Secrecy Analysis of Distributed CDD-Based Cooperative Systems with Deliberate Interference

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 is studied and a scheme to improve its physical layer security is proposed. In particular, a distributed cyclic delay diversity (dCDD) scheme is employed and a deliberate interfering method is introduced, which degrades the signal-to-interference-plus-noise ratio (SINR) over the channels from a group of remote radio heads (RRHs) to an eavesdropper, while minimizing the signal-to-noise ratio loss over the channels from the RRHs to an intended user. This is obtained by selecting one RRH that acts as an interfering RRH and transmits an interfering artificial noise sequence to the eavesdropper. Through the use of the dCDD scheme, a channel that minimizes the receive SINR at the eavesdropper is selected for the interfering RRH. This choice enhances the secrecy rate of the CP-SC system. The system performance is evaluated by considering the secrecy outage probability and the probability of non-zero achievable secrecy rate, which are formulated in a closed-form analytical expression for identically and non-identically distributed frequency selective fading channels. Based on the proposed analytical framework, in addition, the diversity order of the system is studied. Monte Carlo simulations are employed to verify the analytical derivations for numerous system scenarios.**

***Index Terms*—Distributed single carrier systems, physical layer security, distributed cyclic delay diversity, secrecy outage probability, probability of non-zero achievable secrecy rate.**

I. Introduction

It is necessary to enhance physical layer security between legitimate terminals from the broadcast nature of radio channels. In this light, we investigate the physical layer security of a cooperative wireless system that employes the distributed transmit diversity scheme, in which several remote radio heads (RRHs) are connected with a central control unit (CU) via reliable backhaul connections. In non-secure cooperative systems, a signal targeting a legitimate user (LU) or an intended user can be intercepted by a non-legitimate user or an eavesdropping user (EU). To maximize the communication range, the RRHs that constitute the cooperative system 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 attention [2]–[7]. Secure communication systems can be realized only if the signal quality of the LU's communication link is better than the signal quality of the EUs' communication links. Otherwise, the EUs can intercept the legitimate transmission at the physical layer.

Although explicit channel feedback enables the CU and cooperative RRHs to choose an appropriate transmission mode, e.g., maximum ratio transmission (MRT) [8], [9], and achieve a higher scheduling gain [10], the channel state information (CSI) can be easily intercepted by the EU to lessen the effectiveness of physical layer security. Thus, the explicit feedback of CSI is not an adequate choice for increasing the physical layer security. Motivated by these considerations, the authors of [11] proposed to use the distributed cyclic delay diversity (dCDD) scheme for application to cyclic prefixed-single carrier (CP-SC) transmissions, since it does not require the explicit feedback of the CSI. The dCDD scheme is capable of increasing the signal quality at the LU. To achieve this performance, sufficient conditions to convert a multi-input single-output (MISO) channel into an intersymbol interference (ISI)-free single-input single-output (SISO) channel without causing ISI among the RRHs were identified [12]. It was proved that the maximum achievable diversity order can be achieved for CP-SC transmissions by receiving the multiple copies of the same transmission symbol. However, the EU also receives the multiple copies of the same transmission symbol, so that the receive signal-to-noise ratio (SNR) at the EU will be increased. Thus, the original dCDD scheme is not fit to the physical layer security system.

Jamming has been proposed as a promising approach for improving the physical layer security [3], [13]–[18]. The main idea is to degrade the quality of the signal received at the EU, i.e., the signal-to-interference-plus-noise ratio (SINR) of the channels from the RRHs to the EUs without affecting the desired SNR over the channels from the RRHs to the LU. To this end, an intentional jamming signal, which can be decoded only by the LU, is embedded into the transmitted signal. A cooperative jamming scheme was proposed in [3] and [13]. A source cooperation-aided opportunistic jamming scheme was proposed in [16]. In [17], two relay nodes are opportunistically selected for assisting relaying operations and jamming the EU, respectively. A joint relay and jamming selection scheme was proposed in [18]. For point-to-point secrecy communication systems with multiple jamming sources and EUs, an optimal power allocation scheme was proposed and its secrecy outage probability was studied in [19]. As for multiuser downlink transmission schemes, the authors of [20] investigated a power

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

H. Liu is with Shandong Jiaotong 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.

Parts of this paper were presented at the 2018 IEEE International Conference on Communications [1].

allocation scheme between the information signal and the artificial noise (AN) under perfect and imperfect CSI scenarios. Under the assumption that multiple relays are available in the system, the authors of [21] investigated optimal distributed jamming schemes that maximize the secrecy rate. A game theoretic approach was proposed in [22], which optimizes the secrecy performance of wireless networks with selfish jamming. As for spectrum sharing systems, cooperative jamming was proposed to decrease the intercept probability in [16]. It is shown that intentional jamming can greatly improve the secrecy performance. Recently, jamming techniques have been applied in [23] to enhance the physical layer security of full-duplex relay networks. In [24], lower and upper bounds on the secrecy capacity of multi-carrier systems were established in the context of multiple parallel relay channels. It has been shown that the secrecy capacity of the multi-carrier system can be achieved if each subchannel achieves its own secrecy capacity by secrecy coding or jamming [24]–[26].

There are two possible methods to generate the AN. In the first method, the AN is generated in the null space of the legitimate channels. Thus, AN-based jamming interferes only with the EU without interfering with the LU. Although an equivalent channel matrix can be derived at the LU, its null space does not exist. As an alternative method, we could use a sequence, for example, Zadoff-Chu sequence [1] [27], [28] as the AN sequence (ANS), known only at the CU and LU. By capitalizing on the benefits of the dCDD scheme, we propose to modify the dCDD scheme by assigning one of the RRHs as an interfering RRH, which transmits the ANS to the EU, an approach that enhances the physical layer security. With the unique strength of dCDD, the interfering RRH interferes only with the EU without affecting the LU.

A. Contribution

To the best of our knowledge, the dCDD scheme has never been applied to cooperative CP-SC systems (and to any other communication systems) with the objective of protecting the transmission from illegitimate EUs. Thus, the main contributions made by the present paper include the following:

1) We introduce a systematic procedure for choosing the interfering RRH. The proposed joint data RRHs and interfering RRH selection is somewhat similar to the solution introduced in [16]–[18]. The main difference is that it has never been considered in the context of dCDD operation. Without the explicit feedback of legitimate channels' CSI, the SNR at the LU can be increased compared with the simpler selection scheme proposed by [17] and [18], thanks to the use of the dCDD scheme. Note that since the EU can intercept this explicit feedback to lower the secrecy level, it is desirable to avoid this feedback type from physical layer security perspective. In addition, the SINR at the EU can be significantly reduced compared with [16]. This is possible by first choosing a channel for the interfering RRH that minimizes the SINR over the EU channels, and then by applying the dCDD scheme, over the LU channels, to the remaining RRHs. Thus, the proposed interfering RRH selection scheme in the context of the dCDD scheme decreases the SINR at the EU, while minimizing the SNR loss at the LU. Note that since exact CSI for the legitimate channels is not available, the interfering RRH is selected first to minimize the SINR, and then data RRHs are selected from the remaining set of RRHs.
2) We introduce an analytical framework to study the physical layer security of the proposed scheme. The analytical framework is applicable to identically distributed frequency-selective channels for the EUs and non-identically distributed frequency-selective channels for the LU. A new analytical expression for the SINR at the EU is introduced and its probability density function (PDF) is derived. Based on these new findings, a closed-form expression for the secrecy outage probability is obtained. To shed light on the system performance, approximated analytical expressions for the secrecy outage probability and probability of non-zero achievable secrecy rate are computed.
3) With the aid of asymptotic analysis, the diversity order of the system is derived. It is proved that the physical layer security can be improved at the cost of reducing the diversity order. In particular, we show that the reduction of diversity order that is due to using one of the RRHs as the interfering RRH is usually acceptable, especially if the channels of the EUs are identically distributed.

The rest of the paper is organized as follows. In Section II, the system and channel models are introduced. The dCDD scheme is summarized and the method for selecting the interfering RRH is described. In Section III, the receive SNR and SINR at the LU and EU, respectively, are computed. Furthermore, the secrecy outage probability is studied. Simulation results are illustrated in Section IV and conclusions are drawn in Section V.

Notation: The superscript $(\cdot)^T$ denotes transposition; $E\{\cdot\}$ denotes expectation; $\boldsymbol{I}_N$ denotes an $N \times N$ identity matrix; $\mathbf{0}$ denotes an all-zero matrix of appropriate size; $\mathcal{CN}\left(\mu, \sigma^2\right)$ denotes a complex Gaussian distribution with mean μ and 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 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 $\boldsymbol{a}(l)$; $\mathbb{L}(\boldsymbol{a})$ denotes the cardinality of a vector $\boldsymbol{a}$. For a set of continuous random variables, $\{x_1, x_2, \ldots, x_N\}$, $x_{(i)}$ denotes the ith largest random variable, and becomes the ith order statistic. For the set $\mathbb{S}_M \triangleq \{1, 2, \ldots, M\}$, $\mathbb{S}_M \setminus \{j\}$ denotes $\mathbb{S}_M$ excluding j.

II. System and Channel Model

A block diagram of the considered cooperative CP-SC system is sketched in Fig. 1. The CU provides broadband wireless access with ideal backhaul links, $\{b_m, \forall m\}$, to M RRHs $\{\mathrm{RRH}_m, \forall m\}$. The RRHs are assumed to be equipped

[1] The amplitude of the Zadoff-Chu sequence is constant in the time (frequency) domain and its autocorrelation is zero for all non-zero cyclic shifts [27].

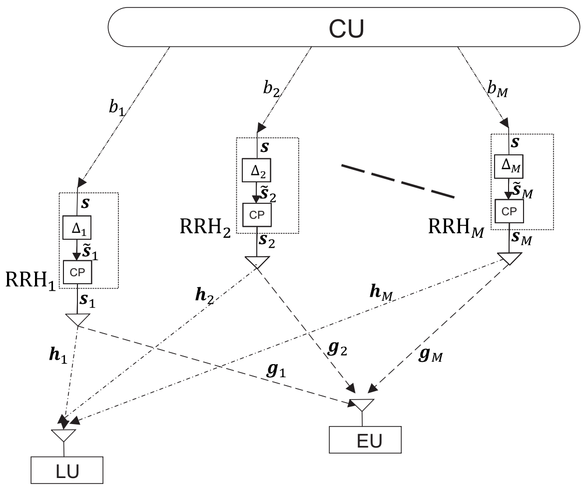

Fig. 1. Block diagram of the considered cooperative system, which communicates with the CU via a set of ideal backhaul links $\{b_1, \ldots, b_M\}$. Based on the dCDD scheme, M RRHs communicate with the LU through the legitimate channels $\{\boldsymbol{h}_m, \forall m\}$. The wireless links from the RRHs to the LU can be intercepted by an EU through the illegitimate channels $\{\boldsymbol{g}_m, \forall m\}$.

with a single antenna, due to practical constraints on the hardware complexity and power limitation. In addition, each of the LU and EU is assumed to be equipped with a single antenna. Cooperative communications occur between the RRHs and the LU in the presence of an EU. To protect the confidential information from being illegitimately intercepted by the EU, one of the RRHs is selected as the interfering RRH. Its main role is to transmit a deliberately interfering ANS to the EU. The remaining RRHs, on the other hand, transmit data signals. To increase the receive SNR at the LU, the dCDD communication scheme is employed to ensure the communication between the RRHs and the LU under the control of the CU.

The EU is considered to be an active user, and, thus, the CSI from the RRHs to the EU can be monitored by the CU [3]. As a practical consideration, only partial CSI is assumed in the system. Frequency selective fading channels from the mth RRH to the EU are considered and are denoted by $\boldsymbol{g}_m$ with $\mathbb{L}(\boldsymbol{g}_m) = N_g$. The same number of multipath components over the EU channels is assumed. The LU is placed at a random location with respect to the RRHs, and, thus, independent and non-identically distributed frequency selective fading channels from the RRHs to the LU are assumed. The channel from the mth RRH to the LU is denoted by $\boldsymbol{h}_m$ with $\mathbb{L}(\boldsymbol{h}_m) = N_{h,m}$. The LU is assumed to have knowledge of the number of multipath components of the LU channels. For CP-SC transmissions, CSI can be estimated with the aid of either sending the training sequence [29] or adding the pilot as the suffix to each symbol block [30], [31]. With the aid of this a priori information, the CU is capable of computing the maximum number of RRHs for dCDD operation. Since the LU does not require explicit CSI feedback, the interception probability of the system can be reduced.

We consider CP-SC transmission. In this case, the CP length, N_p, can be optimized in order to remove the ISI as follows [11]

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

where $N_{h,m}$ denotes the number of multipath components of the frequency fading channel $\boldsymbol{h}_m$.

The CDD delay, Δ_m, of the mth RRH is set equal to

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

which allows the system to convert the MISO channel into an ISI-free SISO channel.

From (1) and (2), the number of RRHs for dCDD operation is as follows [11][2]:

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

where $\lfloor \cdot \rfloor$ denotes the floor function with respect to the symbol block size, Q, and N_p. The CU determines Q based on CP-SC transmissions, whereas the LU feeds N_p back to the CU according to (1).

In the present paper, we are interested in two fundamental questions related to dCDD operation in the context of physical later security:

Q_1 : How should one RRH be chosen as the interfering RRH?

Q_2 : What is the impact of the proposed interfering RRH selection on the secrecy performance?

A. Selection of the interfering RRH

For the M available RRHs, the CU has the knowledge of $\{\|\boldsymbol{g}_m\|^2, \forall m\}$, i.e., the frequency selective fading channel from the mth RRH to EU. The channel magnitude is $\|\boldsymbol{g}_m\|^2$, so that the CU has M channel magnitudes

$$\|\boldsymbol{g}_{(1)}\|^2 \leq \ldots \leq \|\boldsymbol{g}_{(M)}\|^2. \tag{4}$$

From this knowledge, the CU can choose the RRH connected to a channel having the largest channel magnitude as the interfering RRH. The remaining RRHs act as data RRHs. Since the EU channels are independent of the LU channels, the set of data RRHs changes according to the EU channels. In the sequel, s^* denotes the index of the interfering RRH.

B. Received Signals at the EU and LU

The mth RRH applies the CDD delay $\Delta_{\tilde{m}}$ to the original input symbol block $\boldsymbol{s} \in \mathbb{C}^{Q\times 1}$. This operation is expressed by $\tilde{\boldsymbol{s}}_m = \boldsymbol{P}_Q^{\Delta_{\tilde{m}}}\boldsymbol{s}$, with $\boldsymbol{P}_Q^{\Delta_{\tilde{m}}} \in \mathbb{C}^{Q\times Q}$ denoting the orthogonal permutation matrix obtained by circularly shifting down the identity matrix $\boldsymbol{I}_Q$ by $\Delta_{\tilde{m}}$. For the cyclically shifted symbol block $\tilde{\boldsymbol{s}}_m$, a CP of N_p symbols is appended to the front of $\tilde{\boldsymbol{s}}_m$, then a resulting symbol block $\boldsymbol{s}_m \triangleq \begin{bmatrix} \tilde{\boldsymbol{s}}_m(Q-N_p+1:Q,1) \\ \tilde{\boldsymbol{s}}_m \end{bmatrix} \in \mathbb{C}^{(Q+N_p)\times 1}$ is transmitted sequentially to the LU via a frequency selective fading

[2]Interested readers can find relevant information about the dCDD scheme and its operation in [11].

channel $\boldsymbol{h}_m$. After the removal of the CP signal, the received signal at the LU is given by

$$\tilde{\boldsymbol{r}}_L = \sum_{\tilde{m}\in\mathbb{S}_M\setminus\{(M)\}, m\in\mathbb{S}_M\setminus\{s^*\}} \sqrt{P_T\alpha_{h,m}}\boldsymbol{H}_m\boldsymbol{P}_Q^{\Delta_{\tilde{m}}}\boldsymbol{s}+ \sqrt{P_J\alpha_{h,s^*}}\boldsymbol{H}_{s^*}\boldsymbol{P}_Q^{\Delta_{(M)}}\boldsymbol{j}+\boldsymbol{z}_L \quad (5)$$

where P_T and P_J are the transmission powers for data and ANS transmissions, respectively. Note that $\tilde{m} \neq m$ and $\tilde{s} \neq s^*$. To reduce the decoding probability of an interfering ANS at the EU, we also apply a random selection for $\Delta_{\tilde{s}^*}$. According to [11], it is verified that dCDD provides the same performance if different cyclic delays are assigned to different RRHs. Since the LU also feeds back a list, which specifies RRHs' order by the magnitude of their channels connected to the LU, the CU can use this list. To reduce feedback overhead, we assume that the CU chooses the index of the RRH connected to the best channel to the LU. That is, $\tilde{s}$ corresponds to the index (M) of $\boldsymbol{h}_{(M)}$. Then, the remaining cyclic delays are assigned to the data RRHs. Thus, $\tilde{m} \in \mathbb{S}_M \setminus \{(M)\}$ and $m \in \mathbb{S}_M \setminus \{s^*\}$. Accordingly, (2) should be changed to $\Delta_{\tilde{m}} = (\tilde{m}-1)N_p$. The additive vector noise over the LU channels is denoted by $\boldsymbol{z}_L \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_Q)$. Additionally, $\alpha_{h,m}$ accounts for the distant-dependent large scale fading over the channel $\boldsymbol{h}_m$. For a distance d_m from the mth RRH to LU, $\alpha_{h,m}$ is given by $\alpha_{h,m} = d_m^{-\epsilon}$, where ϵ denotes the path loss exponent. Right circulant matrices are denoted by $\{\boldsymbol{H}_m, \forall m, m \neq s^*\}$ and $\boldsymbol{H}_{s^*}$, which are mainly specified by the channel vectors $\{\boldsymbol{h}_m, \forall m, m \neq s^*\}$ and $\boldsymbol{h}_{s^*}$ with additional zeros to make them have a length Q. For example, for $Q = 4$, $N_{h,m} = 2$, and $N_{h,s^*} = 3$, $\boldsymbol{H}_m$ and $\boldsymbol{H}_{s^*}$ are given by

$$\boldsymbol{H}_m = \begin{bmatrix} \boldsymbol{h}_m(1) & 0 & 0 & \boldsymbol{h}_m(2) \\ \boldsymbol{h}_m(2) & \boldsymbol{h}_m(1) & 0 & 0 \\ 0 & \boldsymbol{h}_m(2) & \boldsymbol{h}_m(1) & 0 \\ 0 & 0 & \boldsymbol{h}_m(2) & \boldsymbol{h}_m(1) \end{bmatrix} \text{ and }$$
$$\boldsymbol{H}_{s^*} = \begin{bmatrix} \boldsymbol{h}_{s^*}(1) & 0 & \boldsymbol{h}_{s^*}(3) & \boldsymbol{h}_{s^*}(2) \\ \boldsymbol{h}_{s^*}(2) & \boldsymbol{h}_{s^*}(1) & 0 & \boldsymbol{h}_{s^*}(3) \\ \boldsymbol{h}_{s^*}(3) & \boldsymbol{h}_{s^*}(2) & \boldsymbol{h}_{s^*}(1) & 0 \\ 0 & \boldsymbol{h}_{s^*}(3) & \boldsymbol{h}_{s^*}(2) & \boldsymbol{h}_{s^*}(1) \end{bmatrix}. \quad (6)$$

For the deliberate interfering ANS, $\boldsymbol{j} \in \mathbb{C}^{Q\times 1}$, we assume that $E\{\boldsymbol{j}\} = \boldsymbol{0}$, and $E\{\boldsymbol{j}\boldsymbol{j}^H\} = \boldsymbol{I}_Q$. The interfering ANS is known to the CU and LU, and we assume that the channel estimate is very accurate at the LU; thus (5) can be expressed as follows:

$$\boldsymbol{r}_L = \sum_{\tilde{m}\in\mathbb{S}_M\setminus\{(M)\}, m\in\mathbb{S}_M\setminus\{s^*\}} \sqrt{P_T\alpha_{h,m}}\boldsymbol{H}_m\boldsymbol{P}_Q^{\Delta_{\tilde{m}}}\boldsymbol{s}+\boldsymbol{z}_L. \quad (7)$$

Note that the two conditions specified by Eqs. (1) and (2), assure that the ANS $\boldsymbol{j}$ does not interfere with the desired data symbol $\boldsymbol{s}$. Thus, dCDD operation introduces interference free reception at the LU [3]. By using the properties of right circulant matrices, the product of two right circulant matrices is another right circulant matrix, and the right circulant matrix is specified by its first column vector, so that we can further express (7) as:

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

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

$$\begin{aligned}\boldsymbol{h}_{\mathrm{CDD},s^*} \triangleq \sqrt{P_T}\Big[&\sqrt{\alpha_{h,1}}(\boldsymbol{h}_1)^T, \boldsymbol{0}_{1\times(N_p-N_{h,1})}, \sqrt{\alpha_{h,2}}(\boldsymbol{h}_2)^T, \\ &\boldsymbol{0}_{1\times(N_p-N_{h,2})}\cdots, \sqrt{\alpha_{h,s^*-1}}(\boldsymbol{h}_{s^*-1})^T, \\ &\boldsymbol{0}_{1\times(N_p-N_{h,s^*-1})}, \sqrt{\alpha_{h,s^*+1}}(\boldsymbol{h}_{s^*+1})^T, \\ &\boldsymbol{0}_{1\times(N_p-N_{h,s^*+1})}, \ldots, \sqrt{\alpha_{h,M}}(\boldsymbol{h}_M)^T, \\ &\boldsymbol{0}_{1\times(N_p-N_{h,M})}\Big]^T. \end{aligned} \quad (9)$$

Note that since the location of a missing channel vector, $\boldsymbol{h}_{(M)}$, is determined by $\Delta_{(M)}$, (9) corresponds to the case of $(M) = s^*$. We can readily derive an equivalent form for a general value of $(M) \neq s^*$. However, without loss of generality, we assume that $(M) = s^*$ in the sequel to simplify mathematical expressions. The received signal at the EU is given by

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

where $\boldsymbol{G}_{\mathrm{CDD},s^*}$ and $\boldsymbol{G}_{s^*}$ are right circulant matrices specified by the equivalent channel vectors $\boldsymbol{g}_{\mathrm{CDD},s^*}$ and $\boldsymbol{g}_{s^*}$, respectively. Additionally, α_g is used to model the distance-dependent large scale fading over the EU channels. Note that $\boldsymbol{g}_{\mathrm{CDD},s^*}$ can be specified as $\boldsymbol{h}_{\mathrm{CDD},s^*}$ using $\boldsymbol{g}_m$s. The additive vector noise over the EU channels is given by $\boldsymbol{z}_E \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_Q)$. Since $\boldsymbol{P}_Q^{\Delta_{s^*}}$ is determined from the LU channels, we assume that the EU is not able to decode the ANS. Thus, $\boldsymbol{P}_Q^{\Delta_{s^*}}\boldsymbol{j}$ can be recognized as interference at the EU [4].

III. Performance Analysis

To study the performance of the proposed physical layer secrecy system that is based on the interfering RRH that sends interfering ANS under dCDD operation, we need to know the distribution of the receive SNRs at the LU and EU.

[3]For the two-user interference channel in which only one user has a confidential message to send, the transmit power of the helpful interference is optimized to maximize the secrecy rate of the Gaussian wiretap channel. With the optimized interference power, the LU is able to cancel the interference, whereas the interception performance decreases at the EU [32]. In contrast, the considered system utilizes the unique strength of the dCDD scheme for interference cancellation at the LU.

[4]The system model is somewhat similar to that of [33]. When two RRHs are available for dCDD operation, one RRH is used for data transmission. The other RRH is used for transmission of the interfering ANS independently of the desired target transmission symbol, $\boldsymbol{s}$.

A. Receive SNR at the LU over non-identically distributed channels

In contrast to the dCDD system under the assumption $M < K$, where K denotes the number of RRHs in the system, the considered system foresees the condition $M \geq K$ for dCDD operation. This implies that ordered statistics are not required for the computation of the aggregate SNR at the LU. When $M < K$, the dCDD chooses only M RRHs connected to the channels having the largest magnitude. Thus, ordered statistics are required when the selection of the RRHs is employed in the system [11]. In the sequel, we assume that $M = K$.

For non-identically distributed frequency selective fading channels, the receive SNR at the LU, employing the maximum number of RRHs allowed by dCDD operation, is given by

$$\gamma_R = \sum_{s^*=1}^{M} \sum_{m=1, m\neq s^*}^{M} \gamma_{R,m} P_r\big(s^* = \underset{j\in[1,\ldots,M]}{\operatorname{argmax}} (\|\boldsymbol{g}_j\|^2)\big) \quad (11)$$

where $\gamma_{R,m} \overset{\triangle}{=} \tilde{\alpha}_{h,m} \sum_{l=1}^{N_{h,m}} |\boldsymbol{h}_m(l)|^2$ with $\tilde{\alpha}_{h,m} \overset{\triangle}{=} \frac{P_T \alpha_{h,m}}{\sigma_z^2}$, and $P_r(s^*)$ denotes the probability that the s^*th RRH is selected as the interfering RRH. Note that $\gamma_{R,m}$ is the receive SNR provided by the mth data RRH. Since $\tilde{\alpha}_{h,m} \sum_{l=1}^{N_{h,m}} |\boldsymbol{h}_m(l)|^2$ is distributed as $\tilde{\alpha}_{h,m} \sum_{l=1}^{N_{h,m}} |\boldsymbol{h}_m(l)|^2 \sim \chi^2(2N_{h,m}, \tilde{\alpha}_{h,m})$, its PDF and CDF are, respectively, expressed as follows:

$$f_{\gamma_{R,m}}(x) = \frac{1}{\Gamma(N_{h,m})(\tilde{\alpha}_{h,m})^{N_{h,m}}} x^{N_{h,m}-1} e^{-\frac{x}{\tilde{\alpha}_{h,m}}} \text{ and}$$
$$F_{\gamma_{R,m}}(x) = 1 - e^{-\frac{x}{\tilde{\alpha}_{h,m}}} \sum_{l=0}^{N_{h,m}-1} \frac{1}{l!}\Big(\frac{x}{\tilde{\alpha}_{h,m}}\Big)^l. \quad (12)$$

With the aid of (12), the distribution of γ_R is provided in the following theorem.

Theorem 1: By assuming identically distributed frequency selective fading EU channels, the distribution of the aggregate receive SNR at the LU is given by

$$f_{\gamma_R}(x) = \frac{1}{M} \sum_{s^*=1}^{M} f_{A,s^*}(x) \text{ and}$$
$$F_{\gamma_R}(x) = \frac{1}{M} \sum_{s^*=1}^{M} F_{A,s^*}(x) \quad (13)$$

where

$$\begin{aligned} f_{A,s^*}(x) &= \sum_{m=1}^{M-1} \sum_{j=1}^{N_{h,m}} \frac{(-1)^m \theta_{m,j,s^*}}{\Gamma(j)} x^{j-1} e^{-\frac{x}{\tilde{\beta}_{h,m,s^*}}} \text{ and} \\ F_{A,s^*}(x) &= \sum_{m=1}^{M-1} \sum_{j=1}^{N_{h,m}} \frac{(-1)^m \theta_{m,j,s^*}}{\Gamma(j)} \Big(\frac{1}{\tilde{\beta}_{h,m,s^*}}\Big)^{-j} \\ & \quad \gamma_l\Big(j, \frac{x}{\tilde{\beta}_{h,m,s^*}}\Big) \\ &\overset{(a)}{=} \sum_{m=1}^{M-1} \sum_{j=1}^{N_{h,m}} (-1)^m \theta_{m,j,s^*} (\tilde{\beta}_{h,m,s^*})^j - \\ & \quad \sum_{m=1}^{M-1} \sum_{j=1}^{N_{h,m}} \sum_{l=0}^{j-1} \frac{\theta_{m,j,s^*}(-1)^m (\tilde{\beta}_{h,m,s^*})^{j-l}}{\Gamma(l+1)} x^l \\ & \quad e^{-\frac{x}{\tilde{\beta}_{h,m,s^*}}} \end{aligned} \quad (14)$$

where $\gamma_l(\cdot,\cdot)$ is the lower incomplete gamma function, $\theta_{m,j,s^*} \overset{\triangle}{=} \frac{(-1)^{N_{h,m}}}{(\tilde{\beta}_{h,m,s^*})^{N_{h,m}}} \sum_{S(m,j)} \prod_{k=1,k\neq m}^{M-1} \binom{N_{h,k}+q_k-1}{q_k} \frac{(\tilde{\beta}_{h,k,s^*})^{q_k}}{(1-\frac{\tilde{\beta}_{h,k,s^*}}{\tilde{\beta}_{h,m,s^*}})^{N_{h,k}+q_k}}$, $\tilde{\beta}_{h,m,s^*}$, the mth component of $\tilde{\beta}_{h,s^*} \overset{\triangle}{=} [\tilde{\alpha}_{h,1}, \ldots, \tilde{\alpha}_{h,s^*-1}, \tilde{\alpha}_{h,s^*+1}, \ldots, \tilde{\alpha}_{h,M}]$, and $S(i,j)$, a set of $(M-1)$-tuples satisfying the following condition

$$S(i,j) \overset{\triangle}{=} \{(q_1, \ldots, q_{M-1}) : \sum_{k=1}^{M-1} q_k = N_{h,i} - j \text{ with } q_i = 0\}.$$

Proof: Note that $\tilde{\beta}_{h,s^*}$ is a set of $\tilde{\alpha}_{h,j}$s except for $\tilde{\alpha}_{h,s^*}$. We first exploit the fact that $P_r\big(s^* = \underset{j\in[1,\ldots,M]}{\operatorname{argmax}} (\|\boldsymbol{g}_j\|^2)s\big) = \frac{1}{M}$ over identically distributed frequency selective fading EU channels. Then, we compute $f_{A,s^*}(x)$, which is the PDF of the sum of the receive SNRs except for γ_{R,s^*}, i.e., the SNR provided by the interfering RRH. According to [34], we can derive $f_{A,s^*}(x)$. The corresponding CDF $F_{A,s^*}(x)$ can be derived from $f_{A,s^*}(x)$. With the aid of the total probability theorem, we can derive (13). The expression (a) in (14) is provided for the future use of $F_{\gamma_R}(x)$. ∎

B. Receive SINR at the EU over identically distributed channels

The receive signal power and noise-plus-interference power due to interfering signal at the EU are given by

$$S_E = P_T \sum_{m=1,m\neq s^*}^{M} \alpha_g \sum_{l=1}^{N_g} |\boldsymbol{g}_m(l)|^2 \text{ and}$$
$$N_E = P_J \alpha_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{s^*}(l)|^2 + \sigma_z^2 \quad (15)$$

where S_E is the signal power aggregated from $(M-1)$ data RRHs. One of the EU channels, the one that provides the largest channel magnitude, is selected for the interfering RRH under the control of the CU. Thus, S_E/N_E decreases in general as the number of RRHs increases, which is beneficial for increasing the security of the proposed cooperative system.

According to (15), the SINR at the EU is given by

$$\begin{aligned} \gamma_E = \frac{S_E}{N_E} = \frac{S_E/\sigma_z^2}{N_E/\sigma_z^2} &= \frac{\tilde{\alpha}_g \sum_{m=1}^{M-1} \sum_{l=1}^{N_g} |\boldsymbol{g}_{(m)}(l)|^2}{\gamma_I \tilde{\alpha}_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{(M)}(l)|^2 + 1} \\ &= \frac{\sum_{k=1}^{M-1} \tilde{S}_{E,(k)}}{\gamma_I \tilde{S}_{E,(M)} + 1} \end{aligned} \quad (16)$$

where $\tilde{\alpha}_g \overset{\triangle}{=} \frac{P_T \alpha_g}{\sigma_z^2}$, $\gamma_I \overset{\triangle}{=} \frac{P_J}{P_T}$, $\tilde{S}_{E,(k)} \overset{\triangle}{=} \tilde{\alpha}_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{(k)}(l)|^2$, and $\tilde{S}_{E,(M)} \overset{\triangle}{=} \tilde{\alpha}_g \sum_{l=1}^{N_g} |\boldsymbol{g}_{s^*}(l)|^2$. Note that we have used ordered statistics in (16) so that $0 < \tilde{S}_{E,(1)} < \tilde{S}_{E,(2)} < \ldots < \tilde{S}_{E,(M-1)} < \tilde{S}_{E,(M)} < \infty$.

A closed-form expression for the distribution of the SINR at the EU is provided in the following theorem.

Theorem 2: For identically distributed frequency selective fading over the illegitimate EU channels, the distribution of the receive SINR at the EU, from the $(M-1)$ RRHs and degraded by the interfering RRH, is given by (17) at the next page.

Proof: See Appendix A. ■

In (17), we have defined $M_m N_g \triangleq (M-1)N_g$, $c_1 \triangleq MN_g + p_1 - p_2 + p_3 - 1$, and $\sum_{\substack{q_1,\ldots,q_{N_g} \\ q_1+\ldots+q_{N_g}=n}}$ denotes the sum of all positive integer indices of q_js satisfying $q_1 + \ldots + q_{N_g} = n$, and $\tilde{q} \triangleq \sum_{t=0}^{N_g-1} t q_{t+1}$. Theorem 2 shows that the PDF of the receive SINR at the EU can be obtained in closed form, which is given by the weighted summation of either lower incomplete gamma functions or gamma functions. We can also see that three equations compose (17), two of which, $(\mathrm{ftn}_1, \mathrm{ftn}_2)$, are easy to be used for performance analysis.

C. Secrecy Outage Probability

The transmission capacity achieved by the legitimate transmissions is given by

$$C_R = \log_2(1+\gamma_R) \tag{18}$$

whereas the interceptable capacity is defined as [4]:

$$C_E = \log_2(1+\gamma_E). \tag{19}$$

Then, the secrecy capacity C_s is defined as follows:

$$C_s = [C_R - C_E]^+ \tag{20}$$

where $[x]^+ \triangleq \max(x, 0)$.

At a given secrecy rate R_s, the secrecy outage probability is defined by

$$\begin{aligned} P_{\text{out}}(R_s) &= Pr(C_s < R_s) \\ &= \int_0^\infty F_{\gamma_R}(J_R(1+x)-1) f_{\gamma_E}(x)dx \end{aligned} \tag{21}$$

where $J_R \triangleq 2^{R_s}$.

According to (21), a closed form expression for the secrecy outage probability, $P_{\text{out}}(R_s)$, can be derived in the next theorem.

Theorem 3: For frequency selective fading over legitimate and illegitimate channels, the proposed CP-SC system that improves physical layer security by dCDD operation and the interfering RRH provides the secrecy outage probability at secrecy rate R_s, as follows:

$$\begin{aligned} P_{\text{out}}(R_s) = \frac{1}{M}\sum_{s^*=1}^{M} \big(P_{\text{out},1,s^*}(R_s) + P_{\text{out},2,s^*}(R_s) + \\ P_{\text{out},3,s^*}(R_s)\big) \end{aligned} \tag{22}$$

where

$$\begin{aligned} P_{\text{out},1,s^*}(R_s) + P_{\text{out},2,s^*}(R_s) \triangleq \Delta_{1,1,s^*} - \Delta_{1,2,s^*}(R_s) + \\ \Delta_{2,1,s^*} - \Delta_{2,2,s^*}(R_s). \end{aligned} \tag{23}$$

Proof: See Appendix B for a corresponding expression for $P_{\text{out},3,s^*}(R_s)$. ■

In (23), we have defined several definitions provided in (24) at the next page. In (24), $G_{p,q}^{m,n}\left(t \middle| \begin{matrix} a_1,\ldots,a_n,a_{n+1},\ldots,a_p \\ b_1,\ldots,b_m,b_{m+1},\ldots,b_q \end{matrix}\right)$ denotes the Meijer G-function [35, Eq. (9.301)]. For a specific set of parameters $\{m=1, n=2, p=2, q=1\}$, $G_{2,1}^{1,2}\left(z \middle| \begin{matrix} a_1, a_2 \\ b_1 \end{matrix}\right)$ can be expressed in terms of the hypergeometricU function [35, Eq. (9.211.4)] with the condition of $z \notin \{-1, 0\}$ [36, Eq. (07.34.03.0392.01)]. Note that $\Delta_{1,1,s^*}$ and $\Delta_{2,1,s^*}$ are independent of the secrecy rate R_s. Due to a non-existing integral formula incorporating the third equation in (17), $P_{\text{out},3,s^*}(R_s)$ is obtained by numerical integration. Since $P_{\text{out},3,s^*}(R_s) \approx 0$ as $1/\sigma_z^2 \to \infty$, we can obtain a closed-form expression for an approximate secrecy outage probability in the following proposition.

Proposition 1: In the high SNR regime, the proposed secrecy scheme provides an approximate secrecy outage probability as follows:

$$\begin{aligned} P_{\text{out}}^{ap}(R_s) &= \frac{1}{M}\sum_{s^*=1}^{M} \big(P_{\text{out},1,s^*}(R_s) + P_{\text{out},2,s^*}(R_s)\big) \\ &= \frac{1}{M}\sum_{s^*=1}^{M} \big(\Delta_{1,1,s^*} - \Delta_{1,2,s^*}(R_s) + \Delta_{2,1,s^*} - \\ &\quad \Delta_{2,2,s^*}(R_s)\big). \end{aligned} \tag{25}$$

D. Probability of Non-Zero Achievable Secrecy Rate

The secrecy rate is zero when the EU's SINR is higher than the SNR of the LU, that is, $C_s = 0$ if $\gamma_R < \gamma_E$. The probability of system non-zero achievable secrecy rate is given by

$$Pr(C_s > 0) = 1 - \int_0^\infty F_{\gamma_R}(x) f_{\gamma_E}(x)dx. \tag{26}$$

The expression for (26) is very similar to that of the secrecy outage probability. Since the probability of system non-zero achievable secrecy rate depends on ftn_3, a closed-form expression of the approximate non-zero achievable secrecy rate can be derived in the following theorem.

Theorem 4: The proposed secrecy system that employs the interfering RRH by dCDD operation provides the approximate non-zero achievable secrecy rate in frequency selective fading channels as follows:

$$\begin{aligned} Pr(C_s > 0) = 1 - \frac{1}{M}\sum_{s^*=1}^{M} \big(\Delta_{1,1,s^*} + \Theta_{1,2,s^*} + \Delta_{2,1,s^*} + \\ \Theta_{2,2,s^*}\big) \end{aligned} \tag{27}$$

where $\Theta_{1,2,s^*}$ and $\Theta_{2,2,s^*}$ are defined in (28) at the next page.

Proof: Similar to the proof in Appendix B, (28) can be obtained. ■

E. Asymptotic Diversity Gain Analysis

From [6], [7], and [37], it is known that the asymptotic diversity gain of the secrecy performance is mainly determined by the channels connecting the LU.

Proposition 2: From the receive SNR at the LU, the diversity gain of the secrecy outage probability is given by

$$G_d = \min_{s^*}\Big(\sum_{m=1, m\neq s^*}^{M} N_{h,m}\Big) = \min_{s^*} G_{d,s^*} \tag{29}$$

$$f_{\gamma_E}(x) = \frac{M}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}}\Big[\frac{\mathrm{ftn}_1}{\Gamma(M_m N_g)} + \sum_{n=1}^{M-1}\binom{M-1}{n}(-1)^n \sum_{\substack{q_1,\ldots,q_{N_g}\\ q_1+\ldots+q_{N_g}=n}} \frac{n!}{q_1!q_2!\ldots q_{N_g}!}$$

$$\prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}\frac{1}{\Gamma(M_m N_g-\tilde{q})}\big(\mathrm{ftn}_2 \mathrm{U}(\gamma_I x-n)+\mathrm{ftn}_3\mathrm{U}(n-\gamma_I x)\big)\Big] \quad (17)$$

where

$$\mathrm{ftn}_1 \triangleq \sum_{p_1=0}^{M_m N_g}\binom{M_m N_g}{p_1}\gamma_I^{p_1}\Gamma(N_g+p_1)x^{M_m N_g-1}\tilde{\alpha}_g^{N_g+p_1}(1+\gamma_I x)^{-N_g-p_1}e^{-x/\tilde{\alpha}_g},$$

$$\mathrm{ftn}_2 \triangleq \sum_{p_1=0}^{1}\sum_{p_2=0}^{M_m N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\binom{1}{p_1}\binom{M_m N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\gamma_I^{p_1+p_3}(-n)^{M_m N_g-\tilde{q}-p_2-1}$$
$$\tilde{\alpha}_g^{c_1}x^{p_2}(1+\gamma_I x)^{-c_1}\Gamma(c_1)e^{-x/\tilde{\alpha}_g}, \text{ and}$$

$$\mathrm{ftn}_3 \triangleq \sum_{p_1=0}^{1}\sum_{p_2=0}^{M_m N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\binom{1}{p_1}\binom{M_m N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\gamma_I^{p_1+p_3}(-n)^{M_m N_g-\tilde{q}-p_2-1}$$
$$\tilde{\alpha}_g^{c_1}x^{p_2}(1+\gamma_I x)^{-c_1}\gamma_l\Big(c_1,\frac{x(1+\gamma_I x)}{\tilde{\alpha}_g(n-\gamma_I x)}\Big)e^{-x/\tilde{\alpha}_g}.$$

$$\Delta_{1,1,s^*} \triangleq \frac{M}{\Gamma(N_g)\Gamma((M-1)N_g)\tilde{\alpha}_g^{N_g}}\sum_{ij=1}^{M-1}\sum_{j=1}^{N_{h,ij}}\sum_{p_1=0}^{(M-1)N_g}\binom{(M-1)N_g}{p_1}\theta_{ij,j,s^*}(\tilde{\beta}_{h,ij,s^*})^j(-1)^j\gamma_I^{p_1}\tilde{\alpha}_g^{c_1}$$
$$G_{2,1}^{1,2}\Big(\gamma_I\tilde{\alpha}_g\Big|\begin{matrix}1-(M-1)N_g, 1-c_1\\ 0\end{matrix}\Big),$$

$$\Delta_{1,2,s^*}(R_s) \triangleq \frac{M}{\Gamma(N_g)\Gamma((M-1)N_g)\tilde{\alpha}_g^{MN_g}}\sum_{ij=1}^{M-1}\sum_{j=1}^{N_{h,ij}}\sum_{p_1=0}^{(M-1)N_g}\sum_{m=0}^{j-1}\sum_{r=0}^{m}\binom{(M-1)N_g}{p_1}\binom{m}{r}$$
$$\theta_{ij,j,s^*}(\tilde{\beta}_{h,ij,s^*})^{j-m}(-1)^j\gamma_I^{p_1}\tilde{\alpha}_g^{c_1}\frac{(J_R-1)^{m-r}J_R^r}{\Gamma(m+1)}\Big(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\Big)^{-(M-1)N_g-rr}e^{-\frac{(J_R-1)}{\tilde{\beta}_{h,ij,s^*}}}$$
$$G_{2,1}^{1,2}\Big(\frac{\gamma_I}{\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}}\Big|\begin{matrix}1-(M-1)N_g-r, 1-c_1\\ 0\end{matrix}\Big),$$

$$\Delta_{2,1,s^*} \triangleq \frac{M}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}}\sum_{n=1}^{M-1}\sum_{ij=1}^{M-1}\sum_{j=1}^{N_{h,ij}}\sum_{\substack{q_1,\ldots,q_{N_g}\\ q_1+\ldots+q_{N_g}=n}}\frac{n!}{q_1!q_2!\ldots q_{N_g}!}\prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}\sum_{p_1=0}^{1}\sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\sum_{w=0}^{p_2}$$
$$\binom{1}{p_1}\binom{(M-1)N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\binom{p_2}{w}\theta_{ij,j,s^*}(\tilde{\beta}_{h,ij,s^*})^j(-1)^j\gamma_I^{p_1+p_3}(-n)^{(M-1)N_g-\tilde{q}-1-p_2}\tilde{\alpha}_g^{c_1}$$
$$e^{-n/\gamma_I/\tilde{\alpha}_g}\frac{(1+n)^{-c_1}}{\Gamma((M-1)N_g-\tilde{q})}(n/\gamma_I)^{p_2-w}\tilde{\alpha}_g^{1+w}G_{2,1}^{1,2}\Big(\frac{\gamma_I\tilde{\alpha}_g}{1+n}\Big|\begin{matrix}-w, 1-c_1\\ 0\end{matrix}\Big), \text{ and}$$

$$\Delta_{2,2,s^*}(R_s) \triangleq \frac{M}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}}\sum_{n=1}^{M-1}\sum_{\substack{q_1,\ldots,q_{N_g}\\ q_1+\ldots+q_{N_g}=n}}\frac{n!}{q_1!q_2!\ldots q_{N_g}!}\prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}\sum_{p_1=0}^{1}\sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\sum_{ij=1}^{M-1}\sum_{j=1}^{N_{h,ij}}\sum_{m=0}^{j-1}\sum_{r=0}^{m}$$
$$\binom{1}{p_1}\binom{(M-1)N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\binom{m}{r}\binom{p_2+r}{w}\theta_{ij,j,s^*}(\tilde{\beta}_{h,ij,s^*})^{j-r}(-1)^j\gamma_I^{p_1+p_3}(1+n)^{-c_1}\tilde{\alpha}_g^{c_1}$$
$$(J_R-1)^{m-r}\frac{J_R^r}{\Gamma(m+1)}(n/\gamma_I)^{p_2+r-w}\Big(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\Big)^{-1-w}e^{-n\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)\frac{1}{\gamma_I}}$$
$$G_{2,1}^{1,2}\Big(\frac{\gamma_I}{(1+n)(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g})}\Big|\begin{matrix}-w, 1-c_1\\ 0\end{matrix}\Big). \quad (24)$$

$$\Theta_{1,2,s^*} \triangleq \frac{M}{\Gamma(N_g)\Gamma((M-1)N_g)\tilde{\alpha}_g^{MN_g}} \sum_{ij=1}^{M-1} \sum_{j=1}^{N_{h,ij}} \sum_{p_1=0}^{(M-1)N_g} \sum_{m=0}^{j-1} \binom{(M-1)N_g}{p_1} \theta_{ij,j,s^*} (\tilde{\beta}_{h,ij,s^*})^{j-m}$$
$$(-1)^j \gamma_I^{p_1} \tilde{\alpha}_g^{c_1} \frac{1}{\Gamma(m+1)} G_{2,1}^{1,2}\left(\frac{\gamma_I}{\frac{1}{\tilde{\beta}_{h,ij,s^*}} + \frac{1}{\tilde{\alpha}_g}} \middle| \begin{array}{c} 1-(M-1)N_g-m, 1-c_1 \\ 0 \end{array} \right) \text{ and}$$

$$\Theta_{2,2,s^*} \triangleq \frac{M}{\Gamma(N_g)\tilde{\alpha}_g^{MN_g}} \sum_{n=1}^{M-1} \sum_{\substack{q_1,\ldots,q_{N_g} \\ q_1+\ldots+q_{N_g}=n}} \frac{n!}{q_1! q_2! \ldots q_{N_g}!} \prod_{t_1=0}^{N_g-1} \left(\frac{1}{t_1!}\right)^{q_{t_1+1}}$$
$$\sum_{p_1=0}^{1} \sum_{p_2=0}^{(M-1)N_g-\tilde{q}-1} \sum_{p_3=0}^{p_2} \sum_{ij=1}^{M-1} \sum_{j=1}^{N_{h,ij}} \sum_{m=0}^{j-1} \sum_{w=0}^{p_2+m} \binom{1}{p_1} \binom{(M-1)N_g-\tilde{q}-1}{p_2} \binom{p_2}{p_3}$$
$$\binom{p_2+m}{w} \theta_{ij,j,s^*} (\tilde{\beta}_{h,ij,s^*})^{j-m} (-1)^j \gamma_I^{p_1+p_3} (1+n)^{-c_1} \tilde{\alpha}_g^{c_1} \frac{(-n)^{c_1}}{\Gamma(m+1)} (n/\gamma_I)^{p_2+m-w} \left(\frac{1}{\tilde{\beta}_{h,ij,s^*}} + \frac{1}{\tilde{\alpha}_g} \right)^{-1-w}$$
$$G_{2,1}^{1,2}\left(\frac{\gamma_I}{(1+n)\left(\frac{1}{\tilde{\beta}_{h,ij,s^*}} + \frac{1}{\tilde{\alpha}_g}\right)} \middle| \begin{array}{c} -w, 1-c_1 \\ 0 \end{array} \right) e^{-\frac{n}{\gamma_I}\left(\frac{1}{\tilde{\beta}_{h,ij,s^*}} + \frac{1}{\tilde{\alpha}_g}\right)}. \quad (28)$$

---

where $G_{d,s^*} \triangleq \sum_{m=1, m\neq s^*}^{M} N_{h,m}$. Equation (29) shows that depending on the interfering RRH selection, due to independent LU and EU channels, G_{d,s^*}, which is the summation of the number of multipath components over the LU channels except for the number of multipath components over the channel connected with the interfering RRH, is different for non-identically distributed frequency selective fading channels. However, the overall diversity gain of the proposed secrecy system is determined as the minimum of the $\{G_{d,s^*}, \forall s^*\}$.

Proof: Based on the approach provided by [6], [7], and [37], we can derive the secrecy diversity gain from the distribution of γ_R. Let the moment generating function (MGF) of γ_R be denoted by $M_{\gamma_R}(s)$, then it is given by

$$\begin{aligned} M_{\gamma_R}(s) &\propto \prod_{s^*=1}^{M} \prod_{m=1, m\neq s^*}^{M} \frac{1}{(\tilde{\alpha}_{h,m})^{N_{h,m}}} \left(s + \frac{1}{\tilde{\alpha}_{h,m}}\right)^{-N_{h,m}} \\ &\overset{s\to\infty}{\approx} \prod_{s^*=1}^{M} \prod_{m=1, m\neq s^*}^{M} \frac{1}{(\alpha_{h,m})^{N_{h,m}}} \left(\frac{s}{\alpha_z^2}\right)^{-N_{h,m}} \\ &= \prod_{s^*=1}^{M} \prod_{m=1, m\neq s^*}^{M} \left(\frac{1}{(\alpha_{h,m})^{N_{h,m}}}\right) \left(\frac{s}{\alpha_z^2}\right)^{-G_{d,s^*}} \end{aligned} \quad (30)$$

with G_{d,s^*} being the secrecy diversity gain for the case when the s^*th EU channel or the s^*th RRH is used by the interfering RRH. Since the secrecy performance is dominated by $\min_{s^*}(G_{d,s^*})$, the overall diversity gain is derived as $G_d = \min_{s^*}(G_{d,s^*})$. ■

Note that one RRH is selected as the interfering RRH independently of the LU channels, so that only $(M-1)$ RRHs, that is, the number of data RRHs, are involved in the asymptotic performance in the high SNR region. Thus, comparing with the analysis conducted by [33], this proposition provides scalability of the number of RRHs on the security diversity gain with the dCDD based physical layer security system.

IV. Simulation Results

In this section, we first verify the derived closed form expression for the approximate secrecy outage probability. To this end, we compare the derived approximate secrecy outage probability (denoted by **Ap**) with the exact secrecy outage probability (denoted by **Ex**) for various scenarios. In addition, an asymptotically derived secrecy outage probability is denoted by **As**. Then, we show the secrecy outage probability for various scenarios taking into account various parameters, for example, the frequency selectivity, RRH cooperation, and γ_I, interference power ratio over the data transmission power. The simulation setup is as follows. Quadrature phase shift keying (QPSK) modulation is used, the transmission block size is made of 64 QPSK symbols ($Q = 64$). The CP length is given by 16 QPSK symbols. In all scenarios, we fix $P_T = 1$ and $R_s = 1$. We consider two different simulation scenarios with $\mathbb{S}_1 \triangleq \{\alpha_{h,1} = 5.3361, \alpha_{h,2} = 3.4086, \alpha_{h,3} = 5.0064, \alpha_{h,4} = 2.5640\}$ and $\mathbb{S}_2 \triangleq \{\alpha_{h,1} = 3.3569, \alpha_{h,2} = 2.4186, \alpha_{h,3} = 1.0264, \alpha_{h,4} = 1.5620\}$. Distances from RRHs to the LU are denoted by $\{\alpha_{h,m}, \forall m\}$. We also assume a fixed value of $\alpha_g = 1.2983$. In this section, M denotes the maximum allowable number of RRHs for dCDD operation.

A. Secrecy Outage Probability

We first verify the closed form expression for the approximate secrecy outage probability derived in Proposition 1.

In Fig. 2, we assume $M = 3$ RRHs. For different number of multipath components over the LU channels, this figure shows a tight approximation of the derived approximate secrecy outage probability over its corresponding exact secrecy outage probability. In this scenario, we fix $\gamma_I = 3$ dB. As any of $N_{h,k}$s increases, a lower secrecy outage probability is achieved. In addition, as $1/\alpha_z^2$ increases, a negligible difference between the exact outage probability and the asymptotic outage probability can be observed.

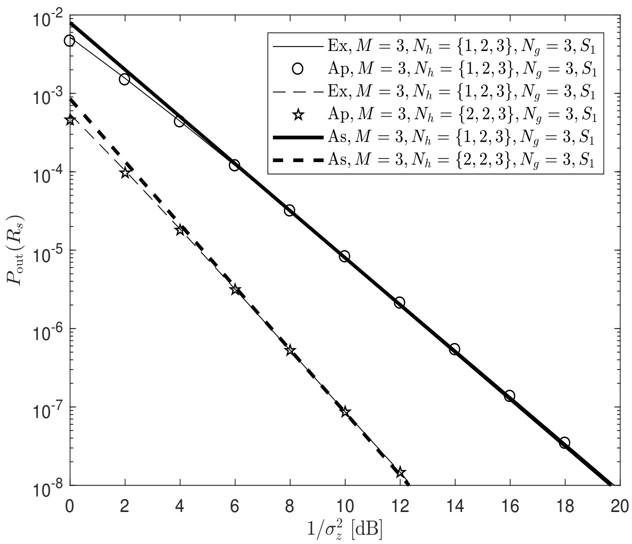

Fig. 2. Approximate secrecy outage probability compared with exact secrecy outage probability.

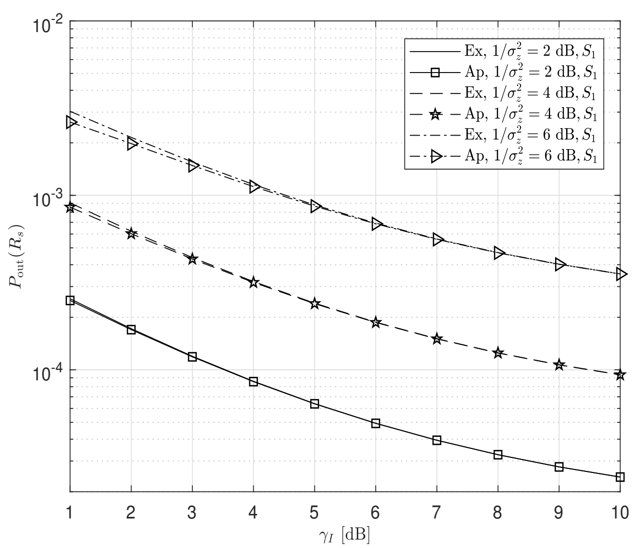

Fig. 3. Approximate secrecy outage probability compared with exact secrecy outage probability as a function of γ_I.

In Fig. 3, we also verify the approximate secrecy outage probability as a function of γ_I. We assume $M = 3$, $N_{h,1} = 1, N_{h,2} = 2, N_{h,3} = 3$, and $N_g = 3$. As γ_I increases, a lower secrecy outage probability is obtained due to an increased SINR at the EU, but without changing the SNR at the LU. For different values of the SNR over the LU channels, this figure shows that at a lower SNR and γ_I, a slight difference can be observed from the approximate secrecy outage probability. However, as either the SNR over the LU channels or γ_I increases, the difference from the approximate secrecy outage probability becomes negligible.

In Fig. 4, we compare the secrecy outage probability of the proposed interfering RRH selection over other selection

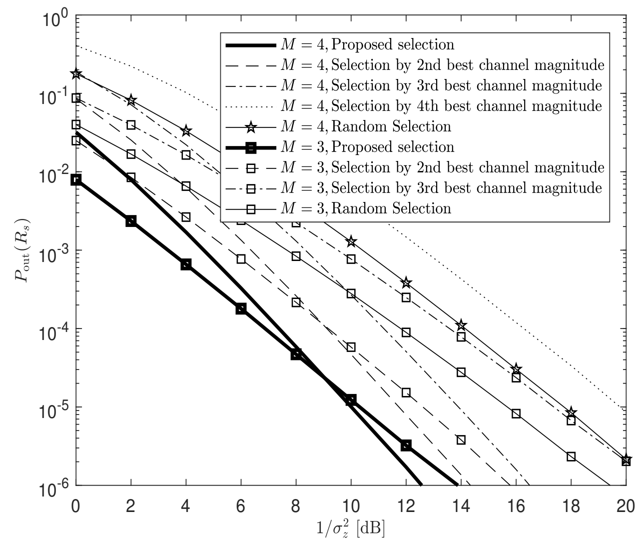

Fig. 4. Secrecy outage probability with different types of selection schemes of the interfering RRH. Scenario $\mathbb{S}_1$ is used for the location of the RRHs.

schemes, such as to use an RRH providing either the second best channel magnitude, the worst channel magnitude, or a random selection [16]. For a fixed setting $(M = 3, N_{h,1} = 1, N_{h,2} = 2, N_{h,3} = 2, N_g = 3)$ and $(M = 4, N_{h,1} = 1, N_{h,2} = 2, N_{h,3} = 2, N_{h,4} = 1, N_g = 3)$, the proposed opportunistic selection for the interfering RRH achieves the best secrecy outage probability performance by decreasing the SINR at the EU to the utmost limit. In general, assigning an RRH connected to the EU via a channel having a greater channel magnitude as the interfering RRH, we can achieve a better secrecy performance. For instance, for $M = 3$, at least 5 dB and 7 dB gains can be achieved at 1×10^{-5} secrecy outage probability over the random selection and the selection scheme that uses a channel having the worst channel magnitude, respectively. At the same secrecy outage probability, when four RRHs are used at maximum, then a 7.5 dB gain over the random selection can be achieved by the proposed selection scheme. Thus these results show an improved secrecy outage probability by the proposed selection scheme.

Fig. 5 shows the diversity gain analysis for various system settings, $N_{h,k}$s, N_g, location of the RRHs with three RRHs ($M = 3$). Since the number of total RRHs is fixed, and one RRH is used as the interfering RRH, the diversity gain is determined by the sum of the multipath components over all the LU channels. For instance, we have $G_d = \min((1 + 2), (1 + 3), (2 + 3))) = 3$ with $(N_h = \{1, 2, 3\}, N_g = 3)$ and scenario S_2. If we study the slope of the corresponding curve of the secrecy outage probability in the log-log scale, we have 3.0837. For scenario the S_1, it is 2.9793. Moreover, the analytical diversity gain is equal to 2.9759. Thus, we can verify Proposition 2 empirically. For different combinations of the multipath components over the LU channels, we can have a similar verification. For instance, we can have 2.8925 and 2.9194 respectively for $(N_h = \{2, 3, 1\}, N_g = 3)$ and $(N_h = \{3, 2, 1\}, N_g = 3)$ with scenario S_2. We also investi-

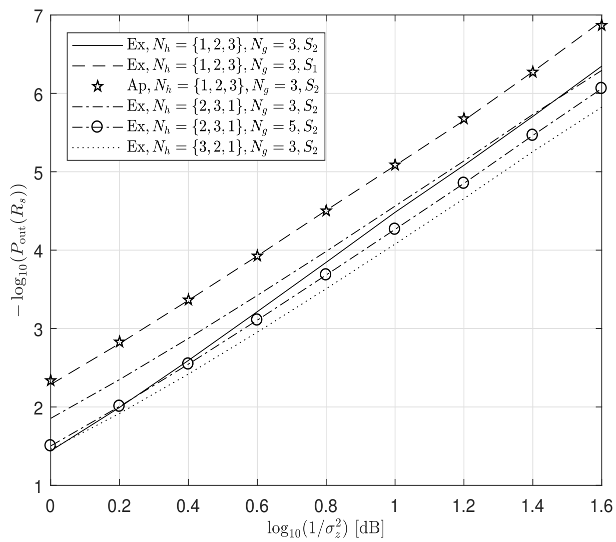

Fig. 5. Secrecy outage probability for various system settings.

gate the effect of N_g on the diversity gain for a particular setting of $(N_h = \{2,3,1\}, N_g = 5)$. Owing to a larger number of multipath components over the EU channels, a higher secrecy outage probability is obtained. However, the number of multipath components over the EU channels has no effect on the diversity gain as verified by Proposition 2. For this scenario, the empirical diversity gain is 2.9766. We can see the effect of multipath diversity on the diversity gain. In the following figure, we can see the effect of transmit diversity by assuming a different maximum number of RRHs.

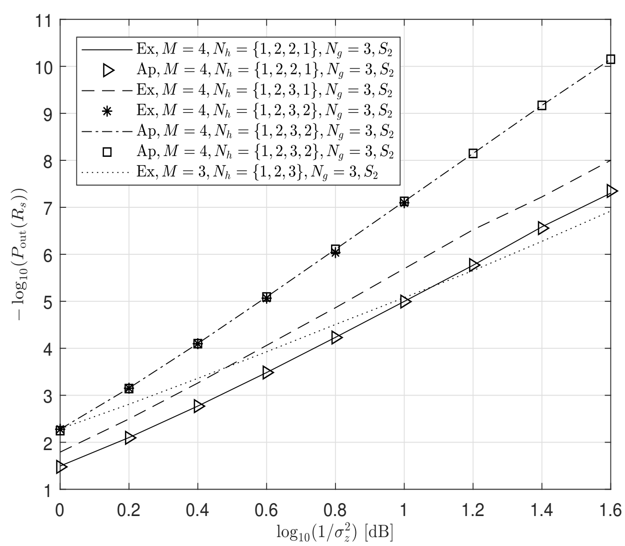

Fig. 6. Secrecy outage probability in the $\log - \log$ scale for various system settings.

For a fixed value of $N_g = 3$, and scenario $\mathbb{S}_2$, Fig. 6 shows that that empirical diversity gains are 3.8638, 3.8908, 4.9131, and 2.9793 for $(M = 4, N_h = \{1,2,2,1\})$, $(M = 4, N_h = \{1,2,3,1\})$, $(M = 4, N_h = \{1,2,3,2\})$, and $(M = 3, N_h = \{1,2,3\})$ in the considered SNR range. In a much higher SNR region, we can expect $4, 4, 5, 3$, respectively, for the diversity gain. From Fig. 6, we can see a tight approximation of the derived secrecy outage probability in the high SNR regime.

B. Probability of Non-Zero Achievable Secrecy Rate

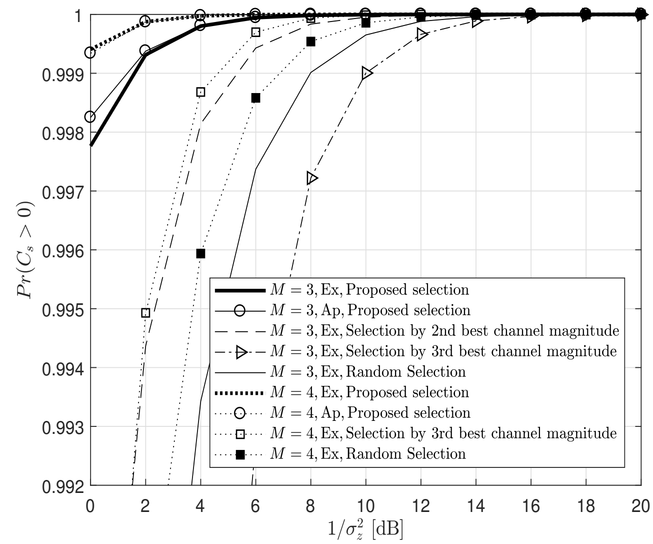

Fig. 7. Probability of non-zero achievable secrecy rate with different types of selection schemes of the interfering RRH. Scenario $\mathbb{S}_2$ is used for the location of RRHs.

In generating Fig. 7, we use fixed values of $(N_h = \{1,2,2\}, \gamma_I = 3)$ dB for $M = 3$ and $(N_h = \{1,2,2,1\}, \gamma_I = 3)$ dB for $M = 4$. From Figs. 7 and 8, we first verify the ac-

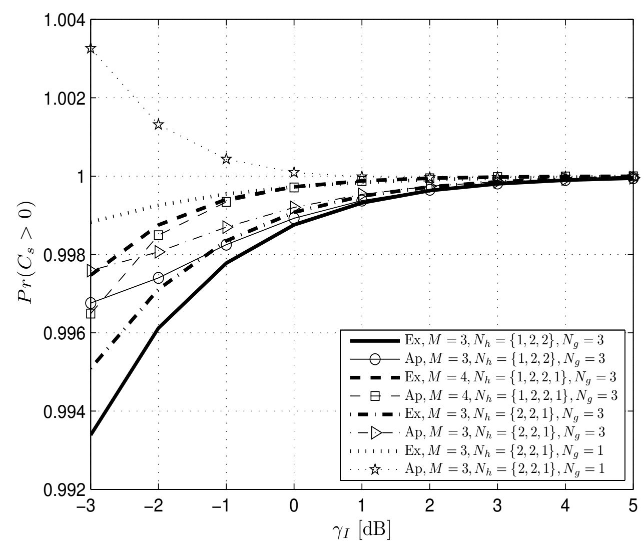

Fig. 8. Probability of non-zero achievable secrecy rate as a function of γ_I. Scenario $\mathbb{S}_2$ is used for the location of RRHs.

curacy of the approximate probability of non-zero achievable secrecy rate. We can see that as either M or γ_I increases, a tight approximation can be obtained. Especially, when $M = 4$, the derived approximation provides a negligible performance loss compared with the exact one. Also, for various system settings, when γ_I is larger than 2 dB, a negligible performance loss is obtained. From Fig. 7, we can see a different convergence behavior of the probability of non-zero achievable secrecy rate. As M increases, $Pr(C_s > 0) = 1$ is obtained due to a larger diversity gain. Compared with other types of selection schemes of the interfering RRH, the proposed scheme provides the fastest convergence to $Pr(C_s > 0) = 1$ due to an increased ratio of the LU's SNR to EU's SINR. For instance, for $M = 3$, $Pr(C_s > 0) = 0.999$ is obtained with 3 dB and 8 dB SNR gain over other selection schemes that use the RRH connected to a channel having the second and third best channel magnitudes among the EU channels, respectively. Comparing with random selection for the interfering RRH, the proposed selection provides a 6 dB gain. As M increases, Fig. 7 shows that the difference between the proposed selection and random selection schemes increases. Moreover, the proposed selection scheme provides a faster convergence to $Pr(C_s > 0) = 1$ over the other considered selection schemes.

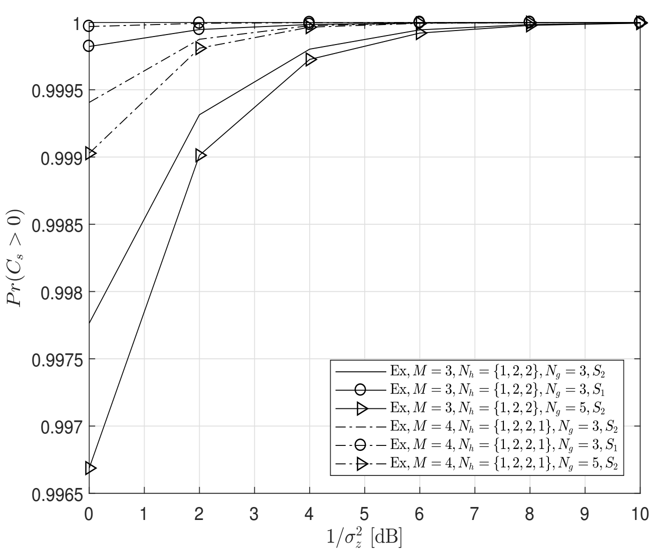

Fig. 9. Probability of non-zero achievable secrecy rate with different settings.

In Fig. 9, we investigate the effects of N_g and distance of RRH from the LU. This figure shows that as N_g increases, a slower convergence to a target probability of non-zero achievable secrecy rate is achieved due to an increased EU's SINR. Since the signal power propagates isotopically in space, and it is decreased inversely proportional to the square of the distance travelled, scenario $\mathbb{S}_2$ results in a slower convergence to a target probability of non-zero achievable secrecy rate due to a decreased LU's SNR. For a fixed $M = 3$, a different convergence behavior can be obtained due to different distances of the RRHs from the LU.

V. Conclusions

In this paper, we have investigated a new physical layer secrecy system that transmits the interfering ANS by assuming a dCDD scheme. Among a set of RRHs, one RRH that is connected to a channel having the best channel magnitude to the EU is selected by the CU as an interfering RRH that transmits the interfering ANS to the EU. This selection is shown to be effective in decreasing the SINR at the EU. In addition, without explicit channel feedback, data RRHs are able to aggregate the receive SNR by their joint collaboration. This has been made possible by removing ISI and a deliberate interfering ANS from the simultaneous legitimate CP-SC transmissions. The proposed secrecy system yields improved secrecy performance by positively affecting the SNR and SINR on both side of the LU and EU. With the aid of simulations, it has been verified that the number of data RRHs and the sum of multipath components jointly determine the achievable diversity gain in the high SNR region.

Appendix A: Derivation of Theorem 2

For the notation, we define $r_m \overset{\triangle}{=} \tilde{S}_{E,(m)}$ in the sequel. Let $z_1 \overset{\triangle}{=} r_M$ and $z_2 \overset{\triangle}{=} \sum_{m=1}^{M-1} r_m$. The bivariate MGF for two random variables z_1 and z_2 is given by (A.1). In (A.1), $f(z_j)$ denotes the PDF of the RV z_j. After replacing $f(z_1)$ with its expression, $f(z_1) = \frac{1}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}} z_1^{N_g-1} e^{-z1/\tilde{\alpha}_g}$, and applying the inverse MGF, we can have the corresponding joint PDF expression for J_1:

$$f_1(z_1, z_2) = \frac{1}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}} \frac{e^{-\frac{1}{\tilde{\alpha}_g}(z_1+z_2)}}{\Gamma(M_m N_g)} z_1^{N_g-1} z_2^{M_m N_g - 1}. \quad \text{(A.2)}$$

Similarly, the corresponding joint PDF expression for J_2 is given by

$$f_2(z_1, z_2) = \frac{1}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}} \frac{e^{-\frac{1}{\tilde{\alpha}_g}(z_1+z_2)}}{\Gamma(M_m N_g - \tilde{q})} z_1^{N_g+\tilde{q}-1} \\ (-nz_1 + z_2)^{M_m N_g - \tilde{q} - 1} \mathrm{U}(-nz_1 + z_2) \quad \text{(A.3)}$$

where $\mathrm{U}(\cdot)$ denotes the unit step function. Now from $f_1(z_1, z_2)$ and $f_2(z_1, z_2)$, the corresponding PDF of the desired quantity $\gamma_E = \frac{z_2}{1+\gamma_I z_1}$ are given by

$$\begin{aligned} f_1(x) &= \frac{x^{M_m N_g - 1} e^{-\frac{x}{\tilde{\alpha}_g}}}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}\Gamma(M_m N_g)} \sum_{p_1=0}^{M_m N_g} \binom{M_m N_g}{p_1} \gamma_I^{p_1} \\ &\quad \int_0^\infty e^{-\frac{(1+\gamma_I x)w}{\tilde{\alpha}_g}} w^{p_1+N_g-1} dw \\ &= \frac{x^{M_m N_g - 1} e^{-\frac{x}{\tilde{\alpha}_g}}}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}\Gamma(M_m N_g)} \sum_{p_1=0}^{M_m N_g} \binom{M_m N_g}{p_1} \gamma_I^{p_1} \\ &\quad \left(\frac{1+\gamma_I x}{\tilde{\alpha}_g}\right)^{-(p_1+N_g)} \Gamma(p_1 + N_g). \end{aligned} \quad \text{(A.4)}$$

To derive a feasible PDF expression from (A.3), we rewrite $g_1(w, x) \overset{\triangle}{=} (1 + \gamma_I w) f_2(w, (1 + \gamma_I w)x)$ into

$$g_1(w, x) =$$

$$
\begin{aligned}
MGF(-S_1,-S_2) &= M!\int_0^\infty e^{-S_1 z_1} f(z_1)dz_1 \int_0^{r_M} e^{-S_2 r_{M-1}} f(r_{M-1})dr_{M-1}\dots\int_0^{r_2} e^{-S_2 r_1} f(r_1)dr_1\\
&= \frac{M!}{(M-1)!}\int_0^\infty e^{-S_1 z_1} f(z_1)dz_1 \Big(\int_0^{z_1} e^{-S_2 r_{M-1}} f(r_{M-1})dr_{M-1}\Big)^{M-1}\\
&= \frac{M!}{(M-1)!}\frac{1}{\tilde{\alpha}_g^{M_m N_g}} \underbrace{\int_0^\infty e^{-S_1 z_1} f(z_1)\Big(S_2+\frac{1}{\tilde{\alpha}_g}\Big)^{-M_m N_g} dz_1}_{J_1} +\\
&\qquad \frac{M!}{(M-1)!}\frac{1}{\tilde{\alpha}_g^{M_m N_g}}\sum_{n=1}^{M-1}\binom{M-1}{n}(-1)^n \sum_{\substack{q_1,\dots,q_{N_g}\\ q_1+\dots+q_{N_g}=n}} \frac{n!}{p_1!\dots p_{N_g}!}\prod_{t_1=0}^{N_g-1}\Big(\frac{1}{t_1!}\Big)^{q_{t_1+1}}\\
&\qquad \underbrace{\int_0^\infty e^{-S_1 z_1} f(z_1) z_1^{\tilde{q}}\Big(S_2+\frac{1}{\tilde{\alpha}_g}\Big)^{\tilde{q}-M_m N_g} e^{-(S_2+\frac{1}{\tilde{\alpha}_g})z_1 n} dz_1}_{J_2}. \qquad \text{(A.1)}
\end{aligned}
$$

$$
\begin{aligned}
&\frac{1}{\Gamma(N_g)\tilde{\alpha}_g^{N_g}}\frac{e^{-\frac{1}{\tilde{\alpha}_g}(w+(1+\gamma_I w)x)}}{\Gamma(M_m N_g-\tilde{q})}\\
&\underbrace{(1+\gamma_I w)w^{N_g+\tilde{q}-1}(-nw+(1+\gamma_I w)x)^{M_m N_g-\tilde{q}-1}}_{J_3}\\
&\mathrm{U}(-nw+(1+\gamma_I w)x). \qquad \text{(A.5)}
\end{aligned}
$$

Since J_3 is combinations of powers of w and powers of binomials of the form $(\alpha+\beta w)$, we express J_3 using only powers of w as:

$$
\begin{aligned}
J_3 = &\sum_{p_1=0}^{1}\sum_{p_2=0}^{M_m N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\binom{1}{p_1}\binom{M_m N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\\
&\gamma_I^{p_1+p_3}(-n)^{M_m N_g-\tilde{q}-p_2-1} w^{c_1-1} x^{p_2}. \qquad \text{(A.6)}
\end{aligned}
$$

Due to the presence of the unit step function in (A.6), the variable w runs over the two exclusive intervals: $\gamma_I x - n < 0$ and $\gamma_I x - n \geq 0$. Thus, we can have

$$
\int_0^{\frac{x}{n-\gamma_I x}} e^{-\frac{w}{\tilde{\alpha}_g}(1+\gamma_I x)} w^{c_1-1} dw, \text{ for } \gamma_I x - n < 0 \quad \text{(A.7)}
$$

$$
\int_0^{\infty} e^{-\frac{w}{\tilde{\alpha}_g}(1+\gamma_I x)} w^{c_1-1} dw, \text{ for } \gamma_I x - n > 0 \quad \text{(A.8)}
$$

which are respectively given by

$$
\begin{aligned}
&\Big(\frac{1+\gamma_I x}{\tilde{\alpha}_g}\Big)^{-c_1}\gamma_l\Big(c_1,\frac{x(1+\gamma_I x)}{\tilde{\alpha}_g(n-\gamma_I x)}\Big), \text{ for } \gamma_I x-n<0\\
&\Big(\frac{1+\gamma_I x}{\tilde{\alpha}_g}\Big)^{-c_1}\Gamma(c_1), \text{ for } \gamma_I x-n>0.
\end{aligned}
$$

Collecting terms, we can obtain (17).

Appendix B: Derivation of Theorem 3

Since the computation of $\Delta_{2,2,s^*}(R_s)$ in (22) is the most challenging, we will mainly focus on the derivation of this equation in the sequel. We first compute $F_{\gamma_R}(J_R(1+x)-1)$,

$$
\begin{aligned}
&(J_R(1+x)-1)^l e^{-(J_R(1+x)-1)/(\tilde{\beta}_{h,ij,s^*})} = e^{-(J_R-1)/(\tilde{\beta}_{h,ij,s^*})}\\
&\sum_{r=0}^{l}\binom{l}{r}(J_R-1)^{l-r} J_R^r x^r e^{-(J_R x)/(\tilde{\beta}_{h,ij,s^*})}. \qquad \text{(B.1)}
\end{aligned}
$$

Thus, $\Delta_{2,2,s^*}(R_s)$ is concluded in the computation of (B.2) at the next page. In (B.2), we have expressed $\big(1+\frac{\gamma_I x}{1+n}\big)^{-c_1}$ via well known formula [36, Eq. (07.34.03.0271.01)] as follows:

$$
\Big(1+\frac{\gamma_I x}{1+n}\Big)^{-c_1} = \frac{1}{\Gamma(c_1)} G_{1,1}^{1,1}\Big(\frac{\gamma_I x}{1+n}\Big|\begin{matrix}1-c_1\\0\end{matrix}\Big). \quad \text{(B.3)}
$$

And then using the Laplace transform of a particular Meijer G-function [36, Eq. (07.34.22.0003.01)], [38, Eq. (2.24.3.1)], (B.2) is evaluated as the one in (B.4) at the next page. After some manipulations, we can obtain $\Delta_{2,2,s^*}(R_s)$ in (22). Similarly, we can readily compute other terms in (22).

Based on (13) and ftn_3 provided in (17), $P_{\text{out},3,s^*}(R_s)$ is computed as the one in (B.5) at the next page.

References

[1] K. J. Kim, H. Liu, M. D. Renzo, P. V. Orlik, and H. V. Poor, "Secrecy performance analysis of distributed CDD based cooperative systems with jamming," in *Proc. IEEE Int. Conf. Commun.*, Kansas City, MO, USA, May 2018.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

$$\Delta_{2,2,s^*}(R_s) \propto e^{-\frac{n}{\gamma_I}\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)}(1+n)^{-c_1}\int_0^\infty \left(x+\frac{n}{\gamma_I}\right)^{p_2+r} e^{-x\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)}\left(1+\frac{\gamma_I x}{1+n}\right)^{-c_1}$$
$$= e^{-\frac{n}{\gamma_I}\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)}\frac{(1+n)^{-c_1}}{\Gamma(c_1)}\sum_{w=0}^{p_2+r}\binom{p_2+r}{w}\int_0^\infty x^w e^{-x\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)} G_{1,1}^{1,1}\left(\frac{\gamma_I x}{1+n}\middle|\begin{array}{c}1-c_1\\0\end{array}\right)dx. \quad \text{(B.2)}$$

$$\Delta_{2,2,s^*}(R_s) \propto e^{-\frac{n}{\gamma_I}\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)}\frac{(1+n)^{-c_1}}{\Gamma(c_1)}\sum_{w=0}^{p_2+r}\binom{p_2+r}{w}\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)^{-1-w}$$
$$G_{2,1}^{1,2}\left(\frac{\gamma_I x}{(1+n)\left(\frac{J_R}{\tilde{\beta}_{h,ij,s^*}}+\frac{1}{\tilde{\alpha}_g}\right)}\middle|\begin{array}{c}-w, 1-c_1\\0\end{array}\right). \quad \text{(B.4)}$$

$$P_{\text{out},3,s^*}(R_s) = \frac{1}{M}\sum_{s^*=1}^{M}\sum_{m=1}^{M-1}\sum_{j=1}^{N_{h,m}}\sum_{p_1=0}^{1}\sum_{p_2=0}^{M_m N_g-\tilde{q}-1}\sum_{p_3=0}^{p_2}\frac{(-1)^m\theta_{m,j,s^*}}{\Gamma(j)}\left(\frac{1}{\tilde{\beta}_{h,m,s^*}}\right)^{-j}\binom{1}{p_1}\tilde{\alpha}_g^{c_1}$$
$$\binom{M_m N_g-\tilde{q}-1}{p_2}\binom{p_2}{p_3}\gamma_I^{p_1+p_3}(-n)^{M_m N_g-\tilde{q}-p_2-1}$$
$$\int_0^{\frac{n}{\gamma_I}}\gamma_l\left(j, \frac{J_R(1+x)-1}{\tilde{\beta}_{h,m,s^*}}\right)x^{p_2}(1+\gamma_I x)^{-c_1}\gamma_l\left(c_1, \frac{x(1+\gamma_I x)}{\tilde{\alpha}_g(n-\gamma_I x)}\right)e^{-x/\tilde{\alpha}_g}dx. \quad \text{(B.5)}$$

[11] 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.*, vol. 65, no. 12, pp. 5514–5528, Dec. 2017.

[12] 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.

[13] 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.

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

[15] 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.

[16] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319–1329, 2017.

[17] 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.

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

[19] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.

[20] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.

[21] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, May 2011.

[22] K. Wang, L. Yuan, T. Miyazaki, S. Guo, and Y. Sun, "Antieavesdropping with selfish jamming in wireless networks: A Bertrand game approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6268–6279, Jul. 2017.

[23] 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.

[24] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[25] Z. Li, R. Yates, and W. Trappe, *Securing Wireless Communications at the Physical Layer - Secrecy Capacity of Independent Parallel Channels*. Boston, MA: Springer, 2009.

[26] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "On secure transmission over parallel relay eavesdropper channel," in *Proc. Annual Allerton Conference on Communication, Control, and Computing.*, Allerton, IL, Sep.-Oct. 2010, pp. 859–866.

[27] K. Lee, J. Kim, J. Jung, and I. Lee, "Zadoff-Chu sequence based signature identification for OFDM," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 4932–4942, Oct. 2013.

[28] J. Blumenstein and M. Bobula, "Coarse time synchronization utilizing symmetric properties of Zadoff-Chu sequences," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 1006–1009, May 2018.

[29] L. Deneire, B. Gyselinckx, and M. Engels, "Training sequence versus cyclic prefix-a new look on single carrier communication," *IEEE Commun. Lett.*, vol. 5, no. 7, pp. 292–294, Jul. 2001.

[30] Y. Zeng and T. S. Ng, "Pilot cyclic prefixed single carrier communication: channel estimation and equalization," *IEEE Signal Process. Lett.*, vol. 12, no. 1, pp. 56–59, Jan. 2005.

[31] Y. Hou and T. Hase, "Improvement on the channel estimation of pilot cyclic prefixed single carrier (PCP-SC) system," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 719–722, Aug. 2009.

[32] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[33] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1243–1254, Jul. 2013.

[34] X. W. Cui, Q. T. Zhang, and Z. M. Feng, "Outage performance for maximal ratio combiner in the presence of unequal-power co-channel interferers," *IEEE Commun. Lett.*, vol. 8, no. 5, pp. 289–291, May 2004.

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

[36] Wolfman research inc. [Online]. Available: http://functions.wolfman.com

[37] K. P. Peppas, N. C. Sagias, and A. Maras, "Physical layer security for multiple-antenna systems: A unified approach," *IEEE Trans. Commun.*, vol. 64, pp. 314–328, Jan. 2016.

[38] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integral and Series. Vol. 3: More Special Functions*, 3rd ed. London: Gordon and Breach, 1992.