual array and send the sensitive patient data to a hotspot receiver outside. Then it is expected a threat is more likely to arise at the destination end, where an eavesdropper close to the hotspot wants to intercept the message. Note that such an assumption will be used only in this section, and a more general topology will be considered in the following sections.

There have been two approaches to use the available relays [16], [17]. One is to use all available relays, which could give optimal reception reliability but require large system overhead for accurate node coordination. On the other hand, it is a low system overhead solution to just invite a single relay which can yield the best performance for cooperation. Both approaches will be studied in the following.

A. Orthogonal projection beamforming using all qualified relays

Provided there are K qualified relays which can decode the messages, recall that during the second time slot, the source and the qualified relays will together perform distributed beamforming. First define $\mathbf{h}_M=\begin{bmatrix}h_M & g_{M,R_1} & \cdots & g_{M,R_K}\end{bmatrix}^T$ as the channel vector associated with the destination and $\mathbf{h}_E=\begin{bmatrix}h_E & g_{E,R_1} & \cdots & g_{E,R_K}\end{bmatrix}^T$ as the one for the eavesdropper, where g_{M,R_k} is the channel between the destination and the k-th relay and g_{E,R_k} is the channel between the eavesdropper and the k-th relay. Denote $\mathbf{p}_K$ as the $(K+1)\times 1$ vector containing the beamforming coefficients for the source and relays. The achievable perfect secrecy rate by using distributed beamforming is written as

$$\mathcal{I}=\begin{cases} \frac{1}{2}\{\log[1+\rho|\mathbf{p}_K^H\mathbf{h}_M|^2]-\log[1+\rho|\mathbf{p}_K^H\mathbf{h}_E|^2]\}^+, & K\geq 1 \\ \frac{1}{2}\{\log[1+\rho|h_M|^2]-\log[1+\rho|h_E|^2]\}^+, & K=0 \end{cases}$$

[1]The proposed secrecy transmission protocol can also be applied to the scenarios described in [14], [15] where the destination and eavesdropper are located far away from the source, and the relays are located in the middle. For such a scenario, the proposed secrecy scheme can still work by discarding the direct link between the source and destination.

The choice of the beamforming weighting factor needs to maximize the following objective function

$$\begin{aligned} \underset{\mathbf{p}_K}{\arg\max} \quad & \frac{1+\rho|\mathbf{p}_K^H\mathbf{h}_M|^2}{1+\rho|\mathbf{p}_K^H\mathbf{h}_E|^2} \\ s.t. \quad & \mathbf{p}_K^H\mathbf{p}_K = 1. \end{aligned} \tag{2}$$

Note that the total transmission power has been constrained for the proposed precoding scheme as shown in the above equation. This maximization problem has been solved by using general eigenvalue decomposition, and the optimal solution is $\mathbf{p}_K^* = \mathbf{B}^{-\frac{1}{2}}\mathbf{w}/|\mathbf{B}^{-\frac{1}{2}}\mathbf{w}|^2$ where $\mathbf{w}$ is the eigenvector of the matrix $\mathbf{B}^{-\frac{1}{2}}\mathbf{A}\mathbf{B}^{\frac{1}{2}}$ corresponding to the largest eigenvalue, $\mathbf{A} = \mathbf{I}_{K+1} + \rho\mathbf{h}_M\mathbf{h}_M^H$ and $\mathbf{B} = \mathbf{I}_{K+1} + \rho\mathbf{h}_E\mathbf{h}_E^H$ [18], [19]. However, the use of $\mathbf{p}_K^*$ will cause some difficulties in obtaining an explicit expression for the outage probability. An interesting observation is that for high SNR, the original objective function in (2) is simplified as

$$\begin{aligned} \underset{\mathbf{p}_K}{\arg\max} \quad & \frac{1+\rho|\mathbf{p}_K^H\mathbf{h}_M|^2}{1+\rho|\mathbf{p}_K^H\mathbf{h}_E|^2} \sim \frac{|\mathbf{p}_K^H\mathbf{h}_M|^2}{|\mathbf{p}_K^H\mathbf{h}_E|^2} \\ s.t. \quad & \mathbf{p}_K^H\mathbf{p}_K = 1. \end{aligned} \tag{3}$$

For such a maximization problem, the optimal solution of the beamforming vector $\mathbf{p}_K$ is orthogonal to the channel vector between the source/relay and the eavesdropper receiver, $\mathbf{p}_K^H\mathbf{h}_E = 0$. Based on such an approximation, the maximization problem is expressed as

$$\begin{aligned} \underset{\mathbf{p}_K}{\arg\max} \quad & (1+\rho|\mathbf{p}_K^H\mathbf{h}_M|^2) \\ s.t. \quad & \mathbf{p}_K^H\mathbf{p}_K = 1 \quad \& \quad \mathbf{p}_K^H\mathbf{h}_E = 0. \end{aligned} \tag{4}$$

By using such a beamformer, the outage probability of the secrecy rate is shown as

$$\begin{aligned} P(\mathcal{I} \le 2R) \quad = \quad & \sum_{k=1}^{L} P\left(\log[1+\rho|\mathbf{p}_K^H\mathbf{h}_M|^2] < 2^{2R} | K=k\right) \\ & \times P(K=k) + P_0, \end{aligned} \tag{5}$$

where $P_0 = P\left(\frac{1+\rho|h_M|^2}{1+\rho|h_E|^2} < 2^{2R} \middle| \frac{|h_M|^2}{|h_E|^2} > 1\right) P(|h_M|^2 > |h_E|^2) P(K=0) + P\left(\frac{|h_M|^2}{|h_E|^2} < 1\right) P(K=0)$. The main difference between the equation for $P(\mathcal{I} < 2R)$ in Section II and (5) is the first factor. This conditional probability can be evaluated by using the following proposition which provides the closed form expression of the optimal solution for the above maximization problem.

Proposition 1: The optimal solution for the maximization problem in (4) is

$$\mathbf{p}_K^* = \frac{\tilde{\mathbf{p}}_K}{\sqrt{\tilde{\mathbf{p}}_K^H\tilde{\mathbf{p}}_K}} \tag{6}$$

where $\tilde{\mathbf{p}}_K = \left[\mathbf{I}_{K+1} - \frac{1}{\mathbf{h}_E^H\mathbf{h}_E}\mathbf{h}_E\mathbf{h}_E^H\right]\mathbf{h}_M$.

Proof: See Appendix. ∎

Define d and r as the diversity gain and multiplexing gain as in [12]. Furthermore $f(\rho)$ is said to be exponentially equal to ρ^d, denoted as $f(\rho) \doteq \rho^d$, when $\lim_{\rho\to\infty} \frac{\log[f(\rho)]}{\log\rho} = d$, where $f(\rho) \dot{\le} \rho^d$ is defined similarly. By using Proposition 1, we have the following theorem for the performance of the cooperative secrecy communication scheme.

Theorem *1:* Consider a symmetric secrecy communication scenario with i.i.d. Raleigh fading channels. Provided there are L single antenna relays and high SNR, the outage probability achieved by the proposed cooperative protocol using all qualified relays is asymptotically equivalent to

$$P(\mathcal{I} \le 2R) \sim \left(\frac{2^{2R}-1}{\rho}\right)^L C_{fbm}, \tag{7}$$

where $C_{fbm} = \sum_{k=1}^{L} \frac{L!}{(L-k)!(k!)^2} + \frac{1}{2}\left(2 - \frac{1}{2^{2R}+1}\right)$. And the achievable diversity-multiplexing tradeoff for the addressed secrecy communication scenario is

$$d_{single,all}(r) = L(1-2r).$$

Proof: See Appendix. ∎

Remark 1: As shown in (1), the straightforward extension of cooperative protocols in [11] always suffers severe outage/error probability, regardless of the transmission power. Theorem 1 demonstrates that error-free secrecy communication, conditioned on a fixed secrecy data rate and large SNR, can be realized by implementing distributed beamforming.

Remark 2: Compared with distributed beamforming for non-secrecy communications, the existence of eavesdroppers has an impact on the obtainable diversity gain. Without eavesdroppers, the diversity gain will be $(L+1)$ [17]. To avoid source information intercepted by the eavesdropper, the obtainable diversity gain has been reduced to the number of relays L.

B. Distributed Beamforming using a single best relay

To reduce system overhead, it may be desirable to invite only the single relay for cooperation which gives the best system performance. And hence the criterion of relay selection is to maximize the following objective function

$$\begin{aligned} \underset{n,\mathbf{p}_n}{\arg} \quad & \max \frac{1+\rho|\mathbf{p}_n^H\mathbf{h}_{M,n}|^2}{1+\rho|\mathbf{p}_n^H\mathbf{h}_{E,n}|^2} \sim \max \frac{|\mathbf{p}_n^H\mathbf{h}_{M,n}|^2}{|\mathbf{p}_n^H\mathbf{h}_{E,n}|^2} \\ s.t. \quad & \mathbf{p}_n^H\mathbf{p}_n = 1. \end{aligned} \tag{8}$$

where the approximation is obtained at high SNR, $\mathbf{h}_{M,n} = \begin{bmatrix} h_M & g_{M,R_n} \end{bmatrix}^T$ is the channel vector associated with the destination, and $\mathbf{h}_{E,n} = \begin{bmatrix} h_E & g_{E,R_n} \end{bmatrix}^T$ is the channel vector associated with the eavesdropper. The optimal beamforming vector for each relay is the the vector orthogonal to the channel vectors associated with the eavesdropper, e.g., $\mathbf{p}_n = \begin{bmatrix} g_{E,R_n} & -h_E \end{bmatrix}^H / \sqrt{\mathbf{h}_{E,n}^H\mathbf{h}_{E,n}}$. And hence the secrecy rate achieved by the n-th relay is written as

$$\mathcal{I}_n = \log\left(1+\rho|g_{E,R_n}h_M - h_E g_{M,R_n}|^2 / \mathbf{h}_{E,n}^H\mathbf{h}_{E,n}\right). \tag{9}$$

Define $\upsilon_n = \frac{g_{E,R_n}h_M - h_E g_{M,R_n}}{\sqrt{\mathbf{h_{E,n}}^H\mathbf{h_{E,n}}}}$ and recall the fact that h_M and g_{M,R_n} are i.i.d. Complex Gaussian distributed. By treating h_E and g_{E,R_n} as the weighting factors and utilizing the fact they are normalized, we can find the variable υ_n is still conditionally complex Gaussian with zero mean and unit variance, or classical Raleigh distributed. Define the effective receive SNR as $\psi_n = \frac{|g_{E,R_n}h_M - h_E g_{M,R_n}|^2}{\mathbf{h_{E,n}}^H\mathbf{h_{E,n}}}$ which is exponentially distributed, with the mean and variance as $\mathcal{E}\{\psi_n\} = 1$ and $Cov\{\psi_n\} = 1$. Unfortunately these effective channel gains, ψ_n, are not independent, which causes the difficulty to resolve

the probability of $P\left(\max\{\psi_1,\cdots,\psi_K\} < \frac{2^{2R}-1}{\rho}\middle| K=k\right)$. A general explicit expression to show the relationship between the outage probability and SNR is not obtainable for the best relay scheme and thus we have relied on computer simulations. As shown in the section of numerical results, the fact that the K effective channel gains ψ_n are correlated to each other has a negative impact on the reception reliability. Compared with the scheme using all relays, the achievable diversity gain for the relay selection scheme is no longer proportional to the relay number L. However, it it is important to point out that the use of the single best relay can yield less complexity, compared to the one with all relays.

IV. Cooperative MIMO Secrecy Communications

In this section we will focus on a more general cooperative MIMO secrecy communication scenario, where the eavesdropper is equipped with M antennas and the other nodes, including the source, the destination and all L relays, are equipped with N antennas. It is assumed $N > M^2$, which means that the legitimate transceiver has better capability than the eavesdropper. In particular, the transmission is divided into two time slots. During the first time slot, the source will broadcast its messages to all other nodes, and assume that K out of the all L relays can decode the source messages correctly. At the second time slot, we can either ask all qualified relays or the best relay to forward the source messages to the destination. The eavesdropper tries to decode the source messages based on its observations from both time slots.

During the first time slot, denote the transmitted signal vector as $\tilde{\mathbf{s}} = \mathbf{P}_s\mathbf{s}$, where $\mathbf{s}$ is the $x\times 1$ information bearing vector, $\mathbf{P}_s$ is the $N\times x$ precoding matrix and x is the number of information bearing symbols. Both $\mathbf{P}_s$ and x are unknown variables, whose values are chosen to maximize the achievable secrecy data rate with the transmission power constraint $E\{\tilde{\mathbf{s}}^H\tilde{\mathbf{s}}\}=1$. At the second time slot, we can either invite all qualified relays, or only use the best relay to forward the source messages. Hence the signal model at the destination is written as

$$\begin{bmatrix}\mathbf{y}_{M,1}\\ \mathbf{y}_{M,2}\end{bmatrix} = \begin{bmatrix}\mathbf{H}_M\mathbf{P}_s\\ \mathbf{G}_M\tilde{\mathbf{P}}_r\end{bmatrix}\mathbf{s} + \begin{bmatrix}\mathbf{n}_{M,1}\\ \mathbf{n}_{M,2}\end{bmatrix}, \tag{10}$$

where the signal model at the eavesdropper can be defined similarly, $\mathbf{H}_M$ is the $N\times N$ source-destination channel matrix, $\mathbf{G}_{M,k}$ is the $N\times N$ kth relay-destination channel matrix, $\mathbf{P}_{M,k}$ is the precoding matrix for the k-th relay and the destination, $\mathbf{G}_M = \begin{bmatrix}\mathbf{G}_{M,1} & \cdots & \mathbf{G}_{M,K}\end{bmatrix}$ and $\tilde{\mathbf{P}}_r = \begin{bmatrix}\mathbf{P}_{r,1} & \cdots & \mathbf{P}_{r,K}\end{bmatrix}$ if all relays have been used for joint beamforming, or $\mathbf{G}_M = \begin{bmatrix}\mathbf{G}_{M,best}\end{bmatrix}$ and $\tilde{\mathbf{P}}_r = \begin{bmatrix}\mathbf{P}_{r,best}\end{bmatrix}$ if only the best relay has been used. The channel matrices $\mathbf{H}_E$ and $\mathbf{G}_E$ have been defined similar to $\mathbf{H}_M$ and $\mathbf{G}_M$.

Hence the achievable secrecy rate for such a cooperative MIMO protocol is written as

$$\mathcal{I}_K = \log\frac{\det\left(\mathbf{I}_x + \rho\mathbf{P}_s^H\mathbf{H}_M^H\mathbf{H}_M\mathbf{P}_s + \rho\tilde{\mathbf{P}}_r^H\mathbf{G}_M^H\mathbf{G}_M\tilde{\mathbf{P}}_r\right)}{\det\left(\mathbf{I}_x + \rho\mathbf{P}_s^H\mathbf{H}_E^H\mathbf{H}_E\mathbf{P}_s + \rho\tilde{\mathbf{P}}_r^H\mathbf{G}_E^H\mathbf{G}_E\tilde{\mathbf{P}}_r\right)}. \tag{11}$$

[2]When $N \le M$, it is still possible to achieve secrecy transmission by inviting relays to generate artificial noise [8], [20], which is out of the scope of this paper.

As discussed previously, x is the number of information bearing symbols, or the rank of the covariance matrix of the transmitted signals, $\mathbf{K} = E\{\tilde{\mathbf{s}}\tilde{\mathbf{s}}^H\}$. Recall the point-to-point MIMO secrecy rate is written as [3] $\mathcal{I}_{pp} = \log\frac{\det\left(\mathbf{I}_N+\rho\mathbf{H}_M^H\mathbf{K}\mathbf{H}_M\right)}{\det\left(\mathbf{I}_N+\rho\mathbf{H}_E^H\mathbf{K}\mathbf{H}_E\right)}$. As pointed out in [3], $\mathbf{K}$ is typically rank deficient, which provides us an intuition that the precoding matrix is a tall matrix, e.g., $x < N$. In the following, analytical results will be developed to show how to select x and the precoding matrices.

The outage probability for a fixed secrecy data rate is expressed as

$$\begin{aligned}P(\mathcal{I}\le 2R) = &\sum_{k=1}^{L} P\left(\mathcal{I}_k < 2R\right)P(K=k) + P(K=0)\\ &\times P\left(0<\mathcal{I}_{pp}<2^{2R}\right) + P\left(\mathcal{I}_{pp}<0\right)P(K=0),\end{aligned} \tag{12}$$

whose closed-form expression will be developed in the following sections for the best relay scheme and the scheme that uses all of the relays respectively.

A. MIMO secrecy cooperative transmission based on relay selection

Provided that there are K qualified relays, the use of n-th relay yields the secrecy rate shown in (13). And hence the maximization problem considered in this section is written as

$$\begin{aligned}\arg\max_{n,\mathbf{P}_s,\mathbf{P}_{r,n}} \quad & \mathcal{I}_{K,n} \\ s.t. \quad & trace\{\mathbf{P}_s^H\mathbf{P}_s\} = 1 \\ s.t. \quad & trace\{\mathbf{P}_{r,n}^H\mathbf{P}_{r,n}\} = 1 \quad \forall n\in\{1,\cdots,K\}.\end{aligned} \tag{14}$$

It is difficult to find the solution of the addressed maximization as the objective function is too complicated. The following proposition provides an approximation for the optimization problem at high SNR.

Proposition 2: At high SNR, the optimization problem in (14) is asymptotically equivalent to

$$\begin{aligned}\max \quad & \log\det\left(\tilde{\mathbf{X}}_{s,2}^H\tilde{\mathbf{H}}_{M,2}^H\tilde{\mathbf{H}}_{M,2}\tilde{\mathbf{X}}_{s,2} + \tilde{\mathbf{X}}_{n,2}^H\tilde{\mathbf{G}}_{n,2}^H\tilde{\mathbf{G}}_{n,2}\tilde{\mathbf{X}}_{n,2}\right)\\ s.t. \quad & trace\{\tilde{\mathbf{X}}_{s,2}\tilde{\mathbf{X}}_{s,2}^H\} = 1 \quad \& \quad trace\{\tilde{\mathbf{X}}_{n,2}\tilde{\mathbf{X}}_{n,2}^H\} = 1,\end{aligned}$$

where $\tilde{\mathbf{H}}_M = \mathbf{H}_M\mathbf{U}_s$, $\tilde{\mathbf{X}}_s = \mathbf{U}_s^H\mathbf{X}_s$, $\tilde{\mathbf{H}}_{M,2}$ is the $N\times(N-M)$ right submatrix of $\tilde{\mathbf{H}}_M$, $\tilde{\mathbf{X}}_{s,2}$ is the $(N-M)\times x$ lower submatrix of $\tilde{\mathbf{X}}_s$, e.g., $\tilde{\mathbf{H}}_M = \begin{bmatrix}\tilde{\mathbf{H}}_{M,1} & \tilde{\mathbf{H}}_{M,2}\end{bmatrix}$, $\tilde{\mathbf{X}}_s = \begin{bmatrix}\tilde{\mathbf{X}}_{s,2}^T & \tilde{\mathbf{X}}_{s,2}^T\end{bmatrix}^T$, $\mathbf{X}_s = (\tilde{\mathbf{P}}_s)^{-1}\mathbf{P}_s$, $\tilde{\mathbf{P}}_s = (\mathbf{I}_N - \mathbf{H}_E^H(\mathbf{H}_E\mathbf{H}_E^H)^{-1}\mathbf{H}_E)$, and $\mathbf{U}_s$ is from the eigenvalue decomposition of $\tilde{\mathbf{P}}_s$, $\tilde{\mathbf{P}}_s = \mathbf{U}_s\Lambda_s\mathbf{U}_s^H$. The matrices associated with the relays, such as $\tilde{\mathbf{X}}_{n,2}$ and $\tilde{\mathbf{G}}_{n,2}$, are defined similar to $\tilde{\mathbf{H}}_{M,2}$ and $\tilde{\mathbf{X}}_{s,2}$.

Proof: See Appendix. ∎

Since $\mathbf{U}_s$ is an unitary matrix, the virtual channel matrices, $\tilde{\mathbf{H}}_{M,2}$ and $\tilde{\mathbf{G}}_{n,2}$, are still classical $N\times(N-M)$ random complex Gaussian matrices. Therefore, an interesting observation is that the $N\times N$ MIMO secrecy communication scenario has been degraded to the $N\times(N-M)$ MIMO scenario due to the existence of the eavesdropper, which is exactly the motivation to introduce cooperative transmission into MIMO secrecy communications and compensate the loss of degrees of freedom.

$$\mathcal{I}_{K,n} = \log \frac{\det\left(\mathbf{I}_x + \rho \mathbf{P}_s^H \mathbf{H}_M^H \mathbf{H}_M \mathbf{P}_s + \rho \mathbf{P}_{r,n}^H \mathbf{G}_{M,n}^H \mathbf{G}_{M,n} \mathbf{P}_{r,n}\right)}{\det\left(\mathbf{I}_x + \rho \mathbf{P}_s^H \mathbf{H}_E^H \mathbf{H}_E \mathbf{P}_s + \rho \mathbf{P}_{r,n}^H \mathbf{G}_{E,n}^H \mathbf{G}_{E,n} \mathbf{P}_{r,n}\right)} \tag{13}$$

Since the form in Proposition 2 is a joint objective function of $\tilde{\mathbf{X}}_{s,2}$ and $\tilde{\mathbf{X}}_{n,2}$, the closed-form expression of the optimal solution is difficult to obtain. In the following, we focus on a suboptimal solution based on block diagonalization, which yields an explicit expression to an achievable diversity-multiplexing tradeoff.

Achievable diversity-multiplexing tradeoff: Perform eigenvalue decomposition as $\tilde{\mathbf{H}}_{M,2}^H \tilde{\mathbf{H}}_{M,2} = \mathbf{U}_M \Lambda_M \mathbf{U}_M^H$ and $\tilde{\mathbf{G}}_{n,2}^H \tilde{\mathbf{G}}_{n,2} = \tilde{\mathbf{U}}_{r,n} \tilde{\Lambda}_{r,n} \tilde{\mathbf{U}}_{r,n}^H$. The use of the diagonalization based method results in

$$\tilde{\mathbf{X}}_{s,2} = \frac{1}{N-M} \mathbf{U}_M \quad \& \quad \tilde{\mathbf{X}}_{n,2} = \frac{1}{N-M} \tilde{\mathbf{U}}_{r,n}. \tag{15}$$

Since the choice of the upper submatrix of $\tilde{\mathbf{X}}_s$ has no impact on the achievable rate, a simple choice of $\tilde{\mathbf{X}}_s$ is to have $\tilde{\mathbf{X}}_s = \begin{bmatrix}\mathbf{0}_{M,N-M}^T & \mathbf{U}_M^T\end{bmatrix}^T$, which means $\mathbf{X}_s = \mathbf{U}_s \tilde{\mathbf{X}}_s$. Similarly we can have $\tilde{\mathbf{X}}_{r,n} = \begin{bmatrix}\mathbf{0}_{M,N-M}^T & \tilde{\mathbf{U}}_{r,n}^T\end{bmatrix}^T$ and $\mathbf{X}_s = \tilde{\mathbf{U}}_s \tilde{\mathbf{X}}_s$. Summarizing all above steps, the diagonalization based solutions for the precoding matrices at the source and relays can be written as

$$\begin{aligned} \mathbf{P}_s &= \frac{1}{N-M} \tilde{\mathbf{P}}_s \mathbf{U}_s \begin{bmatrix}\mathbf{0}_{M\times(N-M)}^T & \mathbf{U}_M^T\end{bmatrix}^T, \quad (16) \\ \mathbf{P}_{r,n} &= \frac{1}{N-M} \tilde{\mathbf{P}}_{r,n} \mathbf{U}_{r,n} \begin{bmatrix}\mathbf{0}_{M\times(N-M)}^T & \tilde{\mathbf{U}}_{r,n}^T\end{bmatrix}^T. \end{aligned}$$

where recall that the orthogonal project matrix $\tilde{\mathbf{P}}_s$ is defined as $(\mathbf{I}_N - \mathbf{H}_E^H(\mathbf{H}_E\mathbf{H}_E^H)^{-1}\mathbf{H}_E)$ and $\tilde{\mathbf{P}}_{r,n}$ is defined as the projection matrix of $\mathbf{G}_{E,n}$ similarly. Such a diagonalization based solution only causes small system overhead since no information exchange is required between the source and multiple relays. Each node, the source or relays, can decide its precoding matrix based only on local CSI.

Theorem *2:* Based on the proposed orthogonal projection based precoding, the achievable outage probability for the best relay scheme is asymptotically equivalent to

$$P(\mathcal{I} \le 2R) \quad \dot{\le} \quad \rho^{-(L+1)[(N-M-2r)(N-2r)]},$$

and the achievable diversity-multiplexing tradeoff is

$$d(r) \quad \doteq \quad (L+1)[(N-M-2r)(N-2r)].$$

Proof: See Appendix. ∎

Remark 1: Theorem 2 demonstrates the benefit of introducing cooperative transmission into secrecy communications. Without using cooperative transmission, the degree of freedom has been reduced, e.g., a $N \times N$ point-to-point MIMO system degraded to a $N \times (N-M)$ scheme. However, by using cooperative diversity, the achievable diversity gain can be improved from $(N-M)N$ up to $(L+1)(N-M)N$.

Remark 2: Compared with the scheme without relays, the use of cooperative diversity causes some loss of multiplexing gain, which is due to the fact that two time slots have been used to transmit the same symbol. By using more sophisticated cooperative protocols, such as non-orthogonal transmission schemes [15], [21], such a loss of the multiplexing gain can be avoided.

B. MIMO secrecy cooperative transmission by using all available relays

Provided all qualified relays have been used, the expression of the secrecy rate is written as

$$\mathcal{I}_K = \log \frac{\det\left(\mathbf{I}_x + \rho \mathbf{P}_s^H \mathbf{H}_M^H \mathbf{H}_M \mathbf{P}_s + \rho \mathbf{P}_r^H \mathbf{G}_M^H \mathbf{G}_M \mathbf{P}_r\right)}{\det\left(\mathbf{I}_x + \rho \mathbf{P}_s^H \mathbf{H}_E^H \mathbf{H}_E \mathbf{P}_s + \rho \mathbf{P}_r^H \mathbf{G}_E^H \mathbf{G}_E \mathbf{P}_r\right)}.$$

Following similar steps to those in the previous section, at high SNR, the maximization problem considered in this section is asymptotically equivalent to

$$\begin{aligned} &\max \ \log\det\left(\mathbf{X}_s^H \tilde{\mathbf{P}}_s^H \mathbf{H}_M^H \mathbf{H}_M \tilde{\mathbf{P}}_s \mathbf{X}_s + \mathbf{X}_r^H \tilde{\mathbf{P}}_r^H \mathbf{G}_M^H \mathbf{G}_M \tilde{\mathbf{P}}_r \mathbf{X}_r\right). \\ &s.t. \qquad trace\{\Lambda \mathbf{X}_s \mathbf{X}_s^H\} = 1 \quad \& \quad trace\{\mathbf{X}_r \mathbf{X}_r^H\} = 1. \end{aligned}$$

where $\tilde{\mathbf{P}}_s$ is defined in the previous section and $\tilde{\mathbf{P}}_r = (\mathbf{I}_{NK} - \mathbf{G}_E^H(\mathbf{G}_E\mathbf{G}_E^H)^{-1}\mathbf{G}_E)$. By utilizing the feature of idempotent matrices, the addressed objection function can be simplified as

$$\begin{aligned} &\max \ \log\det\left(\tilde{\mathbf{X}}_{s,2}^H \tilde{\mathbf{H}}_{M,2}^H \tilde{\mathbf{H}}_{M,2} \tilde{\mathbf{X}}_{s,2} + \tilde{\mathbf{X}}_{r,2}^H \tilde{\mathbf{G}}_{M,2}^H \tilde{\mathbf{G}}_{M,2} \tilde{\mathbf{X}}_{r,2}\right) \\ &s.t. \qquad trace\{\tilde{\mathbf{X}}_{s,2} \tilde{\mathbf{X}}_{s,2}^H\} = 1 \quad \& \quad trace\{\tilde{\mathbf{X}}_{r,2} \tilde{\mathbf{X}}_{r,2}^H\} = 1, \end{aligned}$$

where the eigenvalue decomposition of $\tilde{\mathbf{P}}_r$ denotes as $\tilde{\mathbf{P}}_r = \mathbf{U}_G \Lambda_G \mathbf{U}_G^H$, $\tilde{\mathbf{G}}_M$ denotes the new $N \times NK$ virtual channel $\tilde{\mathbf{G}}_M = \mathbf{G}_M \mathbf{U}_G$, $\tilde{\mathbf{G}}_{M,2}$ is the $N \times (NK-M)$ right submatrix of $\tilde{\mathbf{G}}_M$, e.g., $\tilde{\mathbf{G}}_M = \begin{bmatrix}\tilde{\mathbf{G}}_{M,1} & \tilde{\mathbf{G}}_{M,2}\end{bmatrix}$, $\tilde{\mathbf{X}}_r = \mathbf{U}_G^H \mathbf{X}_r$, and $\tilde{\mathbf{X}}_{r,2}$ is the $(NK-M) \times x$ lower submatrix of $\tilde{\mathbf{X}}_r$, e.g., $\tilde{\mathbf{X}}_r = \begin{bmatrix}\tilde{\mathbf{X}}_{r,1}^T & \tilde{\mathbf{X}}_{r,2}^T\end{bmatrix}^T$.

Achievable diversity-multiplexing tradeoff: In contrast to the best relay scheme, the virtual channel matrix $\tilde{\mathbf{G}}_{M,2}$ here becomes row full rank for $N > 1$. Denote the eigenvalue decomposition of $\tilde{\mathbf{G}}_{M,2}^H \tilde{\mathbf{G}}_{M,2}$ as $\tilde{\mathbf{G}}_{M,2}^H \tilde{\mathbf{G}}_{M,2} = \tilde{\mathbf{U}}_r \Lambda_r \tilde{\mathbf{U}}_r^H$. As a result, it can be shown that $\tilde{\mathbf{G}}_{M,2}^H \tilde{\mathbf{G}}_{M,2}$ has N non-zero eigenvalues, rather than $N-M$ as in the previous section. To make block diagonalization applicable, we set $x = N$ and the precoding matrices at the source and relays as

$$\begin{aligned} \mathbf{P}_s &= \left[\tfrac{1}{N-M} \tilde{\mathbf{P}}_s \mathbf{U}_s \begin{bmatrix}\mathbf{0}_{M\times(N-M)}^T & \mathbf{U}_M^T\end{bmatrix}^T \quad \mathbf{0}_{N\times M}\right], \\ \mathbf{P}_r &= \frac{1}{N} \tilde{\mathbf{P}}_r \mathbf{U}_G \begin{bmatrix}\mathbf{0}_{M\times N}^T & \tilde{\mathbf{U}}_{r,N}^T\end{bmatrix}^T, \end{aligned}$$

where $\tilde{\mathbf{U}}_{r,N}$ is the $(NK-M) \times N$ submatrix of $\tilde{\mathbf{U}}_r$ and contains the N eigenvectors corresponding to the non-zero eigenvalues. Based on such a choice of the precoding matrices, the secrecy rate is expressed as

$$\mathcal{I}_K = \log\det\left(\mathbf{I}_N + \rho\tilde{\Lambda}_M + \rho\Lambda_r\right), \tag{17}$$

where $\tilde{\Lambda}_M$ is a $N \times N$ diagonal matrix with its first $(N-M)$ diagonal elements the same as the ones of Λ_M and the rest

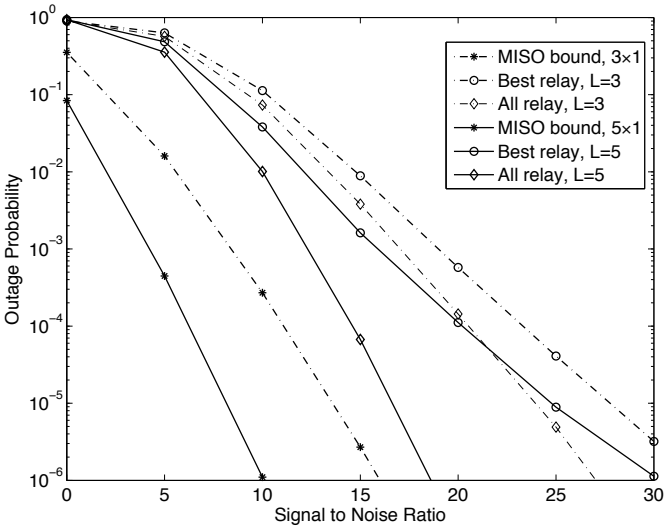


Fig. 1. The outage probability vs SNR. The targeted secrecy data rate is set as $R = 1$ bit per channel use.

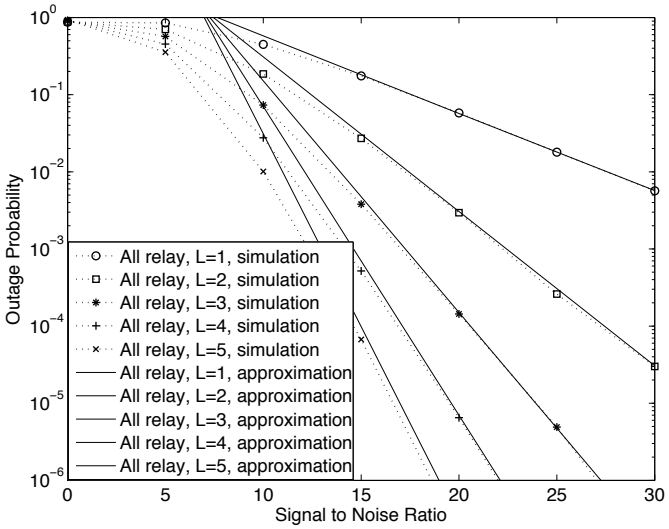


Fig. 2. The outage probability for the best relay scheme as a function of SNR. The targeted secrecy data rate is set as $R = 1$ bit per channel use.

as zeros. So it can be easily found that the outage probability when there are K qualified relays is expressed as [12]

$$P(\mathcal{I}_K < 2R) \dot{\leq} \rho^{-[(N(K+1)-2M-4r)(N-2r)]}. \qquad (18)$$

And the overall outage probability can be bounded at high SNR as in the previous subsection and we obtain the following theorem for the outage performance of the proposed protocol.

Theorem *3:* Based on the proposed orthogonal projection based precoding, the outage probability for a fixed secrecy data rate for the scheme using all available relays can be upper bounded at high SNR as

$$P(\mathcal{I} \leq 2R) \quad \dot{\leq} \quad \rho^{-(L+1)[(N-M-2r)(N-2r)]},$$

and the achievable diversity-multiplexing tradeoff is

$$d(r) \quad \doteq \quad (L+1)[(N-M-2r)(N-2r)].$$

Remark 1: Comparing Theorem 2 to Theorem 3 it can be observed that the diversity gain achievable for both schemes is the same. Such a phenomenon is actually expected, similar to the fact that maximum ratio combining can achieve the same diversity gain as the selection scheme for single-input multiple-output scenarios. For intermediate SNR, the scheme using all qualified relays can outperform the best relay scheme in terms of reception reliability, but the coordination among relays could consume extra bandwidth resource. By only inviting the single best relay, the system overhead can be reduced without decreasing the achievable diversity gain.

Remark 2: The performance shown in Theorem 3 is based on (17), where the eigenvalues have been randomly placed. Recall that the determinant of the sum of two matrices can be enlarged by aligning their eigenvalues in the same order [22]. By using such a result, the achievable secrecy rate can be further increased by carefully aligning the eigenvalues of $\tilde{\Lambda}_M$ and Λ_r. Such a technique can be also applied to the best relay scheme.

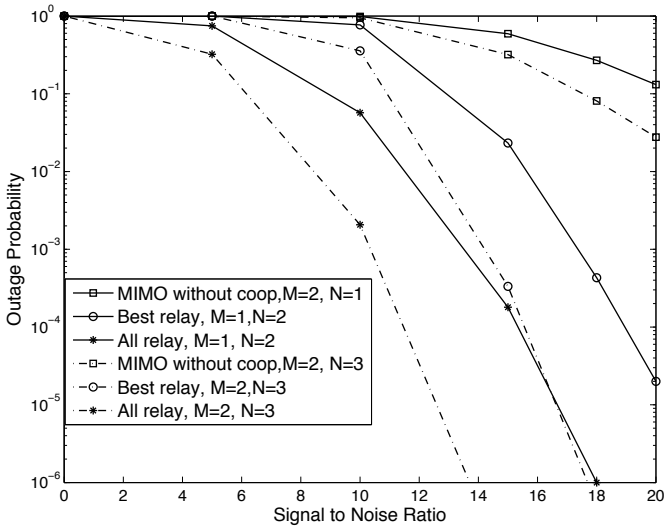
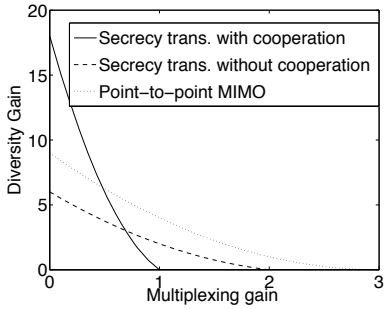


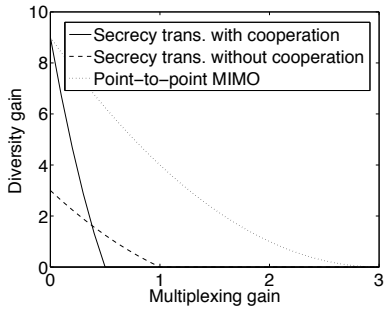
Fig. 3. The outage probability vs SNR. The targeted secrecy data rate is set as $R = 3$ bit per channel use.

V. Numerical Results

First we focus on the secrecy communication scenario where all nodes are equipped with a single antenna. Fig. 1 shows the outage performance of three schemes: the best relay scheme, the cooperative scheme using all qualified relays, and the MISO lower bound. As can be seen from the figure, the curves for the scheme using all qualified relays have the same slope as the ones for the MISO bound, which confirms that this cooperative scheme can achieve the diversity gain L. On the other hand, it is interesting to observe that the curve of the best relay scheme with $L = 3$ relays has the same slope as the one with $L = 5$, which is due to the fact that the effective channel gains realized by different relays are correlated. In Fig. 2, the high SNR approximations developed in Theorem 1 are compared to the simulation results. As demonstrated in the figure, the developed analytic results at the high SNR are perfectly matched with the computer simulation results.



(a) $M = 1$, $L = 2$ and $N = 3$



(b) $M = 2$, $L = 2$ and $N = 3$

Fig. 4. Achievable diversity-multiplexing tradeoff for three comparable schemes.

Second we focus on the MIMO secrecy communication setup, where the eavesdropper is equipped with M antennas and all other nodes are equipped with N antennas. Fig. 3 demonstrates the outage performance of three schemes: the best relay scheme, the all relay scheme and the direct transmission scheme. As can be seen from Fig. 3, the increase of the number of antennas can increase the achievable secrecy rate and therefore improve the reception reliability for all schemes. With the same system setup, Fig. 3 demonstrates that the two cooperative schemes can achieve the same diversity gain since the curves of the two schemes have the same slope, which is consistent with Theorem 2 and Theorem 3. At intermediate SNR the scheme using all qualified relays can outperform the best relay scheme, but it should be noticed that the best relay scheme requires much less system overhead as no information exchange among relays and the source is needed.

Finally Fig. 4 shows the diversity-multiplex tradeoff achievable for the three schemes: the point-to-point MIMO scheme, the secrecy transmission scheme with and without cooperation. In general, the existence of the eavesdropper will cause some loss of the diversity/multiplexing gain, particularly in the case that $(N - M)$ is small. Recall for the case with a small value of $(N - M)$ the eavesdropper has the similar capability to the legitimate receiver, so the loss of degrees of freedom becomes the price to avoid eavesdropping. By introducing cooperative diversity into secrecy communications, the loss of diversity gain can be compensated as shown by the two figures, where the achievable diversity gain can be the same or even larger than the MIMO non-secrecy scheme. Because of the use of the orthogonal cooperative transmission strategy, the proposed cooperative scheme suffers some loss of the multiplexing gain compared with the two non-cooperative schemes. However, by implementing more advanced cooperative strategies, such as the non-cooperative schemes [15], [21], the loss of the multiplexing gain can be compensated.

VI. Conclusions

By introducing cooperative transmission into secrecy communication systems, it has been shown that zero approaching outage probability can be achieved. The scenario without MIMO was studied first, where the optimal beamformer has been developed together with its outage performance. Then the scenario with MIMO was considered, where the optimization problem for the design of source/relay precoders was formulated and a suboptimal solution with low system overhead was proposed. Note that distributed beamforming and precoding have been focused on here, but there are other ways to exploit relay transmission, such as cooperative jamming and relay chatting [8], [20], [23].

Appendix

Proof for Proposition 1 : To find an explicit expression of the optimal solution for (4), note that a desirable solution of the maximization problem can be expressed in a form as $\mathbf{p} = \mathbf{P}\mathbf{x}$, where $\mathbf{P} = \left[\mathbf{I}_{K+1} - \frac{1}{\mathbf{h}_E^H \mathbf{h}_E}\mathbf{h}_E\mathbf{h}_E^H\right]$ is the projection matrix to ensure $\mathbf{p} \perp \mathbf{h}_E$ and $\mathbf{x}$ will be a $(K+1) \times 1$ auxiliary vector. To simplify notations, the subscript K of $\mathbf{p}$ is omitted. It can be shown that the projection matrix $\mathbf{P}$ is an idempotent and symmetric matrix. And hence the original maximization problem in (4) can be written as

$$\begin{aligned} \arg\max_{\mathbf{x}} \quad & \mathbf{x}^H\mathbf{P}^H\mathbf{h}_M\mathbf{h}_M^H\mathbf{P}\mathbf{x} \\ s.t. \quad & \mathbf{x}^H\mathbf{P}^H\mathbf{P}\mathbf{x} = 1. \end{aligned} \tag{19}$$

By constructing the objective function $L(\mathbf{x}) = \mathbf{x}^H\mathbf{P}^H\mathbf{h}_M\mathbf{h}_M^H\mathbf{P}\mathbf{x} + \lambda(\mathbf{p}^H\mathbf{p} - 1)$, the optimal solution of $\mathbf{x}$ and the Lagrange multiplier λ can be obtained from the following linear equations

$$\begin{aligned} \mathbf{P}^H\mathbf{h}_M\mathbf{h}_M^H\mathbf{P}\mathbf{x} + \lambda\mathbf{p} &= 0 \\ \mathbf{x}^H\mathbf{P}^H\mathbf{P}\mathbf{x} &= 1, \end{aligned} \tag{20}$$

which gives the optimal choice of $\mathbf{x}^*$ and the Lagrange multiplier λ as

$$\begin{aligned} \lambda &= -\mathbf{x}^{*H}\mathbf{P}^H\mathbf{h}_M\mathbf{h}_M^H\mathbf{P}\mathbf{x}^* \\ \mathbf{P}^H\mathbf{h}_M &= \mathbf{x}^{*H}\mathbf{P}^H\mathbf{h}_M\mathbf{P}\mathbf{x}^*, \end{aligned} \tag{21}$$

where the fact that $\mathbf{P}$ is an idempotent and symmetric matrix has been used, e.g., $\mathbf{P}\mathbf{P} = \mathbf{P}$ and $\mathbf{P}^H = \mathbf{P}$. It is easy to see that $\mathbf{x}^* = \frac{\mathbf{h}_M}{\sqrt{\mathbf{h}_M^H\mathbf{P}\mathbf{h}_M}}$ is the solution of (21). The optimal choice for the beamforming vector shown in the proposition can be obtained in a straightforward way. ■

Proof for Theorem 1 : First define the projection matrix as $\mathbf{P}_K = \left[\mathbf{I}_{K+1} - \frac{1}{\mathbf{h}_E^H \mathbf{h}_E}\mathbf{h}_E\mathbf{h}_E^H\right]$. Since $\mathbf{P}_K$ is an idempotent matrix, the power normalization factor $\tilde{\mathbf{p}}_K^H\tilde{\mathbf{p}}_K$ can be expressed as $\tilde{\mathbf{p}}_K^H\tilde{\mathbf{p}}_K = \mathbf{h}_M^H\mathbf{P}_K^H\mathbf{P}_K\mathbf{h}_M = \mathbf{h}_M^H\mathbf{P}_K\mathbf{h}_M$. Hence

the received SNR by using distributed beamforming can be written as

$$|\mathbf{p}_K^H\mathbf{h}_M|^2=\frac{|\tilde{\mathbf{p}}_K^H\mathbf{h}_M|^2}{\tilde{\mathbf{p}}_K^H\tilde{\mathbf{p}}_K}=\mathbf{h}_M^H\left[\mathbf{I}_{K+1}-\frac{1}{\mathbf{g}^h\mathbf{g}}\mathbf{g}\mathbf{g}^H\right]\mathbf{h}_M.$$

To find $\tilde{P}=P\left(\log[1+\rho\mathbf{h}_M^H\mathbf{P}\mathbf{h}_M]<2^{2R}|K=k\right)$, we can use the fact that $\mathbf{P}$ is an idempotent matrix, which means the eigenvalues of the $\mathbf{P}$ are either zero or ones. Alternatively we can first perform eigenvalue decomposition for $\frac{1}{\mathbf{g}^h\mathbf{g}}\mathbf{g}\mathbf{g}^H$ as $\frac{1}{\mathbf{g}^h\mathbf{g}}\mathbf{g}\mathbf{g}^H=\mathbf{U}_g^H\Sigma\mathbf{U}_g$, where Σ is a $(K+1)\times(K+1)$ diagonal matrix with its first diagonal being one and the rest being zeros. By using such an observation, we can obtain

$$\mathbf{h}_M^H\left[\mathbf{I}_{K+1}-\frac{1}{\mathbf{g}^h\mathbf{g}}\mathbf{g}\mathbf{g}^H\right]\mathbf{h}_M=\mathbf{h}_M^H\mathbf{U}_g^H\left[\mathbf{I}_{K+1}-\Sigma\right]\mathbf{U}_g\mathbf{h}_M.$$

Because of the structure of Σ, the diagonal matrix $(\mathbf{I}_{K+1}-\Sigma)$ will be the same as the identity matrix except that its first element is zero, which means

$$\mathbf{h}_M^H\left[\mathbf{I}_{K+1}-\frac{1}{\mathbf{g}^h\mathbf{g}}\mathbf{g}\mathbf{g}^H\right]\mathbf{h}_M \quad = \quad \sum_{n=1}^{K}|\tilde{h}_n|^2,$$

where $\tilde{h}_K$ are the virtual channels $\tilde{\mathbf{h}}=\mathbf{U}_g\mathbf{h}_M$. Since $\mathbf{U}_g$ is an unitary matrix, the statistical property of $\tilde{\mathbf{h}}$ is the same as the original channel vector $\mathbf{h}$, which yields

$$\tilde{P}=\int_0^{\frac{2^{2R}-1}{\rho}}\frac{x^{k-1}}{(k-1)!}e^{-x}dx\sim\frac{(2^{2R}-1)^k}{k!\rho^k},$$

where the second equation follows the fact that $\sum_{n=1}^{k}|\tilde{h}_n|^2$ is Chi-square distributed with $2k$ degrees of freedom and the approximation is obtained with the high SNR assumption. Note that following the steps in [24], similar results can be also developed. By using order statistics, the following probability can be obtained as [25]

$$P(K=k)\sim\frac{L!}{(L-k)!k!}\left(\frac{2^{2R}-1}{\rho}\right)^{L-k}. \tag{22}$$

Finally the outage probability can be expressed as

$$\begin{aligned}P(\mathcal{I}\le 2R)\sim&\sum_{k=1}^{L}\frac{(2^{2R}-1)^k}{k!\rho^k}\frac{L!}{(L-k)!k!}\left(\frac{2^{2R}-1}{\rho}\right)^{L-k}\\&+\frac{1}{2}\left(2-\frac{e^{-\frac{2^{2R}-1}{\rho}}}{2^{2R}+1}\right)\left(\frac{2^{2R}-1}{\rho}\right)^{L}.\end{aligned} \tag{23}$$

By using (23) and some algebraic manipulations, the theorem can be obtained. ■

*Proof for Proposition 2 :*To simplify the objective function and obtain the closed form expression of the solution, note that at high SNR the mutual information is asymptotically equivalent to

$$\mathcal{I}_{K,n}\sim\log\frac{\det\left(\rho\mathbf{P}_s^H\mathbf{H}_M^H\mathbf{H}_M\mathbf{P}_s+\rho\mathbf{P}_{r,n}^H\mathbf{G}_{M,n}^H\mathbf{G}_{M,n}\mathbf{P}_{r,n}\right)}{\det\left(\rho\mathbf{P}_s^H\mathbf{H}_E^H\mathbf{H}_E\mathbf{P}_s+\rho\mathbf{P}_{r,n}^H\mathbf{G}_{E,n}^H\mathbf{G}_{E,n}\mathbf{P}_{r,n}\right)}. \tag{24}$$

It is desirable to select the precoding matrices which can yield $\det\left(\mathbf{P}_s^H\mathbf{H}_E^H\mathbf{H}_E\mathbf{P}_s+\mathbf{P}_{r,n}^H\mathbf{G}_{E,n}^H\mathbf{G}_{E,n}\mathbf{P}_{r,n}\right)=0$; otherwise, at high SNR the rate is asymptotically equivalent to a ratio which is no longer a function of SNR. Based on such an observation, the addressed maximization problem can be first relaxed as

$$\begin{aligned}\max\quad&\log\det\left(\rho\mathbf{P}_s^H\mathbf{H}_M^H\mathbf{H}_M\mathbf{P}_s+\rho\mathbf{P}_{r,n}^H\mathbf{G}_{M,n}^H\mathbf{G}_{M,n}\mathbf{P}_{r,n}\right).\\ s.t.\quad&trace\{\mathbf{P}_s^H\mathbf{P}_s\}=1\quad\&\quad trace\{\mathbf{P}_{r,n}^H\mathbf{P}_{r,n}\}=1\\ s.t.\quad&\mathbf{H}_E\mathbf{P}_s=\mathbf{0}_{M\times x}\quad\&\quad\mathbf{G}_{E,n}\mathbf{P}_{r,n}=\mathbf{0}_{M\times x}.\end{aligned} \tag{25}$$

To further simplify the optimization problem, note that the orthogonal constraint $\mathbf{H}_E\mathbf{P}_s=\mathbf{0}_{N\times x}$ means that the source precoding matrix can be expressed as

$$\mathbf{P}_s=(\mathbf{I}_N-\mathbf{H}_E^H(\mathbf{H}_E\mathbf{H}_E^H)^{-1}\mathbf{H}_E)\mathbf{X}_s, \tag{26}$$

where $\mathbf{X}_s$ is a $N\times x$ unknown auxiliary matrix and the total transmission power based on such a precoding matrix is

$$\beta_s=trace\{\mathbf{U}_s\Lambda_s\mathbf{U}_s^H\mathbf{X}_s\mathbf{X}_s^H\}=trace\{\Lambda_s\mathbf{X}_s\mathbf{X}_s^H\}, \tag{27}$$

where the first equation is obtained by performing eigenvalue decomposition on the projection matrix. It can be easy to evaluate that the projection matrix $\tilde{\mathbf{P}}_s=(\mathbf{I}_N-\mathbf{H}_E^H(\mathbf{H}_E\mathbf{H}_E^H)^{-1}\mathbf{H}_E)$ is an idempotent matrix. Similarly the precoding matrix for each relay can be expressed as $\mathbf{P}_{r,n}=\tilde{\mathbf{P}}_{r,n}\mathbf{X}_{r,n}$ where $\tilde{\mathbf{P}}_{r,n}=(\mathbf{I}_N-\mathbf{G}_E^H(\mathbf{G}_E\mathbf{G}_E^H)^{-1}\mathbf{G}_E)$ and $\beta_{r,n}=trace\{\Lambda_{r,n}\mathbf{X}_{r,n}\mathbf{X}_{r,n}^H\}$.

By utilizing the orthogonal projection matrices, the orthogonal constraint in (25) can be removed and the addressed optimization problem can be simplified as Note that these projection matrices are the idempotent ones and recall an important property of idempotent matrices that their eigenvalues are either ones or zeros. Since the rank of the projection matrix is $(N-M)$, without loss of generality, assume that the first M diagonal elements of Λ_s and $\Lambda_{r,n}$ are zeros, and the rest are ones. By using such a property and performing eigenvalue decomposition to all these idempotent matrices, the objective function in (28) can be expressed as the one shown in the proposition. The power normalization factor can now be expressed as a function of $\tilde{\mathbf{X}}_{s,2}$ as

$$\beta_s \quad = \quad trace\{\Lambda\tilde{\mathbf{X}}_s\tilde{\mathbf{X}}_s^H\}=trace\{\tilde{\mathbf{X}}_{s,2}\tilde{\mathbf{X}}_{s,2}^H\}, \tag{29}$$

and similarly we can have $\beta_{r,n}=trace\{\tilde{\mathbf{X}}_{n,2}\tilde{\mathbf{X}}_{n,2}^H\}$. And the proposition is proved. ■

Proof for Theorem 2 : By using the precoding matrices in (16), the use of n-th relay yields the secrecy rate as

$$\mathcal{I}_{K,n}=\log\det\left(\mathbf{I}_{N-M}+\rho\Lambda_M+\rho\tilde{\Lambda}_{r,n}\right). \tag{30}$$

Denote the diagonal elements of the two diagonal matrices as $diag(\Lambda_M)=[\lambda_{M,1}\cdots\lambda_{M,N-M}]$ and $diag(\tilde{\Lambda}_{r,n})=[\lambda_{n,1}\cdots\lambda_{n,N-M}]$. And hence the outage probability $P(\mathcal{I}_n<2R)$ can be expressed as

$$\begin{aligned}P(\mathcal{I}_n<2R)&\sim P\left(\prod_{i=1}^{N-M}(\rho\lambda_{M,i}+\rho\lambda_{n,i})<2^{2R}\right)\\&\le P\left(\prod_{i=1}^{N-M}\rho\lambda_{M,i}<2^{2R}\right)P\left(\prod_{i=1}^{N-M}\rho\lambda_{n,i}<2^{2R}\right),\end{aligned} \tag{31}$$

where the first approximation is due to the high SNR assumption and the inequality is

$$\begin{aligned} \max \quad & \log\det\left(\mathbf{X}_s^H\tilde{\mathbf{P}}_s^H\mathbf{H}_M^H\mathbf{H}_M\tilde{\mathbf{P}}_s\mathbf{X}_s + \mathbf{X}_{r,n}^H\tilde{\mathbf{P}}_{r,n}^H\mathbf{G}_{M,n}^H\mathbf{G}_{M,n}\tilde{\mathbf{P}}_{r,n}\mathbf{X}_{r,n}\right). \\ s.t. \quad & trace\{\Lambda_s\mathbf{X}_s\mathbf{X}_s^H\} = 1 \quad \& \quad trace\{\Lambda_{r,n}\mathbf{X}_{r,n}\mathbf{X}_{r,n}^H\} = 1. \end{aligned} \tag{28}$$

due to the fact that the events to satisfy $\left(\prod_{i=1}^{N-M}(\rho\lambda_{M,i}+\rho\lambda_{n,i}) < 2^{2R}\right)$ is a subset of the events to satisfy $\left(\prod_{i=1}^{N-M}\rho\lambda_{M,i} < 2^{2R}\right)$ & $\left(\prod_{i=1}^{N-M}\rho\lambda_{n,i} < 2^{2R}\right)$. As a result, the upper bound of the outage probability $P(\mathbf{I}_{best} < 2R)$ can be expressed as

$$P(\mathcal{I}_{best,K} < 2R) \le P\left(\prod_{i=1}^{N-M}\rho\lambda_{M,i} < 2^{2R}\right)\prod_{n=1}^{K}\tilde{P}_n, \tag{32}$$

where $\tilde{P}_n = P\left(\prod_{i=1}^{N-M}\rho\lambda_{n,i} < 2^{2R}\right)$ and the inequality utilizes the fact that $\lambda_{n,i}$ and $\lambda_{l,i}$ are for different relays and hence independent to each other $\forall n \neq l$. Recall that $\prod_{i=1}^{N-M}\rho\lambda_{M,i} = \det\left(\tilde{\mathbf{H}}_{M,2}^H\tilde{\mathbf{H}}_{M,2}\right)$, where $\tilde{\mathbf{H}}_{M,2}$ is a $N \times (N-M)$ complex Gaussian random matrix. By using the results provided in [12], the probability $P\left(\prod_{i=1}^{N-M}\rho\lambda_{M,i} < 2^{2R}\right)$ is asymptotically equivalent to

$$P\left(\prod_{i=1}^{N-M}\rho\lambda_{M,i} < 2^{2R}\right) \doteq \rho^{-[(N-M-2r)(N-2r)]}. \tag{33}$$

where the probability $P\left(\prod_{i=1}^{N-M}\rho\lambda_{n,i} < 2^{2R}\right)$ shares the same expression. So overall the probability $P(\mathcal{I}_{best} < 2R)$ can be upper bounded as

$$P(\mathcal{I}_{best,K} < 2R) \le \rho^{-(K+1)[(N-M-2r)(N-2r)]}. \tag{34}$$

To calculate the overall outage probability in (12), the probability for the event that there are K qualified relays is required. Recall that the mutual information at the l-th relay is

$$\mathcal{I}_{r,l} = \log\det\left(\mathbf{I}_{N-M} + \rho\tilde{\mathbf{H}}_{l,2}^H\tilde{\mathbf{H}}_{l,2}\right),$$

where $\tilde{\mathbf{H}}_{l,2}$ is defined similar to $\tilde{\mathbf{H}}_M$, a $N\times(N-M)$ complex Gaussian matrix. Consider that all L relays have been ordered to satisfy $\mathcal{I}_{r,(1)} \le \cdots \le \mathcal{I}_{r,(L)}$. Furthermore, by using order statistics, the probability of the event that there are K qualified relays can be expressed as

$$P(K=k) = \frac{L!}{(L-k)!k!}F_{\mathcal{I}}^{L-k}(2R)(1-F_{\mathcal{I}}(2R))^k, \tag{35}$$

where $F_{\mathcal{I}}(x)$ is the cumulative density function of $\mathcal{I}_{r,l}$. Note that $\mathcal{I}_{r,l}$ is i.i.d. and furthermore the probability $P(\mathcal{I}_{r,l} < 2R)$ can approximated as [12]

$$P(\mathcal{I}_{r,l} < 2R) \doteq \rho^{-[(N-M-2r)(N-2r)]}. \tag{36}$$

Combining the above two equations, we can obtain the probability of the event there are k qualified relays

$$P(K=k) \doteq \rho^{-(L-k)[(N-M-2r)(N-2r)]}. \tag{37}$$

Recall the overall outage probability for the MIMO best relay scheme can be expressed as

$$\begin{aligned} P(\mathcal{I} \le 2R) &= \sum_{k=1}^{L} P\left(\mathcal{I}_k < 2R\right)P(K=k) \\ &\quad + P\left(\mathcal{I}_{pp} < 2R\right)P(K=0), \end{aligned} \tag{38}$$

where $P\left(\mathcal{I}_{pp} < 2R\right)$ can be expressed as

$$P\left(\mathcal{I}_{pp} < 2R\right) \doteq \rho^{-[(N-M-2r)(N-2r)]},$$

due to the use of the orthogonal projection matrix. Combining (34), (37) and (38), the achievable diversity-multiplexing tradeoff can be obtained and the theorem is proved. ■

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, July 2010.

[3] F. Oggier and B. Hassibi, "The MIMO wiretap channel," in *Proc. IEEE International Symposium on Information Theory (ISIT-09)*, Jul. 2008.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[5] T. Liu and S. S. (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Nov. 2009.

[6] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[7] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, pp. 137 – 155, May 2011.

[8] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. 2008 Global Telecommunication Conference*, Dec. 2008.

[9] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[10] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 51, pp. 5003–5011, Oct. 2009.

[11] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[12] L. Zheng and D. N. C. Tse, "Diversity and multiplexing : a fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[13] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, pp. 1875 – 1888, Mar. 2010.

[14] A. Ozgur, O. Leveque, and D. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, pp. 3549 – 3572, June 2007.

[15] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, pp. 1099–1109, Aug. 2004.

[16] Z. Ding, W. Chen, and K. Leung, "Distributed beamforming and power allocation for cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 248–255, May 2008.

[17] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 659–672, Mar. 2006.

[18] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 2006 41st Annual Conference on Information Sciences and Systems*, Mar. 2007, pp. 905 – 910.
[19] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033– 4039, Sept. 2009.
[20] Z. Ding, K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1725 – 1729, Jun. 2011.
[21] K. Azarian, H. E. Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Trans. Inf. Theory*, vol. 51, pp. 4152–4172, Dec. 2005.
[22] C.-K. Li and R. Mathias, "The determinant of the sum of two matrices," *Bulletin of Australian Math. Soc.*, vol. 3, pp. 425–429, 1995.
[23] S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung;, "Multi-user diversity for secrecy in wireless networks," in *Proc. Information Theory and Applications Workshop (ITA)*, Feb. 2010.
[24] H. Sampath, P. Stoica, and A. Paulraj, "Generalized linear precoder and decoder design for mimo channels using the weighted mmse criterion," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2198–C2206, Dec. 2001.
[25] Z. Ding, Y. Gong, T. Ratnarajah, and C. Cowan, "On the performance of opportunistic cooperative wireless networks," *IEEE Trans. Commun.*, vol. 56, pp. 1236–1240, Aug. 2008.

Zhiguo Ding (S'03-M'05) received his B.Eng in Electrical Engineering from the Beijing University of Posts and Telecommunications in 2000, and the Ph.D degree in Electrical Engineering from Imperial College London in 2005. From Jul. 2005 to Jun. 2010, he was working in Queen's University Belfast, Imperial College and Lancaster University. Since Oct. 2010, he has been with Newcastle University as a Lecturer. His research interests are cross-layer optimization, cooperative diversity, statistical signal processing and information theory.

Kin K. Leung received his B.S. degree (with first-class honors) from the Chinese University of Hong Kong in 1980, and his M.S. and Ph.D. degrees in computer science from University of California, Los Angeles, in 1982 and 1985, respectively.

He started his career at AT&T Bell Labs in 1986 and worked at its successor companies, AT&T Labs and Bell Labs of Lucent Technologies, until 2004. Since then, he has been the Tanaka Chair Professor in Internet Technology at Imperial College in London. His research interests include network resource allocation, MAC protocol, TCP/IP protocol, distributed optimization algorithms, mobility management, network architecture, real-time applications and teletraffic issues for broadband wireless networks, wireless sensor and ad-hoc networks. He is also interested in a wide variety of wireless technologies, including IEEE 802.11, 802.16, and 3G and future generation cellular networks.

Dennis Goeckel split time between Purdue University and Sundstrand Corporation from 1987-1992, receiving his BSEE from Purdue in 1992. From 1992-1996, he was a National Science Foundation Graduate Fellow and then Rackham Pre-Doctoral Fellow at the University of Michigan, where he received his MSEE in 1993 and his Ph.D. in 1996, both in Electrical Engineering with a specialty in Communication Systems. In September 1996, he joined the Electrical and Computer Engineering department at the University of Massachusetts, where he is currently a Professor. His current research interests are in the areas of communication systems and wireless network theory.

Don Towsley holds a B.A. in Physics (1971) and a Ph.D. in Computer Science (1975) from University of Texas. He is currently a Distinguished Professor at the University of Massachusetts in the Department of Computer Science. He has held visiting positions at IBM T.J. Watson Research Center, Yorktown Heights, NY; Laboratoire MASI, Paris, France; INRIA, Sophia-Antipolis, France; AT&T Labs - Research, Florham Park, NJ; and Microsoft Research Lab, Cambridge, UK. His research interests include networks and performance evaluation.

He currently serves as Editor-in-Chief of *IEEE/ACM Transactions on Networking*, and on the editorial boards of *Journal of the ACM* and *IEEE Journal on Selected Areas in Communications* and has previously served on numerous other editorial boards. He was Program Co-chair of the joint ACM SIGMETRICS and PERFORMANCE '92 conference and the Performance 2002 conference. He is a member of ACM and ORSA.

He has received the 2007 IEEE Koji Kobayashi Award, the 2007 ACM SIGMETRICS Achievement Award, the 1998 IEEE Communications Society William Bennett Best Paper Award, and numerous conference/workshop best paper awards. Last, he has been elected Fellow of both the ACM and IEEE.