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

Secrecy Performance Analysis of Distributed CDD based Cooperative Systems with Jamming

Kim, K.J.; Liu, H.; Renzo, M.D.; Orlik, P.V.; Poor, H.V.

TR2018-053 July 10, 2018

Abstract

In this paper, a cooperative cyclic-prefixed single carrier (CP-SC) system to improve physical layer security is investigated. By considering a distributed cyclic delay diversity dCDD) scheme, a jamming method is proposed to maximize the signal-to-noise ratio (SNR) over the channels from the transmitters to the legitimate user, while degrading the signal-tointerference-plus-noise ratio (SINR) over the channels from the transmitters to the illegitimate user. A CDD transmitter among the set of CDD transmitters is selected as the sentinel transmitter, and it transmits a jamming signal to the illegitimate user. The sentinel transmitter is the transmitter that provides the best channel gain in order to maximize the SNR at the legitimate user and minimize the SINR at the non-legitimate users. This allow us to enhance the security of the CP-SC system. New closed form expressions for the SNR and SINR for the dCDD protocol are derived for frequency selective fading channels. Monte-Carlo simulations are conducted to verify the analytic derivations of the performance metrics for various simulation scenarios.

IEEE International Conference on Communications (ICC)

Secrecy Performance Analysis of Distributed CDD based Cooperative Systems with Jamming

Kyeong Jin Kim, Hongwu Liu, Marco Di Renzo, Philip V. Orlik, and H. Vincent Poor

***Abstract*—In this paper, a cooperative cyclic-prefixed single carrier (CP-SC) system to improve physical layer security is investigated. By considering a distributed cyclic delay diversity (dCDD) scheme, a jamming method is proposed to maximize the signal-to-noise ratio (SNR) over the channels from the transmitters to the legitimate user, while degrading the signal-to-interference-plus-noise ratio (SINR) over the channels from the transmitters to the illegitimate user. A CDD transmitter among the set of CDD transmitters is selected as the sentinel transmitter, and it transmits a jamming signal to the illegitimate user. The sentinel transmitter is the transmitter that provides the best channel gain in order to maximize the SNR at the legitimate user and minimize the SINR at the non-legitimate users. This allow us to enhance the security of the CP-SC system. New closed form expressions for the SNR and SINR for the dCDD protocol are derived for frequency selective fading channels. Monte-Carlo simulations are conducted to verify the analytic derivations of the performance metrics for various simulation scenarios.**

***Index Terms*—Distributed single carrier system, physical layer security, distributed cyclic delay diversity, sentinel transmitter, frequency selective fading.**

I. Introduction

In a non-secure cooperative system, a signal targeting a legitimate user (LR) or an intended user can be intercepted by an illegitimate user or an eavesdropper (ER). To maximize the communication range, the transmitters may use a maximum transmission power. However, since the signal power propagates isotropically in space, any users within the communication range can intercept the signal. Thus, securing data transmission over wireless networks is a challenging problem and has attracted considerable recent attention [1]–[6]. Relay selection was investigated in [1] to enhance physical layer security. The authors in [2] investigated multiuser scheduling to improve physical layer security. Transmit antenna selection was investigated in [3] for security enhancement. Several cooperative relaying schemes including decode-end-forward (DF) and amplify-and-forward (AF) were proposed in [4]. For physical layer security perspective, cyclic-prefixed single carrier (CP-SC) transmissions was investigated in [5] and [6].

K. J. Kim and P. V. Orlik are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA 02139 USA

H. Liu is with Shandong Jiatong University, Jinan, China

M. D. Renzo is with the Laboratoire des Signaux et Systèmes, CNRS, CentraleSupélec, Univ Paris Sud, Université Paris-Saclay, 3 rue Joliot Curie, Plateau du Moulon, 91192, Gif-sur-Yvette, France

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA

This work was supported in part by the U.S. National Science Foundation under Grants CCF-1420575 and ECCS-1647198, and by the Agence Nationale de la Recherche Scientifique (ANR) through the research project SpatialModulation (Société de l'Information et de la Communication – Action Plan 2015).

As one promising approach for improving physical layer security, jamming has been proposed in [4], [7]–[13]. The main idea is to degrade the quality of the received signal, that is, the signal-to-interference-plus-noise ratio (SINR) over the channels from the transmitters to the eavesdroppers, whereas increasing a desired signal-to-noise ratio (SNR) over the channels from the transmitters to the legitimate user. To this purpose, a jamming signal is transmitted to the eavesdroppers. Especially, a cooperative jamming scheme was proposed in [4] and [7]. In [8], [9], an artificial noise is transmitted to eavesdroppers. A source cooperation aided opportunistic jamming scheme was proposed by [10]. In [11], two relay nodes are opportunistically selected for assisting the relaying and jamming the eavesdropper, respectively. Similarly, a joint relay and jammer selection was proposed in [12]. It is shown that the intentional jamming can greatly improve security. Recently, jamming techniques have been applied in [13] to enhance physical layer security for DF full-duplex relay networks.

Although explicit channel feedback enables the central unit (CU) and cooperative transmitters to choose an appropriate transmission mode, for example, maximum ratio transmission (MRT) [14], [15], and achieve a higher scheduling gain [16], the channel state information (CSI) can be easily intercepted by the eavesdropper. Thus, explicit CSI feedback is not preferable in developing a system to increase physical layer security.

As a cooperative transmission scheme, distributed cyclic delay diversity (dCDD) was proposed in [17] for CP-SC transmissions. A sufficient condition was identified to convert the multi-input single-output (MISO) channel into an ISI-free single-input single-output (SISO) channel without causing ISI between CDD transmitters [18]. For CP-SC transmissions, it is shown that the maximum achievable diversity gain can be achieved. By capitalizing on the benefits of dCDD that does not require explicit CSI feedback, we propose to choose a sentinel transmitter that transmits jamming signal to the ER from the set of CDD transmitters.

A. Contribution

To the best of our knowledge, the dCDD scheme has never been applied to a cooperative CP-SC system taking account the issue of protecting the transmission from illegitimate eavesdropping. Thus, the main contributions of this paper include:

1) We provide a systematic procedure for choosing the sentinel transmitter among the set of CDD transmitters. The proposed joint transmitter and jammer selection is somewhat similar to those of [11], [12]. However, our joint selection is proposed under the framework of dCDD.

2) We investigate the impact of dCDD operation on the secrecy outage probability.
3) We derive a closed-form expression for the secrecy outage probability in frequency selective fading channels. Compared with [5] and [6], the proposed CP-SC system employs dCDD.

Notation: The superscript $(\cdot)^T$ denotes transposition; $E\{\cdot\}$ denotes expectation; $\boldsymbol{I}_N$ is an $N\times N$ identity matrix; $\mathbf{0}$ denotes an all zeros matrix of appropriate dimensions; $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes the complex Gaussian distribution with the mean μ and the variance σ^2; $\mathbb{C}^{m\times n}$ denotes the vector space of all $m\times n$ complex matrices; $F_{\varphi}(\cdot)$ denotes the cumulative distribution function (CDF) of the random variable (RV) φ, whereas its probability density function (PDF) is denoted by $f_{\varphi}(\cdot)$; The binomial coefficient is denoted by $\binom{n}{k}\triangleq\frac{n!}{(n-k)!k!}$. The lth element of a vector $\boldsymbol{a}$ is denoted by $\boldsymbol{a}(l)$.

II. System and Channel Model

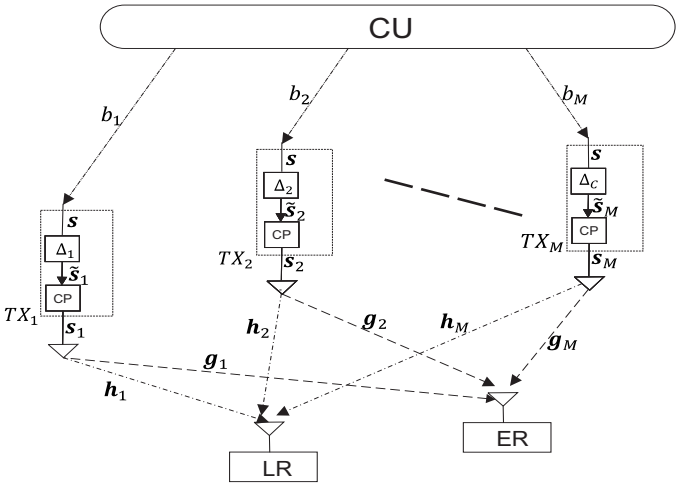

Fig. 1. Block diagram of the considered dCDD-based cooperative physical layer system connected to the CU via ideal backhaul. A set of M cooperative transmitters communicates with the LR via a set of legitimate channels $\{\boldsymbol{h}_m,\ \forall m\}$. Wireless communication between the transmitters and the LR can be intercepted by the ER via a set of illegitimate channels $\{\boldsymbol{g}_m,\forall m\}$. Single antenna transmitters are assumed considering the hardware complexity as in the remote radio head (RRH).

A block diagram of the considered cooperative single carrier system is provided in Fig. 1. The CU provides broadband wireless access with an ideal backhaul connections to M transmitters $\{\mathrm{TX}_m,\ \forall m\}$. Cooperative communications are realized between the transmitters and LR in the presence of an ER. To protect confidential information from being illegitimately intercepted by the ER, one of the CDD transmitters is selected as a sentinel transmitter to transmit a jamming signal to the ER. To increase the received SNR at the LR, dCDD is employed between the transmitters and ER by the control of the CU.

By applying a channel sounding, which estimates the channel impulse response, or CSI, the LR is assumed to have knowledge of the number of multipath components across the channels from the transmitters to itself. Thus, the CU can compute the maximum number of transmitters for CDD operation. We assume that the ER is an active user, so that CSI from the transmitters to ER can be monitored by the CU [4]. Since the ER does not require to explicit CSI feedback, a data interception which mainly uses CSI for its eavesdropping can be reduced. For CP-SC transmissions, the CP length, N_p, can be determined to remove ISI as

$$N_p \geq \max\{N_{h,1},\ldots,N_{h,M}\} \tag{1}$$

where $N_{h,m}$ denotes the number of multipath components of a frequency fading channel $\boldsymbol{h}_m$. The CDD delay, Δ_m, for the mth CDD transmitter is determined as

$$\Delta_m = (m-1)N_p \tag{2}$$

which makes it possible to convert the MISO channel into an ISI-free SISO channel. From (1) and (2), the maximum number of CDD transmitters is limited by

$$K = 1 + \left\lfloor \frac{Q}{N_p} \right\rfloor \tag{3}$$

where $\lfloor\cdot\rfloor$ denotes the floor function with respect to the symbol block size, Q, and N_p. Especially, in this paper, we are interested in the case of $M\leq K$, that is, all the transmitters are used as CDD transmitters.

A. dCDD Operation

For the M CDD transmitters, the CU forms a table for CDD delays, $\mathbb{X}_{\Delta}\triangleq\{0,\Delta_1,\ldots,\Delta_{M-1}\}$. It then assigns a particular CDD delay Δ_m to a CDD transmitter. When a different CDD delay is assigned to a CDD transmitter, the same receiver performance can be obtained [17].

The mth CDD transmitter applies its CDD delay Δ_m to the original input symbol block $\boldsymbol{s}\in\mathbb{C}^{Q\times 1}$, which is expressed as $\tilde{\boldsymbol{s}}_m=\boldsymbol{P}_Q^{\Delta_m}\boldsymbol{s}$, where $\boldsymbol{P}_Q^{\Delta_m}$ is the orthogonal permutation matrix obtained by circularly shifting down the identity matrix $\boldsymbol{I}_Q$ by Δ_m. To obtain ISI-free CP-SC transmissions, $\boldsymbol{P}_Q^{\Delta_m}$ needs to be right circulant as well.

In this paper, we mainly investigate the following two questions with dCDD processing.

$$\begin{aligned} Q_1 &: \text{How should one CDD transmitter be chosen as the sentinel transmitter?} \\ Q_2 &: \text{What are the effects of a propose selection of a sentinel transmitter on dCDD operation?} \end{aligned} \tag{4}$$

B. Selection of the Sentinel Transmitter

For the M CDD transmitters, the CU has the knowledge of $\|\boldsymbol{g}_m\|^2$, a frequency selective fading channel from the mth transmitter to ER. The channel magnitude can be measured as $b_m\|\boldsymbol{g}_m\|^2$, so that the CU has M channel magnitudes as

$$b_{(1)}\|\boldsymbol{g}_{(1)}\|^2 \leq \ldots \leq b_{(M)}\|\boldsymbol{g}_{(M)}\|^2. \tag{5}$$

From this knowledge, the CU can choose the transmitter having the largest channel magnitude as the sentinel CDD transmitter. The remaining transmitters acts as data CDD

transmitters. Since the ER channels are independent of the LR channels, a list of data CDD transmitters keeps changing depending on the ER channels. Let s^* denote the index of the sentinel transmitter in the sequel.

C. Received Signals at the ER and LR

Without loss of generality, we assume that TX_m applies Δ_m for the CDD delay. For the cyclically shifted symbol block $\tilde{\boldsymbol{s}}_m$, a CP of N_p symbols is appended to the front of $\tilde{\boldsymbol{s}}_m$, resulting $\boldsymbol{s}_m \triangleq \begin{bmatrix} \tilde{\boldsymbol{s}}_m(Q-N_p+1:Q,1) \\ \tilde{\boldsymbol{s}}_m \end{bmatrix} \in \mathbb{C}^{(Q+N_p)\times 1}$ is transmitted sequentially to the LR via a frequency selective fading channel $\boldsymbol{h}_m$. After the removal of the CP signal, the received signal at the LR is given by

$$\tilde{\boldsymbol{r}}_L = \sum_{m=1,m\neq s^*}^{M} \sqrt{P_T\alpha_h}\boldsymbol{H}_m\boldsymbol{P}_Q^{\Delta_m}\boldsymbol{s} + \sqrt{P_J\alpha_h}\boldsymbol{H}_{s^*}\boldsymbol{P}_Q^{\Delta_{s^*}}\boldsymbol{J} + \boldsymbol{z}_L \tag{6}$$

where P_T and P_J are the transmission powers for data and jamming signals. An additive vector noise over the LR channels is given by $\boldsymbol{z}_L \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_Q)$. Additionally, α_h models large scale fading. Right circulant matrices are denoted by $\{\boldsymbol{H}_m, \forall m, m \neq s^*\}$ and $\boldsymbol{H}_{s^*}$, which are mainly specified by $\{\boldsymbol{h}_m, \forall m, m \neq s^*\}$ and $\boldsymbol{h}_{s^*}$ with additional zeros to make them have a length Q. A jamming symbol, $\boldsymbol{J} \in \mathbb{C}^{Q\times 1}$, can be composed of pseudorandom or noise-like symbols. We also assume that $E\{\boldsymbol{J}\} = \boldsymbol{0}$, and $\{\boldsymbol{J}\boldsymbol{J}^H\} = \boldsymbol{I}_Q$.

Since the jamming symbol is known both at the CU and LR, (6) can be expressed as follows:

$$\boldsymbol{r}_L = \sum_{m=1,m\neq s^*}^{M} \sqrt{P_T\alpha_h}\boldsymbol{H}_m\boldsymbol{P}_Q^{\Delta_m}\boldsymbol{s} + \boldsymbol{z}_L. \tag{7}$$

Since the product of two right circulant matrices is another right circulant matrix, and the right circulant matrix is specified by the first column vector, we further express (7) as:

$$\boldsymbol{r}_L = \boldsymbol{H}_{\mathrm{CDD},s^*}\boldsymbol{s} + \boldsymbol{z}_L \tag{8}$$

where the first column vector of $\boldsymbol{H}_{\mathrm{CDD},s^*}$ is given by

$$\begin{aligned}\boldsymbol{h}_{\mathrm{CDD},s^*} \triangleq \sqrt{P_T\alpha_h}\Big[&(\boldsymbol{h}_1)^T, \boldsymbol{0}_{1\times(N_p-N_h)}, (\boldsymbol{h}_2)^T, \\ &\boldsymbol{0}_{1\times(N_p-N_h)}\ldots, (\boldsymbol{h}_{s^*-1})^T, \\ &\boldsymbol{0}_{1\times(N_p-N_h)}, (\boldsymbol{h}_{s^*+1})^T, \\ &\boldsymbol{0}_{1\times(N_p-N_h)}, \ldots, (\boldsymbol{h}_M)^T, \boldsymbol{0}_{1\times(N_p-N_h)}\Big]^T\end{aligned} \tag{9}$$

Now the received signal at the ER is given by

$$\begin{aligned}\boldsymbol{r}_E &= \sum_{m=1,k\neq s^*}^{M} \sqrt{P_T\alpha_g}\boldsymbol{G}_m\boldsymbol{P}_Q^{\Delta_m}\boldsymbol{s} + \sqrt{P_J\alpha_g}\boldsymbol{G}_{s^*}\boldsymbol{P}_Q^{\Delta_{s^*}}\boldsymbol{J} + \boldsymbol{z}_E \\ &= \boldsymbol{G}_{\mathrm{CDD},s^*}\boldsymbol{s} + \sqrt{P_J\alpha_g}\boldsymbol{G}_{s^*}\boldsymbol{P}_Q^{\Delta_{s^*}}\boldsymbol{J} + \boldsymbol{z}_E\end{aligned} \tag{10}$$

where $\boldsymbol{G}_{\mathrm{CDD},s^*}$ and $\boldsymbol{G}_{s^*}$ are right circulant matrices specified by an equivalent channel vector $\boldsymbol{g}_{\mathrm{CDD},s^*}$ and $\boldsymbol{g}_{s^*}$. Note that $\boldsymbol{g}_{\mathrm{CDD},s^*}$ can be specified as $\boldsymbol{h}_{\mathrm{CDD},s^*}$. An additive vector noise over the ER channels is given by $\boldsymbol{z}_E \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_Q)$.

III. Performance Analysis

To investigate the performance of the proposed physical layer security that makes the sentinel transmitter send a jamming signal under dCDD processing, we need to know the distributions for the respective receive SNRs at the LR and ER.

A. Distribution of the Receive SNR at the LR

In contrast to the dCDD system, in which $M > K$, the receive SNR with dCDD operation is the summation of the receive SNR without selection process, that is, it is not necessary to use order statistics. However, when $M > K$, it is necessary to use order statistics. With identically distributed frequency selective fading channels, the receive SNR at the LR is given by [17]

$$\gamma_R = \sum_{m=1,m\neq s^*}^{M} \gamma_{R,m} \tag{11}$$

where $\gamma_{R,m} \triangleq \tilde{\alpha}_h \sum_{l=1}^{N_h} |\boldsymbol{h}_m(l)|^2$ with $\tilde{\alpha}_h \triangleq \frac{P_T\alpha_h}{\sigma_z^2}$. Since $\tilde{\alpha}_h \sum_{l=1}^{N_h} |\boldsymbol{h}_m(l)|^2$ is distributed as $\tilde{\alpha}_h \sum_{l=1}^{N_h} |\boldsymbol{h}_m(l)|^2 \sim \chi^2(2N_h, \tilde{\alpha}_h)$, whose PDF and CDF are respectively expressed by the following:

$$\begin{aligned} f_{\gamma_{R,m}}(x) &= \frac{1}{\Gamma(N_h)(\tilde{\alpha}_h)^{N_h}} x^{N_h-1}e^{-\frac{x}{\tilde{\alpha}_h}} \text{ and} \\ F_{\gamma_{R,m}}(x) &= 1 - e^{-\frac{x}{\tilde{\alpha}_h}} \sum_{l=0}^{N_h-1} \frac{1}{l!}\Big(\frac{x}{\tilde{\alpha}_h}\Big)^l \end{aligned} \tag{12}$$

we can have $\gamma_R \sim \chi^2(2N_h(M-1), \tilde{\alpha}_h)$.

B. Distribution of the Receive SNR at the ER

The receive signal power and noise-and-interference power due to jamming at the ER are given by

$$\begin{aligned} S_E &= P_T \sum_{m=1,m\neq s^*}^{M} \alpha_g \sum_{l=1}^{N_g} |\boldsymbol{g}_m(l)|^2 \text{ and} \\ N_E &= P_J\alpha_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{s^*}(l)|^2 + \sigma_z^2. \end{aligned} \tag{13}$$

Since the ER is not able to decode a jamming signal, S_E is a summation of the signal power aggregated from $M-1$ CDD transmitters. Since the channel that provides the largest channel magnitude is selected by the sentinel transmitter, we can increase the ratio of S_R to S_E/N_E as the number of CDD transmitters increases, which is beneficial in protection confidentiality of the cooperative system.

According to (13), the signal-to-interference-plus-noise ratio (SINR) at the ER is given by

$$\gamma_E = \frac{S_E}{N_E} = \frac{S_E/\sigma_z^2}{N_E/\sigma_z^2} = \frac{\tilde{\alpha}_g \sum_{m=1}^{M-1}\sum_{l=1}^{N_g} |\boldsymbol{g}_{(m)}(l)|^2}{\gamma_I\tilde{\alpha}_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{(M)}(l)|^2 + 1} \tag{14}$$

where $\tilde{\alpha}_g \triangleq \frac{P_T\alpha_g}{\sigma_z^2}$ and $\gamma_I \triangleq \frac{P_J}{P_T}$. Note that we have used order statistics in the representation of (14). Since the sum of order statistics $\tilde{\alpha}_g \sum_{m=1}^{M-1}\sum_{l=1}^{N_g} |\boldsymbol{g}_{(m)}(l)|^2$ is dependent of

the maximum order statistics $\tilde{\alpha}_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{(M)}(l)|^2$, it is not straightforward to compute the distribution of the SINR, γ_E. Thus, the closed-form expression for the SINR is provided in the following theorem.

Theorem 1: For identical frequency selective fading over illegitimate channels, the distribution of the receive SINR at the ER, aggregated by $M-1$ CDD transmitters while degraded by the sentinel transmitter that uses a channel that has the largest channel magnitude over the ER channels, is given by (15) in the next page.

Proof: Due to the space limitation, we skip the derivation. Applying order statistics to derive the joint PDF, and some manipulations, we can readily derive the final expression. ■

Theorem 1 shows that the PDF of the receive SINR at the ER is expressed by the weighted summations of either lower incomplete gamma functions or gamma functions. We can also see that three equations compose (15), two of which are easy to use in the performance analysis.

C. Secrecy Outage Probability

The transmission capacity achieved by legitimate transmissions is given by

$$C_R = \log_2(1+\gamma_R) \tag{16}$$

whereas the interceptable capacity is defined as [3]:

$$C_E = \log_2(1+\gamma_E). \tag{17}$$

Then, the secrecy capacity C_s is defined as follows:

$$C_s = [C_R - C_E]^+. \tag{18}$$

When the data transmission is inferred by the ER, a secrecy outage event occurs and the perfect secrecy is compromised [3]. At a given secrecy rate R_s, the secrecy outage probability is defined by

$$\begin{aligned} P_{out}(R_s) &= Pr(C_s < R_s) \\ &= \int_0^\infty F_{\gamma_R}(J(1+x)-1) f_{\gamma_E}(x) dx \end{aligned} \tag{19}$$

where $J_R \triangleq 2^{R_s}$. Now since $F_R(x)$ and $f_{\gamma_E}(x)$ are available, the closed form expression for the secrecy outage probability, $P_{out}(R_s)$, can be derived.

Theorem 2: For frequency selective fading over legitimate and illegitimate channels, the proposed CP-SC system which uses physical layer security via dCDD and sentinel transmitter provides the secrecy outage probability at secrecy rate R_s, which is given by (20) at the next page. In (20), $G_{p,q}^{m,n}\left(t \middle| \begin{matrix} a_1,...,a_n,a_{n+1},...,a_p \\ b_1,...,b_m,b_{m+1},...,b_q \end{matrix}\right)$ denotes the Meijer G-function [19, eq. (9.301)]. Due to complex representation for the second equation in (15), $P_{out,2}(R_s)$ is numerically obtained.

Proof: Due to the space limitation, we skip the derivation. However, with some manipulations, we can readily derive the final expression. ■

D. Asymptotic Diversity Gain Analysis

As was investigated by [5] and [6], an asymptotic diversity gain on the secrecy outage probability is mainly determined by the channels connecting the LR.

Lemma 1: From the receive SNR at the LR, the diversity gain of the secrecy outage probability is given by

$$G_d = (M-1)N_h. \tag{22}$$

Proof: Based on the approach [5], [6], we can derive this gain after some manipulations. ■

Note that one CDD transmitter is selected as sentinel transmitter, so that only $(M-1)$ CDD transmitters are involved in the diversity gain.

IV. Simulation

In the simulations, we first verify the derived closed form expression for the secrecy outage probability. To this, we compared the derived secrecy outage probability (denoted by **An**) with the exact secrecy outage probability (denoted by **Ex**). And then, we show the secrecy outage probability for various scenarios taking account various parameters, for example, frequency selectivity, transmitter cooperation, and γ_I, the jamming power ratio over to the data transmission power. In the simulations, we set $R_s = 1$ and $\gamma_I = 3$ dB.

In Fig. 2, we verify the derived secrecy outage probability comparing with the exact secrecy outage probability for various cases. We can see good matching between them. As the number of CDD transmitters increases, a lower secrecy outage probability obtained due to a larger diversity gain.

In Fig. 3, we verify the diversity gain on the secrecy outage probability via an asymptotically derived outage probability (denoted by **As**). From different cases, $G_d = (M-1)N_h$, can be verified from the $\log - \log$ domain. An increased number of CDD transmitters or a large number of multipath components results in a lower outage probability due to a larger diversity gain. We can see that N_g does not affect the diversity gain.

In Fig. 4, we investigate the impacts of γ_I on the secrecy outage probability. For $M = 4, N_h = 2, N_g = 4$, this figure shows that a larger jamming power over the data transmission power results in a lower secrecy outage probability.

In Fig. 5, we compare the secrecy outage probability of the proposed sentinel transmitter selection comparing with other selections, for example assign a transmitter providing either the second best channel magnitude or the least channel magnitude. From this figure, the proposed selection for the sentinel transmitter leads to achieve the best secrecy outage probability performance.

V. Conclusions

In this paper, we have proposed a new physical layer secrecy system that employs dCDD and a sentinel transmitter. Over the CDD transmitters, one CDD transmitter that provides the best channel magnitude to the ER is selected by the CU to send a jamming signal. For various scenarios, the proposed secrecy system has achieved improved secrecy performance with a slight loss in diversity gain by increasing the receive SNR at the LR while decreasing the receive SINR at the ER.

$$f_{\gamma_E}(x) = \frac{M}{\Gamma(N_g)\Gamma((M-1)N_g)\tilde{\alpha}_g^{MN_g}} \sum_{p_1=0}^{(M-1)N_g} \binom{(M-1)N_g}{p_1} \gamma_I^{p_1} \Gamma(N_g+p_1)$$
$$x^{(M-1)N_g-1}\Big(\frac{1}{\tilde{\alpha}_g}+\frac{\gamma_I x}{\tilde{\alpha}_g}\Big)^{-N_g-p_1} e^{-x/\tilde{\alpha}_g} + \sum_{n=1}^{M-1}\binom{M-1}{n}(-1)^n \sum_{\substack{q_1,\ldots,q_{N_g} \\ q_1+\ldots+q_{N_g}=n}} \frac{n!}{q_1!q_2!\ldots q_{N_g}!} \prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}$$
$$\frac{Me^{-x/\tilde{\alpha}_g}}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}\Gamma((M-1)N_g-\tilde{q})} \begin{cases} f_1, \text{ if } \gamma_I x - n < 0 \\ f_2, \text{ if } \gamma_I x - n \geq 0 \end{cases} \tag{15}$$

where

$$f_1 \stackrel{\triangle}{=} \sum_{p_1=0}^{1} \sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1} \sum_{p_3=0}^{p_2} \binom{1}{p_1}\binom{(M-1)N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\gamma_I^{p_1+p_3}(-n)^{(M-1)N_g-\tilde{q}-p_2-1}$$
$$x^{p_2}((1+\gamma_I x)/\tilde{\alpha}_g)^{-c_1}\gamma_l\Big(c_1, \frac{x(1+\gamma_I x)}{\tilde{\alpha}_g(n-\gamma_I x)}\Big) \text{ and}$$
$$f_2 \stackrel{\triangle}{=} \sum_{p_1=0}^{1} \sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1} \sum_{p_3=0}^{p_2} \binom{1}{p_1}\binom{(M-1)N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\gamma_I^{p_1+p_3}(-n)^{(M-1)N_g-\tilde{q}-p_2-1}$$
$$x^{p_2}((1+\gamma_I x)/\tilde{\alpha}_g)^{-c_1}\Gamma(c_1)$$

with $c_1 \stackrel{\triangle}{=} MN_g + p_1 - p_2 + p_3 - 1$ and $\tilde{q} \stackrel{\triangle}{=} \sum_{t=0}^{N_g-1} t q_{t+1}$.

$$P_{out}(R_s) = P_{out,1}(R_s) + P_{out,2}(R_s) + P_{out,3}(R_s) \tag{20}$$

where

$$P_{out,1}(R_s) \stackrel{\triangle}{=} M - Me^{-(JR-1)/\tilde{\alpha}_h} \sum_{l=0}^{(M-1)N_h} \sum_{m=0}^{l} \sum_{p_1=0}^{(M-1)N_g} \binom{l}{m}\binom{(M-1)N_g}{p_1} \frac{\gamma_I^{p_1}\tilde{\alpha}_g^{p_1+N_g}(JR-1)^{l-m}JR^m}{\Gamma(l+1)\tilde{\alpha}_h^l\Gamma(N_g)\Gamma((M-1)N_g)\tilde{\alpha}_g^{MN_g}}$$
$$\Big(\frac{1}{\tilde{a}_g}+\frac{JR}{\tilde{a}_h}\Big)^{-(M-1)N_g-m} G_{2,1}^{1,2}\Big(\frac{\gamma_I\tilde{\alpha}_g\tilde{\alpha}_h}{\tilde{\alpha}_h+\tilde{\alpha}_g JR}\Big| \begin{matrix} 1-(M-1)N_g-m, 1-N_g-p_1 \\ 0 \end{matrix}\Big),$$
$$P_{out,3}(R_s) \stackrel{\triangle}{=} -(M-1) + Me^{-(JR-1)/\tilde{\alpha}_h} \sum_{n=1}^{M-1}\binom{M-1}{n}(-1)^n \sum_{\substack{q_1,\ldots,q_{N_g} \\ q_1+\ldots+q_{N_g}=n}} \frac{n!}{q_1!q_2!\ldots q_{N_g}!} \prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}$$
$$\frac{1}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}} \sum_{p_1=0}^{1} \sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1} \sum_{p_3=0}^{p_2} \binom{1}{p_1}\binom{(M-1)N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3} \sum_{l=0}^{(M-1)N_h-1} \sum_{m=0}^{l} \sum_{p=0}^{m+p_2}$$
$$\binom{m+p_2}{p}\binom{l}{m} \frac{\gamma_I^{p_1+p_3}(JR-1)^{l-m}JR^m\tilde{\alpha}_g^{c_1}(-n)^{c_2}(1+n)^{c_1}(n/\gamma_I)^{m+p_2-p}}{\Gamma(l+1)\tilde{\alpha}_h^l}\Big(\frac{1}{\tilde{a}_g}+\frac{JR}{\tilde{a}_h}\Big)^{-1-p}$$
$$e^{-n/\gamma_I\left(\frac{1}{\tilde{a}_g}+\frac{JR}{\tilde{a}_h}\right)} G_{2,1}^{1,2}\Big(n\gamma_I\Big(\frac{1}{\tilde{a}_g}+\frac{JR}{\tilde{a}_h}\Big)\Big| \begin{matrix} -p, 1-c_1 \\ 0 \end{matrix}\Big) \frac{1}{\Gamma((M-1)N_g-\tilde{q})} \tag{21}$$

with $c_2 \stackrel{\triangle}{=} (M-1)N_g - \tilde{q} - p_2 - 1$.

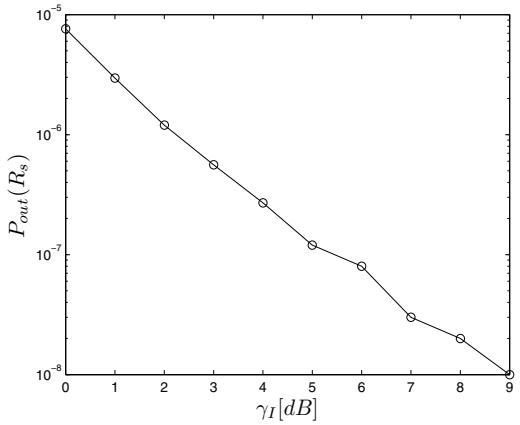

Fig. 4. Secrecy outage probability for various values of γ_I.

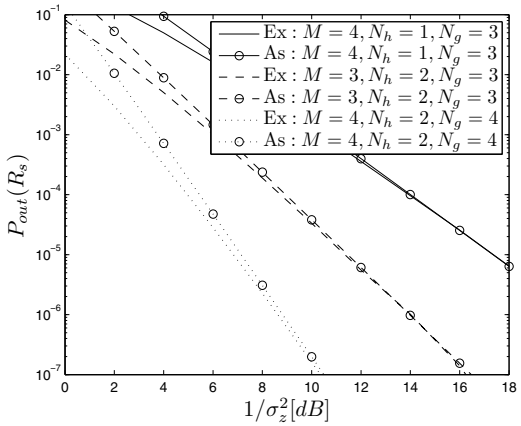

Fig. 3. Secrecy outage probability for various values of M, N_h, and N_g.

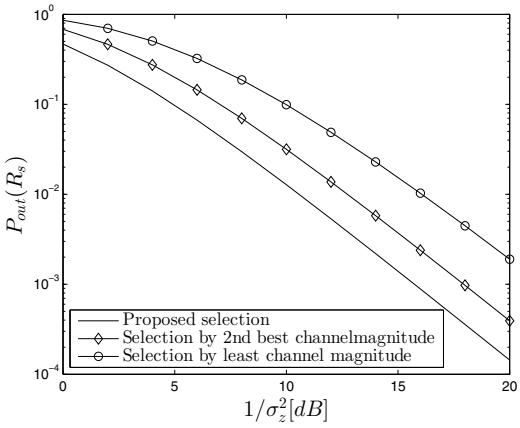

Fig. 5. Secrecy outage probability for three selection methods of the sentinel transmitter for $M = 3$, $N_h = 1$, and $N_g = 3$.

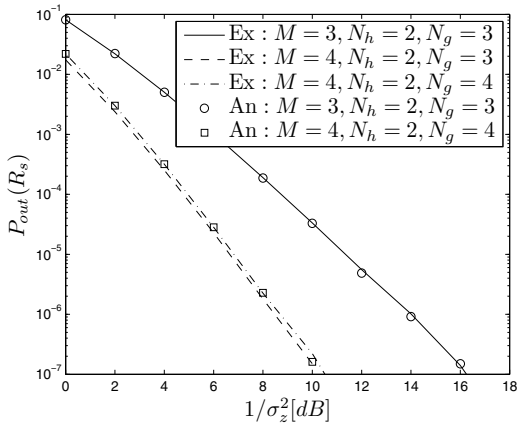

Fig. 2. Secrecy outage probability for various values of M, N_h, and N_g.

REFERENCES

[1] F. Al-Qahtani, C. Zhong, and H. Ainuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, pp. 1756–1770, May 2015.

[2] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio," *IEEE Trans. Commun.*, vol. 61, pp. 5103–5113, Dec. 2013.

[3] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperative relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[5] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90–103, Jan. 2015.

[6] K. J. Kim, P. L. Yeoh, P. Orlik, and H. V. Poor, "Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4403–4416, Spet. 2016.

[7] S. I. Kim, I. M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, Jul. 2015.

[8] G. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jul. 2008.

[9] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 2189–2203, Apr. 2014.

[10] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, 2017, under reviewing.

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

[12] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for sequre two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[13] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[14] T. K. Y. Lo, "Maximum ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.

[15] K. J. Kim, T. Khan, and P. Orlik, "Performance analysis of cooperative systems with unreliable backhauls and selection combining," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2448–2461, Mar. 2017.

[16] B. Clerckx, G. Kim, J. Choi, and Y.-J. Hong, "Elicit vs. implicit feedback for SU and MU-MIMO," in *Proc. IEEE Global Commun. Conf.*, Miami, FL, Dec. 2010, pp. 1–5.

[17] K. J. Kim, M. D. Renzo, H. Liu, P. V. Orlik, and H. V. Poor, "Performance analysis of distributed single carrier systems with distributed cyclic delay diversity," *IEEE Trans. Commun.*, 2017, under publication.

[18] D. Wang and S. Fu, "Asynchronous cooperative communications with stbc coded single carrier block transmission," in *Proc. IEEE Global Commun. Conf.*, Washington, DC, Nov. 2007, pp. 2987–2991.

[19] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York: Academic Press, 2007.