Distributed Asynchronous Cyclic Delay Diversity-Based Cooperative Systems with a Passive Eavesdropper

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

TR2019-136 December 09, 2019

Abstract

A joint data and jamming transmission scheme based on a new distributed asynchronous cyclic delay diversity (dACDD) scheme is proposed for cooperative communication systems. Without any exact knowledge of channel state information (CSI) at the transmitting side, a joint remote radio head (RRH) selection scheme for the data and jamming signal transmissions is proposed for dACDD to achieve the maximum diversity gain at a legitimate user (LU), while degrading the receive signalto-interference-plus-noise ratio at an eavesdropping user (EU). A single RRH connected with the channel having the greatest channel gain is selected as a data RRH that transmits a desired confidential signal, whereas the remaining RRHs are controlled by the central control unit to transmit an artificial noise sequence (ANS) to the LU and EU. Without assuming exact knowledge of CSI of the whole system, the secrecy outage probability of the distributed communication system is analyzed by deriving a closed-form expression, and through link-level simulations over non-identically distributed frequency selective fading channels over the entire system.

IEEE Global Communications Conference (GLOBECOM)

Distributed Asynchronous Cyclic Delay Diversity-Based Cooperative Systems with a Passive Eavesdropper

Kyeong Jin Kim, Hongwu Liu, Miaowen Wen, Philip V. Orlik, and H. Vincent Poor

***Abstract*—A joint data and jamming transmission scheme based on a new distributed asynchronous cyclic delay diversity (dACDD) scheme is proposed for cooperative communication systems. Without any exact knowledge of channel state information (CSI) at the transmitting side, a joint remote radio head (RRH) selection scheme for the data and jamming signal transmissions is proposed for dACDD to achieve the maximum diversity gain at a legitimate user (LU), while degrading the receive signal-to-interference-plus-noise ratio at an eavesdropping user (EU). A single RRH connected with the channel having the greatest channel gain is selected as a data RRH that transmits a desired confidential signal, whereas the remaining RRHs are controlled by the central control unit to transmit an artificial noise sequence (ANS) to the LU and EU. Without assuming exact knowledge of CSI of the whole system, the secrecy outage probability of the distributed communication system is analyzed by deriving a closed-form expression, and through link-level simulations over non-identically distributed frequency selective fading channels over the entire system.**

***Index Terms*—Physical layer security, distributed asynchronous cyclic delay diversity, secrecy outage probability.**

I. Introduction

Physical layer security (PLS) is emerging as a promising approach that enhances the secrecy level of wireless communications by utilizing physical characteristics of wireless channels, and has attracted considerable recent attention [1]–[6]. As one PLS approach, the transmitting side jams an eavesdropping user (EU) by transmitting artificial noise (AN) [1], [7]–[10] to degrade the reception quality at the EU while maximizing the reception quality at a legitimate user (LU). When exact channel state information (CSI) of the entire system is available at the transmitting side, the joint data and jamming signal transmissions can be made either at the same transmitter [7] or separate transmitters [9]–[11]. Similarly, multiple transmitters can be jointly used for the data and jamming transmissions without utilizing secrecy beamforming [12].

Without specific descriptions, it has been assumed that exact CSI for the legitimate channels is available by explicit feedback from the LU for processing of beamforming/precoding and jamming signal transmissions. However, the EU can intercept this type of feedback to lessen the benefit of PLS. Thus, it is desirable to avoid this feedback from the PLS perspective. For this reason, an original distributed cyclic delay diversity (dCDD) scheme [13] has been adapted to the PLS system in the presence of a single active EU [12]. In contrast to other works [9], [10], transmit diversity and intersymbol interference (ISI)-free single carrier transmissions are jointly used in [13] to degrade the reception quality, namely the signal-to-interference-plus-noise ratio (SINR), at the EU, while maximizing it, namely the signal-to-noise ratio (SNR) at the LU.

A. Problem statement and contribution

1) Tight time synchronization among remote radio heads (RRHs): RRHs are connected to the central control unit (CU) via wireless backhaul and implemented by only simple hardware, and thus tight synchronization among them is not achievable. For this reason, synchronous signal reception may not be achievable, which influences the objective of dCDD, namely removing ISI caused by frequency selective fading and multiple transmissions. Thus, one of the objectives of this paper is to propose a distributed asynchronous CDD (dACDD) that supports asynchronous single carrier transmissions.
2) Joint selection scheme: The EU is working usually in a passive mode, so that neither the exact CSI of the legitimate channels nor that of the eavesdropper channels is available at the transmitting side [2], [11]. Thus, the joint selection scheme for the data and interfering RRHs proposed by [12] is inappropriate for this new practical setting due to the requirement of partial CSI. To degrade the reception quality at the EU, it is preferable to use as many RRHs as interfering RRHs without causing ISI at the LU. Thus, we introduce a systematic procedure for selecting the data RRH and interfering RRHs under the framework of dACDD in the presence of one passive EU. The single data RRH transmits an intended data signal to the LU, whereas the interfering RRHs are mainly jamming the EU by transmitting the AN as the jamming signal.

Notation: $\mathbb{N}_0$ denotes the set of non-negative integers; $\mathbb{C}$ denotes the set of complex numbers; $\boldsymbol{I}_N$ denotes an $N \times N$ identity matrix; $\mathbf{0}$ denotes an all-zero matrix of an appropriate size; $\mathcal{CN}\left(\mu, \sigma^2\right)$ denotes a complex Gaussian distribution with mean μ and variance σ^2; $F_{\varphi}(\cdot)$ denotes the cumulative distri-

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. Wen is with South China University of Technology, Guangzhou, China

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-0939370 and CCF-1513915.

bution function (CDF) of the random variable (RV) φ, whereas its probability density function (PDF) is denoted by $f_{\varphi}(\cdot)$; and 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 $\mathbb{S}_M$, composed of M positive integers, $[1, 2, \ldots, M]$, $\mathbb{S}_{M\setminus j}$ denotes $\mathbb{S}_M$ with excluding j; and $\tilde{\mathbb{S}}_M$ is another set that is obtained after randomizing a list of $\mathbb{S}_M$.

II. System and Channel Models

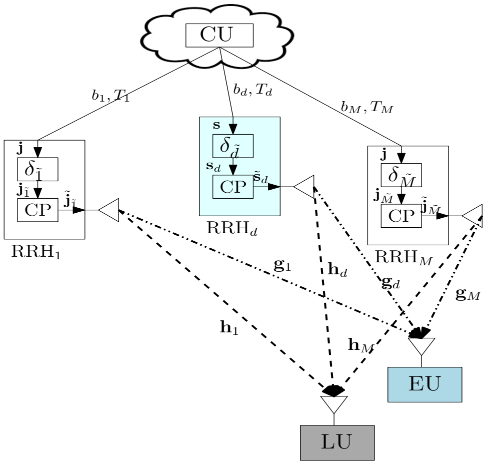

Fig. 1. Illustration of the considered cooperative system. In this example, one RRH highlighted in a different color is assigned as the data RRH, whereas the remaining $(M-1)$ RRHs are assigned as interfering RRHs.

Fig. 1 illustrates the considered distributed communication system. Wireless backhaul links, $\{b_m\}_{m=1}^{M}$, are configured to provide broadband backhaul access to the RRHs via the CU. Each node in the system is assumed to be equipped with a single antenna, due to practical constraints on the hardware complexity and power. To protect the confidential information in communication from the EU, one of the RRHs is assigned as the data RRH, while the remaining RRHs are assigned as interfering RRHs that transmit artificial noise sequences (ANSs). Each RRH acts either as the data RRH or as the interfering RRH under the control of the CU. Since this paper assumes no exact CSI at the transmitting side, optimal selections [8], [9] for the interfering RRHs are not available.

A frequency selective fading channel from the mth RRH to the EU is denoted by $\boldsymbol{g}_m$ with $\mathbb{L}(\boldsymbol{g}_m) = N_{g,m}$. The LU is placed at a specific location with respect to the RRHs, and, thus, independent but non-identically distributed (i.n.i.d.) frequency selective fading channels from the RRHs to the LU are also assumed. A frequency selective fading 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 by either sending a training sequence [14] or adding pilot symbols as the suffix to each symbol block [15].

A. Asynchronous signal reception

Without loss of generality, we assume that RRH_1's signal arrives at the LU first. The relative time difference between the arrival time of the signal transmitted from RRH_m and that of the signal transmitted from RRH_1 is denoted by $T_m \in \mathbb{N}_0$. Due to the use of single carrier transmissions, a transmission symbol block, $\boldsymbol{s} \in \mathbb{C}^{B\times 1}$, comprises B modulated symbols. Also, to eliminate ISI caused by frequency selective fading, N_{CP}-length CP is appended to the front of $\boldsymbol{s}$. One example of asynchronous signal reception at the LU is illustrated in Fig. 2. This paper assumes that the relative arrival time differences are all less than N_{CP}, so that $T_2 < N_{\mathrm{CP}}$ and $T_3 < N_{\mathrm{CP}}$.

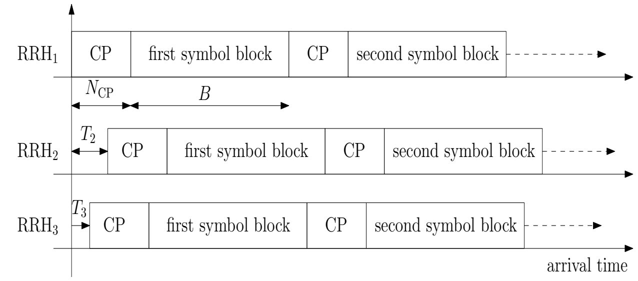

Fig. 2. One example of asynchronous reception at the LU with relative arrival time differences $T_2 \in \mathbb{N}_0$ and $T_3 \in \mathbb{N}_0$.

Due to the frequency selective fading channels from RRHs to the LU, we have $N_{\mathrm{CP}} = \max(\{N_{h,m}\}_{m=1}^{M})$. To apply the correct circular shifting at each of the RRHs, N_{CP} must be fed back by the LU. The index of the data RRH is determined in terms of the channel quality measured and then fed back by the LU. Additionally, independent of the LU and EU channels, the CU forms $\mathbb{S}_M$ and $\tilde{\mathbb{S}}_M$, a randomized set of $\mathbb{S}_M$, and share both of them with only RRHs and LU.

Without considering interference, noise, and dACDD operation, the ideally received signal at the LU is given by

$$\begin{aligned}\boldsymbol{r}_I = &\sqrt{P_T \alpha_{h,1}}\boldsymbol{H}_1\boldsymbol{s} + \sqrt{P_T \alpha_{h,2}}\boldsymbol{\Pi}_2\boldsymbol{H}_2\boldsymbol{s} + \\ &\cdots + \sqrt{P_T \alpha_{h,M}}\boldsymbol{\Pi}_M\boldsymbol{H}_M\boldsymbol{s} \qquad (1)\end{aligned}$$

where P_T is the transmission power at the RRHs and $\boldsymbol{H}_m$ is a right circulant matrix determined by $\boldsymbol{h}_m$. Additionally, $\alpha_{h,m}$ accounts for the distance-dependent large scale fading over the channel $\boldsymbol{h}_m$. For a distance $d_{1,m}$ from the mth RRH to LU, $\alpha_{h,m}$ is given by $\alpha_{h,m} = d_{1,m}^{-\epsilon}$, where ϵ denotes the path loss exponent. Furthermore, $\boldsymbol{\Pi}_M$ denotes the $B \times B$ orthogonal permutation matrix obtained by circularly shifting $\boldsymbol{I}_B$ down by T_m rows. Based on (1), the following theorem provides a condition under which dACDD makes asynchronous transmissions without causing ISI at the LU.

Theorem 1: Let $T_m \in \mathbb{N}_0$, with $m \in \mathbb{S}_M$, be the relative arrival time difference of RRH_m with respect to RRH_1, and $\Delta_{\tilde{m}} = (\tilde{m} - 1)N_{\mathrm{CP}}$, with $\tilde{m} \in \tilde{\mathbb{S}}_M$, be the CDD delay of RRH_m, which assures ISI-free reception at the LU. Then, for ISI-free transmission to the LU, RRH_m needs to apply circular shifting by $\delta_{\tilde{m}} \triangleq \Delta_{\tilde{m}} - T_m$. This can be implemented by multiplying the input symbol $\boldsymbol{s}$ by the permutation matrix,

$\boldsymbol{P}_{B,m,\delta_{\tilde{m}}} \in \mathbb{N}_0^{B\times B}$, which can be obtained by circularly shifting $\boldsymbol{I}_B$ down by $\delta_{\tilde{m}}$ rows.

Proof: From (1), we can first verify that $\boldsymbol{\Pi}_m \boldsymbol{H}_m$ is a right circulant matrix, whose first column vector, $\boldsymbol{h}_m$, is shifted down by T_m from asynchronous reception at the LU. To move down by $\Delta_{\tilde{m}} \geq T_m$ in total, another circular shift by $\delta_{\tilde{m}}$ is required at RRH_m with respect to the input transmission symbol block, $\boldsymbol{s}$. This operation can be expressed mathematically as multiplication by the permutation matrix, $\boldsymbol{P}_{B,m,\delta_{\tilde{m}}}$. ■

Based on Theorem 1, we can specify a condition for dACDD as follows:

$$\Delta_{\tilde{m}} = (\tilde{m}-1)N_{\mathrm{CP}} \text{ with cyclic delay } \delta_{\tilde{m}}. \tag{2}$$

Furthermore, N_{CP} and B jointly determine the maximum allowable number of RRHs for dACDD operation as follows:

$$K = \left\lfloor \frac{B}{N_{\mathrm{CP}}} \right\rfloor \tag{3}$$

where $\lfloor\cdot\rfloor$ denotes the floor function.

For dACDD processing, the set of relative arrival time differences, $\{T_m\}_{m=2}^{M}$ is required at the CU. Thus, the LU first needs to know $\{T_m\}_{m=2}^{M}$ via [16], and then feed them back to the CU. Note that due to an additional random relative arrival time difference over the LU channels, independent of the EU channels, asynchronous reception can prevent the ANS from being decoded by the EU.

According to Fig. 1, wherein the dth RRH is assigned as the data RRH, the symbol block is formed as $\tilde{\boldsymbol{s}}_d \triangleq \begin{bmatrix} \boldsymbol{s}_d(B-N_{\mathrm{CP}}+1:B,1) \\ \boldsymbol{s}_d \end{bmatrix} \in \mathbb{C}^{(B+N_{\mathrm{CP}})\times 1}$, and then transmitted via $\boldsymbol{h}_d$. The corresponding CDD delay is applied to $\boldsymbol{s}$; that is, $\boldsymbol{s}_d = \boldsymbol{P}_{B,d,\delta_{\tilde{d}}}\boldsymbol{s}$, with $d \in \tilde{\mathbb{S}}_M$. Then, the other RRHs are assigned as interfering RRHs. When the mth RRH is assigned as an interfering RRH, the resulting mth ANS is generated as $\boldsymbol{j}_{\tilde{m}} = \boldsymbol{P}_{B,m,\delta_{\tilde{m}}}\boldsymbol{j}$, where $\tilde{m} \in \tilde{\mathbb{S}}_{M\backslash d}$ and $\boldsymbol{j}$ is the original AN sequence. For $\boldsymbol{j}_{\tilde{m}}$, a CP of N_{CP} symbols is appended to the front of $\boldsymbol{j}_{\tilde{m}}$; that is, we have $\tilde{\boldsymbol{j}}_m \triangleq \begin{bmatrix} \boldsymbol{j}_{\tilde{m}}(B-N_{\mathrm{CP}}+1:B,1) \\ \boldsymbol{j}_{\tilde{m}} \end{bmatrix} \in \mathbb{C}^{(B+N_{\mathrm{CP}})\times 1}$. After that $\tilde{\boldsymbol{j}}_m$ is transmitted sequentially to the LU via $\boldsymbol{h}_m$. The EU receives $\tilde{\boldsymbol{j}}_m$ via $\boldsymbol{g}_m$.

B. Received signals

After the removal of the CP signal, the received signal at the LU is given by

$$\tilde{\boldsymbol{r}}_L = \sqrt{P_T\alpha_{h,d}}\boldsymbol{\Pi}_d\boldsymbol{H}_d\boldsymbol{P}_{B,d,\delta_{\tilde{d}}}\boldsymbol{s} + \sum_{m\in\mathbb{S}_{M\backslash d},\tilde{m}\in\tilde{\mathbb{S}}_{M\backslash d}} \sqrt{P_J\alpha_{h,m}}\boldsymbol{\Pi}_m\boldsymbol{H}_m\boldsymbol{j}_{\tilde{m}} + \boldsymbol{z}_L \tag{4}$$

where P_J is the transmission power for ANS transmissions. The additive vector noise over the LU channels is denoted by $\boldsymbol{z}_L \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_B)$.

As for the ANS, $\boldsymbol{j}$, we assume that $E\{\boldsymbol{j}\} = \boldsymbol{0}$, and $E\{\boldsymbol{j}\boldsymbol{j}^H\} = \boldsymbol{I}_B$, so that we have $E\{\boldsymbol{j}_{\tilde{m}}\} = \boldsymbol{0}$, and $E\{\boldsymbol{j}_{\tilde{m}}(\boldsymbol{j}_{\tilde{m}})^H\} = \boldsymbol{I}_B$. Note that in the generation of $\boldsymbol{j}_{\tilde{m}}$, $\boldsymbol{P}_{B,m,\delta_{\tilde{m}}}$ is mainly determined by the LU channels, independent of the EU channels. We can summarize several benefits of dACDD from the PLS perspective as follows:

1) The randomized set $\tilde{\mathbb{S}}_M$ is not available at the EU. Thus, a set of ANSs, $\{\boldsymbol{j}_{\tilde{m}}\}_{\tilde{m}\in\tilde{\mathbb{S}}_{M\backslash d}}$, is known only to the CU, RRHs, and LU. That is, the EU cannot decode ANSs. Thus, the dACDD scheme can provide a deliberate set of ANSs to the EU.
2) Since different relative arrival time differences $\{T_m\}_{m=2}^{M}$ are independent of those of the asynchronous transmissions from RRHs to the EU, $\{T_m\}_{m=2}^{M}$ appears as the set of random variables to the EU, which means the asynchronous transmissions improve protecting of the ANS from decoding by the EU. This significantly enhances the secrecy level. However, to achieve these benefits, ISI-free reception is required at the LU.

Utilizing ISI-free reception and known ANSs at the LU, we can rewrite (4) as follows:

$$\boldsymbol{r}_L = \sqrt{P_T\alpha_{h,d}}\boldsymbol{\Pi}_d\boldsymbol{H}_d\boldsymbol{P}_{B,d,\delta_{\tilde{d}}}\boldsymbol{s} + \boldsymbol{z}_L. \tag{5}$$

In contrast, the received signal at the EU is given by

$$\boldsymbol{r}_E = \sqrt{P_T\alpha_{g,d}}\breve{\boldsymbol{\Pi}}_d\boldsymbol{G}_d\boldsymbol{P}_{B,d,\delta_{\tilde{d}}}\boldsymbol{s} + \sum_{m\in\mathbb{S}_{M\backslash d},\tilde{m}\in\tilde{\mathbb{S}}_{M\backslash d}} \sqrt{P_J\alpha_{g,m}}\breve{\boldsymbol{\Pi}}_m\boldsymbol{G}_m \underbrace{\boldsymbol{P}_{B,m,\delta_{\tilde{m}}}\boldsymbol{j}}_{j_{\tilde{m}}} + \boldsymbol{z}_E \tag{6}$$

where $\boldsymbol{G}_d$ and $\boldsymbol{G}_m$ are right circulant matrices specified by the equivalent channel vectors $\boldsymbol{g}_d$ and $\boldsymbol{g}_m$, respectively. Additionally, $\alpha_{g,m}$ is used to model the distance-dependent large scale fading from the mth RRH to the EU. The set of relative arrival differences from RRHs to the EU, $\{\breve{T}_m\}_{m=1}^{M}$, specifies $\breve{\boldsymbol{\Pi}}_m$. We also assume that $\boldsymbol{z}_E \sim \mathcal{CN}(\boldsymbol{0}, \sigma_z^2\boldsymbol{I}_B)$. Note that the relative arrival time difference T_m is independent of the channels from RRHs to the EU, that is, $T_m \neq \breve{T}_m$. Most importantly, $\mathbb{S}_M$ and $\tilde{\mathbb{S}}_{M\backslash d}$ are shared only by by CU, RRHs, and LU.

III. Performance Analysis

A. Receive SNR at the LU over i.n.i.d. frequency selective fading channels

In the sequel, the mth receive SNR at the LU, achievable by the mth LU channel, is denoted by $\gamma_{L,m} \triangleq \frac{P_T\alpha_{h,m}}{\sigma_z^2}\|\boldsymbol{h}_m\|^2$ since $\boldsymbol{\Pi}_m\boldsymbol{H}_m\boldsymbol{P}_{B,m,\delta_{\tilde{m}}}$ is right circulant.

For i.n.i.d. frequency selective fading channels, the probability that RRH_d is selected as the data RRH is given by (7), shown at the top of the next page. In (7), we have defined

$$\tilde{\alpha}_{h,m} \triangleq \frac{P_T\alpha_{h,m}}{\sigma_z^2}, \tilde{\beta}_d \triangleq \sum\nolimits_{t=1}^{m} 1/\tilde{\beta}_{h,q_t,\backslash d}, \tilde{l}_d \triangleq \sum\nolimits_{t=1}^{m} \ell_t, \text{ and}$$
$$\Upsilon_d \triangleq \sum\nolimits_{q_1=1}^{M-m} \cdots \sum\nolimits_{q_m=q_{m-1}+1}^{M-1} \sum\nolimits_{\ell_1=0}^{N_{h,q_1}-1} \cdots \sum\nolimits_{\ell_m=0}^{N_{h,q_m}-1} \tag{8}$$

For a set of the channel magnitudes over the LU channels, $\tilde{\beta}_{h,j,\backslash d}$ denotes the jth $\tilde{\alpha}_h$s indexed by $j \in \mathbb{S}_{M\backslash d}$.

$$P_r(d)\overset{\triangle}{=}P_r(\mathrm{RRH}_d=\mathrm{dataRRH})=1+\frac{1}{\Gamma(N_{h,d})(\tilde{\alpha}_{h,d})^{N_{h,d}}}\sum_{m=1}^{M-1}(-1)^m\Upsilon_d\prod_{t=1}^{m}\Big(\frac{1}{\ell_t!(\tilde{\beta}_{h,q_t,\backslash d})^{\ell_t}}\Big)$$
$$\Gamma(N_{h,d}+\tilde{l}_d)\big(\tilde{\beta}_d+\frac{1}{\tilde{\alpha}_{h,d}}\big)^{-(N_{h,d}+\tilde{l}_d)}. \tag{7}$$

According to (5), the conditional receive SNR at the LU, given by the channel $\boldsymbol{h}_d$, which was chosen for data transmissions, is given by

$$\gamma_{L,d}=\tilde{\alpha}_{h,d}\sum_{l=1}^{N_{h,d}}|\boldsymbol{h}_d(l)|^2. \tag{9}$$

The CDF of $\gamma_{L,d}$, over an i.n.i.d frequency selective fading channel, is given by (10), shown at the top of the next page. In (10), we have defined

$$\mathbb{X}_{L_1}\overset{\triangle}{=}\sum\nolimits_{l_1=0}^{N_{h,d}-1}1/\Gamma(l_1+1),$$
$$\mathbb{X}_{L_2}\overset{\triangle}{=}\big(\tilde{\beta}_d+\frac{1}{\tilde{\alpha}_{h,d}}\big)^{-(N_{h,d}+\tilde{l}_d)}\frac{\Gamma(N_{h,d}+\tilde{l}_d)}{\Gamma(N_{h,d})(\tilde{\alpha}_{h,d})^{N_{h,d}}}$$
$$\sum\nolimits_{m_1=1}^{M-1}(-1)^{m_1}\Upsilon_d\prod\nolimits_{t=1}^{m_1}\big(\frac{1}{\ell_t!(\tilde{\beta}_{h,q_t,\backslash d})^{\ell_t}}\big),$$

and $\gamma_l(\cdot,\cdot)$ denotes the lower incomplete gamma function [17, Eq. (8.350.1)]. Due to space limitations, we omit the derivation of (10).

B. Receive SINR at the EU over i.n.i.d. frequency selective fading channels

From (6), the received signal at the EU consists of the desired signal being intercepted by the EU, non-decodable interference by the use of ANS, and noise. Thus, the receive signal power, $S_{E,d}$, and noise-plus-interference power due to the interfering signal, $N_{E,d}$, at the EU are respectively given by

$$S_{E,d}=P_T\alpha_{g,d}\sum_{l=1}^{N_{g,d}}|\boldsymbol{g}_d(l)|^2 \text{ and}$$
$$N_{E,d}=P_J\sum_{m\in\mathbb{S}_{M\backslash d}}\alpha_{g,m}\sum_{l=1}^{N_{g,m}}|\boldsymbol{g}_m(l)|^2+\sigma_z^2 \tag{11}$$

where $S_{E,d}$ is the signal power provided by the dth RRH. Note that $\breve{\boldsymbol{\Pi}}_m\boldsymbol{G}_m\boldsymbol{P}_{B,m,\delta_{\tilde{m}}}$ is also right circulant. In addition, the remaining $(M-1)$ RRHs are assigned as the set of interfering RRHs. Thus, $S_{E,d}/N_{E,d}$ decreases in general as the number of RRHs increases, which is beneficial for increasing the security of the proposed cooperative system. Note that the EU channels are independent of the LUs channels, so that the conditional SINR at the EU is given by

$$\gamma_{E,d}=\frac{S_{E,d}}{N_{E,d}}=\frac{\tilde{\alpha}_{g,d}\sum_{l=1}^{N_{g,d}}|\boldsymbol{g}_d(l)|^2}{\sum_{m\in\mathbb{S}_{M\backslash d}}\tilde{\alpha}_{g,m}\sum_{l=1}^{N_{g,m}}|\boldsymbol{g}_m(l)|^2+1} \tag{12}$$

where $\tilde{\alpha}_{g,d}\overset{\triangle}{=}\frac{P_T\alpha_{g,d}}{\sigma_z^2}$ and $\tilde{\alpha}_{g,m}\overset{\triangle}{=}\frac{P_J\alpha_{g,m}}{\sigma_z^2}$. Note that $\tilde{\alpha}_{g,d}$ is multiplied by P_T, whereas $\{\tilde{\alpha}_{g,m}\}_{m\in\mathbb{S}_{M\backslash d}}$ are multiplied by P_J.

Over i.n.i.d. frequency selective fading EU channels, the PDF of the SINR at the EU is given by

$$f_{\gamma_{E,d}}(x)=\mathbb{X}_E e^{-\frac{x}{\tilde{\alpha}_{g,d}}}(x)^{N_{g,d}-1}\left(\frac{x}{\tilde{\alpha}_{g,d}}+\frac{1}{\tilde{\beta}_{g,m_3,\backslash d}}\right)^{-(l_2+j)} \tag{13}$$

where

$$\mathbb{X}_E\overset{\triangle}{=}\frac{1}{\Gamma(N_{g,d})(\tilde{\alpha}_{g,d})^{N_{g,d}}}\sum\nolimits_{m_3\in\mathbb{S}_{M\backslash d}}\sum\nolimits_{j=1}^{N_{g,m_3}}\sum\nolimits_{l_2=0}^{N_{g,d}}$$
$$\frac{(-1)^{m_3}\theta_{m_3,j,\backslash d}}{\Gamma(j)}\binom{N_{g,d}}{l_2}\Gamma(l_2+j)$$

and $\theta_{m_3,j,\backslash d}$ is defined in Appendix A. In addition, $\tilde{\beta}_{g,m_3,\backslash d}$ denotes the m_3th $\tilde{\alpha}_g$s indexed by $m_3\in\mathbb{S}_{M\backslash d}$. Due to space limitations, we omit the derivation of (13). The SNR and SINR expressed by Eqs. (9) and (12) can be empirically derived when we use a maximum-likelihood detector [18], [19] for CP-SC transmissions.

C. Secrecy outage probability

At a given secrecy rate R_s, the conditional secrecy outage probability is defined by [2]

$$\begin{aligned}P_{d,\text{out}}(R_s)&=P_r(C_{s,d}<R_s)\\&=\int_0^\infty F_{\gamma_{L,d}}(J_R(1+x)-1)f_{\gamma_{E,d}}(x)dx\end{aligned} \tag{14}$$

where $J_R\overset{\triangle}{=}2^{R_s}$. A closed form expression for $P_{d,\text{out}}(R_s)$, can be derived in the next theorem.

Theorem 2: For i.n.i.d. frequency selective fading over the entire legitimate and eavesdropper channels, the proposed single carrier system improves PLS by employing dCDD that supports simultaneous data and jamming transmissions. The achievable conditional secrecy outage probability at secrecy rate R_s is given by (15), shown at the top of the next page. In (15), we have defined

$$\Delta J_R\overset{\triangle}{=}J_R(\tilde{\beta}_d+1/\tilde{\alpha}_{h,d})+1/\tilde{\alpha}_{g,d},$$
$$\mathbb{X}_{P_1}\overset{\triangle}{=}\mathbb{X}_{L_1}e^{-\frac{(J_R-1)}{\tilde{\alpha}_{h,d}}}\sum\nolimits_{j_2=0}^{l_1}\binom{l_1}{j_2}\mathbb{X}_E\big(1/\tilde{\beta}_{g,m_3,\backslash d}\big)^{-l_2-j}$$
$$\frac{(J_R-1)^{l_1-j_2}J_R^{j_2}}{\Gamma(l_2+j)}\big(\frac{J_R}{\tilde{\alpha}_{h,d}}+\frac{1}{\tilde{\alpha}_{g,d}}\big)^{-j_2-N_{g,d}}, \text{ and}$$
$$\mathbb{X}_{P_2}\overset{\triangle}{=}e^{-(J_R-1)(\tilde{\beta}_d+\frac{1}{\tilde{\alpha}_{h,d}})}\sum\nolimits_{m_2=0}^{N_{h,d}+\tilde{l}_d-1}\frac{1}{\Gamma(m_2+1)}$$
$$\big(\tilde{\beta}_d+\frac{1}{\tilde{\alpha}_{h,d}}\big)^{m_2}\sum\nolimits_{j_3=0}^{m_2}\binom{m_2}{j_3}(J_R-1)^{m_2-j_3}J_R^{j_3}.$$

$$F_{\gamma_{L,d}}(x) = \frac{1}{P_r(d)} - \frac{\mathbb{X}_{L_1}}{P_r(d)} e^{-\frac{x}{\tilde{\alpha}_{h,d}}} x^{l_1} + \\ \frac{\mathbb{X}_{L_2}}{P_r(d)} \Big(1 - \sum_{m_2=0}^{N_{h,d}+\tilde{l}_d-1} \frac{1}{\Gamma(m_2+1)} \big(\tilde{\beta}_d + \frac{1}{\tilde{\alpha}_{h,d}}\big)^{m_2} x^{m_2} e^{-(\tilde{\beta}_d + \frac{1}{\tilde{\alpha}_{h,d}})x} \Big) \tag{10}$$

$$P_{d,\text{out}}(R_s) = \frac{1}{P_r(d)} - \frac{\mathbb{X}_{P_1}}{P_r(d)} G_{2,1}^{1,2}\left(\frac{\tilde{\beta}_{g,m_3,\backslash d}}{\tilde{\alpha}_{g,d}} \big(\frac{J_R}{\tilde{\alpha}_{h,d}} + \frac{1}{\tilde{\alpha}_{g,d}}\big)^{-1} \middle| \begin{matrix} 1-j_2-N_{g,d}, 1-l_2-j \\ 0 \end{matrix} \right) + \frac{\mathbb{X}_{L_2}}{P_r(d)} \\ \Big[1 - \mathbb{X}_{P_2} G_{2,1}^{1,2}\left(\frac{\tilde{\beta}_{g,m_3,\backslash d}}{\tilde{\alpha}_{g,d}} (\Delta J_R)^{-1} \middle| \begin{matrix} 1-j_3-N_{g,d}, 1-l_2-j \\ 0 \end{matrix} \right)\Big]. \tag{15}$$

In (15), $G_{p,q}^{m,n}\left(t \middle| \begin{matrix} a_1,...,a_n,a_{n+1},...,a_p \\ b_1,...,b_m,b_{m+1},...,b_q \end{matrix}\right)$ denotes the Meijer G-function [17, Eq. (9.301)].

Proof: Due to space limitations, we omit the derivation. ■

Again, at each of the transmissions, only one RRH is selected as the data RRH, so that the selections of the data RRH are mutually exclusive and independent of each other. Thus, the marginal secrecy outage probability achieved by the proposed dCDD based PLS system is given by

$$P_{\text{out}}(R_s) = \sum_{d=1}^{M} P_{d,\text{out}}(R_s) P_r(d). \tag{16}$$

IV. Simulation Results

In this section, we first verify the derived closed form expression for the secrecy outage probability. To this end, we compare the analytically derived performance metric (denoted by **An**) with the exact performance metric (denoted by **Ex**) for various scenarios. The corresponding marginal (unconditional) metrics are denoted by **mAn** and **mEx**. Note that **mAn** is derived by (16).

We assume that the LU and EU are respectively placed at $(x = 0.5, y = R/2)$ and $(x = 1, y = 3)$. The transmission block size is made of 64 symbols ($B = 64$). The CP length is given by 16 symbols ($N_{\text{CP}} = 16$). Thus, four RRHs can be used for dACDD. In all scenarios, we fix $P_T = 1$ and $R_s = 1$. Unless otherwise noted, we assume $P_J/\sigma_z^2 = 2$ dB. A fixed path-loss exponent is assumed to be $\epsilon = 2.09$ [20]. T_m and $\breve{T}_m$ are uniformly generated in the range $(0, N_{\text{CP}})$. Based on $\{T_m\}_{m=1}^{M}$, $\tilde{\mathbb{S}}_M$ is generated from $\mathbb{S}_M$ with the condition $\Delta_{\tilde{m}} = (\tilde{m}-1)N_{\text{CP}} \geq T_m, m = 1, ..., M$.

To verify the analytically derived performance metrics, such as the secrecy outage probability and probability of non-zero achievable secrecy rate, we consider two geometric scenarios depending on the locations of the RRHs as follows:

1) $\mathbb{X}_1$: $M = 3$ with three RRHs placed at $\{Re^{j\pi/2}, Re^{j5\pi/6}, Re^{j7\pi/6}\}$.
2) $\mathbb{X}_2$: $M = 4$ with four RRHs placed at $\{Re^{j\pi/2}, Re^{j3\pi/4}, Re^{j\pi}, Re^{j\pi/4}\}$.

To verify the derived secrecy outage probability over three different locations for a set of RRHs, the following parameters are assumed:

- $\mathbb{X}_{11} : R = 5, N_h s = \{1, 2, 3\}, N_g s = \{3, 3, 3\}$ with $\mathbb{X}_1$.
- $\mathbb{X}_{12} : R = 5, N_h s = \{1, 2, 3\}, N_g s = \{1, 2, 3\}$ with $\mathbb{X}_1$.
- $\mathbb{X}_{21} : R = 5, N_h s = \{1, 2, 3, 1\}, N_g s = 2$ with $\mathbb{X}_2$.
- $\mathbb{X}_{22} : R = 5, N_h s = \{1, 2, 3, 2\}, N_g s = 2$ with $\mathbb{X}_2$.

For scenarios $\mathbb{X}_{11}$ and $\mathbb{X}_{12}$, (7) provides the selection probability as follows: $P_r(d = 1) = 0.56782$, $P_r(d = 2) = 0.28957$, $P_r(d = 3) = 0.14261$. For scenario $\mathbb{X}_{21}$, we have $P_r(d = 1) = 0.40475$, $P_r(d = 2) = 0.27162$, $P_r(d = 3) = 0.11599$, and $Pr(d = 4) = 0.20764$, whereas we have $P_r(d = 1) = 0.302686$, $P_r(d = 2) = 0.169747$, $P_r(d = 3) = 0.0583573$, and $P_r(d = 4) = 0.4692097$ for scenario $\mathbb{X}_{22}$.

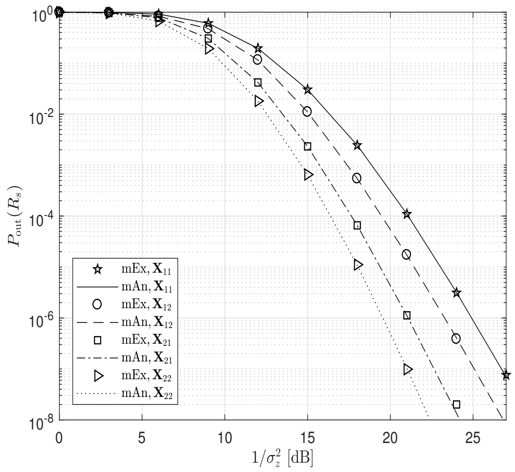

Fig. 3. Marginal secrecy outage probability for various simulation scenarios.

From Fig. 3, we can verify the accuracy of the analytically derived marginal secrecy outage probability for various simulation scenarios.

In generating Fig. 4, we assume that $\sum N_h = 4$ and $N_g s = 3$ for scenarios $\mathbb{X}_1$ and $\mathbb{X}_2$. The primary interest of this simulation is to investigate the effect of the sum of the multipath components over the LU channels on the slope of the performance curve of the marginal secrecy outage probability. We can summarize the following facts:

- When $\sum N_h$ is the same, almost the same slope can be obtained in the high SNR region. For differ-

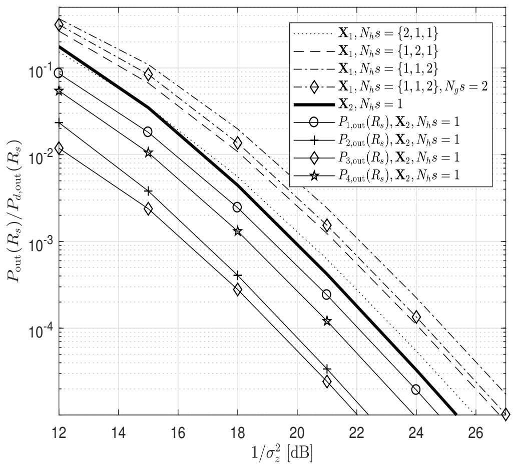

Fig. 4. Secrecy outage probability for various scenarios with the constraint of N_gs=3, $\sum N_h = 4$, and $R = 5$.

ent combinations for $N_{h,m}$s, $\{1,2,1\}, \{1,1,2\}, \{2,1,1\}$ with three RRHs, and $\{1,1,1,1\}$ with four RRHs have the same slope. When there are fewer multipath components over the EU channels, a lower marginal secrecy outage probability is achieved.

- Due to the i.n.i.d frequency selective fading for the LU and EU channels, a different secrecy outage probability is obtained depending on which RRH is selected as the data RRH, while maintaining the same slope in the high SNR region.
- We can see that the slopes for $P_{d,\mathrm{out}}(R_s)$ and $P_{\mathrm{out}}(R_s)$ will be the same as $1/\sigma_z^2$ increases. Note that since the data RRH is selected based on the instantaneous LU channel that has the greatest channel magnitude, the proposed selection scheme can guarantee that $P_{d,\mathrm{out}}(R_s)$ and $P_{\mathrm{out}}(R_s)$ achieve the same diversity gain from i.n.i.d. frequency selective fading channels.

V. Conclusions

In this paper, we have proposed a new joint selection scheme for the data RRH and interfering RRHs for a new proposed dACDD based single carrier transmission scheme without exact CSI of the LU and EU channels at the transmitting side to achieve the maximum achievable diversity gain at the LU, while minimizing the SINR at the EU. For i.n.i.d. frequency selective fading channels, new closed-form expressions for the selection probability of the data RRH and secrecy outage probability have been derived. Their accuracy have also been verified. In the high SNR region, the achievable diversity gain has been shown to be determined mainly by the sum of the number of multipath components over the LU channels, and independent of the index of the RRH that specifies the data RRH.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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, Sep. 2016.

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

[6] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proc. Natl. Acad. Sci. U.S.A.*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[7] G. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jul. 2008.

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

[9] A. S. Khan and I. Chatzigeorgiou, “Opportunistic relaying and random linear network coding for secure and reliable communication,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 223–234, Jan. 2018.

[10] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. Liao, “Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Mar. 2018.

[11] H. Wang, M. Luo, X. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper’s CSI,” *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[12] K. J. Kim, H. Liu, M. D. Renzo, P. V. Orlik, and H. V. Poor, “Secrecy analysis of distributed CDD-based cooperative systems with deliberate interference,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7865–7878, Dec. 2018.

[13] 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.

[14] 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.

[15] 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.

[16] J. M. Peha, “Approaches to spectrum sharing,” *IEEE Commun. Mag.*, pp. 10–11, Feb. 2005.

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

[18] K. J. Kim, Y. Yue, R. A. Iltis, and J. D. Gibson, “A QRD-M/Kalman filter-based detection and channel estimation algorithm for MIMO-OFDM systems,” *IEEE Trans. Wireless Commun.*, vol. 4, pp. 710–721, Mar. 2005.

[19] K. J. Kim and T. A. Tsiftsis, “Performance analysis of QRD-based cyclically prefixed single-carrier transmissions with opportunistic scheduling,” *IEEE Trans. Veh. Technol.*, vol. 60, pp. 328–333, Jan. 2011.

[20] 3GPP, TR 36.828 (V11.0.0), “Further enhancements to LTE time division duplex (TDD) for downlink-uplink (DL-UL) interference management and traffic adaptation,” Jun. 2012.

Appendix A

$$\theta_{m,j,\backslash d} \overset{\triangle}{=} \frac{(-1)^{N_{g,m}}}{(\tilde{\beta}_{g,m,\backslash d})^{N_{g,m}}} \sum_{\mathbb{S}(m,j)} \prod_{k=1,k\neq m}^{M-1} \binom{N_{g,k}+q_k-1}{q_k} \frac{(\tilde{\beta}_{g,k,\backslash d})^{q_k}}{(1-\frac{\tilde{\beta}_{g,k,\backslash d}}{\tilde{\beta}_{g,m,\backslash d}})^{N_{g,k}+q_k}} \tag{A.1}$$

with $\mathbb{S}(m,j)$, the mth component of $\mathbb{S}(i,j)$, which is defined as a set of $(M-1)$-tuples satisfying the following condition:

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