MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Secrecy Rate Analysis of Jamming Superposition in Presence of Many Eavesdropping Users

Koike-Akino, T.; Duan, C.

TR2011-080 December 2011

Abstract

It has been shown that the secrecy capacity of a wireless network is pushed rapidly towards zero as the number of users in the network grows. To deal with this issue, a secure method which intentionally superposes precoded jamming signals has been proposed. In this paper, we analyze its advantage to realize a secure wireless network in the presence of a large number (e.g., hundreds) of eavesdropping users, for transmitting confidential messages. Our analysis and simulations demonstrate that the jamming superposition achieves high secrecy rate even for undesired cases where the channels for many eavesdroppers are noise-less and highly correlated with the intended receiver.

IEEE Global Telecommunication Conference (GLOBECOM)

Secrecy Rate Analysis of Jamming Superposition in Presence of Many Eavesdropping Users

Toshiaki Koike-Akino and Chunjie Duan
Mitsubishi Electric Research Laboratories (MERL), 201 Broadway, Cambridge, MA 02139, U.S.A.
Email: {koike, duan}@merl.com

***Abstract*—It has been shown that the secrecy capacity of a wireless network is pushed rapidly towards zero as the number of users in the network grows. To deal with this issue, a secure method which intentionally superposes precoded jamming signals has been proposed. In this paper, we analyze its advantage to realize a secure wireless network in the presence of a large number (e.g., hundreds) of eavesdropping users, for transmitting confidential messages. Our analysis and simulations demonstrate that the jamming superposition achieves high secrecy rate even for undesired cases where the channels for many eavesdroppers are noise-less and highly correlated with the intended receiver.**

I. Introduction

Since the introduction of information-theoretic security by Shannon [1], there have emerged a lot of studies on secrecy capacity [2–25]. As wireless communication systems are susceptible to eavesdropping due to the broadcast nature of radio wave propagations, a significant amount of effort has been put into improving the physical-layer security. In order to achieve high data-rate while keeping a private message secret from eavesdroppers, it basically requires higher signal-to-noise power ratio (SNR) at the intended user than at eavesdroppers [2]. In [8–11], it was shown that positive secrecy capacity is obtained in fading channels even when the eavesdropper has higher average SNR than the intended user, because the instantaneous SNR of the intended user can exceed that of the eavesdropper with a certain probability. However, for multi-user Rayleigh fading channels where there are a lot of potential eavesdroppers, it was found that high secrecy capacity is hard to achieve even with the best user scheduling [12]. For such cases, the secrecy capacity saturates at a constant low data-rate even in the high SNR regimes because the best eavesdropper considerably constrains the secrecy rate.

When the radio devices at the transmitter and/or the receivers are equipped with multiple antennas, the secrecy capacity can be increased by steering the main beam to the intended user and the nulls to the eavesdroppers as discussed in [21]. However, this technique requires accurate channel state information (CSI) of the eavesdroppers and therefore is impractical for applications. Moreover, it is impossible to null the signal to more eavesdroppers than the number of antennas. Negi and Goel proposed a practical method to solve such issues in [22–24], wherein a jamming noise is superposed with confidential data so that only the intended user can decode it while the other eavesdroppers suffer from artificial noise by making use of dirty-paper-coding (DPC) [25].

In this paper, we make a statistical analysis of the jamming superposition scheme and demonstrate that it significantly outperforms the conventional approaches in the secrecy rate for the wireless networks, in which there exist a large number of eavesdropping users (e.g., hundreds of users) who can have higher SNRs (even with infinite SNRs) and whose CSIs are not available to both the transmitter and the intended receiver. The contribution of this paper includes our analysis of the impact on the secrecy rate by the channel correlation among multiple users, the number of eavesdroppers, the number of antennas, and the channel estimation error.

Notations: Throughout the paper, we denote matrices and vectors by bold-face italic letters in upper cases and lower cases, respectively. Let $\boldsymbol{X} \in \mathbb{C}^{m\times n}$ be a complex-valued $(m \times n)$-dimensional matrix, where $\mathbb{C}$ denotes the complex field. The notations $\boldsymbol{X}^*$, $\boldsymbol{X}^{\mathrm{T}}$, $\boldsymbol{X}^{\dagger}$, $\boldsymbol{X}^{-1}$, $\boldsymbol{X}^{1/2}$, $\det[\boldsymbol{X}]$, and $\|\boldsymbol{X}\|$ represent complex conjugate, transpose, Hermite transpose, inverse, square-root, determinant, and Frobenius norm of $\boldsymbol{X}$, respectively. The operator $\mathrm{vec}[\boldsymbol{X}]$ denotes the vector operation which stacks all columns of $\boldsymbol{X}$ into a single column vector in a left-to-right fashion, and the operator $\otimes$ stands for the Kronecker product of two matrices. We have a relation of $\mathrm{vec}[\boldsymbol{XYZ}] = (\boldsymbol{Z}^{\mathrm{T}} \otimes \boldsymbol{X})\mathrm{vec}[\boldsymbol{Y}]$ for matrices $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{Z}$ of appropriate size. A positive-integer ring from 1 to m is represented by $\mathbb{N}_m \triangleq \{1, 2, \ldots, m\}$. $\boldsymbol{I}_m$ is an m-dimensional identity matrix. A multivariate complex-valued Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Sigma}$ is denoted by $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$. A positive operator is written by $(x)_+ \triangleq \max(0, x)$, and the expectation is represented by $\mathbb{E}[\cdot]$.

II. Secure Wireless Communications

A. Wireless Network System Model

We consider a wireless network with K users and one base station, as shown in Fig. 1. One user wishes to receive some confidential data from the base station. Due to the broadcast nature of radio propagations, all other $K-1$ users are treated as potential eavesdroppers. Without loss of generality, we let the k-th user ($k \in \mathbb{N}_K$) be the one who wishes to download the private message, while the other $K-1$ users (for any user index $j \in \mathbb{N}_K \setminus \{k\}$) are considered possible eavesdroppers.

We assume that the base station is equipped with M antennas and each user is equipped with N antennas. We focus on passive eavesdroppers who do not maliciously attack the communicating pair (such as tamper, impairing jammer and impersonation). Our goal is to analyze achievable data-rate

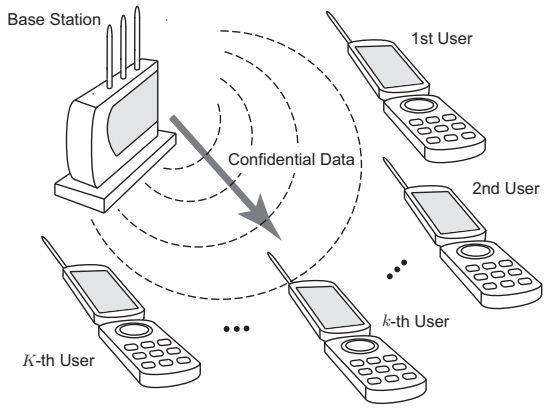

Fig. 1. Wireless communications network with one base station and K users. The k-th user wishes to receive confidential information which shall not be decoded by the other $K-1$ users.

for transmitting confidential messages towards the intended user while any eavesdroppers cannot decode the data by using the DPC jamming [22–25], with a consideration of many eavesdroppers, channel correlation, and CSI estimation error.

The CSI from the base station to the i-th user is denoted by $\boldsymbol{H}_i \in \mathbb{C}^{N\times M}$ for any user index $i \in \mathbb{N}_K$. For slow fading channels, it can be assumed that the uplink channel from the i-th user to the base station is reciprocal to the downlink channel during a time of interest, namely, the CSI from the i-th user to the base station is written as $\boldsymbol{H}_i^\dagger$. We also make a practical assumption that the base station has no CSI knowledge of any eavesdropping users. In addition, the channel gains of eavesdroppers can surpass that of the intended user, i.e., $\|\boldsymbol{H}_j\|^2 > \|\boldsymbol{H}_k\|^2$ for a certain $j \in \mathbb{N}_K \setminus \{k\}$.

We assume each user's channel is a correlated Rayleigh fading, whose probability distribution is Gaussian:

$$\boldsymbol{h}_i \triangleq \mathrm{vec}[\boldsymbol{H}_i] \sim \mathcal{CN}\big(\boldsymbol{0}, \boldsymbol{\Psi}_i\big), \tag{1}$$

where $\boldsymbol{\Psi}_i \triangleq \mathbb{E}\big[\boldsymbol{h}_i\boldsymbol{h}_i^\dagger\big]$ is a channel covariance for the user $i \in \mathbb{N}_K$. The channels between two users, k and j, are mutually correlated as $\boldsymbol{\Theta}_{k,j} \triangleq \mathbb{E}\big[\boldsymbol{h}_k\boldsymbol{h}_j^\dagger\big]$, where $\boldsymbol{\Theta}_{k,j} \in \mathbb{C}^{MN\times MN}$ is a cross-correlation matrix. Hence, we can express

$$\begin{bmatrix}\boldsymbol{h}_k\\ \boldsymbol{h}_j\end{bmatrix} = \begin{bmatrix}\boldsymbol{\Psi}_k & \boldsymbol{\Theta}_{k,j}\\ \boldsymbol{\Theta}_{k,j}^\dagger & \boldsymbol{\Psi}_j\end{bmatrix}^{1/2}\begin{bmatrix}\boldsymbol{n}_k\\ \boldsymbol{n}_j\end{bmatrix}, \tag{2}$$

where $\boldsymbol{n}_k \in \mathbb{C}^{MN\times 1}$ and $\boldsymbol{n}_j \in \mathbb{C}^{MN\times 1}$ are random variables following the Gaussian distribution $\mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}_{MN})$. After some manipulations, we can write the channel of the j-th user by the channel of the intended user k as follows:

$$\boldsymbol{h}_j = \boldsymbol{\Theta}_{k,j}^\dagger\boldsymbol{\Psi}_k^{-1}\boldsymbol{h}_k + \big(\boldsymbol{\Psi}_j - \boldsymbol{\Theta}_{k,j}^\dagger\boldsymbol{\Psi}_k^{-1}\boldsymbol{\Theta}_{k,j}\big)^{1/2}\boldsymbol{n}_j. \tag{3}$$

This equation will be later used for secrecy analysis.

B. Secure Communication Protocol

Our transmission protocol consists of two phases.

- In an uplink phase, the intended user sends a request packet to the base station to download confidential data. The base station obtains an estimate of the CSI.
- In a downlink phase, the base station transmits the confidential data superposed with a random jamming signal which is confined on the null-space of the user channel.

1) Channel Sounding in Request Uplink Phase: To initiate the secure downlink transmissions, the intended user k sends a request packet, which contains a training sequence to allow the base station to estimate the CSI, $\boldsymbol{H}_k$, for coherent detections. We model the received signal at the base station as follows:

$$\boldsymbol{Y} = \boldsymbol{H}_k^\dagger\boldsymbol{X}_k + \boldsymbol{Z} \in \mathbb{C}^{M\times L}, \tag{4}$$

where $\boldsymbol{X}_k \in \mathbb{C}^{N\times L}$, $\boldsymbol{Y} \in \mathbb{C}^{M\times L}$ and $\boldsymbol{Z} \in \mathbb{C}^{M\times L}$ are the uplink packet with L symbols, the received signal and the additive Gaussian signals, respectively. We can rewrite (4) in a vector representation as follows:

$$\boldsymbol{y} = (\boldsymbol{I}_M \otimes \boldsymbol{X}_k^\dagger)\boldsymbol{h}_k + \boldsymbol{z} \in \mathbb{C}^{LM\times 1}, \tag{5}$$

where $\boldsymbol{y} \triangleq \mathrm{vec}[\boldsymbol{Y}^\dagger]$ and $\boldsymbol{z} \triangleq \mathrm{vec}[\boldsymbol{Z}^\dagger]$.

The conditional probability of $\boldsymbol{y}$ given $\boldsymbol{X}_k$ and $\boldsymbol{h}_k$ follows the Gaussian distribution:

$$\boldsymbol{y} \mid \boldsymbol{X}_k, \boldsymbol{h}_k \sim \mathcal{CN}\big((\boldsymbol{I}_M \otimes \boldsymbol{X}_k^\dagger)\boldsymbol{h}_k, \boldsymbol{\Sigma}\big), \tag{6}$$

where $\boldsymbol{\Sigma} \triangleq \mathbb{E}\big[\boldsymbol{z}\boldsymbol{z}^\dagger\big] \in \mathbb{C}^{LM\times LM}$ denotes the noise covariance at the base station. With the statistical knowledge, the maximum *a posteriori* (MAP) estimation of the channel $\boldsymbol{h}_k$ at the base station is obtained as

$$\hat{\boldsymbol{h}}_k = \boldsymbol{\Omega}(\boldsymbol{I}_M \otimes \boldsymbol{X}_k)\boldsymbol{\Sigma}^{-1}\boldsymbol{y}, \tag{7}$$

where $\boldsymbol{\Omega} \in \mathbb{C}^{MN\times MN}$ is the estimation error covariance:

$$\begin{aligned}\boldsymbol{\Omega} &\triangleq \mathbb{E}\big[(\boldsymbol{h}_k - \hat{\boldsymbol{h}}_k)(\boldsymbol{h}_k - \hat{\boldsymbol{h}}_k)^\dagger\big]\\ &= \Big((\boldsymbol{I}_M \otimes \boldsymbol{X}_k)\boldsymbol{\Sigma}^{-1}(\boldsymbol{I}_M \otimes \boldsymbol{X}_k^\dagger) + \boldsymbol{\Psi}_k^{-1}\Big)^{-1}.\end{aligned} \tag{8}$$

This MAP estimate achieves the Cramér-Rao bound for the unbiased estimation of Rayleigh fading channels.

Using the estimation error covariance $\boldsymbol{\Omega}$, we can model the estimated channel with error as follows:

$$\hat{\boldsymbol{h}}_k = \boldsymbol{h}_k + \boldsymbol{\Omega}^{1/2}\boldsymbol{n}, \tag{9}$$

where $\boldsymbol{n} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}_{NM})$ is a white Gaussian random variable. This expression will be later used for secrecy analysis to consider the CSI estimation error.

2) Jammer Superposition in Secure Downlink Phase: Upon receiving the request, the base station transmits the downlink confidential data to the intended user k. To prevent eavesdropping by the other users, a precoded random jamming signal is superposed with the confidential data using DPC techniques. Note that the jamming signal is not known by anyone including the intended user.

With the DPC jamming, the base station transmits

$$\boldsymbol{X}' = \boldsymbol{Q}\boldsymbol{X} + \boldsymbol{P}\boldsymbol{W} \in \mathbb{C}^{M\times L'}, \tag{10}$$

where $\boldsymbol{Q} \in \mathbb{C}^{M\times D}$ and $\boldsymbol{P} \in \mathbb{C}^{M\times M}$ are linear precoding matrices for the desired data and for the jammer, respectively. The confidential data packet is denoted as $\boldsymbol{X} \in \mathbb{C}^{D\times L'}$, and the random jamming signal is written by $\boldsymbol{W} \in \mathbb{C}^{M\times L'}$, where

L' is the downlink packet length in symbol. The number of multiplexing streams D is set to be $D \leq N$ since we have $\mathrm{rank}[\boldsymbol{H}_k] = N$ almost surely for Rayleigh fading channels.

We assume Gaussian-distributed signaling for both the data packet and the superposed jamming:

$$\boldsymbol{x} \triangleq \mathrm{vec}[\boldsymbol{X}] \sim \mathcal{CN}\big(\boldsymbol{0}, \boldsymbol{I}_{DL'}\big), \tag{11}$$

$$\boldsymbol{w} \triangleq \mathrm{vec}[\boldsymbol{W}] \sim \mathcal{CN}\big(\boldsymbol{0}, \boldsymbol{I}_{ML'}\big). \tag{12}$$

The total transmission power is constrained as

$$\frac{1}{L'}\mathbb{E}\big[\|\boldsymbol{X}'\|^2\big] = \mathrm{tr}\big[\boldsymbol{Q}\boldsymbol{Q}^\dagger + \boldsymbol{P}\boldsymbol{P}^\dagger\big] = E_0, \tag{13}$$

where E_0 is the average transmission power at the base station.

Based on the DPC technique, the precoding matrix $\boldsymbol{P}$ may be chosen to be orthogonal to the estimated channel matrix for the intended user, more specifically, we have

$$\hat{\boldsymbol{H}}_k \boldsymbol{P} = \boldsymbol{0}, \tag{14}$$

which can be achieved by an orthogonal projection:

$$\boldsymbol{P} = \beta\Big(\boldsymbol{I}_M - \hat{\boldsymbol{H}}_k^\dagger\big(\hat{\boldsymbol{H}}_k\hat{\boldsymbol{H}}_k^\dagger\big)^{-1}\hat{\boldsymbol{H}}_k\Big), \tag{15}$$

whose rank is $M - N$ almost surely, and whose eigenvalues are either β or zero. Here, the parameter β is a control factor of the jamming power. This projection matrix can realize a reliable link only for the intended user because of $\boldsymbol{H}_k\boldsymbol{P} \simeq \boldsymbol{0}$. The parameter β is further defined as $\beta = \beta'\sqrt{E_0/(M-N)}$ with $0 \leq \beta' \leq 1$ being the normalized power coefficient.

We may use a matched filter precoding given as

$$\boldsymbol{Q} = \alpha\hat{\boldsymbol{H}}_k^\dagger, \tag{16}$$

where $\alpha = \alpha'\sqrt{E_0}/\|\hat{\boldsymbol{H}}_k\|$ is a power control factor with $0 \leq \alpha' \leq 1$ being the normalized power for the data packet. This transmission precoder can maximize the diversity gains for the intended user. (Note that we may use other precoding methods such as optimal eigen-mode beamforming based on a singular-value decomposition). The power constraint in (13) yields

$$\alpha'^2 + \beta'^2 = 1. \tag{17}$$

The optimal power allocation for confidential data and jamming signals will be discussed later.

C. Secrecy Rate

The downlink packet received by the i-th user for any $i \in \mathbb{N}_K$ is expressed as

$$\boldsymbol{Y}_i = \boldsymbol{H}_i\boldsymbol{X}' + \boldsymbol{Z}_i = \boldsymbol{H}_i\boldsymbol{Q}\boldsymbol{X} + \boldsymbol{H}_i\boldsymbol{P}\boldsymbol{W} + \boldsymbol{Z}_i, \tag{18}$$

where $\boldsymbol{Y}_i \in \mathbb{C}^{N\times L'}$ is the received signal and $\boldsymbol{Z}_i \in \mathbb{C}^{N\times L'}$ is the additive Gaussian noise. It is rewritten in a vector form:

$$\boldsymbol{y}_i = \big(\boldsymbol{I}_{L'} \otimes \boldsymbol{H}_i\boldsymbol{Q}\big)\boldsymbol{x} + \big(\boldsymbol{I}_{L'} \otimes \boldsymbol{H}_i\boldsymbol{P}\big)\boldsymbol{w} + \boldsymbol{z}_i, \tag{19}$$

with $\boldsymbol{y}_i \triangleq \mathrm{vec}[\boldsymbol{Y}_i]$ and $\boldsymbol{z}_i \triangleq \mathrm{vec}[\boldsymbol{Z}_i]$. The first term corresponds to the desired data, whereas the second term is an interference due to the superposed jamming signal.

The mutual information between the received signal $\boldsymbol{y}_i$ and the confidential data $\boldsymbol{x}$ given $\boldsymbol{H}_i$, $\boldsymbol{P}$ and $\boldsymbol{Q}$ is written as

$$\begin{aligned} R_i &\triangleq \mathcal{I}(\boldsymbol{y}_i; \boldsymbol{x} \mid \boldsymbol{H}_i, \boldsymbol{P}, \boldsymbol{Q}) \\ &= \log\Big|\boldsymbol{I}_{NL'} + \big((\boldsymbol{I}_{L'} \otimes \boldsymbol{H}_i\boldsymbol{P}\boldsymbol{P}^\dagger\boldsymbol{H}_i^\dagger) + \boldsymbol{\Sigma}_i\big)^{-1} \\ &\qquad \big(\boldsymbol{I}_{L'} \otimes \boldsymbol{H}_i\boldsymbol{Q}\boldsymbol{Q}^\dagger\boldsymbol{H}_i^\dagger\big)\Big|, \end{aligned} \tag{20}$$

where $\boldsymbol{\Sigma}_i \triangleq \mathbb{E}\big[\boldsymbol{z}_i\boldsymbol{z}_i^\dagger\big] \in \mathbb{C}^{NL'\times NL'}$ is the noise covariance at the user i, and $\mathcal{I}(\cdot)$ denotes the conditional mutual information. The secrecy rate [2, 3, 17] averaged over the possible channel realizations is then expressed as

$$R_{\mathrm{S}} = \mathop{\mathbb{E}}_{\{\boldsymbol{H}_i\}}\Big[\Big(R_k - \max_{j\in\mathbb{N}_K\setminus\{k\}} R_j\Big)_+\Big]. \tag{21}$$

It implies that the intended user k should have higher signal-to-interference-plus-noise power ratio (SINR) than any eavesdroppers to achieve a positive secrecy rate.

III. Secrecy Rate Analysis

According to the previous section, we can numerically analyze the secrecy rate for the correlated Rayleigh fading. To obtain more viable insights, we focus on a specific channel condition to analyze the achievable secrecy rate.

A. Specific Channel Model

We focus on a channel model:

$$\boldsymbol{\Sigma} = \sigma^2\boldsymbol{I}_L \otimes \boldsymbol{I}_M, \qquad \boldsymbol{\Sigma}_i = \sigma_i^2\boldsymbol{I}_{L'} \otimes \boldsymbol{I}_N, \quad \boldsymbol{X}_k\boldsymbol{X}_k^\dagger = L\boldsymbol{I}_N,$$
$$\boldsymbol{\Psi}_i = \psi_i^2\boldsymbol{I}_M \otimes \boldsymbol{I}_N, \quad \boldsymbol{\Theta}_{k,j} = \theta_{k,j}\boldsymbol{I}_M \otimes \boldsymbol{I}_N,$$

where σ^2, σ_i^2, ψ_i^2, and $\theta_{k,j}$ are the noise variance at the base station, the noise variance at the i-th user, the channel gains of the i-th user, and the channel cross-correlation between users k and j, respectively. Let $\theta'_{k,j} \triangleq \theta_{k,j}/\psi_k\psi_j$ be the normalized correlation, whose value is bounded by $0 \leq |\theta'_{k,j}|^2 \leq 1$.

For this case, using (3), (8) and (9), we can write

$$\boldsymbol{\Omega} = \Big(\frac{L}{\sigma^2} + \frac{1}{\psi_k^2}\Big)^{-1}\boldsymbol{I}_M \otimes \boldsymbol{I}_N \triangleq \omega^2\boldsymbol{I}_M \otimes \boldsymbol{I}_N,$$
$$\hat{\boldsymbol{H}}_k = \boldsymbol{H}_k + \omega\boldsymbol{\mathcal{N}},$$
$$\boldsymbol{H}_j = \frac{\theta^*_{k,j}}{\psi_k^2}\hat{\boldsymbol{H}}_k + \sqrt{\psi_j^2 - \frac{(\psi_k^2 - \omega^2)|\theta_{k,j}|^2}{\psi_k^4}}\boldsymbol{\mathcal{N}}'_j,$$
$$R_i = L'\log\Big|\boldsymbol{I}_N + \big(\boldsymbol{H}_i\boldsymbol{P}\boldsymbol{P}^\dagger\boldsymbol{H}_i^\dagger + \sigma_i^2\boldsymbol{I}_N\big)^{-1}\boldsymbol{H}_i\boldsymbol{Q}\boldsymbol{Q}^\dagger\boldsymbol{H}_i^\dagger\Big|.$$

Here, $\boldsymbol{\mathcal{N}} \in \mathbb{C}^{N\times M}$ and $\boldsymbol{\mathcal{N}}'_j \in \mathbb{C}^{N\times M}$ have unit-variance white Gaussian random variables. In consequence, we can express the channel for any user $i \in \mathbb{N}_K$ as follows:

$$\boldsymbol{H}_i = a_i\hat{\boldsymbol{H}}_k + b_i\boldsymbol{\mathcal{N}}'_i, \tag{22}$$

where

$$a_i = \begin{cases} 1, & i = k, \\ \theta'^*_{k,i}\psi_i/\psi_k, & i \neq k, \end{cases} \tag{23}$$

$$b_i = \begin{cases} -\sigma\psi_k/\sqrt{\sigma^2 + L\psi_k^2}, & i = k, \\ \psi_i\sqrt{1 - \big(1 - \sigma^2/(\sigma^2 + L\psi_k^2)\big)|\theta'_{k,i}|^2}, & i \neq k. \end{cases} \tag{24}$$

B. Single-Antenna Case

We may consider the case where each user is equipped with a single antenna ($N = 1$). For this case, we have

$$\boldsymbol{H}_i\boldsymbol{Q} = \alpha\Big(a_i\big\|\hat{\boldsymbol{H}}_k\big\|^2 + b_i\boldsymbol{\mathcal{N}}'_i\hat{\boldsymbol{H}}_k^\dagger\Big), \tag{25}$$

$$\boldsymbol{H}_i\boldsymbol{P} = b_i\boldsymbol{\mathcal{N}}'_i\boldsymbol{P}. \tag{26}$$

Here, $\boldsymbol{H}_i\boldsymbol{Q}$ given $\hat{\boldsymbol{H}}_k$ follows a complex Gaussian distribution, $\mathcal{CN}(\alpha a_i\|\hat{\boldsymbol{H}}_k\|^2, \alpha^2 b_i^2\|\hat{\boldsymbol{H}}_k\|^2)$. We can express

$$\begin{aligned}\boldsymbol{H}_i\boldsymbol{Q}\boldsymbol{Q}^\dagger\boldsymbol{H}_i^\dagger &= \alpha^2|a_i|^2\big\|\hat{\boldsymbol{H}}_k\big\|^4 + \alpha^2 b_i^2\big\|\hat{\boldsymbol{H}}_k\big\|^2\frac{1}{2}\chi_2^2 \\ &\quad + 2\sqrt{\alpha^4|a_i|^2 b_i^2\big\|\hat{\boldsymbol{H}}_k\big\|^6\frac{1}{2}\chi_2^2}\cos(\phi_i), \qquad (27)\\ \boldsymbol{H}_i\boldsymbol{P}\boldsymbol{P}^\dagger\boldsymbol{H}_i^\dagger &= b_i^2\boldsymbol{\mathcal{N}}'_i\boldsymbol{P}\boldsymbol{P}^\dagger\boldsymbol{\mathcal{N}}'^\dagger_i \\ &= \frac{E_0}{2(M-1)}\beta'^2 b_i^2\chi^2_{2(M-1)}, \qquad (28)\end{aligned}$$

where χ_d^2 denotes a random variable which follows the chi-square distribution with d degrees of freedom. The angle factor ϕ_i is a uniform random variable over $0 \le \phi_i < 2\pi$.

Hence, the effective SINR at the i-th user is bounded as

$$\frac{\alpha'^2\big(|a_i|\psi_k\chi_{2M} - |b_i|\chi_2\big)^2}{\frac{2}{E_0}\sigma_i^2 + \frac{1}{M-1}\beta'^2 b_i^2\chi^2_{2(M-1)}} \le \gamma_i \le \frac{\alpha'^2\big(|a_i|\psi_k\chi_{2M} + |b_i|\chi_2\big)^2}{\frac{2}{E_0}\sigma_i^2 + \frac{1}{M-1}\beta'^2 b_i^2\chi^2_{2(M-1)}}. \tag{29}$$

Note that $\|\hat{\boldsymbol{H}}_k\|^2$ is a random variable following the chi-square distribution with $2M$ degrees of freedom: $\frac{1}{2}\chi^2_{2M}$.

C. Uncorrelated Case

We optimize the jammer power β'^2 to maximize the secrecy rate for the case where there is no channel correlation between intended receiver and eavesdroppers, i.e., $|\theta'_{k,j}| = 0$. From (29), the SINR at the eavesdropper j and the SINR at the intended user k are bounded as

$$\gamma_j \le \frac{(M-1)\alpha'^2\chi_2^2}{\beta'^2\chi^2_{2(M-1)}} = \frac{\alpha'^2}{\beta'^2}\varphi_{2,2(M-1)}, \tag{30}$$

$$\gamma_k \ge \frac{\alpha'^2\big(\psi_k\chi_{2M} - \omega\chi_2\big)^2}{\frac{2}{E_0}\sigma_k^2 + \frac{1}{M-1}\beta'^2\omega^2\chi^2_{2(M-1)}} \simeq \frac{\alpha'^2 E_0\psi_k^2}{2\sigma_k^2}\chi^2_{2M}, \tag{31}$$

where φ_{d_1,d_2} is a random variable which follows the Fisher-Snedecor F-distribution with d_1 and d_2 degrees of freedom. Here, we focus on the worst case in which the receivers are assumed of noise-free, more specifically, the noise variance at the eavesdropper σ_j^2 is infinitesimally small to be neglected.

As in (30), the instantaneous SINRs at eavesdroppers are bounded by the F-distributed random variable $\varphi_{2,2(M-1)}$, proportional to a power fraction $\eta \triangleq \alpha'^2/\beta'^2$. The cumulative distribution function (CDF) of the F-distribution is given as

$$F_{\gamma_j}(x) = 1 - \Big(\frac{\eta(M-1)}{x + \eta(M-1)}\Big)^{M-1}. \tag{32}$$

Hence, the maximum SINR amongst $K-1$ eavesdroppers, $\gamma_{\max} \triangleq \max_j\{\gamma_j\}$, has the following CDF

$$F_{\gamma_{\max}}(x) = \big(F_{\gamma_j}(x)\big)^{K-1}. \tag{33}$$

Its probability density function (PDF) is written as

$$f_{\gamma_{\max}}(x) = \sum_{i=1}^{K-1}\binom{K-1}{i}\frac{(-1)^{i+1}}{\eta}\Big(1 + \frac{x}{\eta(M-1)}\Big)^{(1-M)i-1}. \tag{34}$$

For $M \ge 3$, the mean of the maximum SINR around $K-1$ eavesdroppers is given as

$$\bar{\gamma}_{\max} \triangleq \eta\left(\frac{-\Gamma(K)\Gamma(-\frac{1}{M-1})}{\Gamma(K-\frac{1}{M-1})} - (M-1)\right), \tag{35}$$

with $\Gamma(x)$ being the gamma function. It indicates that the average maximum SINR of the eavesdroppers is proportional to the power fraction η and asymptotically proportional to $K^{1/(M-1)}$ since $\Gamma(K)/\Gamma(K-\frac{1}{M-1}) \simeq K^{1/(M-1)}$ for a large number of users, $K \gg 1$.

As in (31), the SINR at the intended user asymptotically follows the chi-square distribution with $2M$ degrees of freedom. Hence, the average SINR is obtained as

$$\bar{\gamma}_k \triangleq M\frac{\alpha'^2 E_0\psi_k^2}{\sigma_k^2}. \tag{36}$$

It suggests that the average SINR is asymptotically proportional to α'^2 for high SNR regimes. After some manipulations [21], we obtain the lower and upper bounds of the unconstrained capacity at the intended user as follows

$$\log\left(1 + \frac{M-1}{M}\bar{\gamma}_k\right) \le R_k \le \log\Big(1 + \bar{\gamma}_k\Big), \tag{37}$$

where Jensen's inequality is used for a convex function $\log(1+1/x)$ and for a concave function $\log(1+x)$, respectively. Therefore, we obtain the closed-form expression for the lower bound of the secrecy rate as follows

$$R_{\mathsf{S}} \ge \log\left(1 + \frac{M-1}{M}\bar{\gamma}_k\right) - \log\big(1 + \bar{\gamma}_{\max}\big). \tag{38}$$

The optimal power fraction $\eta = \alpha'^2/\beta'^2$, which maximizes the lower bound of the secrecy rate, is obtained as

$$\eta_{\text{opt}} = \frac{1}{1+A}\Big(\sqrt{\frac{A}{B}(1+A-B)} - 1\Big) \underset{A\to\infty}{\longrightarrow} \frac{1}{\sqrt{B}}, \tag{39}$$

where $A \triangleq (M-1)E_0\psi_k^2/\sigma_k^2$ and $B \triangleq 1 - M - \Gamma(K)\Gamma(-1/(M-1))/\Gamma(K-1/(M-1))$. Hence, the asymptotically optimal power fraction η in the high SNR regimes is determined by B only, which is a function of K and M. For example, the optimal power fraction η_{opt} becomes 0.8, 0.42, 0.25, and 0.16 for $K = 2$, 10, 100, and 1000 users, respectively, with $M = 4$ transmitting antennas. It suggests that the appropriate jamming power is comparable to the confidential message power ($\eta \cong 1$) in typical situations.

IV. Performance Evaluations

We first evaluate the impact on the secrecy rate by the total number of users, K, for an average SNR of 20 dB in Fig. 2. We assume uncorrelated Rayleigh fading channels $|\theta'_{k,j}|^2 = 0.0$, identical channel gains $\psi_1^2 = \cdots = \psi_K^2$, and identical noise

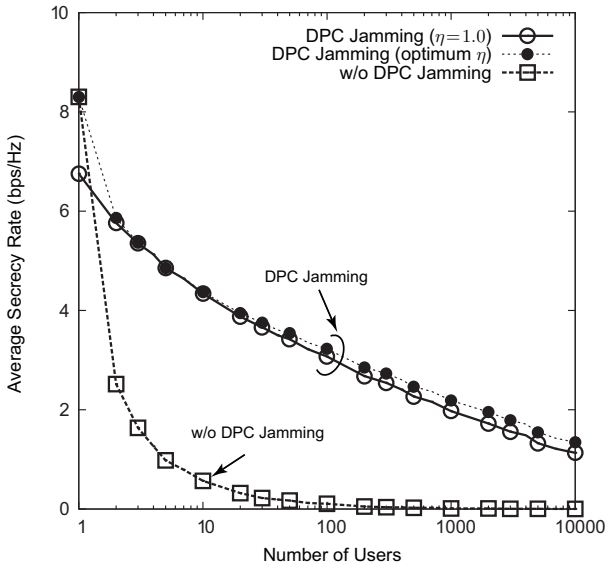

Fig. 2. Average secrecy rate versus the number of users K for a cross-correlation of $|\theta'_{k,j}|^2 = 0.0$ and an average SNR of 20 dB (the number of Tx antennas: $M = 4$, the number of Rx antennas: $N = 1$).

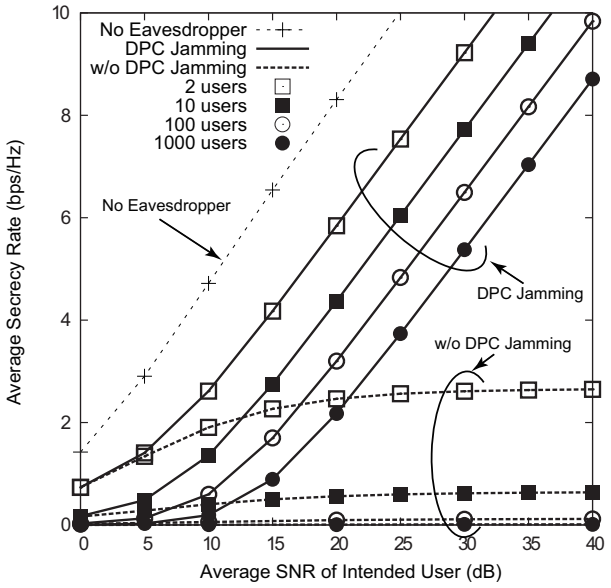

Fig. 3. Average secrecy rate as a function of average SNR of intended user for cross-correlation $|\theta'_{k,j}|^2 = 0.0$ (the number of Tx antennas: $M = 4$, the number of Rx antennas: $N = 1$, the number of users $K \in \{1, 2, 10, 100, 1000\}$, power fraction: $\eta = 1.0$).

variances $\sigma^2 = \sigma_1^2 = \cdots = \sigma_K^2$. The average SNR is defined by $E_0\psi_k^2/\sigma_k^2$. The number of transmitting antennas is $M = 4$ and that of the receiving antennas is $N = 1$. For a single-user case, the secrecy rate becomes the user capacity as there is no eavesdropper. For the conventional approach, we use matched filter precoding without jamming (i.e., $\alpha'^2 = 1$ and $\beta'^2 = 0$).

In Fig. 2, we can observe that the DPC jamming significantly outperfoms the conventional scheme. Without the DPC jamming, the secrecy rate rapidly goes to zero as the number of users increases. To achieve a data rate of 2 bps/Hz, the conventional scheme can accept only one eavesdropper (i.e., $K = 2$) whereas 1000 users can be accomodated by the jamming method. Even when there are an extremely large number of users like 10000, the jamming method achieves a positive rate higher than 1 bps/Hz. In this figure, we present the performance curves achieved by the DPC jamming schemes with optimized power fraction η and identical power allocation $\eta = 1$. One can see that the identical power allocation causes only a slight performance degradation. This fact is rather important for practical applications because we can always use the same power allocation $\eta = 1$ regardless of the total number of eavesdroppers in the wireless networks.

We next show the secrecy rate as a function of average SNR in Fig. 3, where the number of users is chosen from $K \in \{1, 2, 10, 100, 1000\}$. The unconstrained channel capacity (for $K = 1$) is plotted as a reference for the upper bound of the secrecy rate. For the DPC jamming, we use an equal power for jamming and data, i.e., $\eta = \alpha'^2/\beta'^2 = 1$. As shown in Fig. 3, the secrecy rate is seriously constrained by the existence of eavesdroppers when we use the conventional approach. The secrecy rate decreases rapidly as the number of eavesdroppers increases; the secrecy rate is less than 0.1 bps/Hz for a hundred-user system. On the other hand, it is seen that the DPC jamming significantly improves the secrecy rate by simply superposing the jamming signal to the confidential data in physical layer with only the estimated CSI of the intended user, even for network systems with 1000 users.

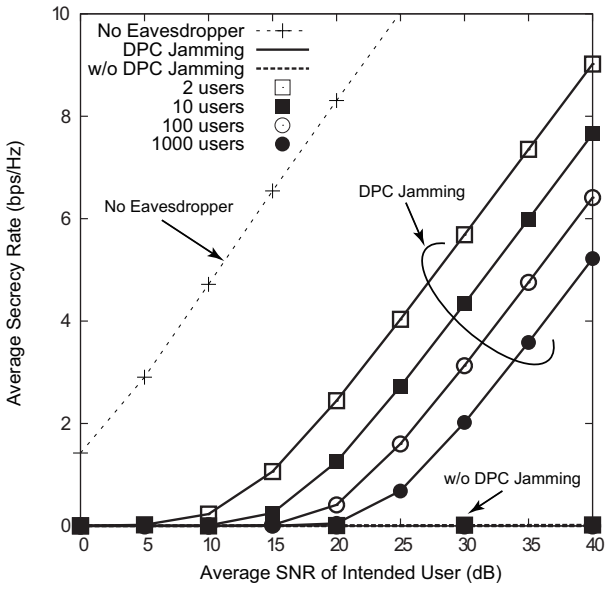

Fig. 4. Average secrecy rate as a function of average SNR of intended user for cross-correlation $|\theta'_{k,j}|^2 = 0.8$ with noise-free eavesdropping receivers (the number of Tx antennas: $M = 4$, the number of Rx antennas: $N = 1$, the number of users $K \in \{1, 2, 10, 100, 1000\}$, power fraction: $\eta = 1.0$).

The performance of the DPC jamming is expected to degrade when the channels of eavesdroppers are highly corre-

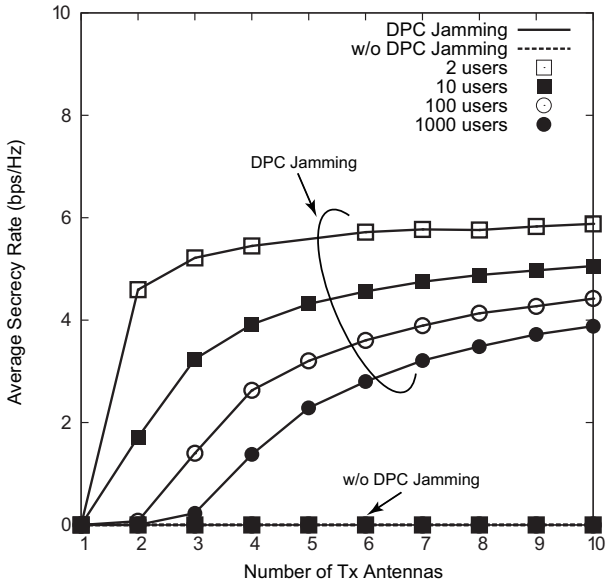

Fig. 5. Average secrecy rate versus the number of Tx antennas M at an average SNR of 30 dB for a cross-correlation of $|\theta'_{k,j}|^2 = 0.8$ with noise-free eavesdropping receivers (the number of Rx antennas: $N = 1$, the number of users $K \in \{1, 2, 10, 100, 1000\}$, power fraction: $\eta = 1.0$).

lated with that of the intended user. We evaluate this effect in Fig. 4, where we consider the worst scenario that all the eavesdroppers have idealistic noise-free receivers (namely, $\sigma_j^2 = 0$ for any eavesdropping user $j \in \mathbb{N}_K \backslash \{k\}$). The channel cross-correlation is set to be $|\theta'_{k,j}|^2 = 0.8$, which corresponds to the geometric distance between the eavesdroppers and the intended user is less than a tenth of wavelength for rich-scattering Rayleigh fading. For such a high correlation case, a considerable degradation of the secrecy rate is observed (all curves without DPC jamming for $K \in \{2, 10, 100, 1000\}$ become nearly zero) when comparing Figs. 3 and 4. However, with DPC jamming, high secrecy rate is still maintained, even when there are hundreds of eavesdroppers who have noise-free receivers. More importantly, the secrecy rate with DPC jamming improves linearly with SNR in dB for high SNRs even with CSI estimation error.

The performance degradation for highly correlated channel conditions can be compensated by increasing the number of transmitting antennas at the base station, as shown in Fig. 5. In this figure, the secrecy rate R_{S} versus the number of transmitting antennas M is presented at an average SNR of 30 dB. For the case of $K = 1000$, the secrecy rate can be improved from 1.4 bps/Hz to 3.5 bps/Hz by increasing the number of antennas from 4 to 8, with the jamming method. In contrast, the conventional beamforming approach does not enjoy any visible gains with the increased number of antennas.

V. Summary

In this paper, we analyzed a secrecy rate of DPC jamming superposition which can improve secrecy rate for transmitting confidential messages without being decoded by eavesdroppers. Our analysis verified that the DPC jamming is advantageous in practice as it preserves high secrecy rate of wireless networks, even for the cases where the number of eavesdroppers is extremely large, the eavesdroppers have highly correlated channels with the intended receiver, and the CSI estimation error for precoding exists.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, pp. 656–715, 1949.

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

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. IT*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. IT*, vol. 32, no. 3, pp. 387–393, May 1986.

[5] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. IT*, vol. 35, no. 3, pp. 572–578, May 1989.

[6] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. IT*, vol. 37, no. 3, pp. 634–638, May 1991.

[7] Y. Oohama, "Coding for relay channels with confidential messages," *IEEE ITW*, 2001.

[8] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channels with multiple eavesdroppers," *IEEE ISIT*, June 2007.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. IT*. vol. 54, no. 6, 2008.

[10] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *IEEE ISIT*, July 2006.

[11] Y. Liang and V. Poor, "Secure communication over fading channels," *Allerton Conf. Commun., Contr., Comput.*, Sept. 2006.

[12] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," *IEEE MILCOM*, Oct. 2009.

[13] L. Zang, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," *Allerton Conf. Commun., Contr., Comput.*, Sept. 2006.

[14] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. IT*, vol. 54, no. 6, June 2008.

[16] Y. Liang and V. Poor, "Generalized multiple access channels with confidential messages," *IEEE ISIT*, 2006.

[17] Y. Liang, G. Kramer, V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Networking*, pp. 1–12, 2009.

[18] R. Liu, I. Marić, R. D. Yates, and P. Spasojević, "The discrete memoryless multiple access channel with confidential messages," *IEEE ISIT*, July 2006.

[19] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. IT*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[20] 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. IT*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.

[21] T. Koike-Akino, A. F. Molisch, C. Duan, Z. Tao, and P. Orlik, "Capacity, MSE and secrecy analysis of linear block precoding for distributed antenna systems in multi-user frequency-selective fading channels," *IEEE Trans. Commun.*, vol. 59, no. 3, pp. 888–900, Mar. 2011.

[22] R. Negi and S. Goel, "Secret communication using artificial noise," *IEEE VTC-Fall*, 2005.

[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[24] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," *IEEE MILCOM*, 2006.

[25] C. Mitrpant, A. J. H. C. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. IT*, vol. 52, no. 5, pp. 2181–2190, 2006.