Securing Large-Scale D2D Networks Using Covert Communication and Friendly Jamming

Shaohan Feng, *Member, IEEE*, Xiao Lu, *Member, IEEE*,

Sumei Sun, *Fellow, IEEE*, Dusit Niyato, *Fellow, IEEE*,

and Ekram Hossain, *Fellow, IEEE*

Abstract

We exploit both covert communication and friendly jamming to propose a friendly jamming-assisted covert communication and use it to doubly secure a large-scale device-to-device (D2D) network against eavesdroppers (i.e., wardens). The D2D transmitters defend against the wardens by: 1) hiding their transmissions with enhanced covert communication, and 2) leveraging friendly jamming to ensure information secrecy even if the D2D transmissions are detected. We model the combat between the wardens and the D2D network (the transmitters and the friendly jammers) as a two-stage Stackelberg game. Therein, the wardens are the followers at the lower stage aiming to minimize their detection errors, and the D2D network is the leader at the upper stage aiming to maximize its utility (in terms of link reliability and communication security) subject to the constraint on communication covertness. We apply stochastic geometry to model the network spatial configuration so as to conduct a system-level study. We develop a bi-level optimization algorithm to search for the equilibrium of the proposed Stackelberg game based on the successive convex approximation (SCA) method and Rosenbrock method. Numerical results reveal interesting insights. We observe that without the assistance from the jammers, it is difficult to achieve covert communication on D2D transmission. Moreover, we illustrate the advantages of the proposed friendly jamming-assisted covert communication by comparing it with the information-theoretical secrecy approach in terms of the secure communication probability and network utility.

Index Terms

Large-scale D2D network, covert communication, physical-layer security, friendly jamming, Stackelberg game, successive convex approximation.

S. Feng and S. Sun are with the Institute for Infocomm Research, Singapore. Email: {fengs, sunsm}@i2r.a-star.edu.sg.

X. Lu is with York University, Toronto, ON M3J 1P3, Canada. Email: luxiao@yorku.ca.

D. Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. Email: DNIYATO@ntu.edu.sg.

E. Hossain is with the Department of Electrical and Computer Engineering, University of Manitoba, Canada. Email: Ekram.Hossain@umanitoba.ca.

I. INTRODUCTION

A. Background and Motivation

Recently, D2D communication has attracted great attention due to its capability of enabling direct communication among proximal mobile devices without the involvement of network infrastructure such as a base station (BS) and the core network [1]. By such, D2D communication has emerged as a promising solution to the provision of energy-efficient communication with low end-to-end latency in supporting miscellaneous location-based peer-to-peer applications [2]. However, the D2D communications are vulnerable to malicious attacks such as eavesdropping due to the broadcast nature of the wireless medium. In general, it is challenging to secure D2D communication due to the following reasons:

- In various application scenarios, the D2D devices are resource-constrained and hence cannot afford high overhead in computation and communication. In this case, heavy resource-dependent methods such as the traditional cryptographic methods may not be feasible [1].

- The D2D networks may not have any centralized support to execute functionalities such as authentication to achieve confidentiality of the transmissions.

- Merely achieving a positive rate difference between legitimate and wiretapping channels is not sufficient from the perspective of privacy protection. For example, in a military application, it may be required to prevent the enemy from detecting transmissions so as to hide the presence and activities of the legitimate army [3].

The above context raises the need for covert communication [4] (also referred to as undetectable communication), which is an enabler for reliable transmission from a legitimate transmitter to its intended receiver while undetectable by a vigilant adversary as shown in Fig. 1(a). Covert communication has a number of advantages. First, the implementation of covert communication does not incur high resource consumption, which makes it suitable for resource-constrained devices and networks. Second, the implementation of covert communication does not rely on the execution of a complicated authentication functionality. Third, the covert communication promises a stronger protection on transmission compared to the information-theoretical secrecy approach as it can hide the transmission itself and thus the information carried by this transmission becomes immune to interception. Also, the performance of covert communication is independent of the adversary's competence. Nevertheless, the covert communication cannot hide the presence of transmission completely and there will be a non-trivial probability of detection by the adversary. Therefore, the following two questions arise: 1) how to reduce the detection probability and improve the communication covertness so as to achieve

Figure 1: (a) Covert communication, (b) friendly jamming, and (c) friendly jamming-assisted covert communication including (d) enhanced covert communication and (e) friendly jamming-enabled countermeasure.

enhanced covert communication? 2) is there any countermeasure when the adversary attempts to wiretap the transmission once it has detected the transmission?

To answer the above questions, we resort to the friendly jamming approach, in which friendly jammers emit jamming signals to interfere with the reception at the adversary (Fig. 1(b)). In this way, the jamming signals will increase the uncertainty in the received signal at the adversary, and thereby, the detection error of the adversary will increase and the communication covertness will improve (Fig. 1(d)) [5]. In addition, since the jamming signals emitted by the jammers will increase the interference power received at the adversary, even in the case that the transmission has been detected, the adversary may not be able to decode the received signal successfully. This will ensure information secrecy. In this way, friendly jamming-assisted covert communication (Fig. 1(c)) will provide an additional level of protection for transmissions (Fig. 1(e)).

B. Contributions

We propose a friendly jamming-assisted covert communication method to secure a large-scale D2D network. As shown in Fig. 2(a), the network under our consideration involves: 1) a large number of power-controlled D2D transmitters cooperating with friendly jammers (which emit jamming signals), 2) their dedicated D2D receivers, and 3) spatially distributed adversaries, namely, wardens. The D2D transmitters randomly transmit information to their dedicated D2D

receivers. The wardens aim to detect the D2D transmissions by following a threshold-based rule on their received signal powers, and once detect, they will wiretap the D2D transmissions. In this case, the decision-making of the wardens is after that of the D2D transmitters, which can be captured by using the framework of a two-stage Stackelberg game with the wardens as the followers at the lower stage and the D2D transmitters together with the friendly jammers as the leaders at the upper stage. The main contributions of this paper can be summarized as follows.

- We propose a friendly jamming-assisted covert communication approach to secure a large-scale D2D network. In this network, the friendly jammers are deployed to cooperate with the D2D network so as to jointly enhance the communication covertness and information secrecy for the D2D transmissions.

- We model the combat between the wardens and the D2D network (i.e., the D2D transmitters and the jammers) by a two-stage Stackelberg game. At the lower stage, the wardens aim to minimize their own detection errors. At the upper stage, the D2D network jointly determines the D2D transmissions power and jamming power in order to maximize network utility subject to the constraint on communication covertness.

- We use stochastic geometry to model the spatial configuration of the large-scale D2D network, namely, the locations of the D2D transmitters, the jammers, and the wardens, and characterize their performance metrics in order to quantitatively analyze the system-level network performance.

- To obtain the equilibrium of our two-stage Stackelberg game, we first analyze the characterizes of the lower-stage problem for the wardens and apply the Rosenbrock method to solve it. The solution is regarded as the best response from the lower stage. Given this best response, we develop a bi-level optimization algorithm based on SCA method to obtain the optimal strategy for the D2D network.

- We present simulation results to verify the optimality of the obtained strategy. We also evaluate and discuss the performance of our proposed approach and demonstrate its advantages by comparing it with the conventional information-theoretical secrecy approach.

C. Organization

The rest of the paper is organized as follows. In Section II, we present the related work. In Section III, we present the system model and the derivation of the performance metrics. The problem statement and the game formulation are presented in Section IV. In Section V, we develop a bi-level algorithm to solve the problem. The numerical results and discussion are

Table I: Symbols and descriptions

Symbol	Description	Default value
d, $w|_d$, j	Indexes of the typical D2D transmitter, the nearest warden of D2D transmitter d, and jammer, respectively.	—
$\mathcal{D}$, $\mathcal{W}$, $\mathcal{J}$	Sets of the D2D transmitters, wardens, and jammers, respectively.	—
$\Phi_{\mathcal{D}}$, $\Phi_{\mathcal{W}}$, $\Phi_{\mathcal{J}}$, $\Phi_{\{\mathcal{D}\backslash\{d\}|d\}}$, $\Phi_{\{\mathcal{D}\backslash\{d\}|w|_d\}}$, $\Phi_{\{\mathcal{J}|d\}}$, $\Phi_{\{\mathcal{J}|w|_d\}}$	PP of D2D transmitters, PP of wardens, PP of jammers, PP of the D2D transmitters that excludes D2D transmitter d with D2D transmitter d as the observation point, PP of the D2D transmitters that excludes D2D transmitter d with warden $w|_d$ as the observation point, PP of the jammers with D2D transmitter d as the observation point, and PP of the jammers with warden $w|_d$ as the observation point, respectively.	—
$\lambda_{\mathcal{D}}$, $\lambda_{\mathcal{W}}$, $\lambda_{\mathcal{J}}$	Densities of $\Phi_{\mathcal{D}}$, $\Phi_{\mathcal{W}}$, and $\Phi_{\mathcal{J}}$, respectively.	$0.1/\mathrm{m}^2$, $0.01/\mathrm{m}^2$, $0.1/\mathrm{m}^2$.
$\mathcal{D}_0$, $\mathcal{D}_1$	Events that D2D transmitter is inactive and active, respectively.	—
$\mathbb{P}^{\mathcal{D}_0}$, $\mathbb{P}^{\mathcal{D}_1}$	Probabilities of events $\mathcal{D}_0$ and $\mathcal{D}_1$, respectively.	0.5, 0.5.
p^{D}, p^{J}, τ	D2D transmission power, jamming power, and power detection threshold, respectively.	$[0, 30]\,\mathrm{dBm}$, $[0, 30]\,\mathrm{dBm}$ [6], —.
$g_{d'd}$, $r_{d'd}$, R	Channel and distance between D2D transmitter d' and the typical D2D receiver, and distance between D2D transmitter and its dedicated D2D receiver, respectively.	$\exp{(1)}$ [7], —, 1m [8].
α, ε, ξ^{D}, ξ^{W}	Path-loss exponent, threshold of detection error, SINR threshold at D2D receiver, and SINR threshold at warden, respectively.	4, 0.01, $-10\mathrm{dB}$, $-10\mathrm{dB}$ [9].
N_d, $N_{w|_d}$	Noises at the typical D2D receiver and warden $w|_d$, respectively.	$-90\mathrm{dBm}$, $-90\mathrm{dBm}$ [6]
$S_d^{\mathcal{D}_1}$, $S_d^{\mathcal{J}}$, $S_{w|_d}^{\mathcal{D}_1}$, $S_{w|_d}^{\mathcal{J}}$	Sum of signal powers from D2D transmitter $d' \in \Phi_{\{\mathcal{D}\backslash\{d\}|d\}}$ received at the typical D2D receiver, sum of signal powers from jammer $j \in \Phi_{\{\mathcal{J}|d\}}$ received at the typical D2D receiver, sum of signal powers from D2D transmitter $d' \in \Phi_{\{\mathcal{D}\backslash\{d\}|w|_d\}}$ received at warden $w|_d$, and sum of signal powers from jammer $j \in \Phi_{\{\mathcal{J}|w|_d\}}$ received at warden $w|_d$, respectively.	—
w^{D}, w^{J}	Reward of stabilizing D2D link conditioned on secure communication and cost of unit jamming power, respectively.	1, 1
f_a, F_a	PDF and CDF of a random variable a, respectively.	—
$\mathbb{P}$, $\mathbb{F}$	Probabilistic and expectation operators, respectively.	—
$\mathcal{L}$, $\mathcal{L}^{-1}$	Laplace and inverse Laplace transforms, respectively.	—

presented in Section VI, which is followed by the conclusions in Section VII. The symbols used in this paper together with their descriptions and default values are given in Table I.

II. Related Work

A. Covert Communication

Covert communication promises reliable while undetectable transmission from the legitimate transmitter to its intended receiver, which thereby completely secures the legitimate transmission [10]. Covert communication was adopted to secure a large-scale wireless network in [11], where the uncertainty caused by the co-channel interference has been leveraged to enhance the communication covertness. Similar idea was adopted in [12], [13], and [4]. In [12], a novel backscatter communication was proposed, where an original message is divided into two parts (i.e., active message and backscatter message). The backscatter message is transmitted by backscattering the active signal (i.e., the signal for transmitting the active message) via ambient backscatter tag. Therein, the active signal can be used to shelter the presence of the backscatter signal (i.e., the signal for transmitting the backscatter message), which thereby can be used to carry secret information. The authors in [13] studied an Internet of Things (IoT) network and used the overt channel as the "spectrum shelter" of the covert channel. The interference from the overt channel was leveraged to hide the presence of the IoT transmission so as to enhance the network security. A large-scale IoT system involving massive IoT gateways (GWs) and IoT devices was secured in [4] against the adversaries from transmission detection. In the system, the in-band full-duplex (IBFD) IoT GWs emit artificial noise, which together with the co-channel interference from the IoT devices can mislead the adversaries in making their decisions. Different from the aforementioned works that leverage the uncertainty caused by the interference/noise, reconfigurable intelligent surface (RIS) was introduced in [14] to improve the communication covertness. Therein, by using RIS to strengthen the directionality of the intended signal, constructive and destructive effects can be achieved on the signals received by the intended receiver and the unintended receiver (i.e., an adversary), respectively. A scenario in which the adversary is unaware of the time of the communication attempt from the legitimate transmitter was investigated in [15]. In this scenario, the legitimate transmitter selects one single slot out of multiple slots for transmission. An upper bound of the achievable covert rate was analytically derived as a performance metric to evaluate the effectiveness of covert communication.

B. Friendly Jamming

The main idea of friendly jamming is to emit jamming signal that will interfere with the receptions at the eavesdropper to achieve confidentiality of legitimate transmissions. Thus the

jamming signals increase the decoding difficulty for the eavesdropper and improve the secrecy outage probability, or equivalently, the secrecy rate [16], [17]. Friendly jamming was adopted together with bandwidth allocation in [18] to secure the unmanned aerial vehicle (UAV)-enabled wireless communication. A UAV-enabled friendly jamming scheme was proposed in [19] to secure industrial IoT (IIoT) against eavesdropping, and its effectiveness in reducing the secrecy outage probability was verified both analytically and numerically. Except for jamming the wiretap channel so as to reduce the secrecy outage probability, friendly jamming can also be applied to improve the communication covertness. This is due to the fact that the jamming signal emitted by the friendly jammer can also increase the uncertainty in the received signal power of the adversary and thereby increase the detection error. For example, the authors in [5] deployed a friendly jammer to transmit jamming signal and prevent the adversary from detecting transmission of the local model updates in order to achieve a covert federated learning (FL) process. As the jamming signal can also reduce transmission reliability, an optimization problem was formulated to determine the optimal jamming power such that both the link reliability and communication covertness for the local model updates in the FL process can be guaranteed. [20] considered a scenario where a transmitter intends to communicate with multiple receivers via orthogonal frequency bands and the adversary is able to monitor all the bands aiming at detecting the transmissions. A friendly jammer was deployed to broadcast jamming signals to distort the adversary's observation in order to increase the detection error for the adversary over all the bands. Different from other works, the authors in [21] considered a scenario where the adversary can optimize not only its detection threshold but also its location aiming to minimize the covert outage probability. To defend against such a powerful adversary, a full-duplex transceiver was deployed, and the jamming signal transmitted by this transceiver was leveraged to maximize the throughput of the legitimate user subject to the constraint on communication covertness.

III. System Model, Assumptions, and Performance Metrics

A. Network Model

We consider a large-scale D2D network under the threat of wardens (Fig. 2(a)). In the network, the spatial distribution of the D2D transmitters follows a homogeneous Poisson point process (PPP) $\Phi_\mathcal{D}$ with density $\lambda_\mathcal{D}$, and each of which has a dedicated D2D receiver located at distance R in a random orientation. The D2D transmitters and their dedicated D2D receivers form a Poisson bipolar network [7]. The ALOHA channel access scheme is adopted for the D2D network, where each D2D transmitter becomes active independently. This event is denoted by $\mathcal{D}_1$ and it

Figure 2: (a) D2D transmitters, D2D receivers, friendly jammers, and the wardens; (b) Stackelberg game-based problem formulation with the wardens at the lower stage and the D2D network (i.e., D2D transmitters and jammers) at the upper stage.

occurs with probability $\mathbb{P}^{\mathcal{D}_1}$ [22]. Accordingly, each D2D transmitter will independently become inactive with probability $\mathbb{P}^{\mathcal{D}_0} \triangleq 1 - \mathbb{P}^{\mathcal{D}_1}$, where $\mathcal{D}_0$ denotes the corresponding inactive event. To analyze the performance of the D2D network, we condition on that there is a D2D receiver at the origin which is considered to be the typical D2D receiver, and its associating D2D transmitter is the typical D2D transmitter and denoted by D2D transmitter d. Following [23], we consider that the wardens are spatially distributed by following an independent homogeneous PPP $\Phi_{\mathcal{W}}$ with density $\lambda_{\mathcal{W}}$. Also, the spatial distribution of the jammers follows another independent homogeneous PPP $\Phi_{\mathcal{J}}$ with density $\lambda_{\mathcal{J}}$.

For D2D transmitter d, since the nearest warden, denoted by $w|_d$, is the most threatening warden, we focus on a scenario where D2D transmitter d defends against warden $w|_d$. Accordingly, we consider that warden $w|_d$ aims to detect, and once detect, wiretaps the transmission of D2D transmitter d. All the entities in the network are equipped with a single antenna and all the channels are assumed to experience Rayleigh fading with unit mean [7]. Note that similar to [24], the discussion in the rest of this paper is based on the performance of the representative network nodes (i.e., D2D transmitter d, the typical D2D receiver, and warden $w|_d$).

B. Performance Metrics

1) Successful Transmission Probability for the D2D Transmitter: The received signal power of the typical D2D receiver regarding the activation status of its associating D2D transmitter

(i.e., D2D transmitter d) is

$$
y_d = \begin{cases} p^{\mathrm{D}} g_d R^{-\alpha} + S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d, & \text{if } \mathcal{D}_1, \\ S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d, & \text{if } \mathcal{D}_0, \end{cases} \tag{1}
$$

where $S_d^{\mathcal{D}_1} = p^{\mathrm{D}} \sum_{d' \in \Phi_{\{\mathcal{D} \backslash \{d\} | d\}}} \mathbb{1}_{d'} g_{d'd} r_{d'd}^{-\alpha}$ and $S_d^{\mathcal{J}} = p^{\mathrm{J}} \sum_{j \in \Phi_{\{\mathcal{J} | d\}}} g_{jd} r_{jd}^{-\alpha}$ are the sum of the signal powers from D2D transmitter $d' \in \Phi_{\{\mathcal{D} \backslash \{d\} | d\}}$ and that from jammer $j \in \Phi_{\{\mathcal{J} | d\}}$ received at the typical D2D receiver, respectively, g_d is the channel between D2D transmitter d and the typical D2D receiver, and N_d is the noise power at the typical D2D receiver. Therein, $\Phi_{\{\mathcal{D} \backslash \{d\} | d\}}$ and $\Phi_{\{\mathcal{J} | d\}}$ are the point process (PP) of the D2D transmitters that excludes D2D transmitter d with the typical D2D receiver as the observation point and that of the jammers with the typical D2D receiver as the observation point, respectively, $\mathbb{1}_{d'}$ is the activation indicator of D2D transmitter $d' \in \Phi_{\{\mathcal{D} \backslash \{d\} | d\}}$ and equal to 1 if D2D transmitter d' is active and 0 otherwise, p^{D} and p^{J} are the D2D transmission power and jamming power, respectively, $g_{d'd}$ and $r_{d'd}$ are the channel and distance between D2D transmitter $d' \in \Phi_{\{\mathcal{D} \backslash \{d\} | d\}}$ and the typical D2D receiver, respectively, and g_{jd} and r_{jd} are the channel and distance between jammer $j \in \Phi_{\{\mathcal{J} | d\}}$ and the typical D2D receiver, respectively. Accordingly, the SINR at the typical D2D receiver regarding the activation status of its associating D2D transmitter (i.e., D2D transmitter d) is

$$
\mathrm{SINR}_d \left(p^{\mathrm{D}}, p^{\mathrm{J}} \right) = \begin{cases} \dfrac{p^{\mathrm{D}} g_d R^{-\alpha}}{S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d}, & \text{if } \mathcal{D}_1, \\ 0, & \text{if } \mathcal{D}_0. \end{cases} \tag{2}
$$

Denoting the SINR threshold at the D2D receiver by ξ^{D} and conditioned on the active status of D2D transmitter d (i.e., $\mathcal{D}_1$), we have the successful transmission probability for the D2D transmitter d as follows:

$$
\mathbb{P} \left[\mathrm{SINR}_d \left(p^{\mathrm{D}}, p^{\mathrm{J}} \right) > \xi^{\mathrm{D}} \big| \mathcal{D}_1 \right]. \tag{3}
$$

The detailed derivation of (3) is given in **Appendix A**. We validate the derivation of (3) by comparing the analytical results with the simulation results in Fig. 3. Note that the simulation results are generated by using Monte Carlo method using the parameter setting given in Table I. We assume the same parameter setting in the rest of this paper. It can be observed from Fig. 3 that our analytical results match with the simulation results.

2) Detection Error at the Warden: The wardens receive the signals transmitted from the D2D transmitters and jammers and aim to detect the D2D transmission independently. Accordingly,

Figure 3: Comparison between simulation results and analytical results on successful transmission probability.

for warden $w|_d \in \Phi_{\mathcal{W}}$, its received signal power regarding the activation status of its target D2D transmitter (i.e., D2D transmitter d) can be expressed as follows:

$$
y_{w|_d} = \begin{cases} p^{\mathrm{D}} g_{d\,w|_d} r_{d\,w|_d}^{-\alpha} + S_{w|_d}^{\mathcal{D}_1} + S_{w|_d}^{\mathcal{J}} + N_{w|_d}, & \text{if } \mathcal{D}_1, \\ S_{w|_d}^{\mathcal{D}_1} + S_{w|_d}^{\mathcal{J}} + N_{w|_d}, & \text{if } \mathcal{D}_0, \end{cases}
\tag{4}
$$

where $S_{w|_d}^{\mathcal{D}_1} = p^{\mathrm{D}} \sum_{d' \in \Phi_{\{\mathcal{D}\setminus\{d\}|w|_d\}}} \mathbb{1}_{d'} g_{d'\,w|_d} r_{d'\,w|_d}^{-\alpha}$ and $S_{w|_d}^{\mathcal{J}} = p^{\mathrm{J}} \sum_{j \in \Phi_{\{\mathcal{J}|w|_d\}}} g_{j\,w|_d} r_{j\,w|_d}^{-\alpha}$ are the sum of the signal powers from D2D transmitter $d' \in \Phi_{\{\mathcal{D}\setminus\{d\}|w|_d\}}$ and that from jammer $j \in \Phi_{\{\mathcal{J}|w|_d\}}$ received at warden $w|_d$, respectively, $g_{d\,w|_d}$ and $r_{d\,w|_d}$ are the channel and distance between D2D transmitter d and warden $w|_d$, respectively, and $N_{w|_d}$ is the additive noise at warden $w|_d$. Therein, $\Phi_{\{\mathcal{D}\setminus\{d\}|w|_d\}}$ and $\Phi_{\{\mathcal{J}|w|_d\}}$ are the PP of the D2D transmitters that excludes D2D transmitter d with warden $w|_d$ as the observation point and that of the jammers with warden $w|_d$ as the observation point, respectively, $g_{d'\,w|_d}$ and $r_{d'\,w|_d}$ are the channel and distance between D2D transmitter $d' \in \Phi_{\{\mathcal{D}\setminus\{d\}|w|_d\}}$ and warden $w|_d$, respectively, and $g_{j\,w|_d}$ and $r_{j\,w|_d}$ are the channel and distance between jammer $j \in \Phi_{\{\mathcal{J}|w|_d\}}$ and warden $w|_d$, respectively.

The warden uses a threshold-based detection rule to detect the transmission of its target D2D transmitter [14]. Specifically, the warden will assume that its target D2D transmitter is active if its received signal power is larger than a predetermined detection threshold, denoted by τ. Otherwise, it will assume that its target D2D transmitter is inactive. It will be a false alarm (FA) for warden $w|_d$ if its received signal power is larger than the predetermined detection

Figure 4: Comparison between the simulation results and analytical results on FA probability with (a) $p^{\text{J}} = 15\text{dBm}$ and (b) $p^{\text{D}} = 15\text{dBm}$.

threshold τ (i.e., $y_{w|_d} > \tau$) while D2D transmitter d is inactive (i.e., $\mathcal{D}_0$). On the other hand, it will be a miss detection (MD) for warden $w|_d$, if its received signal power is lower than the predetermined detection threshold τ (i.e., $y_{w|_d} < \tau$) while D2D transmitter d is active (i.e., $\mathcal{D}_1$).

The FA and MD probabilities for warden $w|_d \in \Phi_{\mathcal{W}}$ are defined as

$$\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) = \mathbb{P}\left[y_{w|_d} > \tau \,\middle|\, \mathcal{D}_0\right] = \mathbb{P}\left[S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} + N_{w|_d} > \tau\right] \tag{5}$$

and

$$\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) = \mathbb{P}\left[y_{w|_d} < \tau \,\middle|\, \mathcal{D}_1\right] = \mathbb{P}\left[p^{\text{D}} g_{dw|_d} r^{-\alpha}_{dw|_d} + S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} + N_{w|_d} < \tau\right], \tag{6}$$

respectively, and the specific expressions of which are derived in **Appendices C** and **D**, respectively. Again, we use simulation results to verify the derivations of $\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$ and $\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$.

As shown in Fig. 4(a), we first fix p^{J} to be 15dBm and vary the values of p^{D} and τ to compare the simulation results and analytical results on $\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$ and observe that these two results are consistent, which validates our derivation of $\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$. The same conclusion can be drawn based on the results in Fig. 4(b), which compares the simulation results and analytical results on $\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$ by fixing p^{D} to be 15dBm and varying the values of p^{J} and τ. Similar outcomes can be observed in Fig. 5, which validates our derivation of $\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$.

Figure 5: Comparison between the simulation results and analytical results on MD probability with (a) $p^{\mathrm{J}} = 15\mathrm{dBm}$ and (b) $p^{\mathrm{D}} = 15\mathrm{dBm}$.

3) Secrecy Outage Probability for the D2D Transmitter: According to the received signal power of warden $w|_d$ given in (4) and conditioned on the active status of its target D2D transmitter (i.e., D2D transmitter d), the secrecy outage probability for D2D transmitter d is

$$\mathbb{P}\left[\mathrm{SINR}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{W}} \,\big|\, \mathcal{D}_1\right], \tag{7}$$

where ξ^{W} is the SINR threshold at warden for successfully decoding the received signal and the expression of which is derived in **Appendix B**. The consistency between the analytical results and simulation results on the secrecy outage probability is shown in Fig. 6.

IV. PROBLEM STATEMENT AND GAME FORMULATION

We model the combat between wardens and the D2D network including D2D transmitters and the jammers in the framework of a two-stage Stackelberg game as shown in Fig. 2(b). Therein, the D2D network jointly decides the D2D transmission power and jamming power first, and the wardens make decision based on their received signal powers later. Hence, the wardens are the followers at the lower stage and the D2D network is the leader at the upper stage. The formulation of the two-stage Stackelberg game regarding the representative network nodes mentioned in Section III is a single-leader-single-follower game and defined as follows:

- At the lower stage, given the strategies of the D2D network (i.e., the D2D transmission power p^{D} and jamming power p^{J}) from the upper stage, warden $w|_d$ acts as a single follower

Figure 6: Comparison between simulation results and analytical results on secrecy outage probability.

and makes decision on the detection threshold τ in order to minimize its detection error [14] as follows:

$$\tau^* = \arg\min_{\tau} \mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) + \mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right), \tag{8}$$

where $\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$ and $\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)$ are defined in (5) and (6), respectively.

In the above, the reason that we omit $\mathbb{P}^{\mathcal{D}_1}$ and $\mathbb{P}^{\mathcal{D}_0}$ in the detection error can be explained as follows. First, as warden $w|_d$ is unaware of the activation status of its target D2D transmitter (i.e., $\mathcal{D}_1$ and $\mathcal{D}_0$), we relax its detection error probability as follows:

$$\begin{aligned}
&\mathbb{P}^{\mathcal{D}_0}\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) + \mathbb{P}^{\mathcal{D}_1}\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) \\
&\leq \max\left\{\mathbb{P}^{\mathcal{D}_0}, \mathbb{P}^{\mathcal{D}_1}\right\}\left[\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) + \mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right)\right],
\end{aligned} \tag{9}$$

where the second row of (9) is the upper bound of the detection error probability (i.e., the first row of (9)) and can be further simplified as the objective shown in (8). As such, the probabilistic terms related to the activation status of the D2D transmitter are avoided in the warden's objective. Also, this enables us to treat FA and MD equivalently so as to avoid any bias between them [25], [26].

- At the upper stage, D2D transmitter d together with the jammers work as a single leader and aim to maximize the network utility (i.e., (10a)) subject to the constraint on communication

covertness with respect to (w.r.t.) warden $w|_d$ (i.e., (10b)). This can be expressed as a nonlinear constrained optimization problem as follows:

$$\max_{p^{\mathrm{D}}, p^{\mathrm{J}}} w^{\mathrm{D}} \mathbb{P}\left[\mathrm{SINR}_d\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{D}} \middle| \mathcal{D}_1\right] \left\{\mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right)\right.$$

$$\left. + \left[1 - \mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right)\right]\left[1 - \mathbb{P}\left[\mathrm{SINR}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{W}} \middle| \mathcal{D}_1\right]\right]\right\} - \frac{\lambda_{\mathcal{J}}}{\lambda_{\mathcal{D}}} w^{\mathrm{J}} p^{\mathrm{J}} \tag{10a}$$

$$\text{s.t. } \mathbb{P}_{w|_d}^{\mathrm{FA}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right) + \mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right) \geq 1 - \varepsilon \tag{10b}$$

$$p^{\mathrm{D}} \in \left[\underline{p}^{\mathrm{D}}, \overline{p}^{\mathrm{D}}\right], \, p^{\mathrm{J}} \in \left[\underline{p}^{\mathrm{J}}, \overline{p}^{\mathrm{J}}\right], \tag{10c}$$

where $\underline{p}^{\mathrm{D}}$ ($\underline{p}^{\mathrm{J}}$) and $\overline{p}^{\mathrm{D}}$ ($\overline{p}^{\mathrm{J}}$) are the lower bound and upper bound of the D2D transmission (jamming) power, respectively. Therein, w^{D} is the reward for guaranteeing D2D link reliability (i.e., $\mathrm{SINR}_d\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{D}}$) conditioned on secure communication. The secure communication happens if and only if the malicious attempt of warden $w|_d$ is unsuccessful (i.e., miss detect the D2D transmission or secrecy outage is avoided if the D2D transmission is detected) when its target D2D transmitter (i.e., D2D transmitter d) is active. In this case, the secure communication excludes the FA, and the probability of which is defined as the sum of the probability that MD occurs at warden $w|_d$ (i.e., $\mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right)$) and the probability that secrecy outage is avoided for D2D transmitter d (i.e., $1 - \mathbb{P}\left[\mathrm{SINR}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{W}} \middle| \mathcal{D}_1\right]$) in the case that its transmission is detected by warden $w|_d$ (i.e., $1 - \mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right)$). Hence, the probability of secure communication is given by

$$\mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right) + \left[1 - \mathbb{P}_{w|_d}^{\mathrm{MD}}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^\star\right)\right]\left[1 - \mathbb{P}\left[\mathrm{SINR}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) > \xi^{\mathrm{W}} \middle| \mathcal{D}_1\right]\right]. \tag{11}$$

In the objective of the optimization problem (i.e., (10a)), the term $\frac{\lambda_{\mathcal{J}}}{\lambda_{\mathcal{D}}} w^{\mathrm{J}} p^{\mathrm{J}}$ is the cost incurred by the assistance from jammers with w^{J} being the cost of unit jamming power. Here, if the area of the region occupied by the large-scale D2D network is A, the expected number of jammers in this region is $\lambda_{\mathcal{W}} A$. In this case, the total jamming power cost is $\lambda_{\mathcal{W}} A w^{\mathrm{J}} p^{\mathrm{J}}$. Let D2D transmitters equally share the total jamming power cost, $\frac{\lambda_{\mathcal{W}} A w^{\mathrm{J}} p^{\mathrm{J}}}{\lambda_{\mathcal{D}} A} = \frac{\lambda_{\mathcal{J}}}{\lambda_{\mathcal{D}}} w^{\mathrm{J}} p^{\mathrm{J}}$ is therefore the jamming power cost for each D2D transmitter, where $\lambda_{\mathcal{D}} A$ is the expected number of D2D transmitters in this region. The inequality constraint (i.e., (10b)) puts a lower bound on the detection error of warden $w|_d$ in order to maintain certain communication covertness for the D2D transmission.

Figure 7: Illustration of the uniqueness of the solution to the lower-stage detection error minimization problem with $p^{\mathrm{D}} = 20\mathrm{dBm}$ and $p^{\mathrm{J}} = 10\mathrm{dBm}$.

V. EQUILIBRIUM ANALYSIS AND ALGORITHM DESIGN OF TWO-STAGE STACKELBERG GAME

In this section, we provide the equilibrium analysis for the two-stage Stackelberg game formulated in Section IV and develop an algorithm to search for the corresponding equilibrium. First, given the strategy from the upper stage, we analyze the lower-stage detection error minimization problem for warden $w|_d$ in Section V-A and choose a suitable algorithm to search for the optimal strategy of warden $w|_d$ as the best response of the lower stage. Taking into account the best response from the lower stage, we design a bi-level algorithm based on the SCA method to search for the optimal strategy of D2D transmitter d and the jammers at the upper stage, which together with the optimal strategy of warden $w|_d$ constitute the equilibrium of the two-stage Stackelberg game.

A. Solution to Lower-Stage Problem: Detection Error Minimization

For the lower-stage detection error minimization problem in (8), given any D2D transmission power and jamming power (i.e., p^{D} and p^{J}, respectively), the objective of warden $w|_d$ will be in a trough shape w.r.t. τ. In this case, we can apply the Rosenbrock method [27] to obtain the optimal strategy for warden $w|_d$. The reason for the trough shape of the warden's objective can

be explained as follows. First, we rewrite the objective function of warden $w|_d$ (i.e., detection error in (8)) as follows:

$$
\begin{aligned}
&\mathbb{P}^{\mathrm{FA}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right) + \mathbb{P}^{\mathrm{MD}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right) \\
&= \mathbb{P}\left[S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} + N_{w|_d} > \tau\right] + \mathbb{P}\left[p^{\mathrm{D}} g_{d\,w|_d} r^{-\alpha}_{d\,w|_d} + S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} + N_{w|_d} < \tau\right] \\
&= 1 - \int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\,\mathrm{d}t + \int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\, F_{p^{\mathrm{D}} g_{d\,w|_d} r^{-\alpha}_{d\,w|_d}}\left(\tau - N_{w|_d} - t\right)\,\mathrm{d}t.
\end{aligned}
\tag{12}
$$

In (12) and given any D2D transmission power and jamming power (i.e., p^{D} and p^{J}, respectively), as $F_{p^{\mathrm{D}} g_{d\,w|_d} r^{-\alpha}_{d\,w|_d}}(\cdot) \in [0,1]$, $\int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\,\mathrm{d}t$ will have a steeper increase w.r.t. τ than $\int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\, F_{p^{\mathrm{D}} g_{d\,w|_d} r^{-\alpha}_{d\,w|_d}}\left(\tau - N_{w|_d} - t\right)\,\mathrm{d}t$ when τ is small, which is demonstrated with the numerical results in Fig. 7, e.g., $\tau = 5$dBm. In this case, $\mathbb{P}^{\mathrm{FA}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right) + \mathbb{P}^{\mathrm{MD}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right)$ will decrease w.r.t. τ. Later, when τ further increases, $\int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\,\mathrm{d}t$ almost approaches its probabilistic upper bound, and its increasing speed becomes slower than that of $\int_0^{\tau - N_{w|_d}} f_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t)\, F_{p^{\mathrm{D}} g_{d\,w|_d} r^{-\alpha}_{d\,w|_d}}\left(\tau - N_{w|_d} - t\right)\,\mathrm{d}t$, which also can be observed from Fig. 7, e.g., $\tau = 25$dBm. In this case, $\mathbb{P}^{\mathrm{FA}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right) + \mathbb{P}^{\mathrm{MD}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right)$ will increase w.r.t. τ. Consequently, $\mathbb{P}^{\mathrm{FA}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right) + \mathbb{P}^{\mathrm{MD}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau\right)$ takes on a trough shape w.r.t. τ, which induces a unique optimal strategy (i.e., $\tau^{\star}$) that minimizes the detection error for warden $w|_d$. Such an optimal strategy is the best response of the lower stage corresponding to the given D2D transmission power and jamming power (i.e., p^{D} and p^{J}, respectively).

B. Solution to Upper-Stage Problem: Friendly Jamming-Assisted Covert Communication

For the friendly jamming-assisted covert communication problem at the upper stage, it is unwieldy to verify its convexity due to the multiple integrals in both the objective and constraint. In this case, we design a bi-level optimization algorithm based on the SCA method [28] and take into account the best response from the lower stage (i.e., $\tau^{\star}$ in (8)). In particular, let $U_0\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right)$ be the negative value of (10a) and $U_1\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) = -\mathbb{P}^{\mathrm{FA}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^{\star}\right) - \mathbb{P}^{\mathrm{MD}}_{w|_d}\left(p^{\mathrm{D}}, p^{\mathrm{J}}, \tau^{\star}\right) + 1 - \varepsilon$, we have the upper-stage friendly jamming-assisted covert communication problem (i.e., (10)) rewritten as follows:

$$
\begin{aligned}
\min_{p^{\mathrm{D}}, p^{\mathrm{J}}} \; & U_0\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) \\
\text{s.t.} \; & U_1\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) \leq 0 \\
& p^{\mathrm{D}} \in \left[\underline{p}^{\mathrm{D}}, \overline{p}^{\mathrm{D}}\right], \; p^{\mathrm{J}} \in \left[\underline{p}^{\mathrm{J}}, \overline{p}^{\mathrm{J}}\right].
\end{aligned}
\tag{13}
$$

According to [28], we can follow Algorithm 1 and switch to solve an approximation convex program of (13) (i.e., (15)) iteratively. The convergence of Algorithm 1 has been proven in [29]. (15)

is formulated by replacing $U_i\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right)$ for all $i \in \{0, 1\}$ of (13) with the surrogate function $\hat{U}_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$ for all $i \in \{0, 1\}$ that satisfies the following conditions [29]:

1) Consistency in function value: $\hat{U}_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) = U_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$;

2) Consistency in gradient: $\nabla_{p^{\mathrm{D}}}\hat{U}_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) = \nabla_{p^{\mathrm{D}}}U_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$ and $\nabla_{p^{\mathrm{J}}}\hat{U}_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) = \nabla_{p^{\mathrm{J}}}U_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$;

3) Convexity: $\hat{U}_i\left(p^{\mathrm{D}}, p^{\mathrm{J}} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$ is strongly convex w.r.t. $\left[p^{\mathrm{D}}, p^{\mathrm{J}}\right]$.

As stated in [29], the surrogate function $\hat{U}_i\left(p^{\mathrm{D}}, p^{\mathrm{J}} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)$ for all $i \in \{0,1\}$ in (15) can be designed by using the following gradient descent update:

$$
\begin{aligned}
\hat{U}_i\left(p^{\mathrm{D}}, p^{\mathrm{J}} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) =& U_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) + \nabla U_i\left(p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right)^{\top} \begin{pmatrix} p^{\mathrm{D}} - p^{\mathrm{D}\langle k\rangle} \\ p^{\mathrm{J}} - p^{\mathrm{J}\langle k\rangle} \end{pmatrix} \\
&+ \frac{\delta}{2}\left(p^{\mathrm{D}} - p^{\mathrm{D}\langle k\rangle}\right)^2 + \frac{\delta}{2}\left(p^{\mathrm{J}} - p^{\mathrm{J}\langle k\rangle}\right)^2.
\end{aligned}
\tag{14}
$$

Algorithm 1: Bi-level Optimization Algorithm

Data: Input $p^{\mathrm{D}\langle k\rangle}$ and $p^{\mathrm{J}\langle k\rangle}$.

1 Initialize $k = 0$ and set error tolerance ϵ;

2 **while** *error* $> \epsilon$ **do**

3   Solve the following optimization problem

$$
\begin{aligned}
&\min_{p^{\mathrm{D}}, p^{\mathrm{J}}} \hat{U}_0\left(p^{\mathrm{D}}, p^{\mathrm{J}} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) \\
&\text{s.t. } \hat{U}_1\left(p^{\mathrm{D}}, p^{\mathrm{J}} \middle| p^{\mathrm{D}\langle k\rangle}, p^{\mathrm{J}\langle k\rangle}\right) \leq 0 \\
&p^{\mathrm{D}} \in \left[\underline{p}^{\mathrm{D}}, \overline{p}^{\mathrm{D}}\right], \, p^{\mathrm{J}} \in \left[\underline{p}^{\mathrm{J}}, \overline{p}^{\mathrm{J}}\right]
\end{aligned}
\tag{15}
$$

    and obtain the solution $\tilde{p}^{\mathrm{D}}$ and $\tilde{p}^{\mathrm{J}}$;

4     $p^{\mathrm{D}\langle k+1\rangle} = p^{\mathrm{D}\langle k\rangle} + \gamma\left(\tilde{p}^{\mathrm{D}} - p^{\mathrm{D}\langle k\rangle}\right)$ and $p^{\mathrm{J}\langle k+1\rangle} = p^{\mathrm{J}\langle k\rangle} + \gamma\left(\tilde{p}^{\mathrm{J}} - p^{\mathrm{J}\langle k\rangle}\right)$;

5     $error = \left\|p^{\mathrm{D}\langle k+1\rangle} - p^{\mathrm{D}\langle k\rangle}\right\|^2 + \left\|p^{\mathrm{J}\langle k+1\rangle} - p^{\mathrm{J}\langle k\rangle}\right\|^2$;

6     $k + 1 \mapsto k$;

7 **end**

VI. PERFORMANCE EVALUATION

In this section, we provide the numerical results to evaluate the system performance. The parameter setting is given in Table I. First, we verify the optimality of the obtained strategy and the effectiveness of the friendly jamming in Fig. 8. Second, we demonstrate the advantages of the proposed friendly jamming-assisted covert communication by comparing it to the information-theoretical secrecy approach in Fig. 9. Third, the impact of the communication covertness

Figure 8: (a) Network utility and (b) detection error w.r.t. D2D transmission power and jamming power (i.e., p^{D} and p^{J}, respectively).

requirement and the warden's density on the network utility are illustrated in Fig. 10. Fourth, we evaluate the impact of the densities of the D2D transmitters and jammers on the network utility in Fig. 11. Finally, we present the impact of the SINR thresholds at the warden and the D2D transmitter on the network utility in Fig. 12.

A. *Effectiveness of Friendly Jamming*

Figure 8 depicts the network utility and detection error as functions of the D2D transmission power p^{D} and jamming power p^{J}. In Fig. 8(a), we can observe that the optimal strategy (i.e., optimal D2D transmission power and jamming power) can maximize the network utility within the feasible domain, where the boundary of the feasible domain is determined by the constraint on communication covertness (i.e., (10b)) as shown in Fig. 8(b). The optimal strategy is obtained by the developed bi-level optimization algorithm (i.e., Algorithm 1) and is consistent with that obtained by the exhaustive search method. The exhaustive search method searches for the optimal strategy via: 1) discretizing the domain of definition of the strategy (i.e., the D2D transmission power and jamming power), 2) enumerating all possible candidates for the strategy taking into account the corresponding best response from the lower stage to evaluate the network utility and detection error, and 3) finding the optimal strategy that jointly maximizes the network utility and satisfies the constraint on communication covertness. In this case, the optimality of the obtained equilibrium strategy is validated. Moreover, as shown in Fig. 8(b), the detection error

Figure 9: Friendly jamming-assisted covert communication versus information-theoretical secrecy approach.

can satisfy the constraint on communication covertness (i.e., (10b)) if and only if the jamming power $p^{\mathrm{J}} \gtrsim 12\mathrm{dBm}$[1]. The reason is that merely relying on the co-channel interference in the D2D network is insufficient and hence difficult to confuse and mislead the decision of the warden. In this case, without adequate assistance from the friendly jammers, the covert communication cannot be achieved.

B. Advantages of Friendly Jamming-Assisted Covert Communication

In Fig. 9, we compare our proposed friendly jamming-assisted covert communication and the information-theoretic secrecy approach in terms of the network utility and the secure communication probability (i.e., (11)). The problem of the information-theoretic secrecy approach is the problem in (10) with the removal of the constraint on communication covertness (i.e., (10b)). By such, the problem of the information-theoretic secrecy approach aims at the joint link reliability maximization and secrecy outage minimization. We can observe that the friendly jamming-assisted covert communication starts to take effect at $\frac{p^{\mathrm{J}}}{\bar{p}^{\mathrm{J}}} \approx -18\mathrm{dB}$, where the network utility becomes nonzero and also the optimal performance is achieved (i.e., the network utility is maximized at around 0.5 with a certain secure communication probability at around 0.97). In this case, the optimal performance of the friendly jamming-assisted covert communication at

---

[1]p^{J} is approximately larger than 12dBm.

Figure 10: Network utility w.r.t. the warden's density $\lambda_{\mathcal{W}}$ with varying communication covertness requirement ε.

$\frac{p^{\mathrm{J}}}{\bar{p}^{\mathrm{J}}} \approx -18\mathrm{dB}$ will be used as a "**Baseline**" for comparison in the following discussion. Regarding the information-theoretical secrecy approach, initially it can achieve a higher utility and a lower secure communication probability compared to the optimal performance of the friendly jamming-assisted covert communication. Later, if we further increase the jamming power, although the secure communication probability of the information-theoretical secrecy approach significantly increases, its network utility decreases dramatically. Until the jamming power approaches the upper bound, the secure communication probability of the information-theoretical secrecy approach is still lower than that of the friendly jamming-assisted covert communication at $\frac{p^{\mathrm{J}}}{\bar{p}^{\mathrm{J}}} \approx -18\mathrm{dB}$ (i.e., around 0.97) while achieving a negative utility, which is much lower than the utility of the friendly jamming-assisted covert communication at $\frac{p^{\mathrm{J}}}{\bar{p}^{\mathrm{J}}} \approx -18\mathrm{dB}$ (i.e., around 0.5). In this case, the friendly jamming-assisted covert communication significantly outperforms the information-theoretical secrecy approach, and its advantages are well demonstrated.

C. Impact of Warden's Density and Communication Covertness Requirement

We evaluate the impact of the warden's density $\lambda_{\mathcal{W}}$ and the communication covertness requirement ε, as given in the nonlinear inequality constraint (10b), on the network utility in Fig. 10. The network utility decreases w.r.t. the increase in the warden's density $\lambda_{\mathcal{W}}$. The reason is that when the warden's density becomes higher, the distance between the warden and

Figure 11: Network utility w.r.t. the jammers's density $\lambda_{\mathcal{J}}$ with varying D2D transmitters' density $\lambda_{\mathcal{D}}$.

its target D2D transmitter becomes shorter. In this case, the large-scale fading caused by the path loss weakens, the signal power received at the warden from its target D2D transmitter becomes stronger, which simultaneously reduces the difficulty in the transmission detection and increases the secrecy outage probability for D2D transmission once being detected. As a result, the network utility deteriorates accordingly. Additionally, the network utility decreases w.r.t. the warden's density $\lambda_{\mathcal{W}}$ with different rates corresponding to different communication covertness requirements (i.e., ε). This is due to the fact that when the value of ε decreases, the communication covertness requirement is tighter and it becomes more difficult to achieve covert communication, which together with the more threatening warden (i.e., higher warden densification) induce a faster decreasing rate in the network utility.

D. Impact of Densities of Friendly Jammers and D2D Transmitters

Figure 11 evaluates the impact of the densities of the friendly jammers and D2D transmitters on the network utility. An interesting result can be observed from Fig. 11 that the increase in the jammers' density improves instead of damaging the network utility. The reason is that although the increase in the jammers' density leads to stronger interference to the D2D communication and weakens the SINR at the D2D receiver, this interference can also enhance the communication covertness. Based on the results shown in Fig. 11, the gain obtained from the enhancement

Figure 12: Network utility w.r.t. the SINR threshold at warden ξ^{W} with varying SINR threshold at D2D receiver ξ^{D}.

of communication covertness overcompensates the loss incurred by the weakened SINR. This again demonstrates the benefit of using the friendly jammers in achieving covert communication. Another interesting result can be observed in Fig. 11 that the improvement due to the increase in jammers' density becomes diminishing when the D2D transmitters' density increases. The reason is that as the density of D2D transmitters increases, the co-channel interference due to the concurrent transmission becomes stronger, which can also distort the observation of the warden and mislead its decision. In this case, it is not necessary to have massive jammers as the assistants in achieving covert communication. Hence, the improvement due to the increase in jammers' density becomes less when the D2D transmitters' density increases.

E. Impact of SINR Thresholds at Warden and D2D Transmitter

We evaluate the impact of the SINR threshold at warden and D2D transmitter (i.e., ξ^{W} and ξ^{D}, respectively). As shown in Fig. 12, the network utility concavely increases w.r.t. ξ^{W}. This is due to the fact that to successfully decode the received signal is of more difficulty for the warden along with the increase in the SINR threshold ξ^{W}. In this case, the secure communication probability (i.e., (11)) will improve, which induces a higher network utility. The concave increasing trend in the network utility regarding the increase in ξ^{W} can be explained as follows. With the increase in ξ^{W}, the secrecy outage probability gradually approaches its

probabilistic lower bound, and its decreasing speed becomes slower than before. In this case, the increasing speed in the secure communication probability becomes slower, which induces a concave increasing trend in the network utility. Regarding the improvement in the network utility corresponding to the decrease in the SINR threshold at D2D transmitter ξ^{D}. This is due to that the decrease in ξ^{D} can improve the successful transmission probability for the D2D transmitter (i.e., (3)), which makes the objective of the D2D network easier in achieving higher value.

VII. CONCLUSION

We leverage both covert communication and friendly jamming to achieve physical-layer security in a large-scale D2D network in order to defend against the wardens. The objective is to jointly increase the detection error at the warden and decrease secrecy outage for the D2D transmitters in case transmissions are detected. The combat between the wardens and the D2D network (i.e., the D2D transmitters and the jammers) is modeled by a Stackelberg game with the wardens as the followers at the lower stage and the legitimate entities as the leaders at the upper stage. For the problem of the warden at the lower stage, we both analytically and numerically validate the existence and uniqueness of its optimal strategy, which is regarded as the best response from the lower stage. Given the best response from the lower stage, we develop a bi-level optimization algorithm based on SCA method to search for the optimal strategy of the D2D network, which together with that of the warden constitute the Stackelberg equilibrium. We have presented numerical results to evaluate the proposed approach and validate the optimality of the obtained equilibrium strategy. Moreover, we have demonstrated the advantages of the proposed friendly jamming-assisted covert communication by comparing it with the information-theoretic secrecy approach in terms of network utility and secure communication probability. Furthermore, we have evaluated the impact of warden's density and communication covertness requirement on system performance. Considering multiple antennas at both the D2D transmitters and receivers and also using the proposed approach to secure D2D communication in a D2D-underlaid cellular network will be future extensions of this work.

APPENDIX A

SINR DISTRIBUTION FOR D2D NETWORK

Based on (3) and conditioned on $\mathcal{D}_1$, the successful transmission probability for D2D transmitter d is

$$
\begin{aligned}
\mathbb{P}\left[\mathrm{SINR}_d\left(p^{\mathrm{D}}, p^{\mathrm{J}}\right) \geq \xi^{\mathrm{D}} \big| \mathcal{D}_1\right] &= \mathbb{P}\left[\frac{p^{\mathrm{D}} g_d R^{-\alpha}}{S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d} \geq \xi^{\mathrm{D}}\right] \\
&= \mathbb{P}\left[g_d \geq \frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}}\left(S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d\right)\right] \\
&\stackrel{(a)}{=} \mathbb{E}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}}\left(S_d^{\mathcal{D}_1} + S_d^{\mathcal{J}} + N_d\right)\right)\right] \\
&\stackrel{(b)}{=} \exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} N_d\right) \mathbb{E}_{S_d^{\mathcal{D}_1}}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} S_d^{\mathcal{D}_1}\right)\right] \mathbb{E}_{S_d^{\mathcal{J}}}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} S_d^{\mathcal{J}}\right)\right],
\end{aligned}
\tag{16}
$$

where (a) follows from the Rayleigh fading of g_d and (b) follows the independence between the random variables $S_d^{\mathcal{D}_1}$ and $S_d^{\mathcal{J}}$. The second term of the final row of (16) (i.e., $\mathbb{E}_{S_d^{\mathcal{D}_1}}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} S_d^{\mathcal{D}_1}\right)\right]$) is derived as follows:

$$
\begin{aligned}
\mathbb{E}_{S_d^{\mathcal{D}_1}}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} S_d^{\mathcal{D}_1}\right)\right] &= \mathbb{E}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}} p^{\mathrm{D}} \sum_{d' \in \Phi_{\{\mathcal{D} \setminus \{d\} | d\}}} \mathbb{1}_{d'} g_{d'd} r_{d'd}^{-\alpha}\right)\right] \\
&\stackrel{(a)}{=} \mathbb{E}_{\Phi_{\{\mathcal{D} \setminus \{d\} | d\}}}\left[\prod_{d' \in \Phi_{\{\mathcal{D} \setminus \{d\} | d\}}}\left(\frac{\mathbb{P}^{\mathcal{D}_1}}{R^\alpha \xi^{\mathrm{D}} r_{d'd}^{-\alpha} + 1} + 1 - \mathbb{P}^{\mathcal{D}_1}\right)\right] \\
&\stackrel{(b)}{=} \exp\left(-2\pi\lambda_{\mathcal{D}} \int_0^\infty \left[1 - \left(\frac{\mathbb{P}^{\mathcal{D}_1}}{R^\alpha \xi^{\mathrm{D}} r_{d'd}^{-\alpha} + 1} + 1 - \mathbb{P}^{\mathcal{D}_1}\right)\right] r_{d'd} \mathrm{d}r_{d'd}\right) \\
&= \exp\left(-2\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}} \int_0^\infty \frac{r}{1 + r^\alpha} \mathrm{d}r\right) \\
&= \exp\left(-2\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}} \int_0^\infty r \int_0^\infty \exp\left(-t\left(1 + r^\alpha\right)\right) \mathrm{d}t \mathrm{d}r\right) \\
&= \exp\left(-2\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}} \int_0^\infty \exp\left(-t\right) \int_0^\infty r \exp\left(-tr^\alpha\right) \mathrm{d}r \mathrm{d}t\right) \\
&= \exp\left(-2\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}} \int_0^\infty t^{-\frac{2}{\alpha}} \exp\left(-t\right) \mathrm{d}t \int_0^\infty \frac{1}{\alpha} \theta^{\frac{2}{\alpha}-1} \exp\left(-\theta\right) \mathrm{d}\theta\right) \\
&= \exp\left(-\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}} \int_0^\infty t^{-\frac{2}{\alpha}} \exp\left(-t\right) \mathrm{d}t \int_0^\infty \theta^{\frac{2}{\alpha}} \exp\left(-\theta\right) \mathrm{d}\theta\right) \\
&\stackrel{(c)}{=} \exp\left(-\frac{\pi\lambda_{\mathcal{D}} \mathbb{P}^{\mathcal{D}_1} R^2 \left(\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}\left(\frac{2}{\alpha}\right)}\right),
\end{aligned}
\tag{17}
$$

where (a) follows from the Rayleigh fading of $g_{d'd}$, (b) follows the probability generating functionals (PGFL) of PPP [30], and (c) is obtained according to the reflection formula in Pi function (i.e., $\Pi(z)\Pi(-z) = \frac{\pi z}{\sin(\pi z)} = \frac{1}{\mathrm{sinc}(z)}$ with $\Pi(z) = z\Gamma(z) = \int_0^\infty t^z \exp(-t)\,\mathrm{d}t$ being

the Pi function and $\Gamma\left(z\right)$ being the gamma function[2]). Similarly, the third term of the final row of (16) can be derived as follows:

$$
\begin{aligned}
\mathbb{E}_{S_d^{\mathcal{J}}}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}}S_d^{\mathcal{J}}\right)\right] &= \mathbb{E}\left[\exp\left(-\frac{R^\alpha \xi^{\mathrm{D}}}{p^{\mathrm{D}}}p^{\mathrm{J}}\sum_{j\in\Phi_{\{\mathcal{J}|d\}}}g_{jd}r_{jd}^{-\alpha}\right)\right] \\
&\overset{(17)}{=}\exp\left(-\frac{\pi\lambda_{\mathcal{J}}R^2\left(\frac{p^{\mathrm{J}}}{p^{\mathrm{D}}}\xi^{\mathrm{D}}\right)^{\frac{2}{\alpha}}}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\right).
\end{aligned}
\tag{18}
$$

APPENDIX B

SECRECY OUTAGE PROBABILITY FOR D2D NETWORK

According to (7) and conditioned on $\mathcal{D}_1$, the secrecy outage probability for D2D transmitter d is

$$
\begin{aligned}
\mathbb{P}\left[\mathrm{SINR}_{dw|_d}\left(p^{\mathrm{D}},p^{\mathrm{J}}\right)\geq\xi^{\mathrm{W}}\,\middle|\,\mathcal{D}_1\right] &= \mathbb{P}\left[\frac{p^{\mathrm{D}}g_{dw|_d}r_{dw|_d}^{-\alpha}}{S_{w|_d}^{\mathcal{D}_1}+S_{w|_d}^{\mathcal{J}}+N_{w|_d}}\geq\xi^{\mathrm{W}}\right] \\
&=\mathbb{P}\left[g_{dw|_d}\geq\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}\left(S_{w|_d}^{\mathcal{D}_1}+S_{w|_d}^{\mathcal{J}}+N_{w|_d}\right)\right] \\
&=\mathbb{E}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}\left(S_{w|_d}^{\mathcal{D}_1}+S_{w|_d}^{\mathcal{J}}+N_{w|_d}\right)\right)\right] \\
&=\mathbb{E}_{r_{dw|_d}}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}N_{w|_d}\right)\mathbb{E}_{S_{w|_d}^{\mathcal{D}_1}}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}S_{w|_d}^{\mathcal{D}_1}\right)\right]\right. \\
&\quad\left.\times\mathbb{E}_{S_{w|_d}^{\mathcal{J}}}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}S_{w|_d}^{\mathcal{J}}\right)\right]\right],
\end{aligned}
\tag{19}
$$

where the probability density function (PDF) of $r_{dw|_d}$ is

$$
f_{r_{dw|_d}}\left(r\right)=\exp\left(-\lambda_{\mathcal{W}}\pi r^2\right)2\lambda_{\mathcal{W}}\pi r,
\tag{20}
$$

$$
\mathbb{E}_{S_{w|_d}^{\mathcal{D}_1}}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}S_{w|_d}^{\mathcal{D}_1}\right)\right]\overset{(17)}{=}\exp\left(-\frac{\pi\lambda_{\mathcal{D}}\mathbb{P}^{\mathcal{D}_1}r_{dw|_d}^2\left(\xi^{\mathrm{W}}\right)^{\frac{2}{\alpha}}}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\right),
\tag{21}
$$

and

$$
\mathbb{E}_{S_{w|_d}^{\mathcal{J}}}\left[\exp\left(-\frac{\xi^{\mathrm{W}}r_{dw|_d}^{\alpha}}{p^{\mathrm{D}}}S_{w|_d}^{\mathcal{J}}\right)\right]\overset{(17)}{=}\exp\left(-\frac{\pi\lambda_{\mathcal{J}}r_{dw|_d}^2\left(\frac{p^{\mathrm{J}}}{p^{\mathrm{D}}}\xi^{\mathrm{W}}\right)^{\frac{2}{\alpha}}}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\right).
\tag{22}
$$

---

[2]Please refer to [31] and (43) in [24] for the definition and details.

APPENDIX C

FALSE ALARM PROBABILITY FOR WARDEN

According to (5) and conditioned on $\mathcal{D}_0$, the FA probability for warden $w|_d$ is

$$
\begin{aligned}
\mathbb{P}^{\text{FA}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) &= \mathbb{P}\left[y_{w|_d} > \tau \,\middle|\, \mathcal{D}_0\right] \\
&= \mathbb{P}\left[S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} > \tau - N_{w|_d}\right] = 1 - F_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}\left(\tau - N_{w|_d}\right).
\end{aligned}
\tag{23}
$$

The cumulative distribution function (CDF) of $S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}$ can be obtained as follows:

1) We first calculate the Laplace transform of $S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}$ as

$$
\begin{aligned}
\mathcal{L}\left\{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}\right\}(s) &= \mathbb{E}\left[\exp\left(-s\left(S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}\right)\right)\right] \\
&= \mathbb{E}\left[\exp\left(-sS^{\mathcal{D}_1}_{w|_d}\right)\right]\mathbb{E}\left[\exp\left(-sS^{\mathcal{J}}_{w|_d}\right)\right] \\
&\overset{(17)}{=} \exp\left(-\frac{\pi\lambda_{\mathcal{D}}\mathbb{P}^{\mathcal{D}_1}\left(sp^{\text{D}}\right)^{\frac{2}{\alpha}}}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\right)\exp\left(-\frac{\pi\lambda_{\mathcal{J}}\left(sp^{\text{J}}\right)^{\frac{2}{\alpha}}}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\right).
\end{aligned}
\tag{24}
$$

2) The CDF of $S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}$ is the inverse Laplace transform of $\mathcal{L}\left\{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}\right\}(s)$ and can be obtained by using the Bromwich inversion theorem in Chapter 2 of [32] as follows:

$$
\begin{aligned}
F_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(t) &= \mathcal{L}^{-1}\left\{\mathcal{L}\left\{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}\right\}(s)\right\}(t) \\
&= 1 - \frac{1}{\pi}\int_0^{\infty}\frac{1}{\theta}\sin\left(\nu\theta^{\frac{2}{\alpha}}\sin\left(\frac{2\pi}{\alpha}\right)\right)\exp\left(-\nu\theta^{\frac{2}{\alpha}}\cos\left(\frac{2\pi}{\alpha}\right) - t\theta\right)\mathrm{d}\theta,
\end{aligned}
\tag{25}
$$

where $\nu = \frac{\pi}{\operatorname{sinc}\left(\frac{2}{\alpha}\right)}\left(\lambda_{\mathcal{D}}\mathbb{P}^{\mathcal{D}_1}\left(p^{\text{D}}\right)^{\frac{2}{\alpha}} + \lambda_{\mathcal{J}}\left(p^{\text{J}}\right)^{\frac{2}{\alpha}}\right)$.

APPENDIX D

MISS DETECTION PROBABILITY FOR WARDEN

According to (6) and conditioned on $\mathcal{D}_1$, the MD probability for warden $w|_d$ is

$$
\begin{aligned}
\mathbb{P}^{\text{MD}}_{w|_d}\left(p^{\text{D}}, p^{\text{J}}, \tau\right) &= \mathbb{P}\left[y_{w|_d} < \tau \,\middle|\, \mathcal{D}_1\right] = \mathbb{P}\left[p^{\text{D}}g_{dw|_d}r^{-\alpha}_{dw|_d} + S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d} + N_{w|_d} < \tau\right] \\
&= \int_0^{\tau - N_{w|_d}} f_{p^{\text{D}}g_{dw|_d}r^{-\alpha}_{dw|_d}}(t)\, F_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}\left(\tau - N_{w|_d} - t\right)\mathrm{d}t,
\end{aligned}
\tag{26}
$$

where $F_{S^{\mathcal{D}_1}_{w|_d} + S^{\mathcal{J}}_{w|_d}}(\cdot)$ is given in (25) and

$$
\begin{aligned}
f_{p^{\text{D}}g_{dw|_d}r^{-\alpha}_{dw|_d}}(t) &= \frac{\mathrm{d}}{\mathrm{d}t}F_{p^{\text{D}}h_{dw|_d}r^{-\alpha}_{dw|_d}}(t) = \frac{\mathrm{d}}{\mathrm{d}t}\mathbb{P}\left[p^{\text{D}}h_{dw|_d}r^{-\alpha}_{dw|_d} \leq t\right] \\
&= \frac{\mathrm{d}}{\mathrm{d}t}\mathbb{P}\left[h_{dw|_d} \leq \frac{tr^{\alpha}_{dw|_d}}{p^{\text{D}}}\right] = \frac{\mathrm{d}}{\mathrm{d}t}\mathbb{E}_{r_{dw|_d}}\left[1 - \exp\left(-\frac{tr^{\alpha}_{dw|_d}}{p^{\text{D}}}\right)\right] \\
&= \int_0^{\infty} f_{r_{dw|_d}}(r)\exp\left(-\frac{tr^{\alpha}}{p^{\text{D}}}\right)\frac{r^{\alpha}}{p^{\text{D}}}\mathrm{d}r
\end{aligned}
\tag{27}
$$

with $f_{r_{dw|_d}}(r)$ given in (20).

REFERENCES

[1] J. Lyu, H.-M. Wang and K.-W. Huang, "Physical layer security in d2d underlay cellular networks with poisson cluster process," *IEEE Transactions on Communications*, vol. 68, no. 11, pp. 7123–7139, 2020.

[2] N. Deng and M. Haenggi, "The energy and rate meta distributions in wirelessly powered d2d networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 269–282, 2019.

[3] B. He, S. Yan, X. Zhou and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.

[4] S. Feng, X. Lu, S. Sun and D. Niyato, "Mean-field artificial noise assistance and uplink power control in covert iot systems," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2022.

[5] N. T. T. Van, N. C. Luong, H. T. Nguyen, F. Shaohan, D. Niyato and D. I. Kim, "Latency minimization in covert communication-enabled federated learning network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 13447–13452, 2021.

[6] S. Iellamo, R. Guiazon, M. Coupechoux and K.-K. Wong, "Securing iot uplink communications against eavesdropping," in *2018 3rd Cloudification of the Internet of Things (CIoT)*, 2018, pp. 1–8.

[7] M. Haenggi, *Stochastic geometry for wireless networks*, Cambridge University Press, 2012.

[8] K. Huang, "Spatial throughput of mobile ad hoc networks powered by energy harvesting," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7597–7612, 2013.

[9] N. Jiang, Y. Deng, X. Kang and A. Nallanathan, "Random access analysis for massive iot networks under a new spatio-temporal model: A stochastic geometry approach," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5788–5803, 2018.

[10] M. Forouzesh, P. Azmi, N. Mokari, K. K. Wong and D. Goeckel, "Information-theoretic security or covert communication," *arXiv preprint arXiv:1803.06608*, 2018.

[11] Z. Liu, J. Liu, Y. Zeng, J. Ma and Q. Huang, "On covert communication with interference uncertainty," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

[12] N. Van Huynh, N. Q. Hieu, N. H. Chu, D. N. Nguyen, D. T. Hoang and E. Dutkiewicz, "A novel covert communication method using ambient backscatter communications," *arXiv preprint arXiv:2201.06204*, 2022.

[13] D. Wang, P. Qi, N. Zhang, J. Si, Z. Li and N. Al-Dhahir, "Covert wireless communication with spectrum mask in internet of things networks," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8402–8415, 2021.

[14] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang and D. Niyato, "Intelligent reflecting surface enabled covert communications in wireless networks," *IEEE Network*, vol. 34, no. 5, pp. 148–155, 2020.

[15] B. A. Bash, D. Goeckel and D. Towsley, "Covert communication gains from adversary's ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[16] Z. Han, N. Marina, M. Debbah and A. Hjorungnes, "Improved wireless secrecy rate using distributed auction theory," in *2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks*, 2009, pp. 442–447.

[17] H. Zhang and L. Duan, "Going beyond secrecy rate via information jamming," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[18] H. Zhang, X. He and H. Dai, "Secure uav communication networks via friendly jamming and bandwidth allocation," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 894–899.

[19] Q. Wang, H.-N. Dai, H. Wang, G. Xu and A. K. Sangaiah, "Uav-enabled friendly jamming scheme to secure industrial internet of things," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 481–490, 2019.

[20] K.-W. Huang, H. Deng and H.-M. Wang, "Jamming aided covert communication with multiple receivers," *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4480–4494, 2021.

[21] X. Chen, W. Sun, C. Xing, N. Zhao, Y. Chen, F. R. Yu and A. Nallanathan, "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 5467–5480, 2021.

[22] M. Haenggi, "The meta distribution of the sir in poisson bipolar and cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2577–2589, 2016.

[23] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569–5585, 2016.

[24] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based d2d communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1867–1880, 2015.

[25] S. A. Mousavifar and C. Leung, "Trust-based energy efficient spectrum sensing in cognitive radio networks," in *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, 2013, pp. 1–6.

[26] Y. Liu, C. Zeng, H. Wang and G. Wei, "Energy detection threshold optimization for cooperative spectrum sensing," in *2010 2nd International Conference on Advanced Computer Control*, 2010, vol. 4, pp. 566–570.

[27] J. J. Leader, *Numerical analysis and scientific computation*, Chapman and Hall/CRC, 2004.

[28] G. Scutari, F. Facchinei, P. Song, D. P. Palomar and J.-S. Pang, "Decomposition by partial linearization: Parallel optimization of multi-agent systems," *IEEE Transactions on Signal Processing*, vol. 62, no. 3, pp. 641–656, 2014.

[29] D. P. Palomar, "Algorithms: Successive convex approximation (sca)," https://palomar.home.ece.ust.hk/ELEC5470_lectures/slides_algorithms_SCA.pdf, 2020.

[30] X. Lu, M. Salehi, M. Haenggi, E. Hossain and H. Jiang, "Stochastic geometry analysis of spatial-temporal performance in wireless networks: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 23, no. 4, pp. 2753–2801, 2021.

[31] J. Havil, "Gamma: exploring euler's constant," *The Australian Mathematical Society*, p. 250, 2003.

[32] A. M. Cohen, *Numerical methods for Laplace transform inversion*, vol. 5, Springer Science & Business Media, 2007.