Physical-Layer Security of Underlay MIMO-D2D Communications by Null Steering Method Over Nakagami-m and Norton Fading Channels

Ajay Kumar, *Student Member, IEEE*, Sudhan Majhi, *Senior Member, IEEE*, and Hsiao-Chun Wu, *Fellow, IEEE*

***Abstract*— Underlay device-to-device (D2D) communication network is becoming a promising solution for the fifth generation (5G) and beyond wireless technology. It exploits the proximity of the D2D pairs and improves the overall network's latency, capacity, and spectral efficiency by sharing/reusing the existing cellular resources. However, due to the frequency-sharing/reusing, the security of the device users (DUs) and the cellular users (CUs) becomes vulnerable. This paper presents a novel physical-layer security (PLS) scheme for the underlay multiple-input multiple-output (MIMO) D2D communications in the presence of multiple eavesdroppers. The proposed new PLS scheme can significantly reduce the information leakage for both CUs and DUs by adopting a null steering scheme at the transmitter. A signal alignment technique is also employed to eradicate the stringent requirement of a larger number of transmitter antennas than that of the receiver antennas. A generalized nonlinear optimization problem has been formulated to improve the PLS performance for MIMO-D2D communications. A closed-form and generalized analytical expression of the secrecy outage probability for CUs and DUs is derived over the imperfect Nakagami-m and Norton fading channels. Theoretical and simulation results of our proposed new PLS scheme have shown significant improvement in the secrecy capacity and secrecy outage probability for both CUs and DUs in comparison with the existing methods.**

***Index Terms*— Physical-layer security, underlay MIMO-D2D communications, Nakagami-m distribution, Norton distribution, imperfect CSI (channel state information), null steering, signal alignment.**

I. Introduction

THE fifth-generation (5G) and beyond wireless technology is on the way to provide high data-rates, low power-consumption, low latency, and high spectral efficiency, resulting in notable improvement in users' *quality-of-experience* [1]. The *underlay device-to-device (D2D) communication* is referred to as a direct communication between two devices which are in each other's vicinity without any help of a base station (BS) [2]. In fact, both BS and D2D users use the same resources and they would interfere each other. The underlay D2D communication technology can significantly improve the network capacity in user-crowded areas such as stadiums or shopping malls. The D2D communication technology is a viable solution to facilitate vehicle-to-everything (V2X) networks [3], direct communications between an aircraft and the nearby ground station, wireless fidelity (WiFi)-direct networks, long term evolution (LTE)-direct networks [4], network traffic offloading, public safety, social services, electronic gaming, and military applications. The D2D communication technology is also a potential solution to establish the millimeter wave (mmWave) and machine-to-machine (M2M) communications [5]. By adopting the multiple-input multiple-output (MIMO) architecture with the D2D communication systems, reliability and spectral efficiency can be further increased. Nonetheless, due to the broadcast and frequency-reuse nature of the underlay MIMO-D2D communication systems, information leakage would take place at both the device users (DUs) and the licensed users (CUs), which may compromise the security. On the other hand, such leaked information could cause interference to other users. Thus, the quality-of-service (QoS) and security of both DUs and CUs can deteriorate considerably thereby. It is desirable to facilitate secured and interference-free communications for the underlaying CUs and DUs. It is favorable to ensure the non-zero secrecy capacity which is defined by the difference between the channel capacities of the legitimate user's link and the eavesdroppers' links [6]–[8]. In underlaying MIMO-D2D communications, an eavesdropper can be any user equipment other than the intended receiver [9].

There are several existing studies of the information leakage or the physical layer security (PLS) for underlaying D2D communications. In [10], the PLS of the D2D communication system was carried out by employment of DUs as friendly jammers; however, the security of DUs were not addressed. Moreover, friendly jammers needed to be synchronized with the transmitter all the time which would not be an easy task in practice. In [11], the authors have used an artificial-noise (AN) based scheme to improve the PLS of the users in the D2D underlay cellular communication network; however, an AN-based PLS scheme requires a tremendous amount of power

Manuscript received 26 September 2021; revised 9 February 2022 and 4 May 2022; accepted 23 May 2022. Date of publication 7 June 2022; date of current version 11 November 2022. This work was supported in part by Mathematical research Impact Centric Support (MATRICS) Project under SERB under Grant MTR/2020/000238 and in part by SERB-Technology Translation Award (SERB-TETRA) Project under SERB under Grant TTR/2021/000128. The associate editor coordinating the review of this article and approving it for publication was M. Caleffi. *(Corresponding author: Sudhan Majhi.)*

Ajay Kumar and Sudhan Majhi are with the Department of Electrical Communication Engineering, Indian Institute of Science Bangalore, Bengaluru 560012, India (e-mail: smajhi@iisc.ac.in).

Hsiao-Chun Wu is with the Department of Electrical Engineering and Computer Science, College of Engineering, Louisiana State University, Baton Rouge, LA 70803 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2022.3178758.

Digital Object Identifier 10.1109/TWC.2022.3178758

when the number of eavesdroppers is large. Authors in [12] analyzed the connection probability and secrecy probability by maximizing the truncated average received signal power beyond a threshold. Both [11] and [12] use the Rayleigh fading channel, which is not a reasonable assumption when LOS is present, which is a highly probable case in closely spaced D2D users. A combined multi-antenna technique with AN is proposed in [13] where power allocation is dependent on channel estimation error. The work proposed in [13] motivates us to consider channel estimation error which is an essential factor in the null steering scheme too. However, it used the iid Rayleigh channel model, which may not be a reasonable assumption for a network where D2D users are closely spaced. The secrecy-capacity maximization problem for D2D communications was tackled using a cooperative or coalition game [14]; however, only the secrecy capacity was considered, but the secrecy outage probability was not analyzed. The access-selection scheme was considered in [2] for D2D users to protect the cellular users against eavesdropping; however, the security issues of D2D links were not considered. In [15], D2D pairs were switched between the overlay and underlay modes to undertake the PLS for CUs; this scheme did improves the spectral efficiency but compromised the security of DUs on the other hand. Furthermore, the mutual interference between CUs and DUs was mitigated by use of the constellation-rotation technique in [16]; though this technique was quite promising for the PLS, neither secrecy capacity nor secrecy outage probability of the network was analyzed.

In [17], a full-duplex (FD) jamming receiver was proposed to protect DUs; nevertheless, this work did not consider the underlaying D2D cellular networks. In [18], jamming signals generated by DUs were used to realize the PLS for both CUs and DUs; in this work, the secrecy outage was not analyzed at all. A collaborative protocol with joint power optimization was proposed in [19] to combat the security problem for underlay D2D communications. In [19], a FD based CU injected a jamming signal to degrade the eavesdropper's channel quality while maintaining the QoS of the intended receiver by a beamforming technique. However, the use of such a jamming signal for PLS is obviously not an energy-efficient solution. Moreover, the number of antennas at the transmitter was kept larger than that of the receiver antennas for employing the beamforming technique [19]. The PLS of MIMO-D2D communication systems was explored in [20] which applied encryption and relays; however, relays are extra costly resources.

As a matter of fact, only very simple channel models have been considered in the existing literature to simplify the analysis and these models may not be appropriate for practical scenarios. In reality, DUs in D2D networks are not far away from each other to ensure proper information transmission between devices directly without even traversing the BS. Due to the proximity between such devices, there is a high chance of existence of a line-of-sight (LOS) link which can be characterized by the *Rician distribution*, a special case of the *Norton distribution* [21]. But the communication system performance analysis based on the Rician fading channel model becomes very challenging due to the presence of Bessel function. In the absence of LOS link between devices on the other hand, the channel model can be characterized by a Rayleigh distribution, a special case of the Nakagami-m distribution [22]. Thus, the Norton and Nakagami-m channels are deemed the generalized channel models of the Rician and Rayleigh fading channels, respectively. Moreover, the Nakagami fading model is appropriate when a maximum-ratio diversity combiner is employed at the receiver. Furthermore, in our opinion, the k-μ distribution (see [23]) can be applied to well approximate all of the aforementioned channel distributions by carefully choosing the proper values of k and μ, respectively. However, to the best of authors' knowledge, PLS for the underlay MIMO-D2D has not been analyzed over the Nakagami-m and the Norton fading channel models.

In order to deal with the drawbacks of the existing solutions, we propose a novel PLS scheme for underlay MIMO-D2D communications by a *null steering approach* in conjunction with a *signal alignment technique* over the Nakagami-m and Norton fading-channel models. The PLS of underlay MIMO-D2D networks will be analyzed in the presence of multiple eavesdroppers. Note that almost all of the existing works study the PLS in the presence of a sole eavesdropper only since the appearance of multiple eavesdroppers would be a very complex scenario. Our main contributions are highlighted as follows:

- We have proposed a novel null steering scheme to improve the PLS for underlay MIMO-D2D communications in the presence of multiple eavesdroppers.
- We formulate a generalized nonlinear optimization problem for underlay MIMO-D2D communications subject to a transmitting-power constraint and solve this problem by a null steering scheme analytically.
- A signal alignment technique is applied to further remove the common stringent constraint that the number of transmitter antennas has to be larger than that of receiver antennas.
- The closed-form and generalized analytical expressions of secrecy capacity (both instantaneous and ergodic) and secrecy outage probability are derived for both CUs and DUs over the non-identical Nakagami-m and Norton fading channels.
- To derive the closed-form expressions of secrecy capacity and secrecy outage probability, we consider two scenarios: (*i*) imperfect channel state information (CSI) available at the transmitters and (*ii*) perfect CSI available at the transmitters (as a special case of (*i*)).
- The performance of our proposed new scheme is compared with other existing methods.

The rest of the paper is organized as follows. The system model and the problem statement for underlay MIMO-D2D communications are presented in Section II. Section III introduces our proposed novel null steering scheme in conjunction with a signal alignment technique for underlay MIMO-D2D communications. In Section IV, we derive the closed-form expression of secrecy capacity (both instantaneous and ergodic) and secrecy outage probability for both Nakagami-m and Norton fading channels. Section V presents

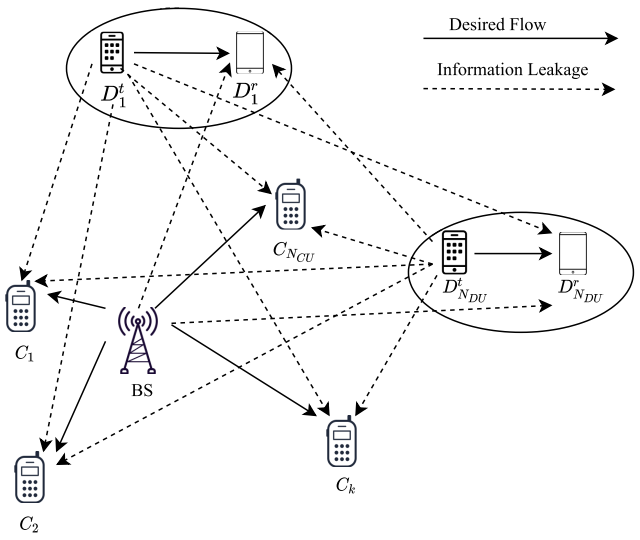


Fig. 1. The system model of an underlay D2D wireless communication network.

numerical and analytical results for evaluating the underlay MIMO-D2D communication systems using different schemes. Conclusion will be finally drawn in Section VI.

Nomenclature: The set of complex numbers is denoted by $\mathbb{C}$ and the statistical expectation is denoted by $\mathbb{E}[\ ]$.

II. System Model and Problem Statement

A. System Model

In this work, we consider a downlink cellular system along with a D2D network, as shown by Fig. 1. The number of CU/DU pairs in the network are denoted by N_{CU} and N_{DU}, respectively. The k-th CU is denoted by C_k where $k = 1, 2, \ldots, N_{\text{CU}}$, while the i-th DU's transmitter and receiver are denoted by D_i^{t} and D_i^{r}, respectively, for $i = 1, 2, \ldots, N_{\text{DU}}$. The BS and each D_i^{t} are equipped with M_{t} transmitting antennas. Each of C_k's and D_i^{r}'s are equipped with M_{r} receiving antennas to make our proposed system an underlay MIMO-D2D cellular network [18]. In the system model, the device user equipment (DUE) is first discovered within the proximity range of the D2D communication [24]. After the DUE is found, a message about the link quality is exchanged. Based on this message, either D2D or cellular communication is established [25]. However, due to the broadcasting nature of the wireless channel, such information can be wiretapped by eavesdropper(s). When the BS communicates with the cellular device C_k, the rest of CUs and all other DUs are considered "eavesdroppers". Similarly, when D_i^{t} communicates with D_i^{r}, the rest of DUs and all other CUs are also considered eavesdroppers. The information signals at C_k and D_i^{t} are represented by s_{C_k} and $s_{\text{D}_i^{\text{t}}}$, respectively. The channel-gain matrices from the BS to C_k, from the BS to D_i^{r}, from D_i^{t} to C_k, and from D_i^{t} to D_i^{r} are denoted by $\mathbf{H}_{\text{B}\rightarrow\text{C}_k} \in \mathbb{C}^{M_{\text{r}}\times M_{\text{t}}}$, $\mathbf{H}_{\text{B}\rightarrow\text{D}_i^{\text{r}}} \in \mathbb{C}^{M_{\text{r}}\times M_{\text{t}}}$, $\mathbf{H}_{\text{D}_i^{\text{t}}\rightarrow\text{C}_k} \in \mathbb{C}^{M_{\text{r}}\times M_{\text{t}}}$, and $\mathbf{H}_{\text{D}_i^{\text{t}}\rightarrow\text{D}_i^{\text{r}}} \in \mathbb{C}^{M_{\text{r}}\times M_{\text{t}}}$, respectively. All of the aforementioned channel-gain matrices are assumed to be invertible. According to these channel-gain matrices, two scenarios have been considered. First, we consider that each entry of a channel-gain matrix is an independent but not identical random variabl (RV) which follows the Nakagami-m distribution. In the presence of multiple paths, a wireless channel can be modeled by the Nakagami-m distribution [26]. However, in D2D communications, we assume that the LOS path leads to the Rician channel model [27]. Second, the Norton distribution is considered as it can characterize the combination of the Rician and Nakagami-m distributions. Let X be a RV which follows the Nakagami-m distribution. According to [28], the probability density function (PDF) of X is given by

$$f_X(x; m, \eta) \overset{\text{def}}{=} \frac{2x^{2m-1}}{\eta^m (m-1)!} \exp\left(-\frac{x^2}{\eta}\right) U(x), \quad (1)$$

where m is the *Nakagami fading parameter* which is a positive integer, $\eta \overset{\text{def}}{=} \mathbb{E}\left[X^2\right]/m$, and $U(x)$ specifies the unit step function. Then, let Y be a RV which follows the Norton distribution. According to [21], the PDF of Y is given by

$$f_Y(y) \overset{\text{def}}{=} \frac{\mu y^{\mu}}{\sigma^2 v^{\mu-1}} \exp\left[-\mu\left(\frac{y^2+v^2}{2\sigma^2}\right)\right] I_{\mu-1}\left(\frac{y\mu v}{\sigma^2}\right) U(y), \quad (2)$$

where μ is the *fading figure*, $I_n(\ )$ represents the *modified Bessel function of the first kind and order* n, $v \geq 0$ manifests the amplitude of the LOS channel-gain, and σ^2 expresses the variance of the associated RV.

The transmitting power $P_{\text{C}_k} = \mathbb{E}\left[\left|s_{\text{C}_k}\right|^2\right]$ is assigned to the BS for serving C_k, the transmitting power $P_{\text{D}_i^{\text{t}}} = \mathbb{E}\left[\left|s_{\text{D}_i^{\text{t}}}\right|^2\right]$ is assigned to each D_i^{t} to serve D_i^{r}. Moreover, $P_{\text{C}_k} + P_{\text{D}_i^{\text{t}}} = P_{\text{tot}}$ where P_{tot} denotes the *total available power* to the network. In our proposed system model, the communication links between BS and C_k and between D_i^{t} and D_i^{r} facilitate the "desired transmissions". The rest of communication links are thus considered the "information-leakage links".

B. Problem Statement

The primary objective of this work is to protect the information of legitimate users from the eavesdropper(s). To serve this purpose, we formulate two generalized nonlinear optimization problems to maximize the secrecy capacity of C_k and D_i^{r} for the underlay MIMO-D2D wireless network. Besides, we also formulate two generalized nonlinear optimization problems here to minimize the secrecy outage probability of C_k and D_i^{r} for the underlay MIMO-D2D wireless network. The optimization problem related to the secrecy capacity $\mathcal{C}_{\text{C}_k}^{\text{s}}(P, \mathbf{H}, \mathbf{W})$ for CUs can be written as

$$\begin{aligned} &\max_{P,w} \mathcal{C}_{\text{C}_k}^{\text{s}}(P, \mathbf{H}, \mathbf{W}) \\ &\text{subject to } \mathcal{C}_{\text{D}_i^{\text{r}}}^{\text{s}}(P, \mathbf{H}, \mathbf{W}) \geq 0, \\ &\qquad P_{\text{C}_k},\ P_{\text{D}_i^{\text{t}}} \geq 0, \\ &\qquad P_{\text{C}_k} + P_{\text{D}_i^{\text{t}}} \leq P_{\text{tot}}. \end{aligned} \quad (3)$$

Similarly, the optimization problem related to the secrecy capacity $\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}(P,\mathbf{H},\mathbf{W})$ for DUs can be expressed by

$$\begin{aligned}&\max_{P,w}\ \mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}(P,\mathbf{H},\mathbf{W})\\ &\text{subject to } \mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}(P,\mathbf{H},\mathbf{W})\geq 0,\\ &\qquad P_{\mathrm{C}_k},\ P_{\mathrm{D}^{\mathrm{t}}_i}\geq 0,\\ &\qquad P_{\mathrm{C}_k}+P_{\mathrm{D}^{\mathrm{t}}_i}\leq P_{\mathrm{tot}}.\end{aligned}\tag{4}$$

The optimization problem related to the secrecy outage probability $\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}(P,\mathbf{H},\mathbf{W})$ for CUs can be written as

$$\begin{aligned}&\min_{P,w}\ \mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}(P,\mathbf{H},\mathbf{W})\\ &\text{subject to } \mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}(P,\mathbf{H},\mathbf{W})\leq \phi_2,\\ &\qquad P_{\mathrm{C}_k},\ P_{\mathrm{D}^{\mathrm{t}}_i}\geq 0,\\ &\qquad P_{\mathrm{C}_k}+P_{\mathrm{D}^{\mathrm{t}}_i}\leq P_{\mathrm{tot}},\end{aligned}\tag{5}$$

where ϕ_2 specifies the target secrecy outage probability of DU. Similarly, the optimization problem related to the secrecy outage probability $\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}(P,\mathbf{H},\mathbf{W})$ for DUs can be expressed by

$$\begin{aligned}&\min_{P,w}\ \mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}(P,\mathbf{H},\mathbf{W})\\ &\text{subject to } \mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}(P,\mathbf{H},\mathbf{W})\leq \phi_1,\\ &\qquad P_{\mathrm{C}_k},\ P_{\mathrm{D}^{\mathrm{t}}_i}\geq 0,\\ &\qquad P_{\mathrm{C}_k}+P_{\mathrm{D}^{\mathrm{t}}_i}\leq P_{\mathrm{tot}},\end{aligned}\tag{6}$$

where $\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}(\ )$ and $\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}(\ )$ denote the secrecy capacities of C_k and $\mathrm{D}^{\mathrm{r}}_i$, respectively; the transmitting power for CUs or DUs: $P\in\{P_{\mathrm{C}_k},P_{\mathrm{D}^{\mathrm{t}}_i}\}$; the channel-gain matrix: $\mathbf{H}\in\left\{\mathbf{H}_{\mathrm{B}\to\mathrm{C}_k},\mathbf{H}_{\mathrm{B}\to\mathrm{D}^{\mathrm{r}}_i},\mathbf{H}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{C}_k},\mathbf{H}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{D}^{\mathrm{r}}_i}\right\}$; the beamforming vector: $\mathbf{W}\in\{\mathbf{W}_{\mathrm{C}_k},\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}\}$; ϕ_1 specifies the target secrecy outage probability of CU. The secrecy capacities $\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}$ and $\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}$ can be computed from the following equations:

$$\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}=\mathcal{C}_{\mathrm{C}_k}-\underbrace{\max\left(\left\{\mathcal{C}_{\mathrm{C}_j}\right\}^{N_{\mathrm{CU}}}_{j\neq k,j=1},\left\{\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i}\right\}^{N_{\mathrm{DU}}}_{i=1}\right)}_{\mathcal{C}_{\mathrm{Ea}}},\tag{7}$$

$$\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}=\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i}-\underbrace{\max\left(\left\{\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_l}\right\}^{N_{\mathrm{DU}}}_{l\neq i,l=1},\left\{\mathcal{C}_{\mathrm{C}_k}\right\}^{N_{\mathrm{CU}}}_{k=1}\right)}_{\bar{\mathcal{C}}_{\mathrm{Ea}}},\tag{8}$$

where $\mathcal{C}_{\mathrm{C}_k}$ and $\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i}$ denote the channel capacities for the legitimate CU and DU links, respectively, and $\mathcal{C}_{\mathrm{Ea}}$ and $\bar{\mathcal{C}}_{\mathrm{Ea}}$ specify the effective channel capacities of CUs and DUs other than the legitimate users. $\left\{\mathcal{C}_{\mathrm{C}_j}\right\}^{N_{\mathrm{CU}}}_{j\neq k,j=1}$ and $\left\{\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i}\right\}^{N_{\mathrm{DU}}}_{i=1}$ represent CU information-leakage capacities of such illegitimate CUs and DUs, respectively. $\left\{\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_l}\right\}^{N_{\mathrm{DU}}}_{l\neq i,l=1}$ and $\{\mathcal{C}_{\mathrm{C}_k}\}^{N_{\mathrm{CU}}}_{k=1}$ express DU information-leakage capacities of illegitimate DUs and CUs, respectively. $\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}$ and $\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}$ are the secrecy outage probability of CU and DU respectively. The secrecy outage probability $\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}$ and $\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}$ are given by

$$\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}\ \stackrel{\text{def}}{=}\ \Pr\left[\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}<\Psi_1\right]\tag{9}$$

and

$$\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}\ \stackrel{\text{def}}{=}\ \Pr\left[\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}<\Psi_2\right],\tag{10}$$

where Ψ_1 and Ψ_2 denote the thresholds of the secrecy capacities of CU and DU, respectively, which specify the secrecy outages of CU and DU. Now the secrecy capacities of CU and DU can be maximized by minimizing the effective eavesdropper's channel capacities $\mathcal{C}_{\mathrm{Ea}}$ and $\bar{\mathcal{C}}_{\mathrm{Ea}}$, respectively. Once such secrecy capacities are maximized, the corresponding secrecy-outage probabilities achieve the optimal (minimum) values. Traditionally, multiple algorithms are proposed in the literature to solve these types of optimization problems [29]. However, most of these are adaptive and iterative, thus these require high computational time. Other simplified algorithms are also used to solve such optimization problem, however, they can miss the optimum solutions. In this work, a "*null steering*" approach has been adopted to obtain the optimum solution. However, to perform null steering, the number of transmitting antennas at $\mathrm{D}^{\mathrm{t}}_i$ and the BS has to be greater than the rest of the receiving antennas at all the unintended DUs and CUs, i.e., the constraints $M_{\mathrm{t}}>M_{\mathrm{r}}(N_{\mathrm{DU}}-1)N_{\mathrm{CU}}$ for DUs and $M_{\mathrm{t}}>M_{\mathrm{r}}(N_{\mathrm{CU}}-1)N_{\mathrm{DU}}$ for CUs have to be imposed. However, for any practical network, satisfying these two constraints is not possible according to [7].

III. Our Proposed New PLS Scheme

Motivated by Eqs. (7) and (8), we propose to modify the original problems described by Eqs. (3) and (4) to the minimization problems of $\mathcal{C}_{\mathrm{Ea}}$ and $\bar{\mathcal{C}}_{\mathrm{Ea}}$, which specify the information leakage from C_k and $\mathrm{D}^{\mathrm{t}}_i$ to the effective eavesdropper, respectively [7], [9], [30], [31]. These can be solved by employing a null steering scheme at the transmitters. Thus, the optimization problems stated by Eqs. (3), (4), (5), and (6) can be solved using such a null steering scheme. CU and DU's leakage can be nullified by multiplying the corresponding null steering vectors $\mathbf{W}_{\mathrm{C}_k}$ and $\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}$ to their leakage channel matrices as given in Eq. (11) and (12), shown at the bottom of the next page. Since each element in the leakage channel matrix is of dimension $M_{\mathrm{r}}\times M_{\mathrm{t}}$, the overall dimension of leakage matrix is $M_{\mathrm{r}}(N_{\mathrm{CU}}-1)N_{\mathrm{DU}}\times M_{\mathrm{t}}$ and $M_{\mathrm{r}}(N_{\mathrm{DU}}-1)N_{\mathrm{CU}}\times M_{\mathrm{t}}$ for CU and DU, respectively.

In order to obtain the non-trivial solution of null steering vectors $\mathbf{W}_{\mathrm{C}_k}$ and $\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}$, the constraints $M_{\mathrm{t}}>M_{\mathrm{r}}(N_{\mathrm{CU}}-1)N_{\mathrm{DU}}$ for CU and $M_{\mathrm{t}}>M_{\mathrm{r}}(N_{\mathrm{DU}}-1)N_{\mathrm{CU}}$ for DU must satisfy. However, the aforementioned constraints are not practical since it is not possible to deploy a larger number of antennas at the transmitter [7]. To remove these constraints before applying the null steering, we propose to perform the information-leakage alignment into a proper subspace for both CU and DU. The information signal-sequence vector is aligned into another subspace such that the information-leakage subspace and the desired information subspace are orthogonal to each other. The aforementioned alignment task can be undertaken by using the signal alignment technique presented in [7]. After aligning the signal-sequence vector into the targeted subspace, we nullify the aligned information-leakage subspace using a null steering vector.

Let $\mathbf{V}_{\mathrm{C}_k}\in\mathbb{C}^{M_{\mathrm{t}}\times S}$ be the information-leakage alignment vector generated at the BS to send information to C_k and $\mathbf{V}_{\mathrm{D}^{\mathrm{r}}_i}\in\mathbb{C}^{M_{\mathrm{t}}\times S}$ be the alignment vector of $\mathrm{D}^{\mathrm{t}}_i$

to align its information-leakage components. After applying information-leakage alignment vector at each element of leakage channel matrix as $\mathbf{H}_{\mathrm{B}\to\mathrm{C}_j}\mathbf{V}_{\mathrm{C}_k} = \mathbf{h}_{\mathrm{B}\to\mathrm{C}_j}$, where $j = 1,2,\ldots,N_{\mathrm{CU}}$, $j \neq k$ and $\mathbf{H}_{\mathrm{B}\to\mathrm{D}_i^{\mathrm{r}}}\mathbf{V}_{\mathrm{C}_k} = \mathbf{h}_{\mathrm{B}\to\mathrm{D}_i^{\mathrm{r}}}$, where $i = 1,2,\ldots,N_{\mathrm{DU}}$ for CU and DU, respectively, the dimension of new leakage channel matrices become $M_{\mathrm{r}}(N_{\mathrm{CU}}-1)N_{\mathrm{DU}}\times S$ and $M_{\mathrm{r}}(N_{\mathrm{DU}}-1)N_{\mathrm{CU}}\times S$ for CU and DU, respectively. Now, we need the null steering vectors $\mathbf{W}_{\mathrm{C}_k}$ and $\mathbf{W}_{\mathrm{D}_i^{\mathrm{t}}}$ of dimension $S\times 1$. This scenario can be expressed by Eq. (13) and (14), shown at the bottom of the page, where $\mathbf{h}_{\mathrm{B}\to\mathrm{C}_j}$ represents the information-leakage channel-gain matrix from the BS to C_j and $\mathbf{h}_{\mathrm{B}\to\mathrm{D}_i^{\mathrm{r}}}$ denotes the information-leakage channel-gain matrix from the BS to $\mathrm{D}_i^{\mathrm{r}}$ both after the interference alignment is applied.

Once the undesired information flow is nullified by employment of null steering vectors, the received signal-to-interference-plus-noise ratio (SINR) at C_k and $\mathrm{D}_i^{\mathrm{r}}$ can be written as

$$\lambda_{\mathrm{C}_k} = \frac{P_{\mathrm{C}_k}\left|\mathbf{H}_{\mathrm{B}\to\mathrm{C}_k}\mathbf{V}_{\mathrm{C}_k}\mathbf{W}_{\mathrm{C}_k}\right|^2}{\sigma^2}, \tag{15}$$

and

$$\lambda_{\mathrm{D}_i^{\mathrm{r}}} = \frac{P_{\mathrm{D}_i^{\mathrm{t}}}\left|\mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_i^{\mathrm{r}}}\mathbf{V}_{\mathrm{D}_i^{\mathrm{t}}}\mathbf{W}_{\mathrm{D}_i^{\mathrm{t}}}\right|^2}{\sigma^2}, \tag{16}$$

respectively, where σ^2 represents the noise variance. Thus, the SINRs at the eavesdroppers (i.e., unintended CU and DU) become

$$\lambda_{\mathrm{Ea}} = 0, \tag{17}$$

and

$$\bar{\lambda}_{\mathrm{Ea}} = 0, \tag{18}$$

respectively. Since the SINRs are equal to zero at the eavesdroppers, their channel capacities $\mathcal{C}_{\mathrm{Ea}}$ and $\bar{\mathcal{C}}_{\mathrm{Ea}}$ also tend to be zero. This condition holds true only when perfect CSI is available at each transmitter. When the CSI is not known precisely, the SINRs at C_k and $\mathrm{D}_i^{\mathrm{r}}$ will actually be different from Eqs. (15) and (16) and thus the eavesdroppers' SINRs will be non-zero thereby. The detailed analysis subject to imperfect CSI will be presented in Section IV subsequently.

IV. PLS Performance Analysis

The presence of LOS connections between transceivers leads to the Rician fading-channel model. However, the multipath effect can be characterized by the Nakagami-m channel model more appropriately. The combination of these two channel characteristics leads to the *Norton distribution*. Hence, a generalized channel model based on the Norton distribution can be a convenient evaluation tool. The non-identical Nakagami-m distribution corresponds to the practical scenario as each path of the channel has different parameters. To the best of our knowledge, the generalized PLS performance analysis for underlay MIMO-D2D communications has not been presented so far. In this paper, we will introduce such a new generalized analysis based on the Norton and non-identical Nakagami-m channel models.

A. Secrecy Capacity for Imperfect CSI

In practice, it is almost impossible to obtain perfect CSI at transmitters as there always exist errors in the channel estimates. According to [32], the channel coefficient from the i-th node to the j-th node in the presence of channel-estimation error can be expressed by

$$\hat{h}_{i,j} = \rho\, h_{i,j} + \sqrt{1-\rho^2}\,\varepsilon, \tag{19}$$

where $h_{i,j}$ denotes the perfect (precise) channel coefficient and $\hat{h}_{i,j}$ denotes the corresponding estimate; ε is a Gaussian RV with zero mean and variance σ^2; ρ is the correlation coefficient ($0 \le \rho \le 1$). When $\rho = 1$, the knowledge of the channel coefficient is *perfect* (precise), and the complete CSI is available to the nodes. When $\rho = 0$, the CSI estimation is random and no knowledge of the channel is available. Due to the imperfect (imprecise) CSI, the null steering approach is not optimal as it leads to non-zero SINRs at the eavesdroppers. Note that without loss of generality, we consider the imperfect CSI for CUs from now on. Nevertheless, similar study can be extended for DUs easily. The imperfect CSI scenario corresponds to following secrecy capacity for CU:

$$\begin{aligned}\mathcal{C}_{\mathrm{C}_k}^{\mathrm{s}} &= \mathcal{C}_{\mathrm{C}_k} - \mathcal{C}_{\mathrm{Ea}}\\ &= \log_2\left(1+\lambda_{\mathrm{C}_k}\right) - \log_2\left(1+\lambda_{\mathrm{Ea}}\right)\\ &= \log_2\left[1+\frac{P_{\mathrm{C}_k}\left|\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{C}_k}\mathbf{V}_{\mathrm{C}_k}\mathbf{W}_{\mathrm{C}_k}\right|^2}{P_{\mathrm{C}_k}(1-\rho^2)\varepsilon^2_{\mathrm{B}\to\mathrm{C}_k}+\rho^2\sigma^2}\right]\\ &\quad - \log_2\left[1+\frac{P_{\mathrm{C}_k}\left|\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{Ea}}\mathbf{V}_{\mathrm{C}_k}\mathbf{W}_{\mathrm{C}_k}\right|^2}{P_{\mathrm{C}_k}(1-\rho^2)\varepsilon^2_{\mathrm{B}\to\mathrm{Ea}}+\rho^2\sigma^2}\right],\end{aligned} \tag{20}$$

where $\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{C}_k}$ and $\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{Ea}}$ denote the estimates of $\mathbf{H}_{\mathrm{B}\to\mathrm{C}_k}$ and $\mathbf{H}_{\mathrm{B}\to\mathrm{Ea}}$ using an arbitrary channel estimator, respectively;

$$\left[\mathbf{H}_{\mathrm{B}\to\mathrm{C}_1}\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{C}_2}\ \ \cdots\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{C}_j}\ \ \cdots\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{C}_{N_{\mathrm{CU}}}}\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{D}_1^{\mathrm{r}}}\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{D}_2^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{D}_i^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{H}_{\mathrm{B}\to\mathrm{D}_{N_{\mathrm{DU}}}^{\mathrm{r}}}\right]\mathbf{W}_{\mathrm{C}_k} = \mathbf{0}, \tag{11}$$

$$\left[\mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_1}\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_2}\ \ \cdots\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_k}\ \ \cdots\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_{N_{\mathrm{CU}}}}\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_1^{\mathrm{r}}}\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_2^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_l^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{H}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_{N_{\mathrm{DU}}}^{\mathrm{r}}}\right]\mathbf{W}_{\mathrm{D}_i^{\mathrm{t}}} = \mathbf{0}, \tag{12}$$

$$\left[\mathbf{h}_{\mathrm{B}\to\mathrm{C}_1}\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{C}_2}\ \ \cdots\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{C}_j}\ \ \cdots\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{C}_{N_{\mathrm{CU}}}}\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{D}_1^{\mathrm{r}}}\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{D}_2^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{D}_i^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{h}_{\mathrm{B}\to\mathrm{D}_{N_{\mathrm{DU}}}^{\mathrm{r}}}\right]\mathbf{W}_{\mathrm{C}_k} = \mathbf{0}, \tag{13}$$

$$\left[\mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_1}\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_2}\ \ \cdots\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_k}\ \ \cdots\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{C}_{N_{\mathrm{CU}}}}\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_1^{\mathrm{r}}}\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_2^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_l^{\mathrm{r}}}\ \ \cdots\ \ \mathbf{h}_{\mathrm{D}_i^{\mathrm{t}}\to\mathrm{D}_{N_{\mathrm{DU}}}^{\mathrm{r}}}\right]\mathbf{W}_{\mathrm{D}_i^{\mathrm{t}}} = \mathbf{0}. \tag{14}$$

$\varepsilon^2_{\mathrm{B}\to\mathrm{C}_k}$ and $\varepsilon^2_{\mathrm{B}\to\mathrm{Ea}}$ specify the channel estimation errors for the "BS$\to$ C_k" and "BS$\to$eavesdropper" links, respectively. Let us write $\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}$ as β_1 for notational convenience. Thus, Eq. (20) becomes

$$\beta_1 = \log_2\left[1+\frac{P_{\mathrm{C}_k}\alpha_1}{P_{\mathrm{C}_k}(1-\rho^2)\lambda_1+\rho^2\sigma^2}\right] - \log_2\left[1+\frac{P_{\mathrm{C}_k}\alpha_2}{P_{\mathrm{C}_k}(1-\rho^2)\lambda_2+\rho^2\sigma^2}\right], \quad (21)$$

where $\alpha_1 \overset{\text{def}}{=} \left|\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{C}_k}\mathbf{V}_{\mathrm{C}_k}\mathbf{W}_{\mathrm{C}_k}\right|^2$ and $\alpha_2 \overset{\text{def}}{=} \left|\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{Ea}}\mathbf{V}_{\mathrm{C}_k}\mathbf{W}_{\mathrm{C}_k}\right|^2$, both of which are sums of squares of M_{r} RVs; $\lambda_1 \overset{\text{def}}{=} \varepsilon^2_{\mathrm{B}\to\mathrm{C}_k}$ and $\lambda_2 \overset{\text{def}}{=} \varepsilon^2_{\mathrm{B}\to\mathrm{Ea}}$. To study the impact of channel gains on the secrecy capacity, we consider two general cases: (*i*) when the channel gains follow the Nakagami-m distribution and the sums of squares of M_{r} Nakagami-m RVs follow the weighted Erlang distribution according to [33] and (*ii*) when the channel gains follow the Norton distribution and the sums of squares of M_{r} Norton RVs follow the k-μ distribution according to [34]. Secrecy capacity in Eq. (20) is instantaneous, which involves RVs. To see the overall/average effect, the ergodic secrecy capacity of C_k is given as

$$\mathcal{C}^{\mathrm{se}}_{\mathrm{C}_k} = \int_0^\infty \beta_1\, f_{\beta_1}(\beta_1)\, d\beta_1, \quad (22)$$

where $f_{\beta_1}(\beta_1)$ denotes the PDF of the RV β_1. In order to enumerate the ergodic capacity given by Eq. (22), we need to formulate $f_{\beta_1}(\beta_1)$, where β_1 involves four RVs α_1, α_2, λ_1, and λ_2. The PDF formulas of α_1 and α_2 are given by Eqs. (44) and (54) corresponding to the Nakagami-m and Norton channel models, respectively, in the appendix (with $\varrho=\alpha_1,\alpha_2$ in Eq. (44) and $\theta_2=\alpha_1,\alpha_2$ in Eq. (54)). Note that λ_1 and λ_2 follow the exponential distribution as λ_1 and λ_2 are squares of $\varepsilon_{\mathrm{B}\to\mathrm{C}_k}$ and $\varepsilon_{\mathrm{B}\to\mathrm{Ea}}$, respectively. Thus, $f_{\beta_1}(\beta_1)$ can be formed using the random-variable transformation. Consider $\psi_2=\alpha_2$, $\delta_1=\lambda_1$, and $\delta_2=\lambda_2$. Since α_1, α_2, λ_1, and λ_2 are independent of each other, the joint PDF can be given by

$$f(\beta_1,\psi_2,\delta_1,\delta_2) = f_{\alpha_1}(\alpha_1)f_{\alpha_2}(\psi_2)f_{\lambda_1}(\delta_1)f_{\lambda_2}(\delta_2)|J|, \quad (23)$$

where, according to Eq. (21), α_1 is given by

$$\alpha_1 = \left\{2^{\beta_1}\left[1+\frac{P_{\mathrm{C}_k}\psi_2}{P_{\mathrm{C}_k}(1-\rho^2)\delta_2+\rho^2\sigma^2}\right]-1\right\} \times \frac{P_{\mathrm{C}_k}(1-\rho^2)\delta_1+\rho^2\sigma^2}{P_{\mathrm{C}_k}}, \quad (24)$$

and $|J|$ is determinant of the Jacobian matrix which is given by

$$J = 2^{\beta_1}\ln(2)\left[1+\frac{P_{\mathrm{C}_k}\psi_2}{P_{\mathrm{C}_k}(1-\rho^2)\delta_2+\rho^2\sigma^2}\right] \times \frac{P_{\mathrm{C}_k}(1-\rho^2)\delta_1+\rho^2\sigma^2}{P_{\mathrm{C}_k}}. \quad (25)$$

The marginal PDF of β_1 is given by

$$f(\beta_1) = \int_0^\infty\int_0^\infty\int_0^\infty f(\beta_1,\psi_2,\delta_1,\delta_2)\, d\psi_2\, d\delta_1\, d\delta_2. \quad (26)$$

Again the secrecy capacity analysis addressed by Eqs. (20)-(26) for the imperfect CSI scenario of CUs can be easily extended for that of DUs as well by substituting $\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k}$, $\mathcal{C}_{\mathrm{C}_k}$, $\mathcal{C}_{\mathrm{Ea}}$, λ_{C_k}, λ_{Ea}, P_{C_k}, $\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{C}_k}$, $\hat{\mathbf{H}}_{\mathrm{B}\to\mathrm{Ea}}$, $\mathbf{V}_{\mathrm{C}_k}$, $\mathbf{W}_{\mathrm{C}_k}$, $\varepsilon^2_{\mathrm{B}\to\mathrm{C}_k}$, and $\mathcal{C}^{\mathrm{se}}_{\mathrm{C}_k}$ with $\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}$, $\mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i}$, $\bar{\mathcal{C}}_{\mathrm{Ea}}$, $\lambda_{\mathrm{D}^{\mathrm{r}}_i}$, $\bar{\lambda}_{\mathrm{Ea}}$, $P_{\mathrm{D}^{\mathrm{r}}_i}$, $\hat{\mathbf{H}}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{D}^{\mathrm{r}}_i}$, $\hat{\mathbf{H}}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{Ea}}$, $\mathbf{V}_{\mathrm{D}^{\mathrm{t}}_i}$, $\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}$, $\varepsilon^2_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{D}^{\mathrm{r}}_i}$, and $\mathcal{C}^{\mathrm{se}}_{\mathrm{D}^{\mathrm{r}}_i}$, respectively.

B. Secrecy Capacity for Perfect CSI

When we set $\rho=1$, we have a special case of imperfect CSI, which actually turns out to be universal perfect CSI (every transmitter can acquire the corresponding perfect CSI). The null steering approach is optimal for the perfect CSI scenario, which leads to zero SINR at any eavesdropper. Consequently, the secrecy capacity of C_k is equal to its channel capacity, i.e., β_1 becomes dependent on α_1 only such that

$$\beta_1 = \log_2\left[1+\frac{P_{\mathrm{C}_k}\alpha_1}{\sigma^2}\right]. \quad (27)$$

The RV involved in Eq. (27) is actually α_1. Next, we would like to express α_1 in terms of β_1 as follows:

$$\alpha_1 = \frac{\sigma^2}{P_{\mathrm{C}_k}}\left(2^{\beta_1}-1\right). \quad (28)$$

Differentiate α_1 with respect to β_1 to produce

$$\frac{d\alpha_1}{d\beta_1} = \frac{\sigma^2}{P_{\mathrm{C}_k}}\left[2^{\beta_1}\ln(2)\right], \quad (29)$$

and the PDF of β_1 in terms of the PDF of α_1 can be written by

$$f_{\beta_1}\left(\frac{\sigma^2}{P_{\mathrm{C}_k}}(2^{\beta_1}-1)\right) = \frac{\sigma^2}{P_{\mathrm{C}_k}}\left[2^{\beta_1}\ln(2)\right] \times f_{\alpha_1}\left(\frac{\sigma^2}{P_{\mathrm{C}_k}}(2^{\beta_1}-1)\right). \quad (30)$$

In the first case (the channel-gains follow the Nakagami-m distribution), the RV α_1 follows the weighted Erlang distribution, its PDF is given by Eq. (44) in the appendix. For the first case, we can obtain the ergodic secrecy capacity of C_k according to Eq. (22) and (30), which is expressed as

$$\mathcal{C}^{\mathrm{se}}_{\mathrm{C}_k} = \frac{1}{ln(2)}\sum_{n=1}^{M_r}\sum_{s=1}^{m_n}\Xi_{M_r} \times\left(n,s,\{m_q\}_{q=1}^{M_r},\{\eta_q\}_{q=1}^{M_r},\{l_q\}_{q=1}^{M_r-2}\right) \times\sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i!}\left(\frac{P_{\mathrm{C}_k}\eta_n}{\sigma^2}\right)^i\frac{\Gamma(s+i)}{\Gamma(s)}, \quad (31)$$

where m_n and η_n are parameters of nth Nakagami distributed RV. For detailed description refer to Appendix. In the second case (the channel-gains follow the Norton distribution), α_1 follows the k-μ distribution and its PDF is given by Eq. (54) in the appendix. This generalized k-μ distribution is shown in Table I, which can be converted to any of the listed specific distribution by adjusting the respective values of k and μ. Similarly, for the second case, we can obtain the ergodic

TABLE I
SPECIAL CASES OF $k-\mu$ DISTRIBUTION

Parameters to Specify	Resulted Distribution
μ=1, k=K	Rician
μ=m, $k\to 0$	Nakagami-m
μ=1, $k\to 0$	Rayleigh
μ=0.5, $k\to 0$	One-sided Gaussian

secrecy capacity of C_k according to Eqs. (22) and (30), which is expressed as

$$\begin{aligned}\mathcal{C}^{\text{se}}_{\mathrm{C}_k} &= \frac{1}{ln(2)}\frac{k}{\mu}\left(\frac{1}{M_r\mu k}\right)^{\frac{M_r\mu}{2}} \\ &\times \exp\left(\frac{-3M_r\mu k}{2}\right)\sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i!} \\ &\times \left(\frac{P_{\mathrm{C}_k}}{\sigma^2}\frac{\Omega}{\mu(k+1)}\right)^{i}\frac{\Gamma(M_r\mu+i)}{\Gamma(M_r\mu)} \\ &\times M_{-(\frac{M_r\mu+2i}{2}),(\frac{M_r\mu-1}{2})}(M_r k),\end{aligned} \tag{32}$$

where k and Ω are shape and scale parameters, respectively and μ is fading figure. $M_{a,b}(.)$ is Whittaker function, a and b are non-negative integers [29, Sec.9.22 and 9.23].

Additionally, the secrecy capacity of $\mathrm{D}^{\mathrm{r}}_i$ for perfect CSI can be written as

$$\begin{aligned}\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i} &= \mathcal{C}_{\mathrm{D}^{\mathrm{r}}_i} \\ &= \log_2\left(1+\lambda_{\mathrm{D}^{\mathrm{r}}_i}\right) \\ &= \log_2\left[1+\frac{P_{\mathrm{D}^{\mathrm{r}}_i}\left|\mathbf{H}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{D}^{\mathrm{r}}_i}\mathbf{V}_{\mathrm{D}^{\mathrm{t}}_i}\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}\right|^2}{\sigma^2}\right],\end{aligned} \tag{33}$$

Let's denote $\mathcal{C}^{\mathrm{s}}_{\mathrm{D}^{\mathrm{r}}_i}$ by β_2 for notational convenience. Then

$$\beta_2 = \log_2\left(1+\frac{P_{\mathrm{D}^{\mathrm{r}}_i}\alpha_3}{\sigma^2}\right), \tag{34}$$

where $\alpha_3 \overset{\text{def}}{=} \left|\mathbf{H}_{\mathrm{D}^{\mathrm{t}}_i\to\mathrm{D}^{\mathrm{r}}_i}\mathbf{V}_{\mathrm{D}^{\mathrm{t}}_i}\mathbf{W}_{\mathrm{D}^{\mathrm{t}}_i}\right|^2$. The PDF of β_2 is given by

$$\begin{aligned}f_{\beta_2}\left(\frac{\sigma^2}{P_{\mathrm{D}^{\mathrm{t}}_i}}(2^{\beta_2}-1)\right) &= \frac{\sigma^2}{P_{\mathrm{D}^{\mathrm{t}}_i}}\left[2^{\beta_2}\ln(2)\right] \\ &\times f_{\alpha_3}\left(\frac{\sigma^2}{P_{\mathrm{D}^{\mathrm{t}}_i}}(2^{\beta_2}-1)\right),\end{aligned} \tag{35}$$

where the PDF of α_3 for the Nakagami-m and Norton channels are given by Eqs. (44) and (54), respectively, in the appendix (with $\varrho=\alpha_3$ in Eq. (44) and $\theta_2=\alpha_3$ in Eq. (54)). The ergodic secrecy capacity of $\mathrm{D}^{\mathrm{t}}_i$ can be expressed by

$$\mathcal{C}^{\text{se}}_{\mathrm{D}^{\mathrm{t}}_i} = \int_0^{\infty}\beta_2\, f_{\beta_2}(\beta_2)\, d\beta_2. \tag{36}$$

The closed form expressions of ergodic secrecy capacity for DU ($\mathcal{C}^{\text{se}}_{\mathrm{D}^{\mathrm{t}}_i}$) will be exactly same as for CU with parameter values change in Eqs. (31) and Eqs. (32) for Nakagami-m and Norton channel, respectively.

C. Secrecy Outage Probability

A secrecy outage occurs when the difference between the channel capacities of the legitimate user and an eavesdropper is less than a target secrecy rate, which is given by

$$\begin{aligned}\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k} &= \Pr\left[\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k} < \Psi_1\right] \\ &= \int_0^{\Psi_1} f\left(\beta_1\right)\, \mathrm{d}\beta_1.\end{aligned} \tag{37}$$

For the imperfect CSI scenario, $f\left(\beta_1\right)$ in Eq. (37) can be established using Eq. (26). The capacity above which the users can be considered secured by eavesdroppers is defined as targeted secrecy capacity. Furthermore, our proposed null steering technique with the perfect CSI makes the channel capacity go to zero for an eavesdropper. Thus, the secrecy outage probability of C_k can be written as

$$\begin{aligned}\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k} &= \Pr\left[\mathcal{C}^{\mathrm{s}}_{\mathrm{C}_k} < \Psi_1\right] \\ &= \Pr\left[\log_2\left(1+\frac{P_{\mathrm{C}_k}\alpha_1}{\sigma^2}\right) < \Psi_1\right] \\ &= \int_0^{\frac{\sigma^2}{P_{\mathrm{C}_k}}(2^{\Psi_1}-1)} f_{\alpha_1}\left(E\right)\, \mathrm{d}E,\end{aligned} \tag{38}$$

where $E \overset{\text{def}}{=} \frac{\sigma^2}{P_{\mathrm{C}_k}(2^{\Psi_1}-1)}$ and

$$\mathrm{d}E = \frac{\sigma^2}{P_{\mathrm{C}_k}}\left[2^{\Psi_1}\log_e(2)\right]\, \mathrm{d}\Psi_1. \tag{39}$$

Substituting Eq. (39) into Eq. (38), we may obtain the secrecy outage probability as

$$\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k} = F_{\alpha_1}\left[\frac{\sigma^2}{P_{\mathrm{C}_k}}\left(2^{\Psi_1}-1\right)\right], \tag{40}$$

where the cumulative distribution function (CDF) $F_{\alpha_1}(\ )$ of α_1 is given by Eqs. (46) and (56) for the Nakagami-m and Norton channel models, respectively, in the appendix. Similarly, according to the appendix, the secrecy outage probability for $\mathrm{D}^{\mathrm{r}}_i$ can be obtained as

$$\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i} = F_{\alpha_3}\left[\frac{\sigma^2}{P_{\mathrm{D}^{\mathrm{r}}_i}}\left(2^{\Psi_2}-1\right)\right], \tag{41}$$

where the CDF $F_{\alpha_3}(\ )$ of α_3 is given by Eqs. (46) and (56) for the Nakagami-m and Norton channel models, respectively, in the appendix. If the SNR of CU, i.e., $\frac{P_{\mathrm{C}_k}}{\sigma^2}\to\infty$ in Eq. (40), the term $\frac{\sigma^2}{P_{\mathrm{C}_k}}(2^{\Psi_1}-1)$ tends to zero which makes the secrecy outage probability $\mathcal{P}^{\text{s-out}}_{\mathrm{C}_k}$ a zero. The similar asymptotic trend can be found for the secrecy outage probability of DU using Eq. (41), i.e., $\mathcal{P}^{\text{s-out}}_{\mathrm{D}^{\mathrm{r}}_i}\to 0$ if $\frac{P_{\mathrm{D}^{\mathrm{r}}_i}}{\sigma^2}\to\infty$.

V. SIMULATION AND DISCUSSION

In this section, the performance of our proposed novel null steering technique is evaluated in terms of the secrecy capacity and the secrecy outage probability. The number of antennas at the BS and each DU transmitter is set to be $M_{\mathrm{t}}=4$. The number of antennas at each receiver is $M_{\mathrm{r}}=1$. The number of DUs present in the network is assumed to be $N_{\mathrm{DU}}=4$. The number of CUs in a specific frequency-band is given by $N_{\mathrm{CU}}=1$. All MIMO channel coefficients are assumed

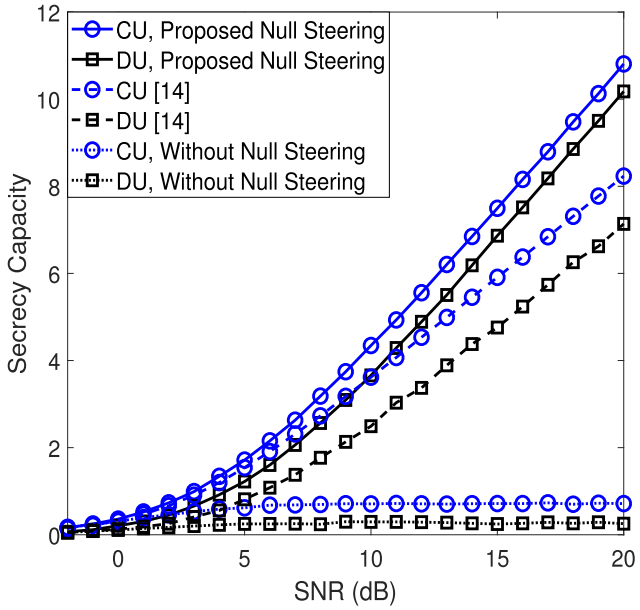


Fig. 2. The secrecy capacities of CU and DU over the non-identical Nakagami-m fading channels.

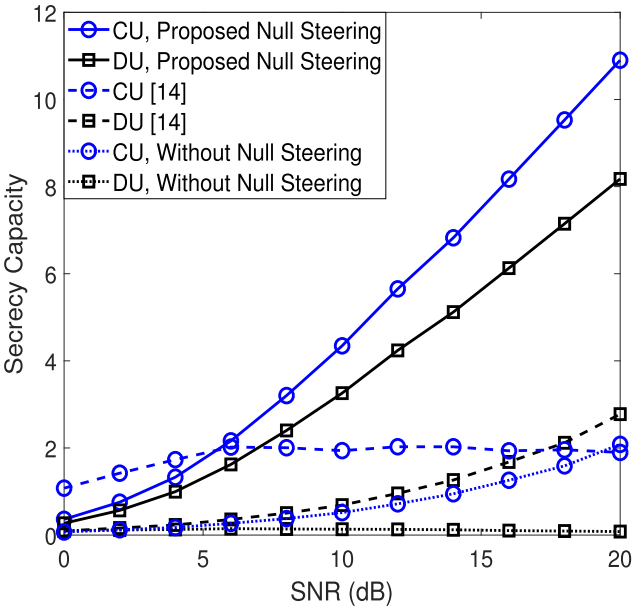


Fig. 4. The secrecy capacities for CU and DU over the Norton fading channel.

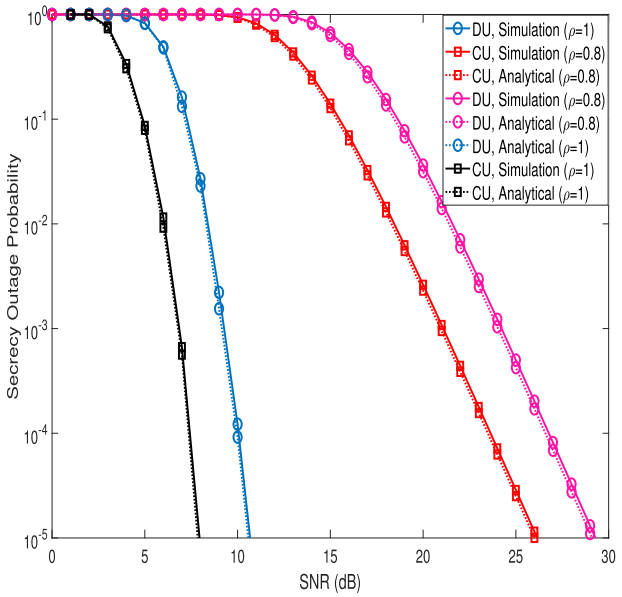


Fig. 3. The secrecy outage probabilities for CU and DU over the non-identical Nakagami-m fading channels.

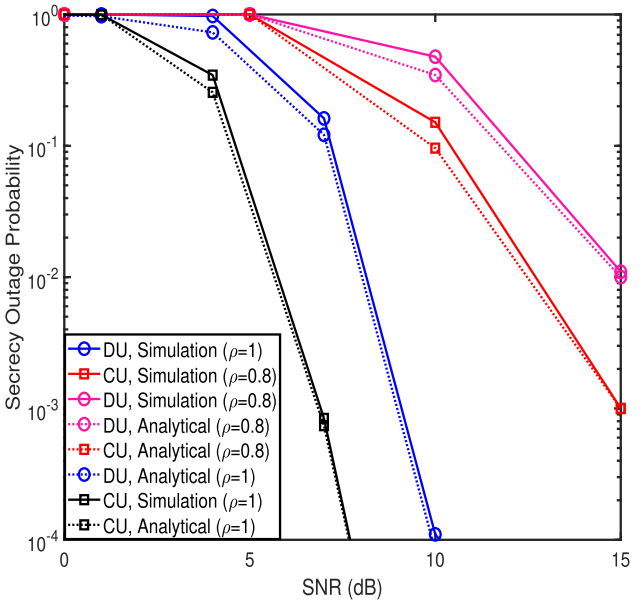


Fig. 5. The secrecy outage probabilities for CU and DU over the Norton fading channel.

to comply with the non-identical Nakagami-m distribution with $m = 1, 2, 3, 4$ and the Norton flat-fading channel with $k = 3$ and $\Omega = 1$. In addition, we emphasize on the secrecy capacity of CU more than that of DU to maintain the QoS of CU by allocating sufficient power to the BS.

Fig. 2 delineates the secrecy capacities of CU and DU over the aforementioned non-identical Nakagami-m fading channel. It shows that the improvement of the secrecy capacity is substantiated by applying a null steering vector at each transmitter. The CU and DU are completely secure for perfect CSI as the data are completely blocked from the active eavesdropper(s) present in the network. However, if the imperfect CSI arises, the leakage of information will occur as previously discussed. The secrecy capacity of CU is higher than that of DU because the power allocated to DU is less than that allocated to CU. Note that when our proposed null steering technique is unavailable, the secrecy capacities cannot satisfy the target values for both CU and DU. As shown in [17], the secrecy capacities for both CU and DU using a jamming technique are higher than those without our proposed null steering technique. However, our proposed null steering scheme can even outperform the jamming technique proposed in [17] in terms of the secrecy capacities for both CU and DU.

Besides, Fig. 3 depicts the secrecy outage probabilities for both CU and DU over the non-identical Nakagami-m fading channels with $m = 1, 2, 3$, and 4. According to Fig. 3, the closed-form secrecy outage probabilities derived from the theoretical analysis (denoted by "Anaytical" in the figure) match the simulation results (denoted by "Simulation" in the figure) closely. For DU's secrecy outage probability

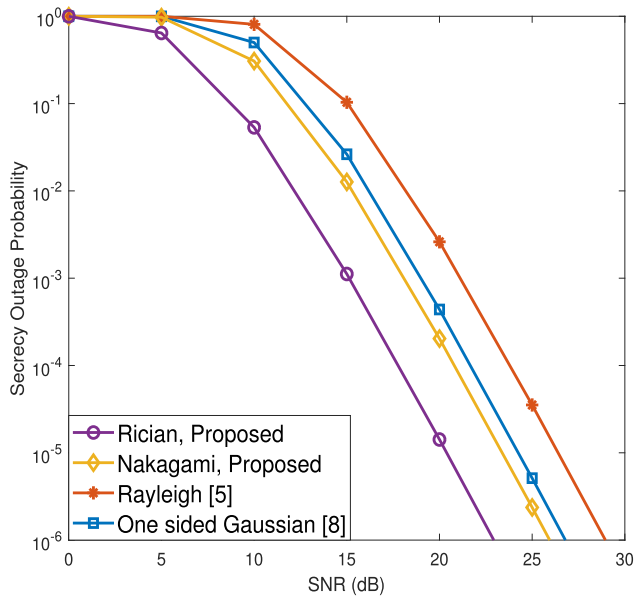


Fig. 6. The secrecy outage probabilities of CU for certain special cases of the k-μ channel-coefficient distribution.

simulation, targeted secrecy outage probability for CU (ϕ_1) is considered 0.0001. For CU's secrecy outage probability simulation, targeted secrecy outage probability for DU (ϕ_2) is considered 0.001. Moreover, CU is more secure than DU (the secrecy outage probabilities of CU are smaller than those of DU) since more power is allocated to CU than DU.

On the other hand, Fig. 4 plots the secrecy capacities of both CU and DU over the Norton flat-fading channel with the shape parameter $k = 3$ and the scale parameter $\Omega = 1$. The Norton fading channel model is very important as it describes more practical scenarios in the presence of both LOS and NLOS (non-light-of-sight) connections. The Norton channel model is the combination of the Nakagami-m and Rician fading channel models. According to Fig. 4, the secrecy capacities for both users increase with the SNR when the null steering technique is applied. The secrecy-capacity performance over the Norton fading channel model is almost the same as those over the Nakagami-m channels by use of the null steering technique. Again, our proposed new null steering scheme outperforms the jamming technique proposed in [17] and the conventional system with neither null steering nor jamming technique.

Fig. 5 demonstrates the secrecy outage probabilities of both CU and DU over the Norton fading channel model. Here the simulation results also match the analytical results again. The secrecy outage probability over the Norton fading channel is almost the same as those over the Nakagami-m fading channels. According to Fig. 5, the secrecy outage probabilities for both CU and DU over the two aforementioned channel models clearly exhibit the asymptotic trend stated at the end of Section IV-C.

Finally, Fig. 6 illustrates the secrecy outage probabilities of CU subject to the k-μ channel-coefficient distribution (for certain special cases) as stated by Table I. Here D2D communications are not considered. The Rician, Nakagami-m, Rayleigh, and one-sided Gaussian distributions are obtained by substituting the respective appropriate values into the parameters k and μ. Note that the Rayleigh and one-sided Gaussian distributions have been applied in [5] and [8], respectively. Fig. 6 shows that the k-μ distribution is a generalized channel model and the performance analysis over this generalized channel model would be much more practical.

VI. Conclusion

In this paper, we study a critical communication security topic, namely the physical-layer security (PLS) for underlay MIMO-D2D wireless communications over the Nakagami-m and Norton fading-channel models. We propose a null steering approach and signal-alignment technique to eliminate the information leakage from the desired transmitter to the eavesdropper(s). The null steering vectors are formulated subject to the knowledge of the global channel state information at each transmitter. A generalized nonlinear optimization problem is formulated thereby to improve the PLS for MIMO-D2D (multi-input/multi-output device-to-device) communications. Our proposed new scheme is capable of improving the secrecy capacities and the secrecy outage probabilities for both cellular users (CUs) and device users (DUs) in the presence of multiple eavesdroppers. The closed-form analytical expressions of the secrecy outage probabilities over the non-identical Nakagami-m and Norton fading channels are derived and compared with the simulation results.

Appendix I
CDF Derivation for Sum of Square of Nakagami-m RVs

In this appendix, we will derive the cumulative distribution function (CDF) of the sum of squares of Nakagami-m RVs. This CDF is important for formulating the secrecy outage probabilities of CU and DU in the main text. The square of a Nakagami-m RV X, i.e., $\Phi_1 \overset{\text{def}}{=} X^2$ follows the Erlang distribution according to [33]. The PDF of Φ_1 is given by

$$f_{\Phi_1}(\phi_1; m, \eta) = \frac{\phi_1^{m-1}}{\eta^m (m-1)!} \exp\left(-\frac{\phi_1}{\eta}\right) U(\phi_1), \tag{42}$$

where the parameters m and η have been defined below Eq. (1). According to Eq. (42), the CDF of Φ_1 is given by

$$\begin{aligned} F_{\Phi_1}(\phi_1; m, \eta) &= \left[1 - \frac{\Gamma(m, \phi_1/\eta)}{(m-1)!}\right] U(\phi_1) \\ &= \left[1 - \exp\left(-\frac{\phi_1}{\eta}\right) \sum_{\mu=0}^{m-1} \frac{1}{\mu!} \left(\frac{\phi_1}{\eta}\right)^{\mu}\right] U(\phi_1), \end{aligned} \tag{43}$$

where $\Gamma(\,)$ is the gamma function [35] and $U(\,)$ has been defined below Eq. (1). On the other hand, the sum of squares of the Nakagami-m RVs X, i.e., $\varrho \overset{\text{def}}{=} \sum_{n=1}^{M_{\rm r}} \Phi_n$ follows the nested finite weighted sum of Erlang distributions, where $M_{\rm r}$ may be any positive integer. According to [33], the PDF of ϱ is thus given by

$$\begin{aligned} f_{\varrho}(\varrho) = &\sum_{n=1}^{M_{\rm r}} \sum_{s=1}^{m_n} \Xi_{M_{\rm r}} \left(n, s, \{m_q\}_{q=1}^{M_{\rm r}}, \{\eta_q\}_{q=1}^{M_{\rm r}}, \{l_q\}_{q=1}^{M_{\rm r}-2}\right) \\ &\times f_{\Phi_1}(\varrho; s, \eta_n), \end{aligned} \tag{44}$$

where $\Xi_{M_\mathrm{r}}(\ )$ denotes the weight function given by

$$\begin{aligned}\Xi_{M_\mathrm{r}}&\left(n,s,\{m_q\}_{q=1}^{M_\mathrm{r}},\{\eta_q\}_{q=1}^{M_\mathrm{r}},\{l_q\}_{q=1}^{M_\mathrm{r}-2}\right)\\ &\stackrel{\text{def}}{=}\sum_{l_1=s}^{m_n}\sum_{l_2=s}^{l_1}\cdots\sum_{l_{M_\mathrm{r}-2}=s}^{l_{M_\mathrm{r}-3}}\Bigg[\frac{(-1)^{W-m_n}\eta_n^s}{\prod_{h=1}^{M_\mathrm{r}}\eta_h^{m_h}}\\ &\quad\times\frac{(m_n+m_{1+U(1-n)}-l_1-1)!}{(m_{1+U(1-n)}-1)!(m_n-l_1)!}\\ &\quad\times\left(\frac{1}{\eta_n}-\frac{1}{\eta_{1+U(1-n)}}\right)^{l_1m_n-m_{1+U(1-n)}}\\ &\quad\times\frac{(l_{M_\mathrm{r}-2}+m_{M_\mathrm{r}-1+U(M_\mathrm{r}-1-n)}-s-1)!}{(m_{M_\mathrm{r}-1+U(M_\mathrm{r}-1-n)}-1)!(l_{M_\mathrm{r}-2}-s)!}\\ &\quad\times\left(\frac{1}{\eta_n}-\frac{1}{\eta_{M_\mathrm{r}-1+U(M_\mathrm{r}-1-n)}}\right)^{s-l_{M_\mathrm{r}-2}-m_{L-1+U(M_\mathrm{r}-1-n)}}\\ &\quad\times\prod_{\Delta=1}^{M_\mathrm{r}-3}\frac{(l_\Delta+m_{\Delta+1+U(\Delta+1-n)}-l_{\Delta+1}-1)!}{(m_{\Delta+1+U(\Delta+1-n)}-1)!(l_\Delta-l_{\Delta+1})!}\\ &\quad\times\left(\frac{1}{\eta_n}-\frac{\frac{1}{\eta_n}}{\frac{1}{\eta_{\Delta+1+U(\Delta+1-n)}}}\right)^{l_{\Delta+1}-l_\Delta-m_{\Delta+1+U(\Delta+1-n)}}\Bigg],\end{aligned}\tag{45}$$

where $W\stackrel{\text{def}}{=}\sum_{n=1}^{M_\mathrm{r}}m_n$. Finally, the CDF of ϱ can be written as

$$\begin{aligned}F_\varrho(\varrho)=\sum_{n=1}^{M_\mathrm{r}}\sum_{s=1}^{m_n}&\Xi_{M_\mathrm{r}}\left(n,s,\{m_q\}_{q=1}^{M_\mathrm{r}},\{\eta_q\}_{q=1}^{M_\mathrm{r}},\{l_q\}_{q=1}^{M_\mathrm{r}-2}\right)\\ &\times F_{\Phi_1}(\varrho,s,\eta_n).\end{aligned}\tag{46}$$

Appendix II
CDF Derivation for Sum of Square of Norton distributed RVs

In this appendix, we will derive the CDF of the sum of squares of Norton RVs. Substituting $\sigma^2=\alpha/2$ and $\mu=\alpha\xi$ in Eq. (2), one may express the Norton PDF as

$$f_Y(y)=\frac{2y^{\alpha\xi}\xi}{v^{\alpha\xi-1}}\exp\left\{-\xi\left(y^2+v^2\right)\right\}I_{\alpha\xi-1}(2yv\xi),\tag{47}$$

where both v and $I_{\mu-1}(\ )$ have been defined below Eq. (2). Now, define Θ_1 by $\Theta_1\stackrel{\text{def}}{=}Y^2$. The PDF of Θ_1 (with the RV θ_1) can thus be expressed by

$$f_{\Theta_1}(\theta_1)=\frac{\theta_1^{\frac{\alpha\xi-1}{2}}\xi}{v^{\alpha\xi-1}}\exp\left\{-\xi\left(\theta_1+v^2\right)\right\}I_{\alpha\xi-1}\left(2v\xi\sqrt{\theta_1}\right).\tag{48}$$

The PDF above can be re-formulated in terms of the shape parameter k and the scale parameter Ω, where $k\stackrel{\text{def}}{=}\frac{v^2}{2\sigma^2}$ (i.e., the ratio between the direct and scattered components) and $\Omega\stackrel{\text{def}}{=}v^2+2\sigma^2$, along with $\xi=\frac{\mu}{\alpha}=\frac{\mu(k+1)}{\Omega}$ and $v^2=\frac{k(k+1)}{\Omega}$. It is given by

$$\begin{aligned}f_{\Theta_1}(\theta_1)=\frac{\mu(k+1)}{\Omega}&\left[\frac{(k+1)\theta_1}{k\Omega}\right]^{\frac{\mu-1}{2}}\exp\left[\frac{-\mu(k+1)\theta_1}{\Omega}\right.\\ &\left.-\mu k\right]I_{\mu-1}\left(\mu\times\sqrt{\frac{4k(k+1)\theta_1}{\Omega}}\right).\end{aligned}\tag{49}$$

The moment-generating function (MGF) of Θ_1 is given by

$$\begin{aligned}M_{\Theta_1}(\theta_1)&=\int_0^\infty e^{t\theta_1}f_{\Theta_1}(\theta_1)d\theta_1\\ &=\int_0^\infty e^{t\theta_1}\frac{\theta_1^{\frac{\alpha\xi-1}{2}}\xi}{v^{\alpha\xi-1}}\exp\left[-\xi\left(\theta_1+v^2\right)\right]\\ &\quad\times I_{\alpha\xi-1}\left(2v\xi\sqrt{\theta_1}\right)d\theta_1\\ &=\xi^{\alpha\xi}\exp(-\xi v^2)\sum_{j=0}^\infty\frac{(\xi^2v^2)^j}{j!\,\Gamma(\alpha\xi+j)}\\ &\quad\times\int_0^\infty\theta_1^{\alpha\xi+j-1}\exp\left[-(\xi-t)\theta_1\right]d\theta_1.\end{aligned}\tag{50}$$

Let $(\xi-t)\theta_1=u$, which implies $(\xi-t)d\theta_1=du$. Consequently, Eq. (50) can be rewritten as

$$\begin{aligned}M_{\Theta_1}(\theta_1)&=\xi^{\alpha\xi}\exp(-\xi v^2)\sum_{j=0}^\infty\frac{(\xi^2v^2)^j}{j!\,\Gamma(\alpha\xi+j)}\\ &\quad\times\int_0^\infty\left(\frac{u}{\xi-t}\right)^{\alpha\xi+j-1}\frac{\exp(-u)}{\xi-1}\,du\\ &=\xi^{\alpha\xi}\exp(-\xi v^2)\sum_{j=0}^\infty\frac{(\xi^2v^2)^j}{j!\,\Gamma(\alpha\xi+j)}\left(\frac{1}{\xi-t}\right)^{\alpha\xi+j}\\ &\quad\times\int_0^\infty u^{\alpha\xi+j-1}e^{-u}\,du\\ &=\xi^{\alpha\xi}\exp(-\xi v^2)\sum_{j=0}^\infty\frac{(\xi^2v^2)^j}{j!\,\Gamma(\alpha\xi+j)}\left(\frac{1}{\xi-t}\right)^{\alpha\xi+j}\\ &\quad\times\Gamma(\alpha\xi+j)\\ &=\left(\frac{\xi}{\xi-t}\right)^{\alpha\xi}\exp(-\xi v^2)\sum_{j=0}^\infty\frac{1}{j!}\left(\frac{\xi^2v^2}{\xi-t}\right)^j\\ &=\left(\frac{\xi}{\xi-t}\right)^{\alpha\xi}\exp(-\xi v^2)\exp\left(\frac{\xi^2v^2}{\xi-t}\right).\end{aligned}\tag{51}$$

If $\Theta_2\stackrel{\text{def}}{=}\sum_{l=1}^{M_\mathrm{r}}\Theta_l$, then MGF of Θ_2 can be expressed by

$$M_{\Theta_2}(\theta_2)=\left(\frac{\xi}{\xi-t}\right)^{M_\mathrm{r}\alpha\xi}\exp(-\xi M_\mathrm{r}v^2)\,\exp\left(\frac{\xi^2M_\mathrm{r}v^2}{\xi-t}\right).\tag{52}$$

To obtain the PDF of Θ_2, we let $\alpha=M_\mathrm{r}\alpha$ and $v^2=M_\mathrm{r}v^2$ in Eq. (48) such that

$$\begin{aligned}f_{\Theta_2}(\theta_2)=\frac{\theta_2^{\frac{M_\mathrm{r}\alpha\xi-1}{2}}\xi}{v^{M_\mathrm{r}\alpha\xi-1}}&\exp\left[-\xi\left(\theta_2+M_\mathrm{r}v^2\right)\right]\\ &\times I_{M_\mathrm{r}\alpha\xi-1}\left(2v\xi\sqrt{M_\mathrm{r}\theta_2}\right).\end{aligned}\tag{53}$$

Moreover, the PDF of Θ_2 can also be expressed in terms of the shape parameter k and the scale parameter Ω as

$$\begin{aligned}f_{\Theta_2}(\theta_2)=\frac{\mu(k+1)}{\Omega}&\left(\frac{(k+1)\theta_2}{M_\mathrm{r}k\Omega}\right)^{\frac{M_\mathrm{r}\mu-1}{2}}\\ &\times\exp\left(\frac{-\mu(k+1)\theta_2}{\Omega}\right.\\ &\left.-\mu M_\mathrm{r}k\right)I_{M_\mathrm{r}\mu-1}\left(\mu\times\sqrt{\frac{4M_\mathrm{r}k(k+1)\theta_2}{\Omega}}\right).\end{aligned}\tag{54}$$

According to Eq. (54) along with $\mu M_{\mathrm{r}} k = \frac{b^2}{2}$ and $\frac{\mu\theta_2(k+1)}{\Omega} = \frac{p^2}{2}$, which implies $\frac{\mu(k+1)d\theta_2}{\Omega} = p\,dp$, we have

$$\begin{aligned} R &= \int_{\theta_2}^{\infty} \frac{\mu(k+1)}{\Omega} \left[\frac{(k+1)\theta_2}{M_{\mathrm{r}} k \Omega}\right]^{\frac{\mu M_{\mathrm{r}}-1}{2}} \exp\left[\frac{-(k+1)\mu\theta_2}{\Omega}\right. \\ &\quad \left. - \mu M_{\mathrm{r}} k\right] I_{\mu M_{\mathrm{r}}-1}\left(\mu \times \sqrt{\frac{4M_{\mathrm{r}} k(k+1)\theta_2}{\Omega}}\right) d\theta_2 \\ &= \int_{\sqrt{\frac{2\mu\theta_2(k+1)}{\Omega}}}^{\infty} p \left(\frac{p}{\sqrt{2\mu M_{\mathrm{r}} k}}\right)^{\mu M_{\mathrm{r}}-1} \exp\left(\frac{-b^2}{2} - \frac{-p^2}{2}\right) \\ &\quad \times I_{\mu M_{\mathrm{r}}-1}\left(p \times \sqrt{2\mu M_{\mathrm{r}} k}\right) dp \\ &= \int_{\sqrt{\frac{2\mu\theta_2(k+1)}{\Omega}}}^{\infty} p \left(\frac{p}{b}\right)^{\mu M_{\mathrm{r}}-1} \exp\left(-\frac{p^2+b^2}{2}\right) I_{\mu M_{\mathrm{r}}-1}(bp) \\ &\quad \times dp \\ &= Q_{\mu M_{\mathrm{r}}}\left(\sqrt{2\mu M_{\mathrm{r}} k}, \sqrt{\frac{2\mu(k+1)\theta_2}{\Omega}}\right). \end{aligned} \tag{55}$$

Consequently, the CDF of Θ_2 is given by

$$F_{\Theta_2}(\theta_2) = 1 - Q_{\mu M_{\mathrm{r}}}\left(\sqrt{2\mu M_{\mathrm{r}} k}, \sqrt{\frac{2\mu(k+1)\theta_2}{\Omega}}\right). \tag{56}$$

REFERENCES

[1] H. A. U. Mustafa, M. A. Imran, M. Z. Shakir, A. Imran, and R. Tafazolli, "Separation framework: An enabler for cooperative and D2D communication for future 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 419–445, 1st Quart., 2016.

[2] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.

[3] M. Gonzalez-Martín, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1155–1166, Feb. 2019.

[4] R. Rajadurai, K. S. Gopalan, M. Patil, and S. Chitturi, "Enhanced interworking of LTE and Wi-Fi direct for public safety," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 40–46, Apr. 2016.

[5] X. Song, W. Rave, N. Babu, S. Majhi, and G. Fettweis, "Two-level spatial multiplexing using hybrid beamforming for millimeter-wave backhaul," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4830–4844, Jul. 2018.

[6] N. Nandan and S. Majhi, "Secrecy outage analysis by applying bi-directional beamforming in underlay MIMO-CRN," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 430–434.

[7] N. Nandan, S. Majhi, and H.-C. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, Aug. 2018.

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

[9] N. Nandan, S. Majhi, and H.-C. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5327–5337, Aug. 2018.

[10] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[11] J. Lyu, H.-M. Wang, and K.-W. Huang, "Physical layer security in D2D underlay cellular networks with Poisson cluster process," *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 7123–7139, Nov. 2020.

[12] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[13] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[14] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[15] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[16] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8767–8774, Oct. 2016.

[17] H.-M. Wang, B.-Q. Zhao, and T.-X. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[18] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Feb. 2017.

[19] Q. Li, P. Ren, and D. Xu, "Security enhancement and QoS provisioning for NOMA-based cooperative D2D networks," *IEEE Access*, vol. 7, pp. 129387–129401, 2019.

[20] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Physical layer security for relay assisted MIMO D2D communication," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 651–656.

[21] M. Ibnkahla, *Signal Processing for Mobile Communication Handbook*. Boca Raton, FL, USA: CRC Press, 2004.

[22] P. Kumar, S. Majhi, and Y. Nasser, "Analysis of outage performance of opportunistic AF OFDM relaying in Nakagami-m channels," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2016, pp. 2527–2531.

[23] X. Wang and N. C. Beaulieu, "Switching rates of two-branch selection diversity in k-μ and α-μ distributed fadings," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1667–1671, Apr. 2009.

[24] Z.-J. Yang *et al.*, "Peer discovery for device-to-device (D2D) communication in LTE—A networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 665–670.

[25] Y. Xu, "A mode selection scheme for D2D communication in heterogeneous cellular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.

[26] D. A. Zogas, G. K. Karagiannidis, and S. A. Kotsopoulos, "Equal gain combining over Nakagami-n (Rice) and Nakagami-q (Hoyt) generalized fading channels," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 374–379, Mar. 2005.

[27] A. Maaref and S. Aissa, "Capacity of MIMO Rician fading channels with transmitter and receiver channel state information," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1687–1698, May 2008.

[28] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "N∗Nakagami: A novel stochastic model for cascaded fading channels," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1453–1458, Aug. 2007.

[29] S. K. Dewangan, S. Choubey, J. Patra, and A. Choubey, "Nonlinear optimization methods—Overview and future scope," in *Modern Optimization Methods for Science, Engineering and Technology*. Bristol, U.K.: IOP Publishing, 2019, pp. 1–4.

[30] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[31] N. Nandan, S. Majhi, and H.-C. Wu, "Beamforming and power optimization for physical layer security of MIMO-NOMA based CRN over imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5990–6001, Jun. 2021.

[32] X. Zhang, J. Xing, Z. Yan, Y. Gao, and W. Wang, "Outage performance study of cognitive relay networks with imperfect channel knowledge," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 27–30, Jan. 2013.

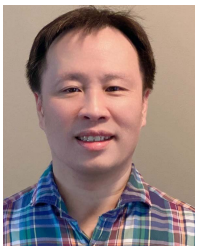
[33] G. K. Karagiannidis, N. C. Sagias, and T. A. Tsiftsis, "Closed-form statistics for the sum of squared Nakagami-m variates and its applications," *IEEE Trans. Commun.*, vol. 54, no. 8, pp. 1353–1359, Aug. 2006.

[34] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over generalized fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[35] M. R. Bhatnagar and Z. Ghassemlooy, "Performance analysis of gamma–gamma fading FSO MIMO links with pointing errors," *J. Lightw. Technol.*, vol. 34, no. 9, pp. 2158–2169, May 1, 2016.

Ajay Kumar (Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Institute of Engineering and Technology, Lucknow, India, in 2015, and the M.Tech. degree in communication system engineering from IIT Patna, Patna, India, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electrical Communication Engineering, Indian Institute of Science at Bangalore, Bengaluru, India. From 2018 to 2020, he was a Wireless Research and Development Engineer with FleetRF Pvt. Ltd. His research interests include physical layer security for wireless communication, orthogonal time-frequency space modulation, non-orthogonal multiple access, and joint radar and communication systems.

Sudhan Majhi (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing from the Indian Institute of Technology Kharagpur, India, in 2004, and the Ph.D. degree from Nanyang Technological University (NTU), Singapore, in 2008. He was a Post-Doctoral Researcher with the University of Michigan–Dearborn, Dearborn, MI, USA, the Institute of Electronics and Telecommunications, Rennes, France, and NTU. He is currently an Associate Professor with the Department of Electrical Communication Engineering, Indian Institute of Science at Bangalore, Bengaluru, India. His research interest includes signal processing for wireless communication.



Hsiao-Chun Wu (Fellow, IEEE) received the B.S. degree in electrical engineering from the National Cheng Kung University, Taiwan, in 1990, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 1993 and 1999, respectively.

From March 1999 to January 2001, he worked at Motorola Personal Communications Sector Research Labs as a Senior Electrical Engineer. From July 2007 to August 2007, he was a Visiting Assistant Professor at the Television and Networks Transmission Group, Communications Research Centre, Canada. From August 2008 to December 2008, he was a Visiting Associate Professor at the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. Since January 2001, he has been a Faculty Member with the Department of Electrical and Computer Engineering, Louisiana State University (LSU), Baton Rouge, LA, USA, where he is currently a Distinguished Professor. He is also a Visiting Professor at the International College of Semiconductor Technology, National Chiao Tung University, Taiwan. He has published more than 300 peer-refereed technical journals and conference papers in electrical and computer engineering. His research interests include wireless communications and signal processing. He is an IEEE Distinguished Lecturer. He currently serves as an Associate Editor for IEEE TRANSACTIONS ON BROADCASTING and IEEE TRANSACTIONS ON SIGNAL PROCESSING, an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE TRANSACTIONS ON MOBILE COMPUTING, an Academic Editor for *Sensors*, an Editor and a Technical Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and *IEEE Communications Magazine*, and an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, IEEE SIGNAL PROCESSING LETTERS, and *IEEE Communications Magazine*. He served for numerous textbooks, IEEE/ACM conferences and journals as the technical committee, the symposium chair, and the track chair or a reviewer in signal processing, communications, circuits, and computers.