Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks

Ranran Sun, Bin Yang, Yulong Shen, *Member, IEEE,* Xiaohong Jiang, *Senior Member, IEEE,* and Tarik Taleb *Senior Member, IEEE,*

***Abstract*—This paper investigates the covertness and secrecy of wireless communications in an untrusted relay-assisted device-to-device (D2D) network consisting of a full-duplex base station BS, a user equipment UE, an untrusted relay R. For the covertness, we attempt to prevent Willie from detecting the very existence of communications via D2D link from UE to R and cellular link from R to BS, while for the secrecy, we aim to prevent the untrusted relay from eavesdropping the UE message. To explore the fundamental covertness and secrecy in such a network, we first provide theoretical modelings for the average minimum detection error rate of Willie, and the average covert/secrecy rate from UE to BS under the underlay and overlay modes, respectively. Based on these models, we further explore the optimal power control at UE, R and BS to achieve the average covert rate maximization (MCR) for UE with the constraints of covertness and security requirements under the underlay mode. We also identify the optimal transmit powers and the optimal spectrum partition factor for MCR under the overlay mode. Finally, the exhaust searching method is adopted to solve the MCR problems, and extensive numerical and simulation results are presented to validate our theoretical analysis and to illustrate the average covert rate and secrecy rate of UE under various scenarios.**

***Index Terms*—Device-to-device (D2D), covertness, secrecy, performance model and optimization.**

I. Introduction

Device-to-device (D2D) networks, which enable nearby devices to communicate directly with each other bypassing base station (BS) over the licensed cellular spectrum, have been recognized as one of the key technology components in the fifth generation (5G) and beyond wireless communication systems [1]. Such networks have appealing and exciting features via exploiting direct communications, such as improving spectrum utilization, reducing latency, enlarging cellular coverage, increasing data rate, conserving energy consumption, etc. Therefore, the D2D networks bring many benefits for wide range of applications [2], like local services, emergency communications, and Internet of things (IoT) enhancement. Because of inherent broadcast and open characteristics of wireless channels [3], the D2D networks face serious security and privacy challenges, especially for the transmissions of financial, e-health and other sensitive information in various IoT applications.

The existing cryptographic technologies at upper layers of the protocol stack usually rely on complex mathematical computations to prevent information transmission from being leaked. However, these techniques also encounter significant challenges in some IoT scenarios, such as smart cities, with millions of low-power devices, which have very limited computing capabilities. In addition, the distribution and management of secret keys are also difficult in highly dynamic IoT scenarios. As an efficient supplement, physical layer security (PHY) technology has the potential to address these issues, which aims at exploiting the inherent randomness nature (e.g., noise, fading) of wireless channels to provide transmission security at the physical layer even to low-power and highly mobile devices. It has been regarded as a promising technology for achieving covertness and security of wireless communications [4]–[7]. For the covertness, its goal is to hide the existing of wireless communications from a warden, i.e., covert communications, which can provide enhanced privacy protection for supporting some critical applications, like unauthorized positioning and tracking in vehicular/military networks [8]–[11]. As for the security, it aims to protect the communication content (e.g., private financial and health data) from eavesdropping, i.e., secure communications [12], [13].

Although many recent works have focused on the covert/secrecy communications in D2D networks [7], [14]–[32] (Please see Related Works of Section II for detail), these works address the issues of covertness and security separately. For supporting various IoT applications with both covertness and security requirements, the joint requirements need to be addressed simultaneously in the upcoming sixth-generation (6G) networks [33], [34]. Some initial works have been devoted to the study of the joint covertness and security in wireless systems [35], [36]. In [35], the authors investigate the average rate maximization with the constraints of covertness and security requirements in a single-input multi-

This work was supported in part by the National Key Research and Development Program of China under Grant No. 2018YFE0207600; in part by the Natural Science Basic Research Program of Shaanxi under Grant No. 2019JC-17; in part by the National Natural Science Foundation of China under Grant No. 61972308 and 61962033; in part by the Academy of Finland Projects: 6Genesis under Grant No. 318927 and IDEA-MILL under Grant No. 335936; in part by the Natural Science Project of Anhui/ChuZhou University under Grant No. KJ2021ZD0128 ,KJ2021ZD0129,and 2022XJZD12. (Corresponding authors: Bin Yang, Yulong Shen)

R. Sun is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China (e-mail: srr_2013@163.com).

B. Yang is with the School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, China (e-mail: yangbinchi@gmail.com).

Y. Shen is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China (e-mail: ylshen@mail.xidian.edu.cn).

X. Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan (e-mail: jiang@fun.ac.jp).

T. Taleb is with the Faculty of Information Technology and Electrical Engineering, University of Oulu, Oulu 90570, Finland, and also with the Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea (e-mail: tarik.taleb@oulu.fi).

output (SIMO) system consisting of a source, two destinations, an eavesdropper and a warden, where these two destinations require covert and secure communications, respectively. The authors in [36] further explore the secrecy rate maximization subject to the covertness requirement in an untrusted relaying system, where one/multiple wardens attempt to detect the presence of communications via the source-relay-destination link, while the untrusted relay also serves as an eavesdropper aiming to wiretap the source information. In addition, for the untrusted relaying networks, the works in [37], [38] are devoted to the studies of secure communications in such networks. The authors in [37] propose a light-weight jamming resistant scheme for achieving the secure communications in the networks, where a destination sends jamming signal to prevent an untrusted relay from intercepting message transmitted by a source, and an adversary jammer also emits noise to interfere with the destination. The authors in [38] further propose a joint relay selection and power allocation method for optimizing the security performance in the untrusted millimeter wave relay networks, where a destination and a source can also send jamming signal to prevent the reception of untrusted relays and eavesdroppers.

Note that these results in [35]–[38] cannot be applied to the D2D networks due to the following two reasons. On one hand, thanks to the intrinsic features (e.g., spectrum sharing) of such networks, each user equipment (UE) can work over either the underlay mode reusing the spectrum resource of a cellular link or the overlay mode using the dedicated spectrum resource orthogonal to that of the cellular link. Moreover, under the overlay mode, how to allocate system spectrum resources to each D2D link and cellular link also significantly affects the covertness and security of such networks. The interference management is another critical issue in D2D networks, which needs to be carefully considered in D2D networks. On the other hand, the works in [37], [38] focus on the secure communications. Different from these works, this paper investigates the joint covert and secure communications in D2D networks under the underlay and overlay modes, respectively. The interference management and spectrum partition are carefully addressed by identifying optimal power control and spectrum partition factor. In this paper, our objective is to hide the transmission of a UE from being detected by a warden and to prevent the transmitted message from being intercepted by an untrusted relay simultaneously.

It is notable that there are fundamental differences between this paper and the work of [36] in terms of communication mode of relay R, spectrum allocation, and cooperative jamming scheme. For this paper, R works over full-duplex communication mode, the spectrum allocation is carefully explored between the D2D and cellular links under the underlay and overly modes, and BS can serve as a friendly jammer. For the work [36], R works over half-duplex communication mode, the spectrum allocation is neglected, and a source and its destination can serve as friendly jammers.

The main contributions of this paper are summarized as follows.

- We consider a D2D network consisting of a full-duplex base station BS, a warden Willie, a relay R and a user equipment UE. The relay R is untrusted such that it also tries to intercept message from UE in the process of forwarding message to BS. To achieve covertness and security, the full-duplex BS emits jamming signal to confuse both R and Willie. In the network, we derive some basic results in terms of optimal detection threshold, minimum detection error rate and its average value under the underlay and overlay modes.
- Under the underlay mode, we provide theoretical modelings for the average covert/secrecy rate from UE to BS. Based on these models, we further explore the optimal power control at UE, R and BS to achieve the average covert rate maximization (MCR) for UE with the constraints of covertness and secure requirements.
- Under the overlay mode, we also model the average covert/secrecy rate. We further jointly optimize transmit powers and spectrum partition factor to achieve MCR with the constraint of covertness and security requirements.
- Extensive numerical/simulation results are presented to validate our theoretical analysis and also to illustrate the impacts of some system parameters on the average covert/secrecy rate under the underlay and overlay modes.

The remaining of this paper is organized as follows. The related works is present in the Section II. Section III introduces the system model. Section IV presents the detection performance at Willie. Section V and Section VI provide the theoretical modeling and optimization of system performances under the underlay mode and the overlay mode, respectively. The extensive numerical results are illustrated in Section VII. Finally, Section VIII concludes this paper.

II. Related Works

Available works mainly conduct the studies of either covert communications or secure communications in D2D networks.

A. Covert Communications in D2D Networks

Previous works on covert communications mainly focus on a special type of D2D networks [25]–[32], where there is no networking infrastructure (e.g., BS) and also covert communications operate over unlicensed spectrum bands (e.g., 2.4 GHz). Recently, some research efforts have been devoted to the investigation of covert communications in D2D networks sharing with the support of BS, where covert communications utilize the spectrum bands for cellular networks [20]–[24]. The work in [20] proposes a power control scheme to guarantee the covert communications of a D2D pair, and evaluates the covert rate performance. In [21], the joint design of spectrum allocation and power control is proposed for maximizing the covert rate of a D2D pair, while the work in [22] investigates the user trust degree evaluation and spectrum allocation for achieving covert rate maximization. The authors in [23] propose two artificial noise injection schemes to confuse the detection of wardens and the maximum covert rate is further explored under each scheme. The work in [24] explores the covert rate maximization in the scenario with a safety area, where the D2D transmitters are distributed such that wardens cannot detect the existence of D2D transmissions.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3201021

B. Secure Communications in D2D Networks

By now, there have been many studies about secure communications in D2D networks [7], [14]–[19], [39]–[42]. The work in [7] proposes a joint guard zone and threshold-based access control scheme for D2D users aiming to maximize the secrecy rate of cellular link. In [16], a closed-form expression is derived for the probability of achieving non-zero secrecy rate of the cellular link under the power power control of D2D transmitters. The authors in [14] derive the probabilities of secrecy outage and non-zero secrecy rate of cellular link as well as the outage probability of D2D link. In [15], stochastic geometry is used to model the D2D networks, where the connection probability and secrecy probability are studied, while the work in [17] first uses Poisson cluster processes (PCPs) and Poisson point process (PPP) to model the locations of all nodes, and then derives coverage outage probability and secrecy outage probability. The work in [18] adopts reconfigurable intelligent surfaces to improve the data transmission rate of D2D link and the secrecy rate of cellular link. The authors in [19] further propose a mode selection scheme allowing D2D pairs to select one between the underlay and overlay modes, and a spectrum partition scheme partitioning spectrum between cellular and D2D links. The secrecy rate and secrecy outage probability are further explored under these two schemes. The work in [39] proposes a lightweight secure and resilient transmission scheme for D2D communications in the presence of a hostile jammer. Under this scheme, the randomness of the wireless channel is utilized to generate frequency hopping sequences for enhancing secrecy of D2D communications against the active jamming.

Considering the secure communications between unmanned aerial vehicles (UAV) and ground user equipments (GUs), the work in [40] jointly optimizes the communication resources, computation resources, and UAV trajectories to maximize the minimum secure computing capacity for the dual UAV-assisted mobile edge computing (MEC) systems against ground eavesdroppers. To against a flying eavesdropper, the work in [41] maximizes the minimum secure calculation capacity maximization by a joint optimization on the resources and trajectory of UAV. Based on [41], the work in [42] proposes a secure communication scheme aiming to maximize the average security computation capacity and also guarantee the minimum secure computation requirement for each GU.

Different from all above works, our paper investigates the covertness and secrecy of wireless communications, which are two typical PHY technologies. Thus, the active jamming can also confuse the detection of the warden and the interception of the untrusted relay for achieving covert and secure communications, through a flexible control of the transmit powers at UE and BS. This indicates that our proposed method is also robust against active jamming in D2D communications.

III. System Model

A. System Model and Spectrum Sharing

As illustrated in Fig. 1, we consider a D2D-enabled uplink cellular network consisting of a base station BS, a user equipment UE, an untrusted relay R and a warden Willie. We assume that the direct link from UE to BS is unavailable. UE desires to send confidential message covertly to BS through the relay R, and R receives and forwards the message simultaneously using the amplify-and-forward protocol and full-duplex (FD) mode. However, R is untrusted such that it also attempts to intercept the message. We consider an intelligent Willie such that it knows the signal is relayed by R. Willie utilizes its received signal from both UE and R to detect the existence of the transmission from UE to BS. BS also works over the FD mode receiving signal from R and emitting jamming signal to confuse the detection of Willie simultaneously. R is equipped with a pair of transmission and reception antennas, and each of UE and Willie has a single antenna.

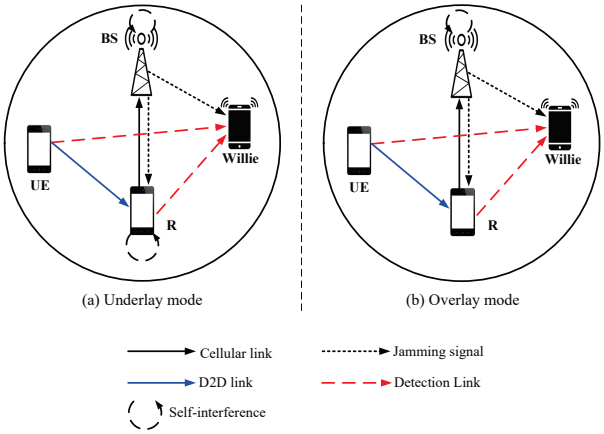

Fig. 1: System Model.

We consider two types of spectrum resource sharing modes, namely underlay and overlay modes. Under the underlay mode, the D2D link from UE to R reuses the spectrum resource of cellular link from R to BS, while under the overlay mode, the system spectrum resource is partitioned into two orthogonal parts: a fraction β of the spectrum resource allocated to the D2D link and the remaining fraction $1-\beta$ allocated to the cellular link.

B. Channel Model

We consider a time-slotted quasi-static Rayleigh fading channel model in our network, where each channel remains constant for one slot while changes randomly and independently from one slot to another. The channel coefficient from node i to node j is denoted as h_{ij}, which is modeled as a complex zero mean Gaussian random variable with variance λ_{ij}. Thus, the corresponding channel gain $|h_{ij}|^2$ is an exponentially distribution random variable with mean λ_{ij}, and the probability density function (pdf) of $|h_{ij}|^2$ is given by $f_{|h_{ij}|^2}(x) = \frac{1}{\lambda_{ij}} \exp(-\frac{x}{\lambda_{ij}})$. Here, $i \in \{s, r, b\}$ and $j \in \{r, b, w\}$ where s, r, b, w denote UE, R, BS and Willie, respectively. Consider channel reciprocity, we assume the channel gain from BS to R is the same as that from R to BS, i.e., $|h_{br}|^2 = |h_{rb}|^2$. To estimate the channel, UE and R send pilot signals to relay and BS, respectively. Thus, the channel coefficient h_{br} is known to UE by using the feedback

from BS. Simultaneously, Willie can also receive the pilot signals from UE and R, and thus Willie can perfectly estimate its channels from UE, R and BS, i.e., Willie knows the channel coefficients h_{sw}, h_{rw} and h_{bw} perfectly. Since Willie does not give any feedback, and thus we assume that UE can only know the statistical channel state information (CSI) of h_{sw}, h_{rw} and h_{bw} by long-term observations. Since R and BS work over the FD mode, Fig. 1 also illustrates the self-interference at BS and R under the underlay and overlay modes.

This paper considers a centralized network scenario, where BS can allocate a total power to different devices (i.e. UE and R), and flexibly control the transmit power of each device for achieving covertness. Only through allocating power to R, it is willing to help UE forward data. The total power for transmitting confidential message is P which is divided into two parts: a fraction ρ of total power allocated to UE and the remaining fraction allocated to R, the total power constraint on two different devices is also explore in previous woks, like [36], [43], [44]. To confuse the detection of Willie, BS emits jamming signal with power P_j following a continuous uniform distribution random variable over the interval $[0, P_j^{\max}]$, where $P_j^{\max}$ is no more than an upper bound Ω. The probability density function (PDF) of P_j is given by

$$f_{P_j}(x) = \begin{cases} \frac{1}{P_j^{\max}}, & 0 \le P_j \le P_j^{\max}. \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

We consider that Willie knows the distribution of P_j by long-term observations of received signals. However, it does not know the realizations of P_j in each time slot. In addition, the additive white Gaussian noises at R, BS, and Willie are denoted by n_r, n_b and n_w with variance σ_r^2, variance σ_b^2 and σ_w^2, respectively. We assume that the total available bandwidth of system spectrum resource is W MHz. Without loss of generality, W is set to one throughout this paper.

C. Detection at Willie

From the perspective of Willie, he has to make a decision on whether the transmission between UE and BS occurs or not according to his observations. Therefore, Willie conducts a binary hypothesis testing on his observations. The null hypothesis H_0 denotes that UE doesn't transmit covert message to BS and the alternative hypothesis H_1 denotes that UE performs the covert transmission. Under the assumption, we use $y_w(i)$ to denote the i-th received signal at Willie, and then we have

$$y_w(i) = \begin{cases} \sqrt{P_j} h_{bw} x_j(i) + n_w(i), & \mathrm{H}_0. \\ \Delta + \sqrt{P_j} h_{bw} x_j(i) + n_w(i), & \mathrm{H}_1. \end{cases} \tag{2}$$

where $\Delta = \sqrt{\rho P} h_{sw} x_s(i) + \sqrt{(1-\rho)P} h_{rw} x_r(i)$, $x_s(i)$, $x_r(i)$ and $x_j(i)$ denote the i-th signal transmitted by UE, R and BS, respectively, and $\mathbb{E}[|x_s(i)|^2] = 1$, $\mathbb{E}[|x_r(i)|^2] = 1$ and $\mathbb{E}[|x_j(i)|^2] = 1$, where $\mathbb{E}[\cdot]$ is the expectation operator. $i = 1, 2, \ldots, n$ is the index of the received signals at Willie in a time slot and n is assumed to be infinity, i.e., $n \to \infty$. To conduct the detection, Willie adopts an optimal power detector [45], which is given by

$$Y_W \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \tag{3}$$

where Y_W is the average received power at each time slot at Willie and $Y_W = \frac{1}{n} \sum_{i=1}^{n} |y_w(i)|^2$. τ is the detection threshold for the power detector adopted at Willie. If the average received power at Willie is lower than τ, Willie decides that UE does not transmit covert signal. Otherwise, it decides that UE transmits covert signal. D_0 and D_1 denote the decisions in favor of H_0 and H_1, respectively. Consider the infinity number of received signals at Willie, we have

$$Y_W = \begin{cases} P_j |h_{bw}|^2 + \sigma_w^2, & \mathrm{H}_0. \\ \rho P |h_{sw}|^2 + (1-\rho) P |h_{rw}|^2 + P_j |h_{bw}|^2 + \sigma_w^2, & \mathrm{H}_1. \end{cases} \tag{4}$$

Willie has to decide whether the transmission between UE and BS occurs, we define two types of errors: false alarm and missed detection. The former one is the event that Willie makes a decision D_1 in favor of H_1 while H_0 is true. The probability of the event occurring P_{FA} is $P_{FA} = \mathcal{P}\{D_1|\mathrm{H}_0\}$. The latter is defined as the event that Willie makes a decision D_0 in favor of H_0 while H_1 is true. It occurring probability P_{MD} is $P_{MD} = \mathcal{P}\{D_0|\mathrm{H}_1\}$. We use ξ to denote the detection error rate at Willie and then formulate $\xi = P_{FA} + P_{MD}$. From the perspective of UE, UE does not know the value of τ, and thus we consider the worst case that Willie has the minimum detection error rate ξ. Once if the minimum detection error rate ξ can satisfy the covertness requirement, the process of covert communications cannot be detected by Willie.

D. Instantaneous covert and security rates

We now model the instantaneous covert rate from UE to BS as well as the instantaneous security rate.

1) Underlay Mode: As illustrated in Fig. 1(a), under the underlay mode, the D2D link from UE to R reuses the spectrum resource of the cellular link from R to BS, and thus the D2D and cellular links will interfere with each other, while the transmission from UE cannot interfere with the cellular link due to the fact that the direct link from UE to BS is unavailable. We use $y_r(i)$ and $y_b(i)$ to denote the i-th received signals at R and BS, respectively. Then,

$$y_r(i) = \sqrt{\rho P} h_{sr} x_s(i) + \sqrt{P_j} h_{br} x_j(i) + x_{si}^{(r)}(i) + n_r(i), \tag{5}$$

$$y_b(i) = \sqrt{(1-\rho)P} h_{rb} x_r(i) + x_{si}^{(b)}(i) + n_b(i), \tag{6}$$

where $x_{si}^{(r)}(i)$ and $x_{si}^{(b)}(i)$ are the self-interference at R and BS. Using self-interference cancellation technology, the self-interference at R and BS can be reduced to a level close to the noise, which can be modeled as a complex Gaussian random variable, i.e., $x_{si}^{(r)} \sim \mathcal{CN}(0, \varphi\sigma_r^2)$, $x_{si}^{(b)} \sim \mathcal{CN}(0, \phi\sigma_b^2)$, where φ and ϕ are the residual self-interference ratio at R and BS [23], and σ_r^2 and σ_b^2 are variances of the additive white Gaussian noise at R and BS. $\varphi = 0$ and $\phi = 0$ indicate that the self-interference can be fully canceled. Since R adopts the amplify-and-forward protocol, $x_r(i) = G y_r(i)$, and G is the amplify factor given by $G = \frac{1}{\sqrt{\rho P |h_{sr}|^2 + P_j |h_{br}|^2 + (\varphi+1)\sigma_r^2}}$. Note that the jamming signal is also amplified by R and then

transmitted to BS, and thus the received signal at BS can be rewritten as

$$y_b(i) = \sqrt{(1-\rho)P}h_{rb}G\sqrt{\rho P}h_{sr}x_s(i) + x_{si}^{(b)}(i) + n_b(i) + \sqrt{(1-\rho)P}h_{rb}G(x_{si}^{(r)}(i) + n_r(i)). \quad (7)$$

The instantaneous signal-to-interference-plus-noise ratio (SINR) SINR_r and SINR_b at R and BS are given by

$$\text{SINR}_r = \frac{\rho P|h_{sr}|^2}{P_j|h_{br}|^2 + (\varphi+1)\sigma_r^2}, \quad (8)$$

and

$$\text{SINR}_b = \frac{\rho P|h_{sr}|^2(1-\rho)P|h_{rb}|^2}{(\rho P|h_{sr}|^2 + P_j|h_{br}|^2)(\phi+1)\sigma_b^2 + \alpha(\varphi+1)}, \quad (9)$$

where $\alpha = \sigma_r^2((1-\rho)P|h_{rb}|^2 + (\phi+1)\sigma_b^2)$. The instantaneous covert rate R_C^u from UE to BS under the underlay mode is given by

$$\text{R}_C^u = \log_2(1 + \text{SINR}_b). \quad (10)$$

The untrusted R also tries to eavesdrop the transmission content when it receives the message from UE, the instantaneous secrecy rate R_S^u of UE can be determined as

$$\text{R}_S^u = [\log_2(1 + \text{SINR}_b) - \log_2(1 + \text{SINR}_r)]^+, \quad (11)$$

where $[x]^+ = \max\{x, 0\}$. According to [46], we know that if the relay adopts the decode-and-forward protocol, the SINR_b is equal to the minimum one between the SINR of the first hop and that of the second hop. Note that in this paper, we consider the relay adopts the amplify-and-forward protocol to amplify and retransmit the signal from UE. This means that the SINR_b can be greater than the SINR_r in the first hop, and thus the secrecy rate defined in (11) can be a positive number, which has been verified in previous works [36]–[38].

2) Overlay Mode: As shown in Fig. 1(b), there is no self-interference at R under the overlay mode. To ensure covert and secure transmission, BS emits jamming signal with power P_j over the total system spectrum. Thus, the received signals at R and BS are given by

$$y_r(i) = \sqrt{\rho P}h_{sr}x_s(i) + \sqrt{P_j}h_{br}x_j(i) + n_r(i), \quad (12)$$

and

$$y_b(i) = \sqrt{(1-\rho)P}h_{rb}x_r(i) + x_{si}^{(b)}(i) + n_b(i) = \sqrt{(1-\rho)P}h_{rb}G'\sqrt{\rho P}h_{sr}x_s(i) + x_{si}^{(b)}(i) + n_b(i) + \sqrt{(1-\rho)P}h_{rb}G'n_r(i), \quad (13)$$

where G' is the amplify factor of R under the overlay mode given by $G' = \frac{1}{\sqrt{\rho P|h_{sr}|^2 + P_j|h_{br}|^2 + \sigma_r^2}}$. Thus, the SINRs at R and BS can be determined as

$$\text{SINR}_r = \frac{\rho P|h_{sr}|^2}{P_j|h_{br}|^2 + \sigma_r^2}, \quad (14)$$

and

$$\text{SINR}_b = \frac{(1-\rho)P|h_{rb}|^2\rho P|h_{sr}|^2}{(\rho P|h_{sr}|^2 + P_j|h_{br}|^2)(\phi+1)\sigma_b^2 + \alpha}. \quad (15)$$

Under the overlay mode, the instantaneous covert rate R_C^o from UE to BS is expressed as

$$\text{R}_C^o = (1-\beta)\log_2(1 + \text{SINR}_b). \quad (16)$$

The instantaneous secrecy rate R_S^o from UE to BS can be modeled as

$$\text{R}_S^o = [(1-\beta)\log_2(1 + \text{SINR}_b) - \beta\log_2(1 + \text{SINR}_r)]^+. \quad (17)$$

Similar to the secrecy rate defined in (11), we know that the secrecy rate defined in (17) can also be a positive number. Regarding the spectrum partition factor β, it could lead to a secrecy rate of zero. Thus, this paper optimizes the setting of β to maximize the average covert rate subject to the constraint of a positive secrecy rate in the optimization problem of (46). As shown in Fig. 10, the simulation result illustrates that the positive secrecy rate is achievable.

E. Performance Metric

We define average covert rate and average security rate as two performance metrics in our study.

We use $\overline{\text{R}}_C^i$ to denote the average covert rate, which is defined as the desirable covert rate without the transmission outage subject to the constraint of covertness requirement. Then, $\overline{\text{R}}_C^i$ can be expressed as

$$\overline{\text{R}}_C^i = r_c(1 - P_{co}^i), \quad (18)$$

where $i \in \{u, o\}$, u and o represent the underlay mode and overlay mode, respectively, r_c is the predetermined covert rate from UE to BS, and P_{co}^i denotes the transmission outage probability under the mode i.

The average secrecy rate $\overline{\text{R}}_S^i$ is defined as the expected value of the instantaneous secrecy rate, which is written as

$$\overline{\text{R}}_S^i = \mathbb{E}[\text{R}_S^i]. \quad (19)$$

IV. Detection Performance

This section investigates the detection performance at Willie in terms of optimal detection threshold, minimum detection error rate and its average value.

We use τ^* and ξ^* to denote the optimal detection threshold and the corresponding minimal detection error rate, which are given in the following theorem.

Theorem 1. *The optimal detection threshold at Willie is determined as*

$$\tau^* \in \begin{cases} [\delta_1, \delta_2], & \delta_1 \le \delta_2 \\ [\delta_2, \delta_1], & \delta_1 > \delta_2 \end{cases} \quad (20)$$

and the corresponding minimum detection error rate is given by

$$\xi^* = \begin{cases} 0, & \delta_1 \le \delta_2 \\ 1 - \frac{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}, & \delta_1 > \delta_2 \end{cases} \quad (21)$$

where $\delta_1 = P_j^{\max}|h_{bw}|^2 + \sigma_w^2$, $\delta_2 = \rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2 + \sigma_w^2$.

Proof. We first determine detection error rate ξ. According to the definitions of P_{FA} and P_{MD} in Section III-C, we have

$$\begin{aligned} P_{FA} &= \mathcal{P}\{Y_W > \tau | \mathrm{H}_0\} \\ &= \mathcal{P}\{P_j |h_{bw}|^2 + \sigma_w^2 > \tau\} \\ &= \mathcal{P}\{P_j > \frac{\tau - \sigma_w^2}{|h_{bw}|^2}\} \\ &\overset{(a)}{=} \begin{cases} 1, & \tau < \sigma_w^2 \\ 1 - \frac{\tau - \sigma_w^2}{P_j^{\max}|h_{bw}|^2}, & \sigma_w^2 \le \tau < \delta_1 \\ 0, & \tau \ge \delta_1 \end{cases} \end{aligned} \tag{22}$$

We further determine the probability of missed detection, which is given by

$$\begin{aligned} P_{MD} &= \mathcal{P}\{Y_W < \tau | H_1\} \\ &= \mathcal{P}\{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2 + P_j|h_{bw}|^2 + \sigma_w^2 < \tau\} \\ &= \mathcal{P}\{P_j < \frac{\tau - \sigma_w^2 - \rho P|h_{sw}|^2 - (1-\rho)P|h_{rw}|^2}{|h_{bw}|^2}\} \\ &\overset{(b)}{=} \begin{cases} 0, & \tau \le \delta_2 \\ \frac{\tau - \delta_2}{P_j^{\max}|h_{bw}|^2}, & \delta_2 < \tau \le P_j^{\max}|h_{bw}|^2 + \delta_2 \\ 1, & \tau > P_j^{\max}|h_{bw}|^2 + \delta_2 \end{cases} \end{aligned} \tag{23}$$

where (a) and (b) are obtained since P_j follows the uniform distribution given in (1).

Then, we can obtain the detection error rate ξ according to the basic results of P_{FA} and P_{MD} under the following two cases: $\delta_1 \le \delta_2$ and $\delta_1 > \delta_2$.

When $\delta_1 \le \delta_2$, ξ can be determined as

$$\begin{aligned} \xi &= P_{FA} + P_{MD} \\ &= \begin{cases} 1, & \tau < \sigma_w^2 \\ 1 - \frac{\tau - \sigma_w^2}{P_j^{\max}|h_{bw}|^2}, & \sigma_w^2 \le \tau < \delta_1 \\ 0, & \delta_1 \le \tau \le \delta_2 \\ \frac{\tau - \delta_2}{P_j^{\max}|h_{bw}|^2}, & \delta_2 < \tau < P_j^{\max}|h_{bw}|^2 + \delta_2 \\ 1, & \tau \ge P_j^{\max}|h_{bw}|^2 + \delta_2 \end{cases} \end{aligned} \tag{24}$$

We can observe from (24) that the minimum detection error rate $\xi^* = 0$ where the optimal detection threshold $\tau^* \in [\delta_1, \delta_2]$.

When $\delta_1 > \delta_2$, ξ is given by

$$\begin{aligned} \xi &= P_{FA} + P_{MD} \\ &= \begin{cases} 1, & \tau < \sigma_w^2 \\ 1 - \frac{\tau - \sigma_w^2}{P_j^{\max}|h_{bw}|^2}, & \sigma_w^2 \le \tau \le \delta_2 \\ 1 - \frac{\delta_2 - \sigma_w^2}{P_j^{\max}|h_{bw}|^2}, & \delta_2 < \tau < \delta_1 \\ \frac{\tau - \delta_2}{P_j^{\max}|h_{bw}|^2}, & \delta_1 \le \tau < P_j^{\max}|h_{bw}|^2 + \delta_2 \\ 1, & \tau \ge P_j^{\max}|h_{bw}|^2 + \delta_2 \end{cases} \end{aligned} \tag{25}$$

Following (25), we have $\frac{\partial \xi}{\partial \tau} < 0$ when $\sigma_w^2 \le \tau \le \delta_2$, which indicates that ξ decreases as τ increases. When $\tau \in [\delta_1, P_j^{\max}|h_{bw}|^2 + \delta_2)$, we have $\frac{\partial \xi}{\partial \tau} > 0$ which means that ξ increases with the increase of τ. Therefore, the minimum detection error rate $\xi^* = 1 - \frac{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}$, and the optimal detection threshold $\tau^* \in [\delta_2, \delta_1]$. □

It is notable that the detection error rate at Willie under the underlay and overlay modes has the same expression. This means that there is no effect of the selection between these two modes on the detection performance of Willie.

A. Average Minimum Detection Error Rate

We use $\overline{\xi}^*$ to denote the average minimum detection error rate at Willie, which is the expected value of ξ^* with respect to $|h_{bw}|^2$, $|h_{rw}|^2$ and $|h_{sw}|^2$. $\overline{\xi}^*$ is given in the following theorem.

Theorem 2. *The average minimum detection error rate $\overline{\xi}^*$ at Willie is determined as*

$$\begin{aligned} \overline{\xi}^* &= \frac{(P_j^{\max}\lambda_{bw})^2}{(P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw})(P_j^{\max}\lambda_{bw} + \rho P\lambda_{sw})} \\ &\times \Big[1 - \frac{\rho P\lambda_{sw} + (1-\rho)P\lambda_{rw}}{P_j^{\max}\lambda_{bw}} \ln \frac{P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw}}{(1-\rho)P\lambda_{rw}} \\ &+ \frac{(1-\rho)P\lambda_{rw}}{P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw}} \\ &+ \frac{P_j^{\max}\lambda_{bw}\rho P\lambda_{sw}}{(P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw})(P_j^{\max}\lambda_{bw} + \rho P\lambda_{sw})} \\ &+ \frac{\rho^2 P\lambda_{sw}\lambda_{sw}}{P_j^{\max}\lambda_{bw}(\rho\lambda_{sw} - (1-\rho)\lambda_{rw})} \ln \frac{\rho\lambda_{sw}(P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw})}{(1-\rho)\lambda_{rw}(P_j^{\max}\lambda_{bw} + \rho P\lambda_{sw})}\Big] \end{aligned} \tag{26}$$

Proof. Based on (21), we know that ξ^* is a function with respect to random variables $|h_{bw}|^2$, $|h_{rw}|^2$ and $|h_{sw}|^2$, each of which follows exponential distribution. The average minimum detection error rate is the expected value of ξ^*, i.e., $\overline{\xi}^* = \mathbb{E}[\xi^*]$. Therefore, we have

$$\begin{aligned} \overline{\xi}^* &= \mathbb{E}[\xi^*] \\ &= \mathcal{P}\{\delta_1 \le \delta_2\}\mathbb{E}[0|\delta_1 \le \delta_2] \\ &+ \mathcal{P}\{\delta_1 > \delta_2\}\mathbb{E}[1 - \frac{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}|\delta_1 > \delta_2] \\ &= \mathcal{P}\{\delta_1 > \delta_2\}\mathbb{E}[1 - \frac{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}|\delta_1 > \delta_2] \end{aligned} \tag{27}$$

Since

$$\begin{aligned} &\mathcal{P}\{\delta_1 > \delta_2\} = \mathcal{P}\left\{|h_{bw}|^2 > \frac{\rho P|h_{sw}|^2 + (1-\rho)P|h_{rw}|^2}{P_j^{\max}}\right\} \\ &= \int_0^\infty \int_0^\infty \int_{\frac{\rho P y + (1-\rho)Pz}{P_j^{\max}}}^\infty f_{|h_{bw}|^2}(x) f_{|h_{sw}|^2}(y) \\ &\times f_{|h_{rw}|^2}(z) dx dy dz \\ &= \frac{(P_j^{\max}\lambda_{bw})^2}{(P_j^{\max}\lambda_{bw} + (1-\rho)P\lambda_{rw})(P_j^{\max}\lambda_{bw} + \rho P\lambda_{sw})}, \end{aligned} \tag{28}$$

and

$$\begin{aligned}
&\mathbb{E}[1-\frac{\rho P|h_{sw}|^2+(1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}|\delta_1>\delta_2]\\
&=1-\mathbb{E}[\frac{\rho P|h_{sw}|^2+(1-\rho)P|h_{rw}|^2}{P_j^{\max}|h_{bw}|^2}|\delta_1>\delta_2]\\
&=1-\int_0^\infty\int_0^\infty\int_{\frac{\rho Py+(1-\rho)Pz}{P_j^{\max}}}^\infty \frac{\rho Py+(1-\rho)Pz}{P_j^{\max}x}f_{|h_{bw}|^2}(x)\\
&\times f_{|h_{sw}|^2}(y)f_{|h_{rw}|^2}(z)dxdydz\\
&=1-\frac{\rho P\lambda_{sw}+(1-\rho)P\lambda_{rw}}{P_j^{\max}\lambda_{bw}}\ln\frac{P_j^{\max}\lambda_{bw}+(1-\rho)P\lambda_{rw}}{(1-\rho)P\lambda_{rw}}\\
&+\frac{(1-\rho)P\lambda_{rw}}{P_j^{\max}\lambda_{bw}+(1-\rho)P\lambda_{rw}}\\
&+\frac{P_j^{\max}\lambda_{bw}\rho P\lambda_{sw}}{(P_j^{\max}\lambda_{bw}+(1-\rho)P\lambda_{rw})(P_j^{\max}\lambda_{bw}+\rho P\lambda_{sw})}\\
&+\frac{\rho^2P\lambda_{sw}\lambda_{sw}}{P_j^{\max}\lambda_{bw}(\rho\lambda_{sw}-(1-\rho)\lambda_{rw})}\\
&\times\ln\frac{\rho\lambda_{sw}(P_j^{\max}\lambda_{bw}+(1-\rho)P\lambda_{rw})}{(1-\rho)\lambda_{rw}(P_j^{\max}\lambda_{bw}+\rho P\lambda_{sw})}
\end{aligned}\tag{29}$$

Substituting (28) and (29) into (27), (26) follows. □

V. Covert and Secrecy Performance under the Underlay Mode

In this section, we first model the average covert rate and the average secrecy rate under the underlay mode, and then explore the maximum average covert rate by optimizing the transmission powers at UE and BS.

A. Average Covert Rate Modeling

According to the definition of average covert rate in Section III-E, the average covert rate under the underlay mode is given by

$$\overline{\mathrm{R}}_C^u=r_c(1-P_{co}^u).\tag{30}$$

To determine $\overline{\mathrm{R}}_C^u$, we first need to derive the transmission outage probability P_{co}^u from UE to BS. It is defined as the probability that the instantaneous covert rate of UE falls below the predetermined covert rate r_c, and then we have

$$P_{co}^u=\mathcal{P}\{\mathrm{R}_C^u<r_c\}.\tag{31}$$

We give the expression of the transmission outage probability P_{co}^u in the following theorem.

Theorem 3. *Under the underlay mode, if* $(1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2\le 0$, $P_{co}^u=1$, *i.e. occurring outage for the cellular communication from R to BS. Otherwise,* P_{co}^u *is determined as*

$$\begin{aligned}
P_{co}^u=1-&\frac{\exp(-\theta\mu\alpha(\varphi+1))}{\theta\mu P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2}\\
&\times[1-\exp(-\theta\mu P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2)],
\end{aligned}\tag{32}$$

where $\theta=2^{r_c}-1$, *and* $\mu=\frac{1}{\rho P\lambda_{sr}[(1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2]}$.

Proof. According to the definition of P_{co}^u in (31), we have

$$\begin{aligned}
P_{co}^u&=\mathcal{P}\{\log_2(1+\mathrm{SINR}_b)<r_c\}\\
&=\mathcal{P}\{\mathrm{SINR}_b<\theta\}\\
&=\mathcal{P}\{\rho P|h_{sr}|^2((1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2)\\
&<\theta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha(\varphi+1))\},
\end{aligned}\tag{33}$$

if $(1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2\le 0$, $P_{co}^u=1$. Otherwise, (33) can be rewritten as

$$\begin{aligned}
P_{co}^u&=\mathcal{P}\left\{|h_{sr}|^2<\frac{\theta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha(\varphi+1))}{\rho P((1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2)}\right\}\\
&=\int_0^{P_j^{\max}}\int_0^{\frac{\theta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha(\varphi+1))}{\rho P((1-\rho)P|h_{rb}|^2-\theta(\phi+1)\sigma_b^2)}}f_{|h_{sr}|^2}(x)f_{P_j}(y)dxdy,
\end{aligned}\tag{34}$$

where $f_{P_j}(y)$ is the PDF of P_j given in (1). Solving (34), (32) follows. □

By substituting (32) into (30), we can obtain the expression of average covert rate under the underlay mode.

B. Average Secrecy Rate Modeling

We use $\overline{\mathrm{R}}_S^u$ to denote the average secrecy rate from UE to BS. According to its definition, we have

$$\overline{\mathrm{R}}_S^u=\mathbb{E}[\mathrm{R}_S^u].\tag{35}$$

We obtain $\overline{\mathrm{R}}_S^u$ in the following theorem.

Theorem 4. *Under the underlay mode, the average secrecy rate* $\overline{R}_S^u$ *from UE to BS can be determined as*

$$\begin{aligned}
\overline{R}_S^u=&\frac{\lambda_{sr}}{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2\ln 2}\left\{a\left[\Phi(\frac{(P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2+(\varphi+1)\alpha)}{a\lambda_{sr}})\right.\right.\\
&\left.-\Phi(\frac{(\varphi+1)\alpha}{a\lambda_{sr}})\right]-(a+b)\left[\Phi(\frac{(P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2+(\varphi+1)\alpha)}{(a+b)\lambda_{sr}})\right.\\
&\left.\left.-\Phi(\frac{(\varphi+1)\alpha}{(a+b)\lambda_{sr}})\right]+b\ln(1+\frac{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2}{(\varphi+1)\alpha})\right\}\\
&-\frac{\rho P\lambda_{sr}}{P_j^{\max}|h_{br}|^2\ln 2}\left[\Phi(\frac{(\varphi+1)\sigma_r^2}{\rho P\lambda_{sr}})-\Phi(\frac{P_j^{\max}|h_{br}|^2+(\varphi+1)\sigma_r^2}{\rho P\lambda_{sr}})\right.\\
&\left.+\ln(1+\frac{P_j^{\max}|h_{br}|^2}{(\varphi+1)\sigma_r^2})\right],
\end{aligned}\tag{36}$$

where $\Phi(x)=\exp(x)\mathrm{Ei}(-x)$, $\mathrm{Ei}(-x)=-\int_x^\infty e^{-t}t^{-1}dt$, $a=\rho P(\phi+1)\sigma_b^2$, *and* $b=\rho(1-\rho)P^2|h_{rb}|^2$.

Proof. According to (35), we have

$$\begin{aligned}
\overline{\mathrm{R}}_S^u&=\mathbb{E}[\log_2(1+\mathrm{SINR}_b)-\log_2(1+\mathrm{SINR}_r)]\\
&=\mathbb{E}[\log_2(1+\mathrm{SINR}_b)]-\mathbb{E}[\log_2(1+\mathrm{SINR}_r)]\\
&=\int_0^{P_j^{\max}}\int_0^\infty\log_2(1+\mathrm{SINR}_b)f_{|h_{sr}|^2}(x)f_{P_j}(P_j)dxdP_j\\
&-\int_0^{P_j^{\max}}\int_0^\infty\log_2(1+\mathrm{SINR}_r)f_{|h_{sr}|^2}(x)f_{P_j}(P_j)dxdP_j,
\end{aligned}\tag{37}$$

where $f_{|h_{sr}|^2}(x)$ and $f_{P_j}(P_j)$ are the PDFs of $|h_{sr}|^2$ and P_j given in Section III-B, respectively. Solving (37), we can obtain (36). □

C. Covert Performance Optimization

Our objective is to maximize the average covert rate from UE to BS. This can be formulated as the following optimization problem.

$$\max_{\rho, P_j^{\max}} \quad \overline{\mathrm{R}}_C^u, \tag{38a}$$

$$\text{s.t.} \quad \overline{\xi}^* \geq 1-\varepsilon, \tag{38b}$$

$$\overline{\mathrm{R}}_S^u \geq r_s, \tag{38c}$$

$$0 \leq \rho \leq 1, \tag{38d}$$

$$0 \leq P_j^{\max} \leq \Omega, \tag{38e}$$

where the constraint (38b) represents the covertness requirement, the constraint (38c) ensures the average secrecy rate is not less than a given threshold r_s, the constraint (38d) represents the range of the power allocation fraction at UE, and the constraint (38e) represents the range of the maximum transmit power of jamming signal. Based on the complex expressions of $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$, it is generally difficult to obtain the closed-form solutions of the optimization problem. Thus, a two-dimensional search over $(\rho, P_j^{\max})$ is used to find the optimal ρ and $P_j^{\max}$.

VI. Covert and Secrecy Performance under the Overlay Mode

In this section, we first model the average covert rate and the average secrecy rate under the overlay mode,and then explore the maximum average covert rate by optimizing the transmission powers at UE and BS.

A. Average Covert Rate Modeling

Under the overlay mode, the average covert rate can be formulated as

$$\overline{\mathrm{R}}_C^o = r_c(1-P_{co}^o). \tag{39}$$

To obtain the exact expression of $\overline{\mathrm{R}}_C^o$, we first need to determine the covert transmission outage probability P_{co}^o under the overlay mode, which is given in the following theorem.

Theorem 5. *Under the overlay mode, the covert transmission outage P_{co}^o from UE to BS can be determined as*

$$P_{co}^o = 1 - \frac{\exp(-\omega\delta\alpha)}{\omega\delta P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2} \times [1-\exp\left(-\omega\delta P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2\right)], \tag{40}$$

if $(1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2>0$. Otherwise, $P_{co}^o=1$. Here, $\delta = 2^{\frac{r_c}{1-\beta}}-1$, and $\omega = \frac{1}{\rho P\lambda_{sr}[(1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2]}$.

Proof. Under the overlay mode, P_{co}^o is formulated as

$$\begin{aligned} P_{co}^o &= \mathcal{P}\{\mathrm{R}_C^o < r_c\} \\ &= \mathcal{P}\{(1-\beta)\log_2(1+\mathrm{SINR}_b) < r_c\} \\ &= \mathcal{P}\{\mathrm{SINR}_b < \delta\} \\ &= \mathcal{P}\{\rho P|h_{sr}|^2((1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2) \\ &< \delta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha)\}, \end{aligned} \tag{41}$$

we can see from (41) that if $(1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2 \leq 0$, $P_{co}^o=1$. Otherwise, (41) is further rewritten as

$$\begin{aligned} P_{co}^o &= \mathcal{P}\{|h_{sr}|^2 < \frac{\delta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha)}{\rho P((1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2)}\} \\ &= \int_0^{P_j^{\max}} \int_0^{\frac{\delta(P_j|h_{br}|^2(\phi+1)\sigma_b^2+\alpha)}{\rho P((1-\rho)P|h_{rb}|^2-\delta(\phi+1)\sigma_b^2)}} f_{|h_{sr}|^2}(x) f_{P_j}(P_j) dx dP_j. \end{aligned} \tag{42}$$

Solving (42), (40) follows. □

Substituting (40) in (39), we obtain the average covert rate $\overline{\mathrm{R}}_C^o$ under the overlay mode.

B. Average Secrecy Rate Modeling

We use $\overline{\mathrm{R}}_S^o$ to denote the average secrecy rate under the overlay mode. According to the definition of the average secrecy rate, we have

$$\overline{\mathrm{R}}_S^o = \mathbb{E}[\mathrm{R}_S^o], \tag{43}$$

which is given in the following theorem.

Theorem 6. *The average secrecy rate from UE to BS under the overlay mode is determined as*

$$\begin{aligned} \overline{R}_S^o = &\frac{(1-\beta)\lambda_{sr}}{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2\ln 2}\Bigg\{a\left[\Phi(\frac{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2+\alpha}{a\lambda_{sr}}) - \Phi(\frac{\alpha}{a\lambda_{sr}})\right] - (a+b)\left[\Phi(\frac{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2+\alpha}{(a+b)\lambda_{sr}}) \right. \\ &\left. - \Phi(\frac{\alpha}{(a+b)\lambda_{sr}})\right] + b\ln(1+\frac{P_j^{\max}|h_{br}|^2(\phi+1)\sigma_b^2}{\alpha})\Bigg\} \\ &- \frac{\beta\rho P\lambda_{sr}}{P_j^{\max}|h_{br}|^2\ln 2}\left[\Phi(\frac{\sigma_r^2}{\rho P\lambda_{sr}}) - \Phi(\frac{P_j^{\max}|h_{br}|^2+\sigma_r^2}{\rho P\lambda_{sr}}) + \ln(1+\frac{P_j^{\max}|h_{br}|^2}{\sigma_r^2})\right], \end{aligned} \tag{44}$$

where a, b and $\Phi(x)$ are given in the Theorem 4.

Proof. According to the definition of average secrecy rate given in (43), we have

$$\begin{aligned} \overline{\mathrm{R}}_S^o &= \mathbb{E}[(1-\beta)\log_2(1+\mathrm{SINR}_b) - \beta\log_2(1+\mathrm{SINR}_r)] \\ &= \mathbb{E}[(1-\beta)\log_2(1+\mathrm{SINR}_b)] - \mathbb{E}[\beta\log_2(1+\mathrm{SINR}_r)] \\ &= (1-\beta)\mathbb{E}[\log_2(1+\mathrm{SINR}_b)] - \beta\mathbb{E}[\log_2(1+\mathrm{SINR}_r)] \\ &= (1-\beta)\int_0^{P_j^{\max}}\int_0^{\infty}\log_2(1+\mathrm{SINR}_b) f_{|h_{sr}|^2}(x) f_{P_j}(P_j) dx dP_j \\ &- \beta\int_0^{P_j^{\max}}\int_0^{\infty}\log_2(1+\mathrm{SINR}_r) f_{|h_{sr}|^2}(x) f_{P_j}(P_j) dx dP_j. \end{aligned} \tag{45}$$

Solving (45), we can obtain the result in (44). □

C. Covert Performance Optimization

Our objective is to maximize the average covert rate, which can be formulated as the following optimization problem.

$$\max_{\rho,\beta,P_j^{\max}} \quad \overline{\mathrm{R}}_C^o, \tag{46a}$$

$$\text{s.t} \quad \overline{\xi}^* \geq 1-\varepsilon, \tag{46b}$$

$$\overline{\mathrm{R}}_S^o \geq r_s, \tag{46c}$$

$$0 \leq \rho \leq 1, \tag{46d}$$

$$0 \leq \beta \leq 1, \tag{46e}$$

$$0 \leq P_j^{\max} \leq \Omega. \tag{46f}$$

where the constraint (46b) represents the covertness requirement, the constraint (46c) represents the average secrecy rate under the overlay mode is not less than a given threshold r_s, and the constraints (46d), (46e) and (46f) represent the ranges of power allocation fraction, spectrum sharing fraction and the maximum transmit power of jamming signal, respectively. Because of the complex expressions of $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$, it is usually difficult to obtain the closed-form solutions of the optimization problem. Thus, we use a multi-dimensional search over $(\rho, \beta, P_j^{\max})$ to solve it.

Note that the optimization problems of (38) and (46) involve the following performance metrics: average covert rates, average minimum detection error rate and average secrecy rates. The expressions of these metrics are very complex such that it is difficult to obtain the closed-form solutions of the optimization problems. However, there are only two variables and three variables in (38) and (46), respectively. This leads to a small solution space for each optimization problem. Thus, we can also rapidly find a better solution in the small solution space through multi-dimensional searching.

VII. Numerical Results

In this section, we present the extensive numerical results to explore the impacts of some key system parameters on the covert and secrecy performances under the underlay mode and the overlay mode. To validate our theoretical covert and secrecy models, we also conduct comparisons between the simulation and theory results. We set the following parameters as $r_c = 0.5$ Mbits/s, $r_s = 0.1$ Mbits/s, $\tau = 0.8$, $|h_{rb}|^2 = 1$, $\phi = 10$, $\varphi = 10^3$, $\lambda_{sr} = 1$, $\lambda_{sw} = 1$, $\lambda_{rw} = 1$, $\lambda_{bw} = 1$, $\sigma_r^2 = 10^{-4}$ W, $\sigma_b^2 = 10^{-4}$ W, and $\sigma_w^2 = 10^{-4}$ W, unless otherwise specified.

A. Average Covert Rate and Average Secrecy Rate under the Underlay Mode

We investigate the impacts of power allocation fraction ρ on the average covert rate $\overline{\mathrm{R}}_C^u$ and the average secrecy rate $\overline{\mathrm{R}}_S^u$ under the underlay mode for the settings of $P_j^{\max} = 30$ W, $\varepsilon = 0.1$, and $P = \{0.3, 0.7\}$ W. We summarize in Figs. 2 and 3 how $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$ vary with ρ, respectively. As shown in these two figures, the theory results well match with the simulation ones, which indicates that our theoretical models can accurately predict $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$.

We can see from Fig. 2 that as ρ increases, the average covert rate $\overline{\mathrm{R}}_C^u$ first increases and then decreases. This is due

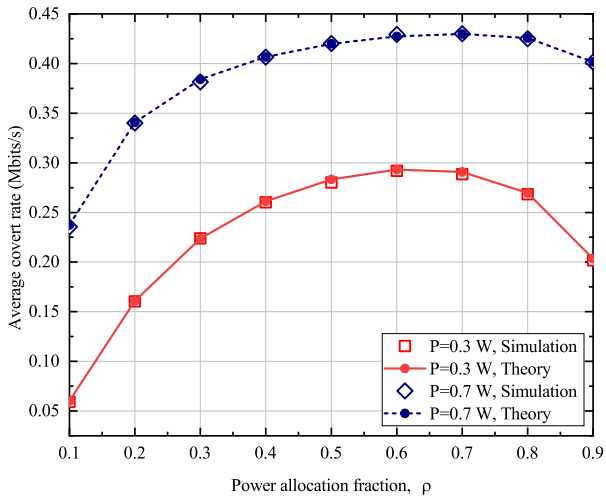

Fig. 2: The impact of ρ on $\overline{\mathrm{R}}_C^u$ under the underlay mode.

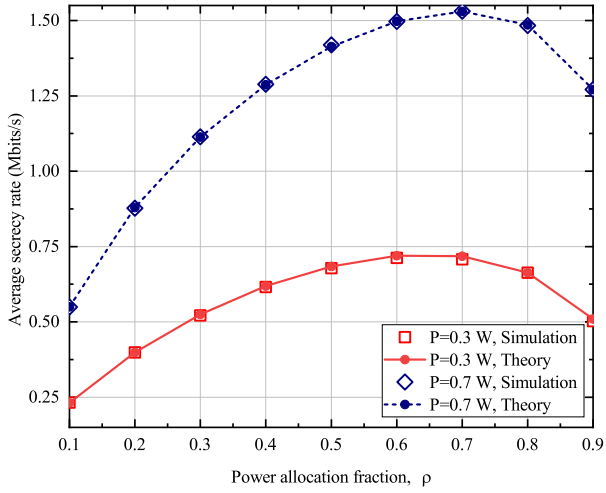

Fig. 3: The impact of ρ on $\overline{\mathrm{R}}_S^u$ under the underlay mode.

to the following reasons. Note that $\overline{\mathrm{R}}_C^u$ from UE to BS is mainly determined by the minimum one between the covert rate from UE to R and that from R to BS. Increasing ρ leads to the increase of the transmit power at UE and the decrease of the transmit power at R, which corresponds to the increase of covert rate from UE to R and the decrease of that from R to BS. When ρ is relatively small, the covert rate from UE to R dominates $\overline{\mathrm{R}}_C^u$, and thus $\overline{\mathrm{R}}_C^u$ increases with the increase of ρ. When ρ continues to increase, the covert rate from R to BS dominates $\overline{\mathrm{R}}_C^u$, and thus $\overline{\mathrm{R}}_C^u$ decreases with the increase of ρ. Another observation from Fig. 2 indicates that $\overline{\mathrm{R}}_C^u$ increases with the increase of the total transmit power P. This is because increasing P leads to the increase of both the transmit powers at UE and R, which corresponds to the covert rate from UE to R and that from R to BS.

Regarding the impact of ρ on the average secrecy rate $\overline{\mathrm{R}}_S^u$, we can see from Fig. 3 that $\overline{\mathrm{R}}_S^u$ first increases and then decreases with the increase of ρ. The reasons behind the

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3201021

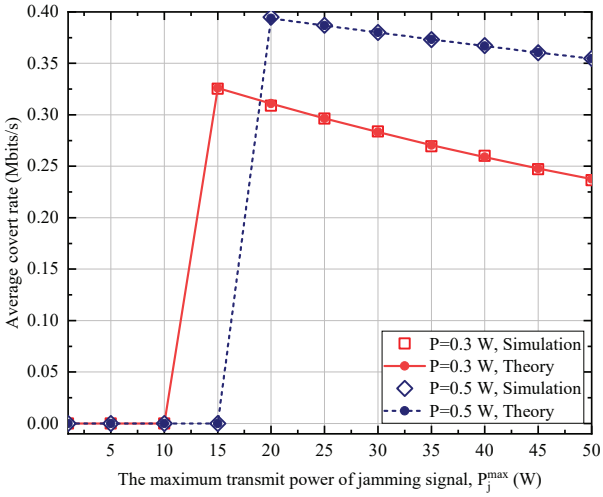

Fig. 4: The impacts of $P_j^{\max}$ on $\overline{\mathrm{R}}_C^u$ under the underlay mode.

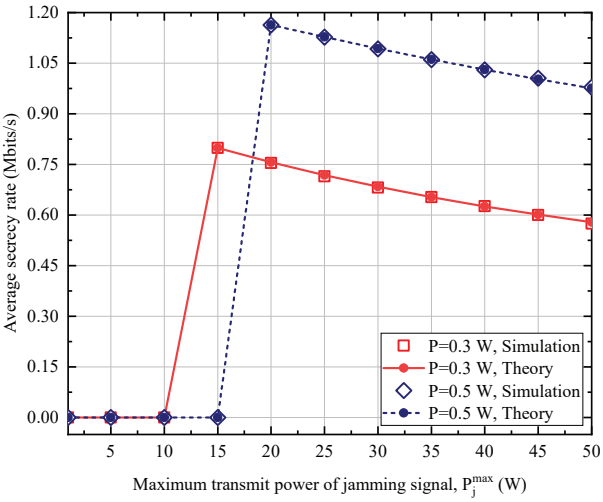

Fig. 5: The impacts of $P_j^{\max}$ on $\overline{\mathrm{R}}_S^u$ under the underlay mode.

phenomena can be explained as follows. When ρ is relatively small, the SINR at BS is mainly determined by the transmit power at UE. As ρ increases, the SINR at BS increases, and thus $\overline{\mathrm{R}}_S^u$ increases. When ρ becomes larger, the SINR at BS is mainly determined by the transmit power at R. As ρ further increases, the SINR at BS decreases, and thus $\overline{\mathrm{R}}_S^u$ decreases. We can also observe that for a fixed ρ, a larger P leads to a larger $\overline{\mathrm{R}}_S^u$. This is because an increase of P can lead to an increase of the SINR at BS.

To illustrate the impact of the maximum transmit power of the jamming signal $P_j^{\max}$ on $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$ under the underlay mode, we summarize in Figs. 4 and 5 how $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$ vary with $P_j^{\max}$ for a setting of $\varepsilon = 0.1$, $\rho = 0.5$ and $P = \{0.3, 0.5\}$ W. Based on these two figures, we can see that our theoretical models can well predict $\overline{\mathrm{R}}_C^u$ and $\overline{\mathrm{R}}_S^u$.

Regarding the impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_C^u$, it can be seen from

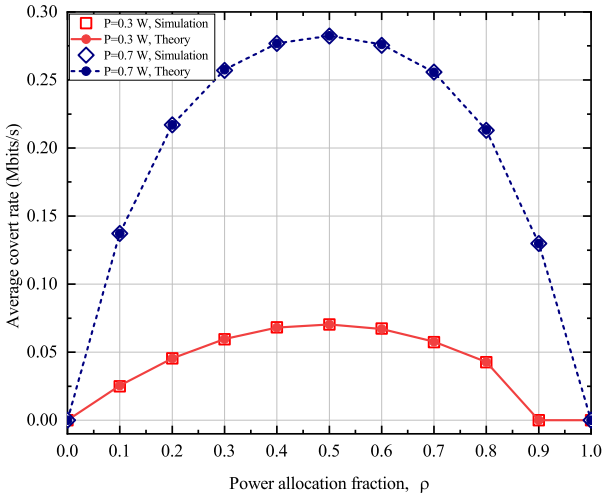

Fig. 6: The impact of ρ on $\overline{\mathrm{R}}_C^o$ under the overlay mode.

Fig. 4 that as $P_j^{\max}$ increases, $\overline{\mathrm{R}}_C^u$ first remains at zero, then reaches a maximum value and decreases. This is because as $P_j^{\max}$ is relatively small, the covertness requirement $\overline{\xi}^* \geq 1-\varepsilon$ cannot hold, and thus $\overline{\mathrm{R}}_C^u$ remains at zero. As $P_j^{\max}$ continues to increase, the covertness requirement holds, and thus $\overline{\mathrm{R}}_C^u$ reaches a maximum value. Meanwhile, increasing $P_j^{\max}$ can also interfere with legitimate link from R to BS, and thus $\overline{\mathrm{R}}_C^u$ decreases with the increase of $P_j^{\max}$.

We now proceed to explore the impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_S^u$, as shown in Fig. 5. We can see from Fig. 5 that as $P_j^{\max}$ increases, $\overline{\mathrm{R}}_S^u$ first keeps at zero, then reaches a maximum value and decreases. This can be explained as follows. A relatively small $P_j^{\max}$ cannot guarantee covert communication, and thus UE does not transmit information. As a result, $\overline{\mathrm{R}}_S^u = 0$. As $P_j^{\max}$ continues to increase, the covert requirement constraint holds, and thus $\overline{\mathrm{R}}_S^u$ reaches a maximum value. However, the increase of $P_j^{\max}$ can also interfere with legitimate link, which leads to the decrease of $\overline{\mathrm{R}}_S^u$.

B. Average Covert Rate and Average Secrecy Rate under the Overlay Mode

As shown in Figs. 6 and 7, we explore the impacts of power allocation fraction ρ on the average covert rate $\overline{\mathrm{R}}_C^o$ and the average secrecy rate $\overline{\mathrm{R}}_S^o$ under the overlay mode for a setting of $P_j^{\max} = 30$ W, $\epsilon = 0.1$, $\beta = 0.8$ and $P = \{0.3, 0.7\}$ W. We can observe from these two figures that our theoretical models can well capture $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ through the comparison between simulation and theory results.

Regarding the impact of ρ on the $\overline{\mathrm{R}}_C^o$, we can see from Fig. 6 that as ρ increases, $\overline{\mathrm{R}}_C^o$ first increases, then achieves a maximum value and decreases. This means that by a proper setting of ρ, we can obtain a maximum $\overline{\mathrm{R}}_C^o$. As for the impact of ρ on the $\overline{\mathrm{R}}_S^o$, we can see from Fig. 7 that $\overline{\mathrm{R}}_S^o$ has the same trend as $\overline{\mathrm{R}}_C^o$. Another observation from Figs. 6 and 7 indicates that for each fixed ρ, a larger P leads to a larger $\overline{\mathrm{R}}_C^o$ as well as $\overline{\mathrm{R}}_S^o$. The reasons behind these observations are similar to these under the underlay mode illustrated in Figs. 2 and 3.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3201021

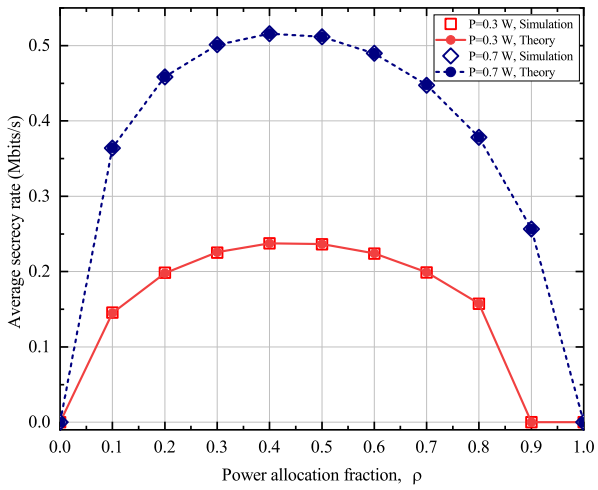

Fig. 7: The impact of ρ on $\overline{\mathrm{R}}_S^o$ under the overlay mode.

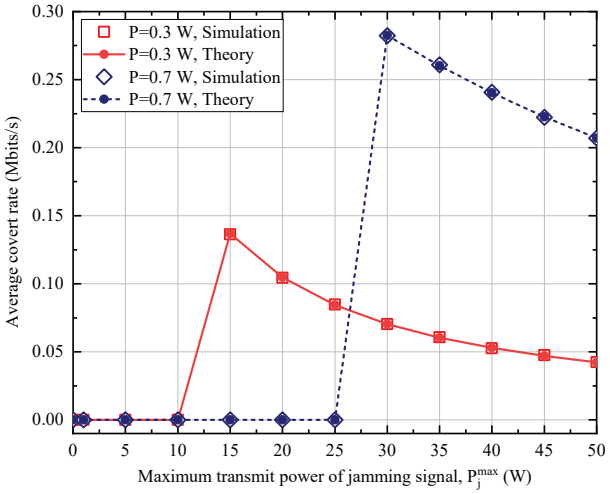

Fig. 8: The impact $P_j^{\max}$ on $\overline{\mathrm{R}}_C^o$ under the overlay mode.

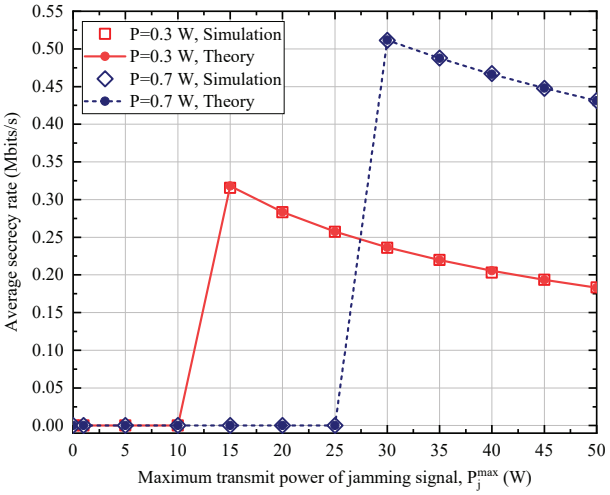

Fig. 9: The impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_S^o$ under the overlay mode.

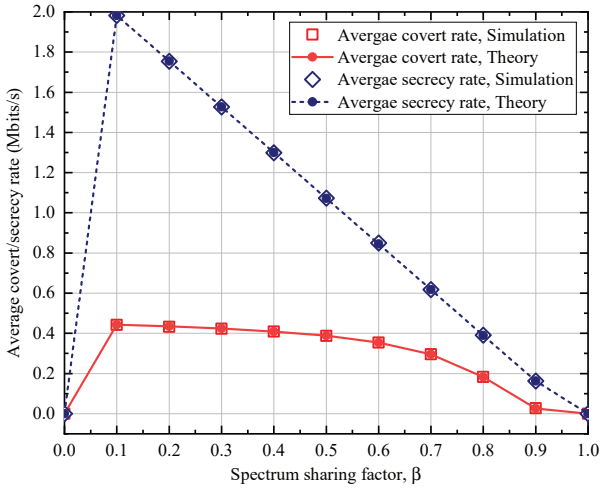

Fig. 10: The impacts of β on $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ under the overlay mode.

We now examine the impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ under the overlay mode for a setting of $\varepsilon = 0.1$, $\beta = 0.8$, $\rho = 0.5$ and $P = \{0.3, 0.7\}$ W. The corresponding simulation and theory results are summarized in Figs. 8 and 9, which illustrate that the theory results well match with the simulation ones.

For the impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_C^o$, it can be seen from Fig. 8 that as $P_j^{\max}$ increases, $\overline{\mathrm{R}}_C^o$ first keeps at zero, then reaches a maximum value and decreases. Regarding the impact of $P_j^{\max}$ on $\overline{\mathrm{R}}_S^o$, we can observe from Fig. 9 that $\overline{\mathrm{R}}_S^o$ has the same trend as $\overline{\mathrm{R}}_C^o$. Figs. 8 and 9 also illustrate that for each fixed $P_j^{\max}$, a larger P leads to a larger $\overline{\mathrm{R}}_C^o$ as well as $\overline{\mathrm{R}}_S^o$. The reasons behind these phenomena are similar to these under the underlay mode illustrated in Figs. 4 and 5.

Finally, we investigate the impact of spectrum sharing factor β on $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ under the overlay mode for a setting of $P = 0.5$ W, $\rho = 0.5$, $P_j^{\max} = 30$ W and $\varepsilon = 0.1$, as shown in Fig. 10. We can see from Fig. 10 that the theory results can well match with the simulation results, and as β increases, both $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ first increase and then decrease. This is because increasing β has a two-fold effect on covert/secrecy rates from UE to R and these from R to BS. On one hand, more system spectrum resources are allocated to the D2D link from UE to R, leading to the increase of covert/secrecy rates from UE to R. On the other hand, less system spectrum resources are allocated to the cellular link from R to BS, leading to the decrease of covert/secrecy rates from R to UE. As β is relatively small, the former dominates the average covert/secrecy rates, and thus the increase of β can lead to the increase of $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$. As β becomes larger, the latter dominates the average covert/secrecy rates, and thus it can lead to the decrease of $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$. A careful observation from Fig. 10 indicates that when $\beta = 0$ and $\beta = 1$, both $\overline{\mathrm{R}}_C^o$ and $\overline{\mathrm{R}}_S^o$ equals to zero. This is because all system spectrum resources are allocated to either the D2D link from UE to R or the cellular link from R to BS, which can cause the transmission from UE to BS to be unreachable.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3201021

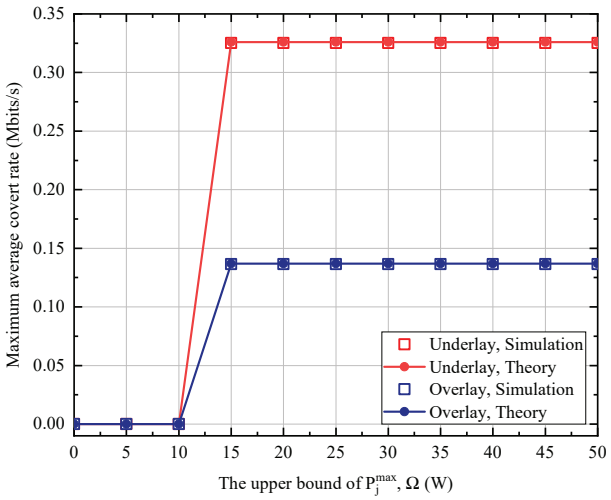

Fig. 11: The impacts of Ω on the maximum average covert rate under the underlay and overlay modes.

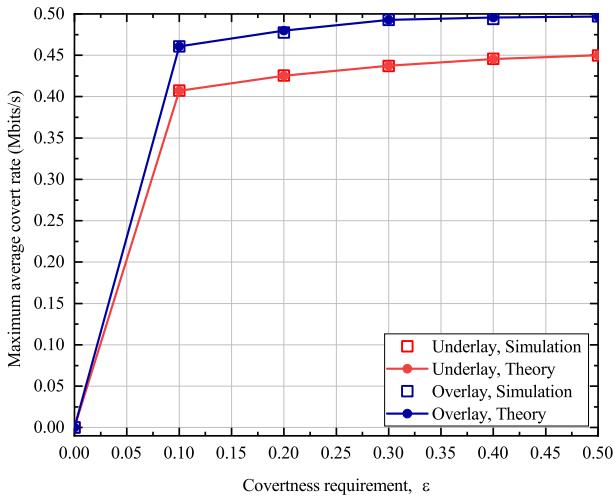

Fig. 12: The impacts of ε on the maximum average covert rate under the underlay and overlay modes.

C. Maximum Average Covert Rate under the Underlay Mode and the Overlay Mode

We now explore the impact of the upper bound Ω of $P_j^{\max}$ on the maximum average covert rate under the underlay and overlay modes for a setting of $\varepsilon = 0.1$, $\rho = 0.5$, $P = 0.3$ W and $\beta = 0.8$. We summarize the theory and simulation results in Fig. 11, which illustrates the theory results well match with the simulation ones. This verifies the validity of our solutions to the optimization problems under these two modes. We can see from Fig. 11 that under each mode, the maximum average covert rate first keeps at zero, then increases up to a constant and keeps unchanged, as Ω increases. The reasons behind the phenomena can be explained as follows. Under these two modes, as Ω is small, the covertness requirement constraint can not hold, and thus the maximum average covert rate equals to zero. As Ω continues to increase, the covertness requirement constraint holds via increasing $P_j^{\max}$, and thus the maximum average covert rate increases. However, as Ω further increases, the optimal $P_j^{\max}$ maximizing average covert rate keeps unchanged due to the fact that increasing $P_j^{\max}$ can also interfere with the legitimate link from UE to BS, which leads to the decrease of the maximum average covert rate. Thus, the maximum average covert rate achieves a maximum value and keeps unchanged.

To illustrate the impact of the covertness requirement ε on the maximum average covert rate under the underlay and overlay modes, we conduct the theory and simulation studies illustrated in Fig. 12 with a setting of $P = 0.5$ W and $\Omega = 30$ W. Based on the observation from Fig. 12, we verify the validity of our solutions to the optimization problems under these two modes. We can observe from Fig. 12 that as ε increases, the maximum average covert rate increases under each mode. Specially, when $\varepsilon = 0$, the maximum average covert rate is also zero. This is due to the following reasons. When $\varepsilon = 0$, the covert requirement constraint $\overline{\xi}^* \geq 1 - \varepsilon$ cannot hold, and thus the maximum average covert rate equals to zero. As ε increases, a small jamming power $P_j^{\max}$ can ensure that the covert requirement constraint holds, and thus the maximum average covert rate increases.

VIII. Conclusion

This paper investigated the joint covert and secure communications in the D2D networks. We first derived the average minimum detection error rate of Willie, and the average covert/secrecy rate under the underlay and overlay modes, respectively. Based on these results, we further explored the optimal power control to achieve MCR with the covertness and security constraints under the underlay mode. We also optimized the transmit powers and the spectrum partition factor to achieve MCR under the overlay mode. The numerical results indicate that the maximum average rate can be improved by optimizing the power allocation between UE and R, transmit power of jamming signal at BS, and spectrum partition factor, while guaranteeing the secure communications under the underlay and overlay modes.

References

[1] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, 2014.

[2] M. Waqas, Y. Niu, Y. Li, M. Ahmed, D. Jin, S. Chen, and Z. Han, "A comprehensive survey on mobility-aware D2D communications: Principles, practice and challenges," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1863–1886, 2020. [Online]. Available: https://doi.org/10.1109/COMST.2019.2923708

[3] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *J. Netw. Comput. Appl.*, vol. 96, pp. 39–61, 2017. [Online]. Available: https://doi.org/10.1016/j.jnca.2017.07.002

[4] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, Oct. 2019.

[5] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542–3553, Jul. 2019.

[6] N. J. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015. [Online]. Available: https://doi.org/10.1109/MCOM.2015.7081071

[7] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 106–109, 2016.

[8] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 19–25, 2019. [Online]. Available: https://doi.org/10.1109/MWC.001.1900057

[9] I. Symeonidis, D. Rotaru, M. A. Mustafa, B. Mennink, B. Preneel, and P. Papadimitratos, "HERMES: scalable, secure, and privacy-enhancing vehicular sharing-access system," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 129–151, 2022. [Online]. Available: https://doi.org/10.1109/JIOT.2021.3094930

[10] S. Yan, S. V. Hanly, and I. B. Collings, "Optimal transmit power and flying location for uav covert wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3321–3333, Nov. 2021.

[11] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.

[12] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 99–114, 2022. [Online]. Available: https://doi.org/10.1109/TIFS.2021.3054507

[13] R. Chen, C. Li, S. Yan, R. A. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 6–11, 2019. [Online]. Available: https://doi.org/10.1109/MWC.001.1900051

[14] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, "Enhancing physical layer security using underlay full-duplex relay-aided D2D communications," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2020, pp. 1–7.

[15] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 229–242, 2014.

[16] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the uplink secrecy capacity analysis in D2D-enabled cellular network," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2297–2307, 2017.

[17] 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.

[18] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1443–1447, 2020.

[19] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2018.

[20] Y. Jiang, L. Wang, H. Zhao, and H. H. Chen, "Covert communications in D2D underlaying cellular networks with power domain noma," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2020.

[21] X. Shi, D. Wu, C. Yue, C. Wan, and X. Guan, "Resource allocation for covert communication in D2D content sharing: A matching game approach," *IEEE Access*, vol. 7, pp. 72 835–72 849, 2019.

[22] X. Shi, D. Wu, C. Wan, M. Wang, and Y. Zhang, "Trust evaluation and covert communication-based secure content delivery for D2D networks: A hierarchical matching approach," *IEEE Access*, vol. 7, pp. 134 838–134 853, 2019.

[23] Y. Jiang, L. Wang, and H.-H. Chen, "Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2980–2992, 2020.

[24] H. Rao, M. Wu, J. Wang, W. Tang, S. Xiao, and S. Li, "D2D covert communications with safety area," *IEEE Systems Journal*, 2020.

[25] L. Wang, G. W. Wornell, and L. Zheng, "Limits of low-probability-of-detection communication over a discrete memoryless channel," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 2525–2529.

[26] M. Ahmadipour, S. Salehkalaibar, M. H. Yassaee, and V. Y. Tan, "Covert communication over a compound discrete memoryless channel," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 982–986.

[27] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communications without channel state information at receiver in IoT systems," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11 103–11 114, 2020.

[28] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6313–6323, 2021.

[29] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 317–320, 2018.

[30] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4766–4779, 2018.

[31] R. Sun, B. Yang, S. Ma, Y. Shen, and X. Jiang, "Covert rate maximization in wireless full-duplex relaying systems with power control," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[32] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, "Intelligent reflecting surface-assisted multi-antenna covert communications: Joint active and passive beamforming optimization," *IEEE Transactions on Communications*, 2021.

[33] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[34] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling massive IoT toward 6G: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11 891–11 915, 2021.

[35] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information-theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7170–7181, 2020.

[36] ——, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.

[37] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6771–6785, 2020.

[38] M. Ragheb, S. M. S. Hemami, A. Kuhestani, D. W. K. Ng, and L. Hanzo, "On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry approach," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 53–68, 2021.

[39] M. Letafati, A. Kuhestani, K.-K. Wong, and M. J. Piran, "A lightweight secure and resilient transmission scheme for the internet of things in the presence of a hostile jammer," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4373–4388, 2020.

[40] Y. Xu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 573–588, 2021.

[41] W. Lu, Y. Ding, Y. Gao, S. Hu, Y. Wu, N. Zhao, and Y. Gong, "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2021.

[42] W. Lu, Y. Ding, Y. Gao, Y. Chen, N. Zhao, Z. Ding, and A. Nallanathan, "Secure NOMA-based UAV-MEC network towards a flying eavesdropper," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3364–3376, 2022.

[43] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2014.

[44] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3801–3807, 2012.

[45] S. Lee and R. J. Baxley, "Achieving positive rate with undetectable communication over awgn and rayleigh channels," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 780–785.

[46] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE transactions on wireless communications*, vol. 10, no. 9, pp. 3074–3085, 2011.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3201021

Ranran Sun received the B.S. and M.S. degrees in computer science from the Henan University of Science and Technology, Luoyang, China, in 2014 and 2017, respectively. She is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Xidian University, Xi'an, China. Her research interest focuses on the covert communication in physical layer.

Bin Yang received his Ph.D. degree in systems information science from Future University Hakodate, Japan in 2015. He was a research fellow with the School of Electrical Engineering, Aalto University, Finland, from Jul. 2019 to Nov. 2021. He is currently a professor with the School of Computer and Information Engineering, Chuzhou University, China. His research interests include unmanned aerial vehicle networks, cyber security and Internet of Things.

Yulong Shen (Member, IEEE) received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

Xiaohong Jiang (Senior Member, IEEE) received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb. 2005 to Mar. 2010. Dr. Jiang's research interests include computer communications networks, mainly wireless networks and optical networks, network security, routers/switches design, etc. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE INFOCOM.

Tarik Taleb (Senior Member, IEEE) received the B.E. degree (with distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the Center of Wireless Communications, University of Oulu, Finland. He is the founder and the Director of the MOSA!C Lab, Finland. He was an Assistant Professor with the Graduate School of Information Sciences, Tohoku University, in a laboratory fully funded by KDDI until 2009. He was a Senior Researcher and a 3GPP Standards Expert with NEC Europe Ltd., Heidelberg, Germany. He was then leading the NEC Europe Labs Team, involved with research and development projects on carrier cloud platforms, an important vision of 5G systems. From 2005 to 2006, he was a Research Fellow with the Intelligent Cosmos Research Institute, Sendai. He has also been directly engaged in the development and standardization of the Evolved Packet System as a member of the 3GPP System Architecture Working Group. His current research interests include architectural enhancements to mobile core networks (particularly 3GPP's), network softwarization and slicing, mobile cloud networking, network function virtualization, software defined networking, mobile multimedia streaming, and unmanned vehicular communications. He was a recipient of the 2017 IEEE ComSoc Communications Software Technical Achievement Award in 2017 for his outstanding contributions to network softwarization and the Best Paper Awards at prestigious IEEE-flagged conferences for some of his research work. He was a corecipient of the 2017 IEEE Communications Society Fred W. Ellersick Prize in 2017, the 2009 IEEE ComSoc Asia–Pacific Best Young Researcher Award in 2009, the 2007 Funai Foundation Science Promotion Award in 2007, the 2006 IEEE Computer Society Japan Chapter Young Author Award in 2006, the Niwa Yasujirou Memorial Award in 2005, and the Young Researcher's Encouragement Award from the Japan Chapter of the IEEE Vehicular Technology Society in 2003. He is a member of the IEEE Communications Society Standardization Program Development Board.