On Joint Covert and Secure Communications in D2D-Enabled Cellular Systems

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

Abstract—This paper explores the joint covert and secure communications in a device-to-device (D2D)-enabled cellular system (DCS) consisting of a base station BS, an eavesdropper Eve, and two user equipments UE and UR. To conduct secure communications with UE against Eve, BS works either under the cellular mode using direct transmission or under the D2D mode replying through UR, while UR is greedy since it opportunistically transmits its own covert message to UE against the detection from BS. To understand the fundamental performance of secrecy rate and covert rate in DCS, we first develop theoretical models to depict the detection probability/secrecy rate of BS and covert rate of UR under different modes (i.e., underlay, overlay, or cellular). Based on these models, we further explore the secrecy rate maximization (SRM) for BS subject to the constraints of detection probability at BS and transmit power at both BS and UR, as well as the covert rate maximization (CRM) for UR subject to the constraints of covertness requirement and covert transmit power. Finally, we employ the Newton-based searching method to solve the SRM/CRM problems and illustrate via numerical results the achievable secrecy rate and covert rate of BS and UR under various DCS scenarios.

Index Terms—Device-to-device, physical layer security, covert communication, secure communication, performance analysis.

1 Introduction

Device-to-device (D2D)-enabled cellular systems (DCSs), which enable the direct communications between nearby devices to be conducted without relaying through a base station (BS), have emerged as a new paradigm in 5G and beyond mobile communication systems [1]–[3]. Such D2D direct communications in close proximity have the potential to achieve high data rate, low delivery latency, large cellular coverage and good load balance, and thus can bring benefits to various proximity-based applications such as local business, emergency communications and Internet-of-Things (IoT) [4], [5]. However, due to the inherent broadcast nature and openness of wireless communications, security becomes a major challenge that hinders the wide deployment of such DCSs [6].

Physical layer security (PLS) technology that exploits the inherent random characteristics of wireless channels (e.g., fading and interferences) to implement secure information transmission, is now recognized as a highly promising approach for security guarantee in DCSs [7], [8]. By now, lots of research efforts have been devoted to the applications of PLS in DCSs to achieve secure communications [9]–[15] or covert communications [16]–[31]. The secure communications aim to prevent eavesdropping attacks from intercepting the content of wireless communications, while the purpose of covert communications is to prevent detection attacks from detecting the existence of the wireless communications. Although the available works study the secure communications and covert communications separately, we may need to jointly consider both secure and covert communications at the same time for some critical applications in DCSs. For instance, for DCS-based military communications, soldiers/leaders from friendly troops usually require secure communications to transmit secret message without being intercepted by spies, while the spies require covert communications to avoid their communications being detected and thereby exposing of their identities.

The joint covert and secure communications in wireless systems was explored in some recent works [32]–[37]. The work in [32] studied the average rate maximization subject to both the covert and secure communication requirements in a single hop wireless system consisting of a source, two receivers, an eavesdropper and a warden, where eavesdropper attempts to intercept the transmission content from source to one receiver, and the warden tries to detect the transmission from source to another receiver. The work

This paper is supported in part by the National Natural Science Foundation of China under Grant No. 62402357, No. 62220106004, No. 92467201, and No. 62372076; in part by the Technology Innovation Leading Program of Shaanxi under Grant No. 2023KXJ-033; in part by the Innovation Capability Support Program of Shaanxi under Grant No. 2023-CX-TD-02; in part by the Fundamental Research Funds for the Central Universities under Grant No. ZDRC2202; in part by the Education Department Research Foundation of Anhui Province under Grant No.DTR2023051; in part by the Innovation Research Team on Future Network Technology of Chuzhou University; in part by the ICTFICIAL Oy, Finland and in part by the European Union's HE Research and Innovation Program HORIZON-JUSNS-2023 through the 6G-Path under Grant No.101139172. (Corresponding authors: Bin Yang; Yulong Shen.)

Ranran Sun is with the Hangzhou Institute of Technology, Xidian University, Hangzhou 311231, China (e-mail: srr_2013@163.com).

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

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

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

Tarik Taleb is with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Bochum 44801, Germany (e-mail: tarik.taleb@rub.de).

in [33] explored the secrecy rate maximization in a two-hop untrusted relay system under the covertness constraint, where the untrusted relay intercepts source's message and the warden detects the communications via the source-relay-receiver link. The work in [34], [35] studied a secure and covert communication for ultra-high reliability and low latency systems with the help of artificial noise, where the secrecy rate maximization problem is explored under the covertness constraint. The work [36] further explored the optimization problem for secrecy rate maximization in the reconfigurable intelligent surface (RIS)-empowered systems. Our previous work [37] investigated the covert rate maximization in a D2D-enabled uplink cellular network with secrecy constraint, where a transmitter attempts to covertly transmit message to a base station (BS) with the help of an untrusted relay adopting the amplify-and-forward transmission protocol, while the relay also tries to eavesdrop message from the transmitter. Although the work [33] explores the joint covert and secure communications in a two-hop system relaying through an untrusted relay who intercepts the message from the source, our work mainly focuses on the greedy relay assisted secure communication against the warden in the D2D-enabled cellular system, where the greedy relay tries to transmit its own message covertly without being detected by the source. It is notable that the research results in [32]–[36] are not directly applicable to the DCS scenario since the fundamental issues of mode selection, spectrum sharing and interference in DCSs are largely ignored in above works. Specifically, in DCSs each user can either select the cellular mode to communicate with BS or the D2D mode to communicate with its nearby user according to a pre-designed mode selection scheme. Furthermore, under the D2D mode, each user can operate over either underlay mode reusing the cellular spectrum or overlay mode using a dedicated spectrum. Here, the spectrum sharing in underlay mode can further cause interference among links sharing the same spectrum.

It is notable that the joint covert and secure communications are desired in many application scenarios. For instance, the security and privacy protection of health data is crucial for all patients and healthcare institutions. In such a scenario, the health data is usually transmitted from a base station (BS) to a terminal, while ensuring that it is not eavesdropped by a malicious user. On the other hand, when the BS is far away from the terminal, it first transmits data to a relay and then the relay forwards the data to the terminal. To stimulate relay cooperation, the BS allocates energy and spectrum resources to the relay for only forwarding the data. However, the relay also wants to utilize these resources to covertly transmit its own data to the terminal, while ensuring that it is not detected by the BS.

As an attempt towards the study of joint covert and secure communications in DCSs, this paper considers a downlink DCS consisting of a base station BS, an eavesdropper Eve, and two user equipments UE and UR. The BS can work either under the cellular mode using direct transmission or under the D2D mode relaying the message through UR when BS is far away from UR. The Eve attempts to intercept message from BS and UR under these two modes. Additionally, BS allocates resource (e.g., spectrum, power) to UR only for forwarding its message. However, UR is greedy such that it also uses the resource to opportunistically transmit its own message to UE covertly. Thus, BS attempts to detect the existence of the covert transmission, while UR wishes to hide the transmission process. Specially, under the D2D mode, the underlay and overlay strategies can be applied for spectrum sharing, where the underlay allows UR to reuse the cellular spectrum and overlay allows UR to use only a dedicated spectrum. Note that the network scenario and the decode-and-forward transmission protocol adopted by the relay in this paper are different from these in [37]. This means that the theoretical analyses are fundamentally different in these two papers.

The main contributions of this paper can be summarized as follows.

- For the DCS, we design a mode selection scheme based on received signal strength (RSS), where the BS adopts the cellular mode to directly communicate with UE if RSS at UE is no less than a pre-determined threshold, or adopts the D2D mode to communicate with UE by replying through UR, otherwise.
- We derive the maximum detection probability and secrecy outage probability of BS under different modes (i.e., cellular, underlay and overlay), and also provide theoretical modelling for the secrecy rate of BS under these three modes, respectively. Based on these results, we then explore the optimal settings of transmit powers at both BS and UR for the secrecy rate maximization (SRM) of BS under each mode.
- We further derive the covert outage probability and covert rate of UR under the underlay and overlay modes of D2D transmission, and also explore the optimal setting of transmit power at UR for covert rate maximization (CRM) of UR subject to the secure communication constraint from BS.
- Finally, we provide extensive numerical results to illustrate both the achievable secrecy rate of BS and covert rate of UR under different DCS scenarios.

The rest of this paper is organized as follows. Section II presents the related works. Section III introduces the system models. Section IV and Section V provide theoretical modeling and optimization of system performances from the perspective of BS and UR, respectively. We provide the extensive numerical results in Section VI. Finally, Section VII concludes this paper.

2 Related Works

2.1 Secure Communications

By now, many works have focused on the study of PLS-based secure communications in DCSs [9]–[15]. The work in [9] proposes a joint guard zone and threshold-based access control scheme for the D2D users to maximize the secrecy rate of cellular links. The performances of both cellular and D2D links are further explored in terms of the secrecy outage probability and probability of non-zero secrecy rate of cellular link as well as the outage probability of D2D link [10]. Based on stochastic geometry theory, the work in [11] studies the connection probabilities and secrecy probabilities of both the cellular and D2D links, where the locations of users follow the distribution of Poisson point

process (PPP). Using Poisson cluster processes (PCPs) to model the locations of users, the work of [13] examines the coverage outage probability and secrecy outage probability of D2D links. A closed-form expression is derived for the probability of achieving nonzero secrecy rate of cellular link, where the transmission power of D2D users can be flexibly controlled [12]. Reconfigurable intelligent surfaces are used to reduce the outage probability of D2D link while improving secrecy performances of cellular link in terms of the secrecy outage probability and the probability of non-zero secrecy rate [14]. Note that all above works largely ignore the fundamental spectrum sharing-based mode selection and spectrum partition issues. The work in [15] proposes a mode selection scheme allowing D2D pairs to select between the underlay and overlay modes as well as a spectrum partition scheme to partition spectrum between cellular users and overlay D2D pairs. The secrecy rate and secrecy outage probability are further derived under these two schemes.

2.2 Covert Communications

Covert communications have been investigated in various wireless systems mainly including the scenarios of single hop [16]–[21], [26] and two hops [22]–[25]. Recently, some initial works conduct the studies of covert communications in DCSs [27]–[31]. The work in [27] proposes a power control scheme to guarantee the covert communications of D2D links, and illustrates the improvement of covert rate performance under such a scheme. Sum covert rate maximization of D2D links can be obtained by jointly optimizing spectrum allocation and power control [28], and by jointly optimizing the user trust degree and spectrum allocation [29]. Two artificial noise injection schemes are proposed to confuse the detection of wardens and the covert rate maximization of D2D link is further explored under each scheme [30]. The work in [31] first designs a safety area based relay selection scheme such that wardens cannot detect the existence of D2D communications, and then maximizes the covert rate of cellular links by jointly optimizing relay selection and transmit power of D2D users.

3 System Models

3.1 System Model

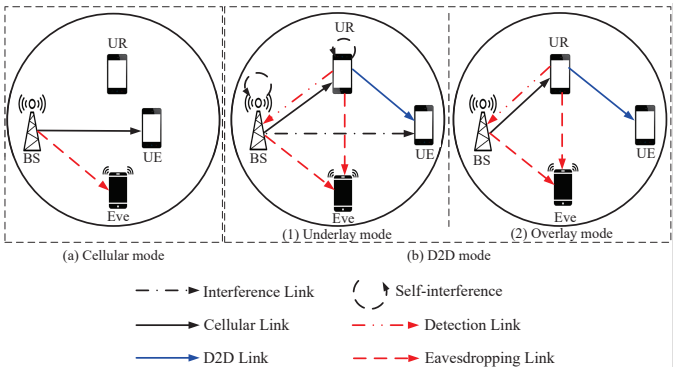

Fig. 1: System Model.

TABLE 1: List of key notations

Notations	Description
$h_{i,j}$	Channel coefficient from node i to node j
$d_{i,j}$	Distance between node i and node j
σ_i^2	Noise variance at node i
P_s	Transmit power of BS
$P_s^{\max}$	Maximum transmit power of BS
P_r, P_c	Transmit powers of UR for forwarding messages from BS and for covert messages
$P_r^{\max}$	Maximum transmit power of UR for forwarding messages
ϕ	Self-interference cancellation coefficient at BS
τ	Detection threshold at BS
P_{th}	Threshold of RSS-based mode selection scheme
R_c	Desirable covert rate
$\overline{R}_c^u$ ($\overline{R}_c^o$)	Covert rate under underlay (overlay) mode
R_s	Desirable secrecy rate
θ	$\theta = 2^{R_s}$
η	$\eta = 2^{2R_s}$
μ	$\mu = 2^{R_c} - 1$
δ	$\delta = 2^{2R_c}$
$\mathbf{P}_b$	Detection probability at BS
$\mathbf{C}_s^c$	Secrecy rate between BS and UE under the cellular mode
$\mathbf{C}_s^{v0}$, $\mathbf{C}_s^{v1}$	Average secrecy rates under H_0 and H_1
$\text{SINR}_{\text{UE}}^{u0}$ ($\text{SINR}_{\text{UE}}^{o0}$)	SINRs from BS to UE under the underlay (overlay) mode when H_0 is true
$\text{SINR}_{\text{UE}}^{u1}$ ($\text{SINR}_{\text{UE}}^{o1}$)	SINRs from BS to UE under the underlay (overlay) mode when H_1 is true
SINR_i^{u0}(SINR_i^{o0}), SINR_i^{u1}(SINR_i^{o1})	SINRs at node i under the underlay (overlay) mode when H_0 and H_1 is true, respectively
P_{ms}	Probability of selecting cellular mode
P_{so}	Secrecy outage probability under cellular mode
P_{sop}^{u0}(P_{sop}^{o0})	Secrecy outage probability under underlay (overlay) mode when H_0 is true
P_{sop}^{u1}(P_{sop}^{o1})	Secrecy outage probability under underlay (overlay) mode when H_1 is true
P_{cop}^{u} (P_{cop}^{o})	Covert outage probability under underlay (overlay) mode

As illustrated in Fig. 1, we consider a downlink transmission scenario in a D2D-enabled cellular system consisting of a BS, an eavesdropper Eve, and two user equipments UR and UE, where the BS can operate over two communication modes (i.e., cellular and D2D) according to a received signal strength (RSS)-based mode selection scheme. In the scheme, if RSS at any user equipment (e.g., UE) is no less than a threshold P_{th}, BS selects the cellular mode under which BS directly sends message to UE. Otherwise, it selects the D2D mode under which another user equipment (e.g., UR) employs decode-and-forward protocol and full-duplex operation to simultaneously receive and forward the message from BS to UE. According to the IEEE 802.11, the received signal strength indicator (RSSI) is presented to represent the signal strength. Wireless hardware manufacturers give the RSSI and the corresponding RSS threshold for every wireless hardware product. Thus, the RSSI and corresponding RSS threshold can be used to decide P_{th}. Herein, Eve tries to eavesdrop the message transmitted from BS to UE silently. For the cellular mode, Eve intercepts the message only from BS. As for the D2D mode, UR not only forwards the legitimate message from BS, but also attempts to covertly send its own message simultaneously. As a result, BS needs to detect the existence of the covert transmission. Meanwhile, Eve receives signals from BS and UR simultaneously aiming to intercept the message. Here, BS and UR adopts full-

duplex communication mode, due to the fact that BS not only sends message, but also receives signal to detect the covert communication simultaneously, while UR utilizes it to improve spectrum utilization and achieve a higher data rate.

We consider two spectrum resource sharing manners in the DCS, namely underlay and overlay, where there are in total six types of links, i.e., cellular, D2D, interference, self-interference, detection and eavesdropping links. Under the underlay mode, the D2D link from UR to UE reuses the same system spectrum resource with the cellular link from BS to UR. Thus, there exists interference between these two links. Since BS transmits legitimate signal and also receives signal from UR simultaneously, there exists self-interference at BS from its transmission to its reception. Under the overlay mode, the system spectrum resource is evenly partitioned into two equal-sized and orthogonal resource blocks, and each of the D2D and cellular links uses a different resource block such that there does not exist interference between them. We assume that UE and Eve have a single antenna. The total bandwidth of the system spectrum resource is W MHz. Without loss of generality W is set to 1 throughout this paper. Additionally, the key notations used in this paper are illustrated in Table 1.

3.2 Channel Model

The quasi-static Rayleigh fading channels are used to model the wireless links in our concerned DCS. In the fading channels, each channel coefficient $h_{i,j}$ from a transmitter i to a receiver j remains unchanged in one slot while changing independently from one slot to another. $h_{i,j}$ is a complex Gaussian random variable with zero mean and variance $\sigma_{i,j}^2 = d_{i,j}^{-\alpha}$, where α denotes the path loss exponent and $d_{i,j}$ denotes the distance between i and j. Here, $i \in \{s, r\}$ and $j \in \{s, r, d, e\}$, where s, r, d and e are associated with BS, UR, UE and Eve, respectively. Specially, $h_{s,s}$ and $h_{r,r}$ are the coefficients of the self-interference channels at BS and UR, respectively. $d_{s,s}$ and $d_{r,r}$ are the distances between the receiving and transmitting antennas at BS and UR, respectively. We use n_s, n_r, n_d and n_e to denote the additive white Gaussian noise at BS, UR, UE and Eve with variances σ_s^2, σ_r^2, σ_d^2 and σ_e^2, respectively. With long-term observations, we assume that BS, UR and Eve can know the statistical channel state information (CSI) of each channel [17], [24]. We also assume that BS employs a transmit power P_s, and allocates transmit power P_r to UR only for forwarding BS's message, where $P_s \leq P_s^{\max}$ and $P_r \leq P_r^{\max}$.

3.3 Detection Model

In our study, when the greedy UR forwards the message from BS to UE, it may also covertly transmit its own message simultaneously. To decide the existence of the covert transmission, BS conducts a binary hypothesis testing including null and alternative hypotheses based on his observations. The null hypothesis H_0 states that UR did not transmit covert information to UE while the alternative hypothesis H_1 states that UR transmitted covert information. For the underlay and overlay modes, the received signal $y_s(i)$ at BS under H_0 and H_1 are given by

$$\mathrm{H}_0 : y_s(i) = \begin{cases} \Delta + \sqrt{\varphi P_s} h_{s,s} x_s(i), & \text{underlay mode.} \\ \Delta, & \text{overlay mode.} \end{cases} \quad (1)$$

$$\mathrm{H}_1 : y_s(i) = \begin{cases} \Delta + \sqrt{P_c} h_{s,r} x_c(i) \\ +\sqrt{\varphi P_s} h_{s,s} x_s(i), & \text{underlay mode.} \\ \Delta + \sqrt{P_c} h_{s,r} x_c(i), & \text{overlay mode.} \end{cases} \quad (2)$$

where $\Delta = \sqrt{P_r} h_{s,r} x_r(i) + n_s(i)$, and P_c is the transmit power of covert message at UR. $x_s(i)$ and $x_r(i)$ represent the ith transmitted signal at BS and UR, respectively, $x_c(i)$ represents the ith covert signal at UR, and they satisfy that $\mathbb{E}[|x_s(i)|^2] = 1$, $\mathbb{E}[|x_r(i)|^2] = 1$ and $\mathbb{E}[|x_c(i)|^2] = 1$, where $\mathbb{E}[\cdot]$ denotes the expectation operator, $i = 1, 2, \cdots, n$ is the index of each signal and n is assumed to be infinity, i.e., $n \to \infty$. φ denotes the self-interference cancellation coefficient at BS. Since the codeword of the signal from BS is known to itself, we consider that BS can cancel the self-interference from the signal to his reception perfectly by utilizing the self-interference cancellation technology [38], i.e., $\varphi = 0$, which corresponds to the case that BS detects the covert transmission without being affected by the self-interference[1]. According to (1) and (2), we know that the received signals at BS have the same expression under the underlay and overlay modes, which can be rewritten as

$$y_s(i) = \begin{cases} \Delta, & \mathrm{H}_0. \\ \Delta + \sqrt{P_c} h_{s,r} x_c(i), & \mathrm{H}_1. \end{cases} \quad (3)$$

Based on the received signal vector $\mathbf{y_s} = [y_s(1), y_s(2), \cdots, y_s(n)]$, BS decides whether $\mathbf{y_s}$ is from H_0 or H_1. According to Neyman-Pearson criterion, BS uses the following threshold-based decision rule to minimize its detection error [39],

$$Y_s \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \quad (4)$$

where $Y_s = \frac{1}{n} \sum_{i=1}^{n} |y_s(i)|^2$ is the average power received at BS in a time slot, D_0 and D_1 represent these two decisions of BS that it approves H_0 and H_1, respectively, τ is the detection threshold. We consider an infinite number of received signals at BS in each time slot, i.e., $n \to \infty$, then the average power received at BS is given by

$$Y_s = \begin{cases} P_r |h_{s,r}|^2 + \sigma_s^2, & \mathrm{H}_0. \\ P_r |h_{s,r}|^2 + P_c |h_{s,r}|^2 + \sigma_s^2, & \mathrm{H}_1. \end{cases} \quad (5)$$

According to (4) and (5), BS has to make a decision on whether UR transmits covert signals or not. We use detection probability $\mathbf{P}_b$ to measure the detection performance at BS, which is defined as the probability that BS can successfully detect the covert transmission at UR under the D2D mode. Formally, we formulate $\mathbf{P}_b$ as

$$\mathbf{P}_b = 1 - P_E, \quad (6)$$

1. $\varphi = 0$ indicates that BSs detection for the covert transmission of UR is not affected by the self-interference. From the perspective of BS, the self-interference negatively affects its detection and results in the decrease of detection probability. If the covert communication of UR can be achieved in the case $\varphi = 0$, UR can also achieve covert communication in the case $\varphi > 0$.

where P_E is the detection error probability at BS, which is expressed as [24]

$$P_E = P_{FA} + P_{MD} \tag{7}$$

where the probability of false alarm $P_{FA} = \mathcal{P}\{Y_s > \tau|\mathrm{H}_0\}$ represents the probability of the event that BS makes a decision D_1 to approve H_1 while H_0 is true, and the probability of missed detection $P_{MD} = \mathcal{P}\{Y_s < \tau|\mathrm{H}_1\}$ represents the probability of the event that BS makes a decision D_0 to approve H_0 while H_1 is true, therein $\mathcal{P}\{\cdot\}$ is the probability operator.

3.4 Performance Metrics

We give the definitions of performance metrics as follows.

Secrecy rate: It is defined as the expected secrecy rate under these two cases that UR transmits and does not transmit covert message. At the secrecy rate, BS can successfully transmit message to UE without being intercepted by Eve.

The secrecy rate denoted as $\mathbf{C}_s^v$ can be expressed as

$$\mathbf{C}_s^v = P_{\mathrm{H}_0}\mathbf{C}_s^{v0} + P_{\mathrm{H}_1}\mathbf{C}_s^{v1}, \tag{8}$$

where $v \in \{c, u, o\}$, c, u, o denote the cellular, underlay and overlay modes, respectively, $\mathbf{C}_s^{v0}$ and $\mathbf{C}_s^{v1}$ are the average secrecy rates under the conditions that H_0 and H_1 are true, respectively, P_{H_0} and P_{H_1} are the probabilities that UR does not transmit covert message and transmits a covert message, respectively. Specially, when UE selects the D2D mode, these two hypotheses would occur with equal probability (i.e., $P_{\mathrm{H}_0} = P_{\mathrm{H}_1} = \frac{1}{2}$) due to the fact that BS did not know which hypothesis would occur [17], [40]. When UE selects the cellular mode, there does not exist covert communications (i.e., $P_{\mathrm{H}_0} = 1$ and $P_{\mathrm{H}_1} = 0$).

Covert rate: It is defined as the transmission rate from UR to UE without occurring secrecy and covert outages under the D2D mode. At the covert rate, BS can detect the existence of the transmission from UR to UE with an arbitrarily low probability.

The covert rate $\overline{R}$ can be formulated as $\overline{R} = R_c P_1^d(1 - P_2)(1 - P_3)$, where R_c denotes the desirable covert rate, P_1^d denotes the probability that UE selects D2D mode, P_2 denotes the secrecy outage probability that UE cannot successfully receive the secure message, and P_3 denotes the covert outage probability that UE cannot successfully receive the covert message.

To derive these performance metrics, we also give the following basic expressions on instantaneous secrecy rate and instantaneous covert rate under the cellular and D2D modes, respectively.

1) *Cellular mode:* The signal-to-noise-ratio (SNR) γ_{sd} at UE and the SNR γ_3 at Eve can be determined as $\gamma_{sd} = \frac{P_s|h_{s,d}|^2}{\sigma_d^2}$, and $\gamma_3 = \frac{P_s|h_{s,e}|^2}{\sigma_e^2}$, where γ_{sd} and γ_3 are the exponentially distributed random variables with mean $\lambda_{sd} = \frac{P_s d_{s,d}^{-\alpha}}{\sigma_d^2}$ and $\lambda_3 = \frac{P_s d_{s,e}^{-\alpha}}{\sigma_e^2}$, respectively. According to [15], we can determine the instantaneous secrecy rate C_s^c under the cellular mode as

$$C_s^c = [\log_2(1 + \gamma_{sd}) - \log(1 + \gamma_3)]^+, \tag{9}$$

where $[v]^+ = \max[v, 0]$.

2) *D2D mode:* We give the basic expressions under the underlay and overlay modes, respectively.

Under the *underlay mode*, when H_0 is true (i.e., transmission without covert message at UR), the signal-to-interference-plus-noise-ratio (SINR) SINR_r^{u0} at UR, the one SINR_d^{u0} at UE and the one SINR_e^{u0} at Eve are given by $\mathrm{SINR}_r^{u0} = \frac{P_s|h_{s,r}|^2}{\phi P_r|h_{r,r}|^2+\sigma_r^2} = \frac{\gamma_1}{\gamma_r+1}$, $\mathrm{SINR}_d^{u0} = \frac{P_r|h_{r,d}|^2}{P_s|h_{s,d}|^2+\sigma_d^2} = \frac{\gamma_4}{\gamma_{sd}+1}$, and $\mathrm{SINR}_e^{u0} = \frac{P_r|h_{r,e}|^2+P_s|h_{s,e}|^2}{\sigma_e^2} = \gamma_2 + \gamma_3$, where ϕ denotes the self-interference cancellation coefficient, and different values of $\phi \in [0, 1]$ correspond to different cancellation levels of the self-interference signal at UR. $\gamma_1 = \frac{P_s|h_{s,r}|^2}{\sigma_r^2}$, $\gamma_r = \frac{\phi P_r|h_{r,r}|^2}{\sigma_r^2}$, $\gamma_2 = \frac{P_r|h_{r,e}|^2}{\sigma_e^2}$, and $\gamma_4 = \frac{P_r|h_{r,d}|^2}{\sigma_d^2}$ with means $\lambda_1 = \frac{P_s d_{s,r}^{-\alpha}}{\sigma_r^2}$, $\lambda_r = \frac{\phi P_r d_{r,r}^{-\alpha}}{\sigma_r^2}$, $\lambda_2 = \frac{P_r d_{r,e}^{-\alpha}}{\sigma_e^2}$ and $\lambda_4 = \frac{P_r d_{r,d}^{-\alpha}}{\sigma_d^2}$, respectively.

Since UR employs decode-and-forward protocol, the end-to-end SINR $\mathrm{SINR}_{\mathrm{UE}}^{u0}$ from BS to UE is given by [41],

$$\mathrm{SINR}_{\mathrm{UE}}^{u0} = \min\{\mathrm{SINR}_r^{u0}, \mathrm{SINR}_d^{u0}\} = \min\{\frac{\gamma_1}{\gamma_r + 1}, \frac{\gamma_4}{\gamma_{sd} + 1}\}. \tag{10}$$

Therefore, the instantaneous secrecy rate C_s^{u0} of the channel from BS to UE under H_0 can be expressed as

$$C_s^{u0} = [\log_2(1 + \mathrm{SINR}_{\mathrm{UE}}^{u0}) - \log_2(1 + \mathrm{SINR}_e^{u0})]^+. \tag{11}$$

When H_1 is true (i.e., transmission with covert message at UR), the SINR SINR_r^{u1} at UR, the one SINR_d^{u1} at UE and the one SINR_e^{u1} at Eve under H_1 are given by $\mathrm{SINR}_r^{u1} = \frac{P_s|h_{s,r}|^2}{\phi P_r^1|h_{r,r}|^2+\sigma_r^2} = \frac{\gamma_1}{\gamma_r^1+1}$, $\mathrm{SINR}_d^{u1} = \frac{P_r|h_{r,d}|^2}{P_c|h_{r,d}|^2+P_s|h_{s,d}|^2+\sigma_d^2} = \frac{\gamma_4}{\gamma_5+\gamma_{sd}+1}$, and $\mathrm{SINR}_e^{u1} = \frac{P_s|h_{s,e}|^2+P_r|h_{r,e}|^2}{P_c|h_{r,e}|^2+\sigma_e^2} = \frac{\gamma_2+\gamma_3}{\gamma_6+1}$, where $P_r^1 = P_r + P_c$, $\gamma_r^1 = \frac{\phi P_r^1|h_{r,r}|^2}{\sigma_r^2}$, $\gamma_5 = \frac{P_c|h_{r,d}|^2}{\sigma_d^2}$ and $\gamma_6 = \frac{P_c|h_{r,e}|^2}{\sigma_e^2}$ with means $\lambda_r^1 = \frac{\phi P_r^1 d_{r,r}^{-\alpha}}{\sigma_r^2}$, $\lambda_5 = \frac{P_c d_{r,d}^{-\alpha}}{\sigma_d^2}$ and $\lambda_6 = \frac{P_c d_{r,e}^{-\alpha}}{\sigma_e^2}$, respectively. The end-to-end SINR $\mathrm{SINR}_{\mathrm{UE}}^{u1}$ from BS to UE under H_1 is determined as

$$\mathrm{SINR}_{\mathrm{UE}}^{u1} = \min\{\mathrm{SINR}_r^{u1}, \mathrm{SINR}_d^{u1}\} = \min\{\frac{\gamma_1}{\gamma_r^1 + 1}, \frac{\gamma_4}{\gamma_5 + \gamma_{sd} + 1}\} \tag{12}$$

Then, the instantaneous secrecy rate C_s^{u1} of the channel from BS to UE under H_1 can be formulated as

$$C_s^{u1} = [\log_2(1 + \mathrm{SINR}_{\mathrm{UE}}^{u1}) - \log_2(1 + \mathrm{SINR}_e^{u1})]^+. \tag{13}$$

Consider the transmission of covert message from UR to UE, the SINR SINR_c^u at UE under the underlay mode can be determined as

$$\mathrm{SINR}_c^u = \frac{P_c|h_{r,d}|^2}{P_r|h_{r,d}|^2 + P_s|h_{s,d}|^2 + \sigma_d^2} = \frac{\gamma_5}{\gamma_4 + \gamma_{sd} + 1}. \tag{14}$$

Then, the instantaneous covert rate C_d^u from UR to UE is expressed as

$$C_d^u = \log_2(1 + \mathrm{SINR}_c^u). \tag{15}$$

Under the *overlay mode*, since Eve adopts the maximal ratio combining (MRC) to maximize its received SNR [42], when H_0 is true, the SNR SNR_e^{o0} at Eve can be determined as

$$\mathrm{SNR}_e^{o0} = \frac{P_r|h_{r,e}|^2 + P_s|h_{s,e}|^2}{\sigma_e^2} = \gamma_2 + \gamma_3. \tag{16}$$

We also obtain the SNR SNR_r^{o0} at UR and SNR_d^{o0} at UE under H_0 as $\text{SNR}_r^{o0} = \frac{P_s|h_{s,r}|^2}{\sigma_r^2} = \gamma_1$ and $\text{SNR}_d^{o0} = \frac{P_r|h_{r,d}|^2}{\sigma_d^2} = \gamma_4$. Then, the end-to-end SNR from BS to UE is given by

$$\text{SINR}_{\text{UE}}^{o0} = \min\{\text{SNR}_r^{o0}, \text{SNR}_d^{o0}\} = \min\{\gamma_1, \gamma_4\}. \quad (17)$$

Thus, the instantaneous secrecy rate C_s^{o0} under the overlay mode is determined as

$$C_s^{o0} = [\frac{1}{2}\log_2(1+\text{SINR}_{\text{UE}}^{o0}) - \frac{1}{2}\log_2(1+\text{SNR}_e^{o0})]^+. \quad (18)$$

When H_1 is true, the SNR SNR_e^{BS} at Eve from BS and the one SINR_e^R at Eve from UR can be given by $\text{SNR}_e^{BS} = \frac{P_s|h_{s,e}|^2}{\sigma_e^2} = \gamma_3$ and $\text{SINR}_e^R = \frac{P_r|h_{r,e}|^2}{P_c|h_{r,e}|^2+\sigma_e^2} = \frac{\gamma_2}{\gamma_6+1}$. By adopting MRC, the total SINR at Eve is determined as

$$\text{SINR}_e^{o1} = \text{SNR}_e^{BS} + \text{SINR}_e^R = \gamma_3 + \frac{\gamma_2}{\gamma_6+1}. \quad (19)$$

The SNR SNR_r^{o1} at UR and the one SINR_d^{o1} at UE are given by $\text{SNR}_r^{o1} = \frac{P_s|h_{s,r}|^2}{\sigma_r^2} = \gamma_1$ and $\text{SINR}_d^{o1} = \frac{P_r|h_{r,d}|^2}{P_c|h_{r,d}|^2+\sigma_d^2} = \frac{\gamma_4}{\gamma_5+1}$.

Based on the decode and forward protocol at UR, the end-to-end SINR $\text{SINR}_{\text{UE}}^{o1}$ from BS to UE can be determined as

$$\text{SINR}_{\text{UE}}^{o1} = \min\{\text{SNR}_r^{o1}, \text{SINR}_d^{o1}\} = \min\{\gamma_1, \frac{\gamma_4}{\gamma_5+1}\}. \quad (20)$$

Then, the instantaneous secrecy rate C_s^{o1} under the overlay mode is expressed as

$$C_s^{o1} = [\frac{1}{2}\log_2(1+\text{SINR}_{\text{UE}}^{o1}) - \frac{1}{2}\log_2(1+\text{SINR}_e^{o1})]^+ \quad (21)$$

For the transmission of covert message under the overlay mode, the SINR SINR_c^o at UE is given by

$$\text{SINR}_c^o = \frac{P_c|h_{r,d}|^2}{P_r|h_{r,d}|^2+\sigma_d^2} = \frac{\gamma_5}{\gamma_4+1}. \quad (22)$$

We then express the instantaneous covert rate C_d^o from UR to UE as

$$C_d^o = \frac{1}{2}\log_2(1+\text{SINR}_c^o). \quad (23)$$

4 Secrecy Performance from the Perspective of BS

In this section, we first derive the detection probability of BS, and then provide the modeling and optimization of secrecy rate performance under different modes.

4.1 Detection Performance at BS

First, we need to derive these two probabilities of false alarm and missed detection at BS under the D2D mode, which are given in the following theorem.

Theorem 1. *We use P_{FA}^v and P_{MD}^v to denote the probabilities of false alarm and missed detection under the mode v, respectively, where $v \in \{u, o\}$, u denotes the underlay mode and o denotes the overlay mode. Then, we have*

$$P_{FA}^v = \begin{cases} 1, & \tau \le \sigma_s^2, \\ \frac{1}{1-P_{sop}^{v0}}\exp(-\frac{\tau-\sigma_s^2}{P_r d_{s,r}^{-\alpha}}), & \tau > \sigma_s^2, \end{cases} \quad (24)$$

and

$$P_{MD}^v = \begin{cases} 0, & \tau \le \sigma_s^2, \\ \frac{1}{1-P_{sop}^{v0}}(1-\exp(-\frac{\tau-\sigma_s^2}{P_r^1 d_{s,r}^{-\alpha}})), & \tau > \sigma_s^2, \end{cases} \quad (25)$$

where P_{sop}^{v0} denotes the secrecy outage probability under the mode v and will be given in the Theorem 5, and $P_r^1 = P_c + P_r$.

Proof. We first derive these two probabilities under the underlay mode. Let $\mathbb{B}$ denote the event that secrecy outage does not occur, the probability of the event occurring $P\{\mathbb{B}\} = 1 - P_{sop}^{u0}$. Given that the events H_0 and $\mathbb{B}$ have already occurred, the probability of false alarm P_{FA}^u can be determined as

$$P_{FA}^u = \mathcal{P}\{Y_s > \tau|\text{H}_0, \mathbb{B}\} = \mathcal{P}\{P_r|h_{s,r}|^2 + \sigma_s^2 > \tau|\mathbb{B}\} = \begin{cases} 1, & \tau \le \sigma_s^2. \\ \mathcal{P}\{|h_{s,r}|^2 > \frac{\tau-\sigma_s^2}{P_r}\}\mathcal{P}\{\mathbb{B}\}^{-1} & \\ = \mathcal{P}\{\mathbb{B}\}^{-1}\int_{\frac{\tau-\sigma_s^2}{P_r}}^{\infty} f_{|h_{s,r}|^2}(x)dx, & \tau > \sigma_s^2. \end{cases} \quad (26)$$

Note that the channel gain $|h_{i,j}|^2$ is an exponentially distributed random variable with mean $d_{i,j}^{-\alpha}$, thus the probability density function (PDF) of $|h_{i,j}|^2$ is given by

$$f_{|h_{i,j}|^2}(x) = \frac{1}{d_{i,j}^{-\alpha}}\exp(-\frac{x}{d_{i,j}^{-\alpha}}). \quad (27)$$

$\mathcal{P}\{\mathbb{B}\}$ has been given in the above. By substituting $f_{|h_{i,j}|^2}(x)$ into (26) and calculating the integration, P_{FA}^u in (24) follows.

The probability of missed detection P_{MD}^u can be determined as

$$P_{MD}^u = \mathcal{P}\{Y_s < \tau|\text{H}_1, \mathbb{B}\} = \mathcal{P}\{P_r|h_{s,r}|^2 + P_c|h_{s,r}|^2 + \sigma_s^2 < \tau|\mathbb{B}\} = \begin{cases} 0, & \tau \le \sigma_s^2. \\ \mathcal{P}\{|h_{s,r}|^2 < \frac{\tau-\sigma_s^2}{P_r^1}\}\mathcal{P}\{\mathbb{B}\}^{-1} & \\ = \mathcal{P}\{\mathbb{B}\}^{-1}\int_0^{\frac{\tau-\sigma_s^2}{P_r^1}} f_{|h_{s,r}|^2}(x)dx, & \tau > \sigma_s^2. \end{cases} \quad (28)$$

By substituting $f_{|h_{i,j}|^2}(x)$ given in (27) into (28), P_{MD}^u in (25) follows. Similar to the derivations of P_{FA}^u and P_{MD}^u, we can also obtain the probabilities of false alarm and missed detection P_{FA}^o and P_{MD}^o under the overlay mode. □

Thus, we can obtain the detection probabilities under the D2D mode based on the definitions of (6) and (7).

We further derive the maximum detection probability under different modes. Towards this end, we need to identify the optimal detection threshold for minimizing the detection error probability, which is given in the following theorem.

Theorem 2. *We use τ^* to denote the optimal detection threshold at BS, and use P_E^{v*} to denote the corresponding minimum detection error probability under the mode v, where $v \in \{u, o\}$, u and o represent the underlay and overlay mode, respectively. Then, we have*

$$\tau^* = \sigma_s^2 + \frac{P_r^1 P_r d_{s,r}^{-\alpha}}{P_c}\ln\frac{P_r^1}{P_r}, \quad (29)$$

and

$$P_E^{v*} = \frac{1}{1-P_{sop}^{v0}}(1-\exp(-\frac{P_r}{P_c}\ln\frac{P_r^1}{P_r}) + \exp(-\frac{P_r^1}{P_c}\ln\frac{P_r^1}{P_r})). \quad (30)$$

Proof. We now determine τ^* and P_E^{u*} under the underlay mode. Since the detection error probability P_E^u equals to the sum of P_{FA}^u and P_{MD}^u, we have

$$P_E^u = \begin{cases} 1, & \tau \le \sigma_s^2. \\ \frac{1}{1-P_{sop}^{u0}}(1-\exp(-\frac{\tau-\sigma_s^2}{P_r^1 d_{s,r}^{-\alpha}}) + \exp(-\frac{\tau-\sigma_s^2}{P_r d_{s,r}^{-\alpha}})), & \tau > \sigma_s^2. \end{cases} \quad (31)$$

We can see from (31) that if $\tau > \sigma_s^2$, $P_E^u \le 1$. Otherwise, $P_E^u = 1$.

To determine τ^* and P_E^{u*}, we take a derivation of P_E^u with respect to τ when $\tau > \sigma_s^2$. Then,

$$\frac{\partial P_E^u}{\partial \tau} = \frac{1}{1-P_{sop}^{u0}}\left(\frac{\exp(-\frac{\tau-\sigma_s^2}{P_r^1 d_{s,r}^{-\alpha}})}{P_r^1 d_{s,r}^{-\alpha}} - \frac{\exp(-\frac{\tau-\sigma_s^2}{P_r d_{s,r}^{-\alpha}})}{P_r d_{s,r}^{-\alpha}}\right). \quad (32)$$

Let $\frac{\partial P_E^u}{\partial \tau} = 0$, we have $\tau = \sigma_s^2 + \frac{P_r^1 P_r d_{s,r}^{-\alpha}}{P_c}\ln\frac{P_r^1}{P_r}$. When $\tau < \sigma_s^2 + \frac{P_r^1 P_r d_{s,r}^{-\alpha}}{P_c}\ln\frac{P_r^1}{P_r}$, $\frac{\partial P_E^u}{\partial \tau} < 0$. This means that P_E^u decreases with the increase of τ. When $\tau > \sigma_s^2 + \frac{P_r^1 P_r d_{s,r}^{-\alpha}}{P_c}\ln\frac{P_r^1}{P_r}$, $\frac{\partial P_E^u}{\partial \tau} > 0$, which indicates that P_E^u increases with the increase of τ. Thus, the optimal detection threshold $\tau^* = \sigma_s^2 + \frac{P_r^1 P_r d_{s,r}^{-\alpha}}{P_c}\ln\frac{P_r^1}{P_r}$. We can also obtain the corresponding minimum detection error probability P_E^{u*} by substituting τ^* into (31).

Similar to the derivation process of τ^* and P_E^{u*} under the underlay mode, we can also obtain the τ^* and P_E^{o*} under the overlay mode. Specially, the optimal detection thresholds under these two modes are the same. It is because the received average powers at BS under both modes are the same under the assumption that BS can cancel his self-interference perfectly. □

Thus, we can determine the optimal detection probability $\mathbf{P}_b^{v*}$ under the mode v as $\mathbf{P}_b^{v*} = 1 - P_E^{v*}$.

We further give the following special case for the Theorem 2 to provide an insight.

A special case of Theorem 2 is that the optimal detection threshold $\tau^* = \sigma_s^2$ and the corresponding minimum detection error probability tends to 1, when the secrecy transmit power P_r allocated by BS is much larger than the covert transmit power P_c at UR.

4.2 Secrecy Rate under the Cellular Mode

4.2.1 Secrecy Rate Modeling

Under the cellular mode, the secrecy rate from BS to UE is given in the following theorem.

Theorem 3. *We use $\mathbf{C}_s^c$ to denote the secrecy rate under the cellular mode. Then, we have*

$$\mathbf{C}_s^c = \frac{\lambda_{sd}\exp(-(\frac{P_{th}}{P_s d_{s,d}^{-\alpha}} + \frac{\theta-1}{\lambda_{sd}}))}{(\theta\lambda_3 + \lambda_{sd})\ln 2}[\Phi(\frac{1}{\lambda_3}) - \Phi(\frac{1}{\lambda_{sd}})], \quad (33)$$

where $\Phi(x) = e^x \mathrm{Ei}(-\mathrm{x})$, $\mathrm{Ei}(-x) = -\int_x^\infty e^{-t}t^{-1}dt$, $\theta = 2^{R_s}$, P_{th} is the power threshold for RSS-based mode selection scheme, and R_s is the desirable secrecy rate.

Proof. We know that the secrecy rate $\mathbf{C}_s^c$ is given by

$$\mathbf{C}_s^c = P_{ms}(1-P_{so})\mathbb{E}[C_s^c]. \quad (34)$$

To derive $\mathbf{C}_s^c$, we need to determine P_{ms} and P_{so}. We first determine the probability P_{ms} of selecting cellular mode as

$$P_{ms} = \mathcal{P}\{P_s|h_{s,d}|^2 \ge P_{th}\} = \mathcal{P}\{|h_{s,d}|^2 \ge \frac{P_{th}}{P_s}\}$$
$$= 1 - F_{|h_{s,d}|^2}(\frac{P_{th}}{P_s}) = \exp(-\frac{P_{th}}{P_s d_{s,d}^{-\alpha}}), \quad (35)$$

where $F_{|h_{s,d}|^2}(\cdot)$ is the cumulative density function (CDF) of $|h_{s,d}|^2$. Since $|h_{s,d}|^2$ is an exponentially distributed random variable with mean $d_{s,d}^{-\alpha}$, $F_{|h_{s,d}|^2}(x) = 1 - \exp(-\frac{x}{d_{s,d}^{-\alpha}})$.

Then, we proceed to derive the secrecy outage probability P_{so} under the cellular mode. Since P_{so} equals to the probability that the instantaneous secrecy capacity is less than a threshold R_s. We have

$$P_{so} = \mathcal{P}\{C_s^c < R_s\} = \mathcal{P}\{\log_2(\frac{1+\gamma_{sd}}{1+\gamma_3}) < R_s\} = \mathcal{P}\{\gamma_{sd} < \theta(\gamma_3+1) - 1\}$$
$$\overset{(a)}{=} \int_0^\infty \int_0^{\theta(y+1)-1} f_{\gamma_{sd}}(x) f_{\gamma_3}(y) dxdy \quad (36)$$

where $\theta = 2^{R_s}$, and the process (a) follows due to the fact that γ_{sd} and γ_3 are two independently exponentially distributed random variables with the PDFs $f_{\gamma_{sd}}(x) = \frac{1}{\lambda_{sd}}\exp(-\frac{x}{\lambda_{sd}})$ and $f_{\gamma_3}(y) = \frac{1}{\lambda_3}\exp(-\frac{y}{\lambda_3})$, respectively. By solving (36), P_{so} is obtained as

$$P_{so} = 1 - \frac{\lambda_{sd}}{\theta\lambda_3 + \lambda_{sd}}\exp(-\frac{\theta-1}{\lambda_{sd}}). \quad (37)$$

According to the definition of the instantaneous secrecy rate in (9), by averaging over γ_{sd} and γ_3, we can also determine the expected value of the instantaneous secrecy rate as

$$\mathbb{E}[C_s^c] = \int_0^\infty \int_0^\infty \log_2(\frac{1+x}{1+y}) f_{\gamma_{sd}}(x) f_{\gamma_3}(y) dxdy = \frac{\Phi(\frac{1}{\lambda_3}) - \Phi(\frac{1}{\lambda_{sd}})}{\ln 2} \quad (38)$$

Finally, (33) follows by substituting (35), (37) and (38) into (34). □

We can have an insight from (33) in Theorem 3 that the secrecy rate $\mathbf{C}_s^c$ is 0 when the ratio of the distance between BS and Eve to the power of the additive white Gaussian noise at Eve is the same as that of the distance between BS and UR to the power of the noise at UR, i.e., $\frac{d_{s,e}^{-\alpha}}{\sigma_e^2} = \frac{d_{s,d}^{-\alpha}}{\sigma_d^2}$. This means that the same SNRs at UR and Eve lead to a secrecy rate of zero.

4.2.2 Secrecy Rate Optimization

The objective of the BS is to maximize the secrecy rate $\mathbf{C}_s^c$ by optimizing its transmit power P_s, which can be formulated as

$$\max_{P_s} \quad \mathbf{C}_s^c \quad (39a)$$
$$\text{s.t.} \quad 0 \le P_s \le P_s^{\max}, \quad (39b)$$

where the constraint in (39b) represents that P_s is subject to a maximum transmit power $P_s^{\max}$.

The optimal solution of (39) is given in the following theorem.

Theorem 4. *Under the cellular mode, we use P_s^{c*} to represent the optimal transmit power at BS. When $P_s^{c*} \leq P_s^{\max}$, it can be implicitly expressed as*

$$\frac{d_{s,e}^{\alpha}\sigma_e^2 - d_{s,d}^{\alpha}(P_{th}+(\theta-1)\sigma_d^2)}{d_{s,d}^{\alpha}\sigma_d^2 - d_{s,d}^{\alpha}(P_{th}+(\theta-1)\sigma_d^2)} = \frac{\Phi(\frac{d_{s,d}^{\alpha}\sigma_d^2}{P_s^{c*}})}{\Phi(\frac{d_{s,e}^{\alpha}\sigma_e^2}{P_s^{c*}})}, \tag{40}$$

where $\Phi(.)$ is defined in Theorem 3, $\theta = 2^{R_s}$. Otherwise, $P_s^{c*} = P_s^{\max}$. For a special case $d_{s,e} = d_{s,d} = d$, (40) in Theorem 4 can be simply written as

$$\frac{\sigma_e^2 - P_{th} - (\theta-1)\sigma_d^2}{(2-\theta)\sigma_d^2 - P_{th}} = \frac{\Phi(\frac{d^{\alpha}\sigma_d^2}{P_s^{c*}})}{\Phi(\frac{d^{\alpha}\sigma_e^2}{P_s^{c*}})}. \tag{41}$$

Proof. To solve the optimization problem in (39), we first take the derivation of $\mathbf{C}_s^c$ with respect to P_s, which is given by

$$\frac{\partial \mathbf{C}_s^c}{\partial P_s} = -\frac{d_{s,d}^{-\alpha}\sigma_e^2 \exp(-\frac{P_{th}+(\theta-1)\sigma_d^2}{P_s d_{s,d}^{-\alpha}})}{(\theta d_{s,e}^{-\alpha}\sigma_d^2 + d_{s,d}^{-\alpha}\sigma_e^2)P_s^2 \ln 2}\Bigg[\Big(\frac{\sigma_e^2}{d_{s,e}^{-\alpha}} - \frac{P_{th}+(\theta-1)\sigma_d^2}{d_{s,d}^{-\alpha}}\Big) \times \Phi\Big(\frac{d_{s,e}^{\alpha}\sigma_e^2}{P_s}\Big) - \frac{(2-\theta)\sigma_d^2 - P_{th}}{d_{s,d}^{-\alpha}}\Phi\Big(\frac{d_{s,d}^{\alpha}\sigma_d^2}{P_s}\Big)\Bigg]. \tag{42}$$

We know from (42) that if $(\frac{\sigma_e^2}{d_{s,e}^{-\alpha}} - \frac{P_{th}+(\theta-1)\sigma_d^2}{d_{s,d}^{-\alpha}})\Phi(\frac{d_{s,e}^{\alpha}\sigma_e^2}{P_s}) \leq \frac{(2-\theta)\sigma_d^2 - P_{th}}{d_{s,d}^{-\alpha}}\Phi(\frac{d_{s,d}^{\alpha}\sigma_d^2}{P_s})$, $\frac{\partial \mathbf{C}_s^c}{\partial P_s} \geq 0$, and thus $\mathbf{C}_s^c$ increases with P_s. Otherwise, $\frac{\partial \mathbf{C}_s^c}{\partial P_s} < 0$, and thus $\mathbf{C}_s^c$ decreases with P_s. Based on this observation, we can obtain the optimal transmit power P_s^{c*} by solving $\frac{\partial \mathbf{C}_s^c}{\partial P_s} = 0$ if (39b) holds. Otherwise, if the solution of $\frac{\partial \mathbf{C}_s^c}{\partial P_s} = 0$ is greater than $P_s^{\max}$, $\mathbf{C}_s^c$ is an increasing function over the interval $[0, P_s^{\max}]$. Thus, $P_s^{c*} = P_s^{\max}$. □

4.3 Secrecy Rate under the Underlay Mode

Under the underlay mode, we first model the average secrecy rates with and without covert message transmission at UR, respectively. We then explore the optimization of secrecy rate.

4.3.1 Secrecy Rate Modeling

According to the definition of the secrecy rate $\mathbf{C}_s^u$, we have

$$\mathbf{C}_s^u = P_{\mathrm{H}_0}\mathbf{C}_s^{u0} + P_{\mathrm{H}_1}\mathbf{C}_s^{u1}, \tag{43}$$

where $\mathbf{C}_s^{u0}$ and $\mathbf{C}_s^{u1}$ are the average secrecy rates when H_0 and H_1 are true, respectively. We need to determine $\mathbf{C}_s^{u0}$ and $\mathbf{C}_s^{u1}$.

a) UR's Transmission Without Covert Message: In the following theorem, we model the average secrecy rate without the transmission of covert message at UR (i.e., H_0 is true).

Theorem 5. *We use $\overline{C}_s^{u0}$ to denote the expected value of the instantaneous secrecy rate, and use P_{sop}^{u0} to denote the secrecy outage probability. Then, $\mathbf{C}_s^{u0} = (1-\exp(-\frac{P_{th}}{P_s d_{s,d}^{-\alpha}}))(1-P_{sop}^{u0})\overline{C}_s^{u0}$, where*

$$\overline{C}_s^{u0} = \frac{\lambda_1\lambda_4}{(\lambda_1-\lambda_r)\ln 2}\Bigg\{\frac{\Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_{sd}}) - \Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_4})}{\lambda_4-\lambda_{sd}} - \frac{\lambda_r}{\lambda_4\lambda_r - \lambda_1\lambda_{sd}} \times \Big[\Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_{sd}}) - \Phi(\frac{\lambda_1+\lambda_4}{\lambda_4\lambda_r})\Big]\Bigg\} - \frac{\lambda_3\Phi(\frac{1}{\lambda_3}) - \lambda_2\Phi(\frac{1}{\lambda_2})}{(\lambda_2-\lambda_3)\ln 2}, \tag{44}$$

and

$$P_{sop}^{u0} = 1 - \frac{\lambda_1\lambda_4}{\theta(\lambda_2-\lambda_3)(\lambda_4\lambda_r - \lambda_1\lambda_{sd})}\Bigg\{\exp\Big(\frac{\theta-1}{\theta\lambda_2}\Big) \times \Big[\Psi\Big(\omega_1\frac{\lambda_1\lambda_4+\theta\lambda_2(\lambda_1+\lambda_4)}{\theta\lambda_1\lambda_2\lambda_{sd}}\Big) - \Psi\Big(\omega_2\frac{\lambda_1\lambda_4+\theta\lambda_2(\lambda_1+\lambda_4)}{\theta\lambda_2\lambda_4\lambda_r}\Big)\Big] - \exp\Big(\frac{\theta-1}{\theta\lambda_3}\Big)\Big[\Psi\Big(\frac{\omega_1(\lambda_1\lambda_4+\theta\lambda_3(\lambda_1+\lambda_4))}{\theta\lambda_1\lambda_3\lambda_{sd}}\Big) - \Psi\Big(\frac{\omega_2(\lambda_1\lambda_4+\theta\lambda_3(\lambda_1+\lambda_4))}{\theta\lambda_3\lambda_4\lambda_r}\Big)\Big]\Bigg\}. \tag{45}$$

Here, $\theta = 2^{R_s}$, $\Psi(\omega x) = e^x\mathrm{Ei}(-\omega x)$, $\omega_1 = 1 + \frac{\lambda_{sd}(\theta-1)}{\lambda_4}$, and $\omega_2 = 1 + \frac{\lambda_r(\theta-1)}{\lambda_1}$.

Proof. Based on the definition of average secrecy rate, we have $\mathbf{C}_s^{u0} = (1-P_{ms})(1-P_{sop}^{u0})\overline{C}_s^{u0}$. To obtain $\mathbf{C}_s^{u0}$, we need to determine the expected value of the instantaneous secrecy rate $\overline{C}_s^{u0}$ and secrecy outage probability P_{sop}^{u0}. According to their definitions, we have

$$\overline{C}_s^{u0} = \mathbb{E}_{\mathrm{SINR}_{\mathrm{UE}}^{u0},\mathrm{SINR}_e^{u0}}[C_s^{u0}], \tag{46}$$

and

$$P_{sop}^{u0} = \mathcal{P}\{\log_2(1+\mathrm{SINR}_{\mathrm{UE}}^{u0}) - \log_2(1+\mathrm{SINR}_e^{u0}) < R_s\}. \tag{47}$$

We note that before solving $\overline{C}_s^{u0}$ and P_{sop}^{u0} of the main channel, we first need to determine the PDFs of $\mathrm{SINR}_{\mathrm{UE}}^{u0}$ and SINR_e^{u0}. Let $X = \mathrm{SINR}_{\mathrm{UE}}^{u0} = \min\{\frac{\gamma_1}{\gamma_r+1}, \frac{\gamma_4}{\gamma_{sd}+1}\}$, $Y = \mathrm{SINR}_e^{u0} = \gamma_2 + \gamma_3$. The CDF of X can be determined as

$$\begin{aligned} F_X(x) &= \mathcal{P}\{X \leq x\} = \mathcal{P}\{\min\{\frac{\gamma_1}{\gamma_r+1}, \frac{\gamma_4}{\gamma_{sd}+1}\} \leq x\} \\ &= 1 - \mathcal{P}\{\min\{\frac{\gamma_1}{\gamma_r+1}, \frac{\gamma_4}{\gamma_{sd}+1}\} > x\} \\ &\overset{(b)}{=} 1 - \mathcal{P}\{\frac{\gamma_1}{\gamma_r+1} > x\}\mathcal{P}\{\frac{\gamma_4}{\gamma_{sd}+1} > x\} \\ &\overset{(c)}{=} 1 - \frac{\lambda_1\lambda_4}{(\lambda_1+x\lambda_4)(\lambda_4+x\lambda_{sd})}\exp(-\frac{(\lambda_1+\lambda_4)x}{\lambda_1\lambda_4}), \end{aligned} \tag{48}$$

and that of Y is determined as

$$\begin{aligned} F_Y(y) &= \mathcal{P}\{\gamma_2+\gamma_3 \leq y\} = \mathcal{P}\{\gamma_2 \leq y-\gamma_3\} \\ &= \mathcal{P}\{\gamma_2 \leq y-\gamma_3, \gamma_3 \leq y\} + \mathcal{P}\{\gamma_2 \leq y-\gamma_3, \gamma_3 > y\} \\ &= \mathcal{P}\{\gamma_2 \leq y-\gamma_3, \gamma_3 \leq y\} = \int_0^y F_{\gamma_2}(y-\gamma_3)f_{\gamma_3}(x)dx \\ &\overset{(d)}{=} 1 + \frac{\lambda_3}{\lambda_2-\lambda_3}\exp(-\frac{y}{\lambda_3}) - \frac{\lambda_2}{\lambda_2-\lambda_3}\exp(-\frac{y}{\lambda_2}), \end{aligned} \tag{49}$$

where $F_{\gamma_2}(\cdot)$ denotes the CDF of γ_2 and $f_{\gamma_3}(\cdot)$ denotes the PDF of γ_3. (b) follows from the theorem of probability distribution of minimization operation, (c) follows based on the property that γ_1, γ_r, γ_4 and γ_{sd} are independent exponentially distributed random variables, and (d) follows from the substitution of the CDF $F_{\gamma_2}(\cdot)$ of γ_2 and PDF $f_{\gamma_3}(\cdot)$ of γ_3.

By calculating the derivatives of $F_X(x)$ and $F_Y(y)$ with respect to x and y, we obtain the PDFs of $\mathrm{SINR}_{\mathrm{UE}}^{u0}$ and SINR_e^{u0} as

$$f_X(x)=\frac{\exp(-\frac{(\lambda_1+\lambda_4)x}{\lambda_1\lambda_4})\left[\lambda_1\lambda_4(\frac{\lambda_r}{\lambda_1+x\lambda_r}+\frac{\lambda_{sd}}{\lambda_4+x\lambda_{sd}})+\lambda_1+\lambda_4\right]}{(\lambda_1+x\lambda_r)(\lambda_4+x\lambda_{sd})} \tag{50}$$

and

$$f_Y(y)=\frac{\exp(-\frac{1}{\lambda_2})-\exp(-\frac{1}{\lambda_3})}{\lambda_2-\lambda_3}. \tag{51}$$

Therefore, we have

$$\begin{aligned}\overline{C}_s^c &= \mathbb{E}_{\mathrm{SINR}_{\mathrm{UE}}^{u0},\mathrm{SINR}_e^{u0}}[\log_2(1+\mathrm{SINR}_{\mathrm{UE}}^{u0})-\log_2(1+\mathrm{SINR}_e^{u0})]\\ &= \mathbb{E}_{\mathrm{SINR}_{\mathrm{UE}}^{u0}}[\log_2(1+\mathrm{SINR}_{\mathrm{UE}}^{u0})]-\mathbb{E}_{\mathrm{SINR}_e^{u0}}[\log_2(1+\mathrm{SINR}_e^{u0})]\\ &= \int_0^\infty \log_2(1+X)f_X(x)dx-\int_0^\infty \log_2(1+Y)f_Y(y)dy. \end{aligned}\tag{52}$$

Substituting (50) and (51) into (52) and calculating the integrations in (52), we obtain the expected value of the instantaneous secrecy rate in (44).

According to (47), we further determine the secrecy outage probability as

$$\begin{aligned}P_{sop}^{u0} &= \mathcal{P}\{\log_2(\frac{1+\mathrm{SINR}_{\mathrm{UE}}^{u0}}{1+\mathrm{SINR}_e^{u0}})<R_s\}=\mathcal{P}\{\log_2(\frac{1+X}{1+Y})<R_s\}\\ &= \mathcal{P}\{X<\theta(1+Y)-1\}\\ &\overset{(e)}{=} \int_0^\infty F_X(\theta(1+y)-1)f_Y(y)dy, \end{aligned}\tag{53}$$

where $\theta=2^{R_s}$, $X=\mathrm{SINR}_{\mathrm{UE}}^{u0}$, $Y=\mathrm{SINR}_e^{u0}$, and (e) follows utilizing the CDF $F_X(\cdot)$ of X and PDF $f_Y(\cdot)$ of Y. By substituting (48) and (51) into (53), we obtain the secrecy outage probability in (45).

Based on (44) and (45), the average secrecy rate $\mathbf{C}_s^{u0}$ follows. □

b) UR's Transmission With Covert Message: In the following theorem, we model the average secrecy rate with the transmission of covert message at UR (i.e., H_1 is true).

Theorem 6. *Under the underlay mode, we use $\mathbf{C}_s^{u1}$ to denote the average secrecy rate when H_1 is true. Then, we have $\mathbf{C}_s^{u1}=(1-\exp(-\frac{P_{th}}{P_s d_{s,d}^{-\alpha}}))(1-P_{sop}^{u1})\overline{C}_s^{u1}$, where $\overline{C}_s^{u1}$ is the expected value of the instantaneous secrecy rate and P_{sop}^{u1} is the secrecy outage probability, which are given by*

$$\begin{aligned}\overline{C}_s^{u1} &= \frac{\lambda_1\lambda_4^2}{\ln 2}\Lambda(x)-\frac{1}{(\lambda_2-\lambda_3)\ln 2}\Bigg[\frac{\lambda_3^2}{\lambda_3-\lambda_6}\left(\Phi\left(\frac{1}{\lambda_3}\right)\right.\\ &\left.-\Phi\left(\frac{1}{\lambda_6}\right)\right)-\frac{\lambda_2^2}{\lambda_2-\lambda_6}\left(\Phi\left(\frac{1}{\lambda_2}\right)-\Phi\left(\frac{1}{\lambda_6}\right)\right)\Bigg]\end{aligned}\tag{54}$$

and

$$\begin{aligned}P_{sop}^{u1} &= 1-\frac{\lambda_1\lambda_4^2\exp(\frac{1}{\lambda_6})}{\lambda_6(\lambda_2-\lambda_3)}\Bigg\{\left(\frac{\lambda_5}{\lambda_4(\lambda_5-\lambda_{sd})}-\frac{\lambda_r^1}{\lambda_4\lambda_r^1-\lambda_1\lambda_{sd}}\right)\\ &\times\exp\left(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_{sd}}\right)[\Theta(a_1,b_1,c_1;x)-\Theta(a_4,b_1,c_4;x)]\\ &+\frac{\lambda_5\exp\left(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_5}\right)}{\lambda_4(\lambda_5-\lambda_{sd})}[\Theta(a_5,b_2,c_5;x)-\Theta(a_2,b_2,c_2;x)]\\ &+\frac{\lambda_r^1\exp\left(\frac{\lambda_1+\lambda_4}{\lambda_4\lambda_r^1}\right)}{\lambda_4\lambda_r^1-\lambda_1\lambda_{sd}}[\Theta(a_3,b_3,c_3;x)-\Theta(a_6,b_3,c_6;x)]\Bigg\},\end{aligned}\tag{55}$$

where $\Lambda(x)=\int_0^\infty\frac{1}{1+x}\frac{\exp(-\frac{(\lambda_1+\lambda_4)x}{\lambda_1\lambda_4})}{(\lambda_1+x\lambda_r^1)(\lambda_4+x\lambda_5)(\lambda_4+x\lambda_{sd})}dx$, $\Theta(a,b,c;x)=\int_1^\infty xe^{cx}\mathrm{Ei}(-(ax+b))dx$,

$$\begin{aligned}&a_1=\frac{\lambda_4+\lambda_{sd}(\theta-1)}{\theta\lambda_2\lambda_{sd}}, b_1=\frac{(\lambda_1+\lambda_4)(\lambda_4+\lambda_{sd}(\theta-1))}{\lambda_1\lambda_4\lambda_{sd}},\\ &c_1=\frac{\lambda_6\lambda_{sd}(\theta-1)-\theta\lambda_2\lambda_{sd}+\lambda_4\lambda_6}{\theta\lambda_2\lambda_6\lambda_{sd}}, a_2=\frac{\lambda_4+\lambda_5(\theta-1)}{\theta\lambda_2\lambda_5},\\ &b_2=\frac{(\lambda_1+\lambda_4)(\lambda_4+\lambda_5(\theta-1))}{\lambda_1\lambda_4\lambda_5}, c_2=\frac{\lambda_6\lambda_5(\theta-1)-\theta\lambda_2\lambda_5+\lambda_4\lambda_6}{\theta\lambda_2\lambda_6\lambda_5},\\ &a_3=\frac{\lambda_1+\lambda_r^1(\theta-1)}{\theta\lambda_2\lambda_r^1}, b_3=\frac{(\lambda_1+\lambda_4)(\lambda_1+\lambda_r^1(\theta-1))}{\lambda_1\lambda_4\lambda_r^1},\\ &c_3=\frac{\lambda_6\lambda_r^1(\theta-1)-\theta\lambda_2\lambda_r^1+\lambda_1\lambda_6}{\theta\lambda_2\lambda_6\lambda_r^1}, a_4=\frac{\lambda_4+\lambda_{sd}(\theta-1)}{\theta\lambda_3\lambda_{sd}},\\ &c_4=\frac{\lambda_6\lambda_{sd}(\theta-1)-\theta\lambda_3\lambda_{sd}+\lambda_4\lambda_6}{\theta\lambda_3\lambda_6\lambda_{sd}}, a_5=\frac{\lambda_4+\lambda_5(\theta-1)}{\theta\lambda_3\lambda_5},\\ &c_5=\frac{\lambda_6\lambda_5(\theta-1)-\theta\lambda_3\lambda_5+\lambda_4\lambda_6}{\theta\lambda_3\lambda_6\lambda_5}, a_6=\frac{\lambda_1+\lambda_r^1(\theta-1)}{\theta\lambda_3\lambda_r^1},\\ &c_6=\frac{\lambda_6\lambda_r^1(\theta-1)-\theta\lambda_3\lambda_r^1+\lambda_1\lambda_6}{\theta\lambda_3\lambda_6\lambda_r^1}, \theta=2^{R_s}.\end{aligned}$$

Proof. According to the definition of the average secrecy rate, we need to determine the expected value of the instantaneous secrecy rate $\overline{C}_s^{u1}$ and the secrecy outage probability P_{sop}^{u1}, which are formulated as $\overline{C}_s^{u1}=\mathbb{E}[C_s^{u1}]$ and $P_{sop}^{u1}=\mathcal{P}\{C_s^{u1}<R_s\}$.

According to the formula of C_s^{u1} in (13) and those of $\mathrm{SINR}_{\mathrm{UE}}^{u1}$ and SINR_e^{u1}, let $Z=\min\{\frac{\gamma_1}{\gamma_r^1+1},\frac{\gamma_4}{\gamma_5+\gamma_{sd}+1}\}$ and $Y=\gamma_2+\gamma_3$, we now determine $\overline{C}_s^{u1}$ as

$$\begin{aligned}\overline{C}_s^{u1} &= \mathbb{E}_{Z,Y,\gamma_6}[\log_2(1+Z)-\log_2(1+\frac{Y}{\gamma_6+1})]\\ &= \mathbb{E}_Z[\log_2(1+Z)]-\mathbb{E}_{Y,\gamma_6}[\log_2(1+\frac{Y}{\gamma_6+1})]\\ &= \int_0^\infty\log_2(1+Z)F_Z^{'}(z)dz\\ &-\int_0^\infty\int_0^\infty\log_2(1+\frac{Y}{\gamma_6+1})f_Y(y)f_{\gamma_6}(\gamma_6)dyd\gamma_6,\end{aligned}\tag{56}$$

where $F_Z(z)$ is the CDF of Z, which will be given later, $F_Z^{'}(z)$ denotes the derivation of $F_Z(z)$ with respect to the random variable Z, $f_Y(y)$ is given in (51), γ_6 is the exponentially distributed random variable with mean λ_6, $f_{\gamma_6}(\gamma_6)=\frac{1}{\lambda_6}\exp(-\frac{\gamma_6}{\lambda_6})$, and the CDF $F_Z(z)$ of Z can be expressed as

$$\begin{aligned}F_Z(z) &= \mathcal{P}\{Z\le z\}=\mathcal{P}\{\min\{\frac{\gamma_1}{\gamma_r^1+1},\frac{\gamma_4}{\gamma_5+\gamma_{sd}+1}\}\le z\}\\ &= 1-\mathcal{P}\{\min\{\frac{\gamma_1}{\gamma_r^1+1},\frac{\gamma_4}{\gamma_5+\gamma_{sd}+1}\}>z\}\\ &\overset{(b)}{=} 1-\mathcal{P}\{\frac{\gamma_1}{\gamma_r^1+1}>z\}\mathcal{P}\{\frac{\gamma_4}{\gamma_5+\gamma_{sd}+1}>z\}\end{aligned}\tag{57}$$

$$\overset{(c)}{=} 1-\frac{\lambda_1\lambda_4^2\exp(-\frac{(\lambda_1+\lambda_4)z}{\lambda_1\lambda_4})}{(\lambda_1+z\lambda_r^1)(\lambda_4+z\lambda_5)(\lambda_4+z\lambda_{sd})},\tag{58}$$

where (b) and (c) follow the process in (48).

With the definition of secrecy outage probability, we proceed to determine P_{sop}^{u1} as

$$\begin{aligned}P_{sop}^{u1} &= \mathcal{P}\left\{\log_2\left(\frac{1+Z}{1+\frac{Y}{\gamma_6+1}}\right)<R_s\right\}\\ &= \mathcal{P}\{z<\theta(1+\frac{y}{\gamma_6+1})-1\}\\ &= \int_0^\infty\int_0^\infty F_Z(\theta(1+\frac{y}{\gamma_6+1})-1)f_Y(y)f_{\gamma_6}(\gamma_6)dyd\gamma_6.\end{aligned}\tag{59}$$

By solving (56) and (59), we can obtain $\mathbf{C}_s^{u1}$. □

4.3.2 Secrecy Rate Maximization

From the perspective of BS, its goal is to maximize the secrecy rate $\mathbf{C}_s^u$ subject to the transmit power P_s and detection requirement at BS.

$$\max_{P_s} \quad \mathbf{C}_s^u, \tag{60a}$$
$$\text{s.t.} \quad \mathbf{P}_{min}^{u*} \geq \xi, \tag{60b}$$
$$0 \leq P_s \leq P_s^{\max}, \tag{60c}$$

where constraint (60b) represents the detection requirement at BS that a minimum detection probability $\mathbf{P}_{min}^{u*}$ at BS is not less than a threshold ξ, and constraint (60c) represents the range of transmission power P_s at BS. Note that $\mathbf{P}_b^{u*}$ is a function of the transmit powers P_r and P_c. Since BS can control the transmit power P_r, it can maximize $\mathbf{P}_b^{u*}$ by optimizing P_r. Meanwhile, it does not know the covert transmission power P_c at UR, and thus it considers a worst case to minimize the maximum $\mathbf{P}_b^{u*}$ by setting P_c. The $\mathbf{P}_{min}^{u*}$ at BS corresponds to the optimal value of the following optimization problem

$$\min_{P_c} \max_{P_r} \quad \mathbf{P}_b^{u*}, \tag{61a}$$
$$\text{s.t.} \quad 0 \leq P_r \leq P_r^{\max}, \tag{61b}$$
$$0 \leq P_c \leq P_c^{\max}, \tag{61c}$$

where constraints (61b) and (61c) represent the range of transmission powers P_r and P_c. For the complex objective functions, it is generally difficult to obtain their closed-form solution. Alternatively, a two-dimensional search over (P_r, P_c) is used to find the optimal solution of (61). With the minimum $\mathbf{P}_{min}^{u*}$, the optimization problem of (60) can be solved using a Newtons method summarized in Algorithm 1. Here, the objective function $\mathbf{C}_s^u$ is the function of P_s denoted by $\mathbf{C}_s^u(P_s)$. $\mathbf{C}_s^{u'}$ denotes the derivative of $\mathbf{C}_s^u$ with respect to P_s, which is also the function of P_s denoted by $\mathbf{C}_s^{u'}(P_s)$. $\mathbf{C}_s^u(P_s^0)$ and $\mathbf{C}_s^{u'}(P_s^0)$ are the values of instituting the initial transmit power P_s into $\mathbf{C}_s^u(\cdot)$ and $\mathbf{C}_s^{u'}(\cdot)$, respectively. P_s^* and $\mathbf{C}_s^{u*}$ denote the optimal transmit power of BS and the corresponding maximum secrecy rate, respectively.

Algorithm 1: Secrecy Rate Maximization

Input: R_s, σ_d^2, σ_e^2, σ_r^2, P_{th}, $d_{s,d}$, $d_{s,e}$, $d_{s,r}$, $d_{r,r}$, $d_{r,e}$, $d_{r,d}$, ϕ, α, $P_s^{\max}$, ε;
Output: P_s^*, $\mathbf{C}_s^{u*}$;
Initialization: The transmit power of BS $P_s^0 = 0$;
Calculate $P_s \cdot (-C_s^{u'}(P_s^0)) + (-C_s^u(P_s^0)) - P_s^0 \cdot (-C_s^{u'}(P_s^0)) = 0$, we can obtain a P_s^i;
for $i \leq 1000$;
  if $P_s^i \leq P_s^{\max}$ then
    Substitute P_s^i into P_{min}^{u*}
      if $P_{min}^{u*} \geq \varepsilon$
        $P_s^{i+1} = P_s^i - \frac{C_s^u(P_s^i)}{C_s^{u'}(P_s^i)}$;
        $i = i + 1$;
      else $\mathbf{C}_s^{u*} = 0$;
  $\mathbf{C}_s^{u*} = 0$;
end for
output $P_s^* = P_s^i$, $\mathbf{C}_s^{u*} = C_s^u(P_s^i)$;

4.4 Secrecy Rate under the Overlay Mode

Under the overlay mode, we first model the average secrecy rates under these two cases with/without covert message transmitted by UR. We further optimize the secrecy rate from the perspective of BS.

4.4.1 Secrecy Rate Modeling

The secrecy rate $\mathbf{C}_s^o$ under the overlay mode can be modeled as

$$\mathbf{C}_s^o = P_{\mathrm{H}_0}\mathbf{C}_s^{o0} + P_{\mathrm{H}_1}\mathbf{C}_s^{o1}. \tag{62}$$

Here, the unknown average secrecy rates $\mathbf{C}_s^{o0}$ and $\mathbf{C}_s^{o1}$ under H_0 and H_1 are given in the following theorems.

a) UR's Transmission Without Covert Message: In the following theorem, we model the average secrecy rate without the transmission of covert message at UR (i.e.,H_0 is true).

Theorem 7. *Under the overlay mode, we use $\mathbf{C}_s^{o0}$ to denote the average secrecy rate when H_0 is true. Then, we have $\mathbf{C}_s^{o0} = (1 - \exp(-\frac{P_{th}}{P_s d_{s,d}^{-\alpha}}))(1 - P_{sop}^{o0})\overline{C}_s^{o0}$, where $\overline{C}_s^{o0}$ is the expected value of the instantaneous secrecy rate and P_{sop}^{o0} is the secrecy outage probability, which are given by*

$$\overline{C}_s^{o0} = \frac{\lambda_2\Phi(\frac{1}{\lambda_2}) - \lambda_3\Phi(\frac{1}{\lambda_3}) + (\lambda_3 - \lambda_2)\Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_4})}{2(\lambda_2 - \lambda_3)\ln 2}, \tag{63}$$

and

$$P_{sop}^{o0} = 1 - \frac{1}{\lambda_2 - \lambda_3}\exp\left(-\frac{(\lambda_1+\lambda_4)(\eta-1)}{\lambda_1\lambda_4}\right) \left[\frac{\lambda_1\lambda_2\lambda_4}{\eta\lambda_2(\lambda_1+\lambda_4)+\lambda_1\lambda_4} - \frac{\lambda_1\lambda_3\lambda_4}{\eta\lambda_3(\lambda_1+\lambda_4)+\lambda_1\lambda_4}\right], \tag{64}$$

where $\eta = 2^{2R_s}$.

Proof. To determine $\mathbf{C}_s^{o0}$, we need to obtain $\overline{C}_s^{o0}$ and P_{sop}^{o0}, which are expressed as $\overline{C}_s^{o0} = \mathbb{E}[C_s^{o0}]$ and $P_{sop}^{o0} = \mathcal{P}\{C_s^{o0} < R_s\}$.

To this end, according to the formula of C_s^{o0} in (18), we first need to determine the PDF of $\mathrm{SINR}_{\mathrm{UE}}^{o0}$. Let $Z' = \mathrm{SINR}_{\mathrm{UE}}^{o0} = \min\{\gamma_1, \gamma_4\}$, the CDF of Z' can be calculated as

$$F_{Z'}(z') = \mathcal{P}\{\min\{\gamma_1,\gamma_4\} \leq z'\} = 1 - \mathcal{P}\{\min\{\gamma_1,\gamma_4\} > z'\} = 1 - \mathcal{P}\{\gamma_1 > z'\}\mathcal{P}\{\gamma_4 > z'\} = 1 - \exp\left(-\frac{(\lambda_1+\lambda_4)z'}{\lambda_1\lambda_4}\right). \tag{65}$$

Therefore, we determine the PDF $f_{Z'}(z)$ of $\mathrm{SINR}_{\mathrm{UE}}^{o0}$ as

$$f_{Z'}(z') = \frac{\partial F_{Z'}(z')}{\partial z'} = \frac{\lambda_1+\lambda_4}{\lambda_1\lambda_4}\exp\left(-\frac{(\lambda_1+\lambda_4)z'}{\lambda_1\lambda_4}\right). \tag{66}$$

We now determine $\overline{C}_s^{o0}$ as

$$\overline{C}_s^{o0} = \mathbb{E}_{\mathrm{SINR}_{\mathrm{UE}}^{o0},\mathrm{SNR}_e^{o0}}[C_s^{o0}] = \mathbb{E}_{Z',Y}\left[\frac{1}{2}\log_2\left(\frac{1+Z'}{1+Y}\right)\right] = \int_0^\infty\int_0^\infty \frac{1}{2}\log_2\left(\frac{1+z'}{1+y}\right) f_{Z'}(z')f_Y(y)dz'dy, \tag{67}$$

where $f_Y(y)$ is given in (51).

We can obtain $\overline{C}_s^{o0}$ in (63) by solving (67). We continue to determine P_{sop}^{o0} as

$$P_{sop}^{o0} = \mathcal{P}\left\{\frac{1}{2}\log_2\left(\frac{1+z^{'}}{1+y}\right) < R_s\right\} = \mathcal{P}\{z^{'} < \eta(1+y)-1\}$$
$$= \int_0^{\infty} F_{Z^{'}}(\eta(1+y)-1) f_Y(y) dy \quad (68)$$

where $F_{Z^{'}}(\cdot)$ is the CDF of $Z^{'}$ given in (65) and $f_Y(y)$ is the PDF of random variable $Y = \text{SINR}_e^{u0}$ given in (51). By solving (68), (64) follows. Finally, we can obtain $\mathbf{C}_s^{o0}$ based on (63) and (64). □

b) UR's Transmission With Covert Message: In the following theorem, we model the average secrecy rate with the transmission of covert message at UR (i.e., H_1 is true).

Theorem 8. *Under the overlay mode, we use $\mathbf{C}_s^{o1}$ to denote the average secrecy rate when H_1 is true. Then, we have $\mathbf{C}_s^{o1} = (1-\exp(-\frac{P_{th}}{P_s d_{s,d}^{-\alpha}}))(1-P_{sop}^{o1})\overline{C}_s^{o1}$, where $\overline{C}_s^{o1}$ is the expected value of the instantaneous secrecy rate and P_{sop}^{o1} is the secrecy outage probability, which are given by*

$$\overline{C}_s^{o1} = \frac{\Phi(\frac{1}{\lambda_3})}{2\ln 2} + \frac{\lambda_4(\Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_5}) - \Phi(\frac{\lambda_1+\lambda_4}{\lambda_1\lambda_4}))}{2(\lambda_4-\lambda_5)\ln 2}$$
$$- \frac{\lambda_2[\exp(\frac{\lambda_3-\lambda_2}{\lambda_3\lambda_6})\Upsilon(\kappa_1 x+\varphi_1) + \Phi(\frac{1}{\lambda_3})\Phi(\frac{\lambda_3-\lambda_2}{\lambda_3\lambda_6})]}{2\lambda_3\lambda_6\ln 2}, \quad (69)$$

and

$$P_{sop}^{o1} = 1 - \frac{\lambda_4}{\lambda_3\lambda_5\lambda_6\eta}\exp\left(\frac{\lambda_6(\lambda_1+\lambda_4)+\lambda_1\lambda_5}{\lambda_1\lambda_5\lambda_6}\right)$$
$$\times\left\{\frac{e^{-c}\mathrm{Ei}(-(a+b)) - e^{\frac{bc}{a}}\mathrm{Ei}(-(a+c)(1+\frac{b}{a}))}{c}\right.$$
$$+\frac{\lambda_2\exp\left(-\left(\frac{\eta(\lambda_1+\lambda_4)(\lambda_4-\lambda_5+\lambda_5\eta)}{\lambda_1\lambda_4\lambda_5\eta}+\frac{\lambda_2}{\lambda_3\lambda_6}\right)\right)}{\lambda_3^2}$$
$$\left.\times\Upsilon(\kappa_2 x+\varphi_2) - \rho(\lambda_6\exp(-\frac{1}{\lambda_6}) - \frac{\lambda_2}{\lambda_3}\exp(-\frac{\lambda_2}{\lambda_3\lambda_6})\mathrm{Ei}(-\frac{\lambda_3-\lambda_2}{\lambda_3\lambda_6}))\right\}, \quad (70)$$

where $\eta = 2^{2R_s}$, $\Upsilon(\kappa x+\varphi) = \int_{\lambda_3-\lambda_2}^{\infty}\frac{1}{x}\Phi(\kappa x+\varphi)\exp(-\frac{x}{\lambda_3\lambda_6})dx$, $\kappa_1 = \frac{1}{\lambda_2\lambda_3}$, $\varphi_1 = \frac{1}{\lambda_3}$, $\kappa_2 = \frac{\lambda_4-\lambda_5+\lambda_5\eta}{\lambda_2\lambda_3\lambda_5\eta}$, $\varphi_2 = \frac{\lambda_4-\lambda_5+\lambda_5\eta}{\lambda_5\eta}(\frac{\eta(\lambda_1+\lambda_4)}{\lambda_1\lambda_4}+\frac{1}{\lambda_3})$, $a = \frac{\lambda_4-\lambda_5+\lambda_5\eta}{\lambda_2\lambda_5\eta}$, $b = \frac{\eta(\lambda_1+\lambda_4)(\lambda_4-\lambda_5+\lambda_5\eta)}{\lambda_1\lambda_4\lambda_5\eta}$, $c = \frac{1}{\lambda_6} - \frac{\lambda_4-\lambda_5+\lambda_5\eta}{\lambda_2\lambda_5\eta}$, *and* $\rho = \exp(\frac{\lambda_4-\lambda_5+\lambda_5\eta}{\lambda_3\lambda_5\eta})\mathrm{Ei}(-\frac{[\lambda_1\lambda_4+\lambda_3\eta(\lambda_1+\lambda_4)](\lambda_4-\lambda_5+\lambda_5\eta)}{\lambda_1\lambda_3\lambda_4\lambda_5\eta})$.

Proof. Similar to the proof of Theorem 7, we first determine the PDF of $\text{SINR}_{\text{UE}}^{o1}$. Let $Y^{'} = \text{SINR}_{\text{UE}}^{o1} = \min\{\gamma_1, \frac{\gamma_4}{\gamma_6+1}\}$, the CDF of $Y^{'}$ can be calculated as

$$F_{Y^{'}}(y^{'}) = \mathcal{P}\{Y^{'} \le y^{'}\} = \mathcal{P}\{\min\{\gamma_1, \frac{\gamma_4}{\gamma_6+1}\} \le y^{'}\}$$
$$= 1 - \mathcal{P}\{\min\{\gamma_1, \frac{\gamma_4}{\gamma_6+1}\} > y^{'}\}$$
$$= 1 - \mathcal{P}\{\gamma_1 > y^{'}\}\mathcal{P}\{\frac{\gamma_4}{\gamma_6+1} > y^{'}\}$$
$$\overset{(f)}{=} 1 - \frac{\lambda_4}{\lambda_4+\lambda_6 y^{'}}\exp\left(-\frac{(\lambda_1+\lambda_4)y^{'}}{\lambda_1\lambda_4}\right), \quad (71)$$

where (f) follows based on the results that γ_1, γ_4 and γ_6 are independently exponentially distributed random variables with PDFs $f_{\gamma_1}(x) = \frac{1}{\lambda_1}\exp(-\frac{x}{\lambda_1})$, $f_{\gamma_4}(x) = \frac{1}{\lambda_4}\exp(-\frac{x}{\lambda_4})$ and $f_{\gamma_6}(x) = \frac{1}{\lambda_6}\exp(-\frac{x}{\lambda_6})$, respectively.

Then, the PDF of $\text{SINR}_{\text{UE}}^{o1}$ can be obtained as

$$f_{Y^{'}}(y^{'}) = \frac{\partial F_{Y^{'}}(y^{'})}{\partial y^{'}} = \left(\frac{\lambda_4\lambda_6}{\lambda_4+\lambda_6 y^{'}} + \frac{\lambda_1+\lambda_4}{\lambda_1}\right)\frac{\exp(-\frac{(\lambda_1+\lambda_4)y^{'}}{\lambda_1\lambda_4})}{\lambda_4+\lambda_6 y^{'}}. \quad (72)$$

Now, we can determine $\overline{C}_s^{o1}$ as

$$\overline{C}_s^{o1} = \mathbb{E}_{Y^{'},\gamma_3,\gamma_2,\gamma_6}[C_s^{o1}] = \mathbb{E}_{Y^{'},\gamma_3,\gamma_2,\gamma_6}[\frac{1}{2}\log_2(\frac{1+Y^{'}}{1+\gamma_3+\frac{\gamma_2}{\gamma_6+1}})]$$
$$= \int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\frac{1}{2}\log_2(\frac{1+Y^{'}}{1+\gamma_3+\frac{\gamma_2}{\gamma_6+1}})$$
$$\times f_{Y^{'}}(y^{'}) f_{\gamma_2}(\gamma_2) f_{\gamma_3}(\gamma_3) f_{\gamma_6}(\gamma_6) dy^{'} d\gamma_2 d\gamma_3 d\gamma_6 \quad (73)$$

Thus, (69) follows by solving (73).

We continue to determine P_{sop}^{o1} as

$$P_{sop}^{o1} = \mathcal{P}\{C_s^{o1} < R_s\} = \mathcal{P}\{\frac{1}{2}\log_2(\frac{1+y^{'}}{1+\gamma_3+\frac{\gamma_2}{\gamma_6+1}}) < R_s\}$$
$$= \mathcal{P}\{y^{'} < \eta(1+\gamma_3+\frac{\gamma_2}{\gamma_6+1})-1\}$$
$$= \int_0^{\infty}\int_0^{\infty}\int_0^{\infty} F_{Y^{'}}(\eta(1+\gamma_3+\frac{\gamma_2}{\gamma_6+1})-1)$$
$$\times f_{\gamma_2}(\gamma_2) f_{\gamma_3}(\gamma_3) f_{\gamma_6}(\gamma_6) d\gamma_2 d\gamma_3 d\gamma_6 \quad (74)$$

Thus, (70) follows by solving (74).

Based on (69) and (70), we can obtain $\mathbf{C}_s^{o1}$. □

4.4.2 Secrecy Rate Maximization

From the perspective of BS, its goal is to maximize the secrecy rate $\mathbf{C}_s^o$ subject to the transmit power P_s and detection requirement at BS.

Similar to the SRM under the underlay mode, the SRM under the overlay mode can also be formulated as the following optimization problem

$$\max_{P_s} \quad \mathbf{C}_s^o, \quad (75a)$$
$$\text{s.t.} \quad \mathbf{P}_{min}^{o*} \ge \xi \quad (75b)$$
$$0 \le P_s \le P_s^{\max}, \quad (75c)$$

where the minimum detection probability $\mathbf{P}_{min}^{o*}$ at BS is the optimal value of the following optimization problem

$$\min_{P_c}\max_{P_r} \quad \mathbf{P}_b^{o*}, \quad (76a)$$
$$\text{s.t.} \quad 0 \le P_r \le P_r^{\max}, \quad (76b)$$
$$0 \le P_c \le P_c^{\max}. \quad (76c)$$

We can solve the two optimization problems using the same search method as these under the underlay mode.

5 Covert Performance from the Perspective of UR

From the perspective of UR, we explore the modeling and optimization of covert performance under the underlay and overlay modes, respectively.

5.1 Covert Rate under the Underlay Mode

5.1.1 Covert Rate Modeling

For the scenario that UR transmits its own covert message when it forwards message from BS to UE, the covert rate $\overline{R}_c^u$ under the underlay mode can be expressed as

$$\overline{R}_c^u = R_c(1-P_{ms})(1-P_{cop}^u)(1-P_{sop}^{u1}), \tag{77}$$

where R_c is the desirable covert rate from UR to UE, P_{ms} is the probability that UE selects cellular mode, P_{cop}^u is the covert outage probability, and P_{sop}^{u1} is the secrecy outage probability.

In the expression of $\overline{R}_c^u$, the covert outage probability P_{cop}^u is unknown, which can be obtained in the following theorem.

Theorem 9. *Under the underlay mode, the covert outage probability P_{cop}^u of the D2D link from UR to UE can be obtained as follows: If $P_c \geq \mu P_r$, $P_{cop}^u = 1$, where $\mu = 2^{Rc} - 1$; Otherwise,*

$$P_{cop}^u = 1 - \frac{(P_c - \mu P_r) d_{r,d}^{-\alpha} d_{s,d}^{-\alpha}}{\mu P_s d_{s,d}^{-\alpha} + (P_c - \mu P_r) d_{r,d}^{-\alpha}} \exp\left(-\frac{\mu \sigma_d^2}{(P_c - \mu P_r) d_{r,d}^{-\alpha}}\right). \tag{78}$$

Proof. According to the definition of covert outage probability, we have

$$\begin{aligned} P_{cop}^u &= \mathcal{P}\{C_d^u < R_c | \mathrm{H}_1\} = \mathcal{P}\{\log_2(1 + \frac{P_c |h_{r,d}|^2}{P_r |h_{r,d}|^2 + P_s |h_{s,d}|^2 + \sigma_d^2}) < R_c\} \\ &= \mathcal{P}\{(P_c - \mu P_r)|h_{r,d}|^2 < \mu P_s |h_{s,d}|^2 + \mu \sigma_d^2\}, \end{aligned} \tag{79}$$

where $\mu = 2^{Rc} - 1$. We can see from (79) that if $P_c - \mu P_r \leq 0$, $P_{cop}^u = 1$. Otherwise, (79) can be rewritten as

$$\begin{aligned} &\mathcal{P}\{|h_{r,d}|^2 < \frac{\mu P_s |h_{s,d}|^2 + \mu \sigma_d^2}{P_c - \mu P_r}\} \\ &= \int_0^\infty F_{|h_{r,d}|^2}\left(\frac{\mu P_s |h_{s,d}|^2 + \mu \sigma_d^2}{P_c - \mu P_r}\right) f_{|h_{s,d}|^2}(x) dx, \end{aligned} \tag{80}$$

where $F_{|h_{r,d}|^2}(\cdot)$ and $f_{|h_{s,d}|^2}(x)$ are the CDF of $|h_{r,d}|^2$ and the PDF of $|h_{s,d}|^2$, respectively. Recall that $|h_{r,d}|^2$ and $|h_{s,d}|^2$ are exponential distribution variables with means $d_{r,d}^{-\alpha}$ and $d_{s,d}^{-\alpha}$, respectively. Thus, $F_{|h_{r,d}|^2}(x) = 1 - \exp(-\frac{x}{d_{r,d}^{-\alpha}})$, and $f_{|h_{s,d}|^2}(x) = \frac{1}{d_{s,d}^{-\alpha}} \exp(-\frac{x}{d_{s,d}^{-\alpha}})$. By solving (80), (78) follows. □

Then, $\overline{R}_c^u$ is obtained by substituting (35), (55) and (78) into (77).

5.1.2 Covert Rate Maximization

From the perspective of UR, its goal is to maximize the covert rate $\overline{R}_c^u$ by optimizing its transmit power P_c when it forwards secrecy message.

For this purpose, we have the following optimization problem

$$\max_{P_c} \quad \overline{R}_c^u, \tag{81a}$$

$$\text{s.t.} \quad \mathbf{P}_b^{u*} \leq \varepsilon, \tag{81b}$$

$$0 \leq P_c \leq P_c^{\max}. \tag{81c}$$

where (81a) is the objective function of CRM, and the constraint (81b) represents the covertness requirement. Here, ε denotes an arbitrary small positive number. Due to the complex expression of $\overline{R}_c^u$, we use one-dimensional search method over P_c to find the optimal solution.

5.2 Covert Rate under the Overlay Mode

5.2.1 Covert Rate Modeling

According to the definition of covert rate, we have

$$\overline{R}_c^o = R_c(1-P_{ms})(1-P_{cop}^o)(1-P_{sop}^{o1}), \tag{82}$$

where $\overline{R}_c^o$ denotes the covert rate, and P_{cop}^o denotes the covert outage probability. Since P_{cop}^o is unknown, we can obtain it in the following theorem.

Theorem 10. *Under the overlay mode, the covert outage probability P_{cop}^o of the D2D link from UR to UE is determined as follows: If $P_c \leq (\delta - 1)P_r$, $P_{cop}^o = 1$, where $\delta = 2^{2R_c}$; Otherwise,*

$$P_{cop}^o = 1 - \exp\left(-\frac{(\delta - 1)\sigma_d^2 d_{r,d}^{\alpha}}{P_c - (\delta - 1)P_r}\right). \tag{83}$$

Proof. P_{cop}^o under the overlay mode can be formulated as

$$\begin{aligned} P_{cop}^o &= \mathcal{P}\{C_d^o < R_c | \mathrm{H}_1\} = \mathcal{P}\{\frac{1}{2}\log_2(1 + \mathrm{SINR}_c^o) < R_c\} \\ &= \mathcal{P}\{\frac{1}{2}\log_2(1 + \frac{P_c |h_{r,d}|^2}{P_r |h_{r,d}|^2 + \sigma_d^2}) < R_c\} \\ &= \mathcal{P}\{(P_c - (\delta - 1)P_r)|h_{r,d}|^2 < (\delta - 1)\sigma_d^2\} \end{aligned} \tag{84}$$

If $P_c \leq (\delta - 1)P_r$, $P_{cop}^o = 1$. Otherwise, P_{cop}^o can be rewritten as

$$\begin{aligned} P_{cop}^o &= \mathcal{P}\left\{|h_{r,d}|^2 < \frac{(\delta - 1)\sigma_d^2}{P_c - (\delta - 1)P_r}\right\} = F_{|h_{r,d}|^2}\left(\frac{(\delta - 1)\sigma_d^2}{P_c - (\delta - 1)P_r}\right) \\ &= 1 - \exp\left(-\frac{(\delta - 1)\sigma_d^2 d_{r,d}^{\alpha}}{P_c - (\delta - 1)P_r}\right) \end{aligned} \tag{85}$$

□

By substituting (35), (70) and (83) into (82), $\overline{R}_c^o$ follows.

5.2.2 Covert Rate Maximization

From the perspective of UR, its goal is to maximize the covert rate $\overline{R}_c^o$ by optimizing its transmit power P_c when it forwards secrecy message. This can be formulated as the following optimization problem

$$\max_{P_c} \quad \overline{R}_c^o, \tag{86a}$$

$$\text{s.t.} \quad \mathbf{P}_b^{o*} \leq \varepsilon, \tag{86b}$$

$$0 \leq P_c \leq P_c^{\max}. \tag{86c}$$

Similar to the method of solving the optimization problem under the underlay model, we can also use a one-dimensional search over P_c to find the optimal solution of the optimization problem. The optimization algorithms of these optimization problems in (60), (61), (75), (76), (81) and (86) are similar to Algorithm 1.

6 Numerical Results

This section provides extensive numerical results to explore the impacts of system parameters on the performances under various DCS scenarios. We develop a simulator on Matlab to validate our theoretical analysis [43]. In this simulation, we consider a D2D-enabled cellular system, where a BS, an Eve, and two user equipments UE and UR are located in a square area of 500500 m^2. Specifically,

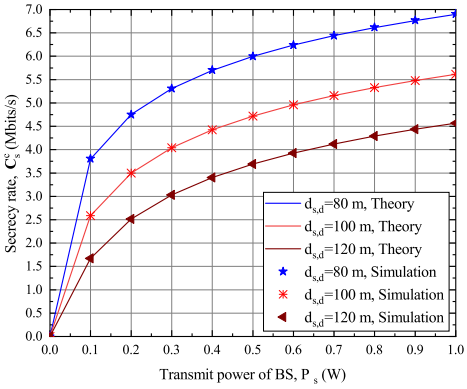

Fig. 2: Secrecy rate vs. P_s under cellular mode.

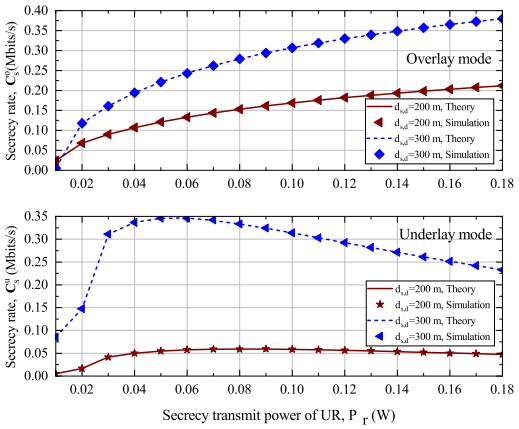

Fig. 3: Secrecy rate vs. P_r under D2D mode.

due to the spectrum sharing under the underlay mode, there exist two types of interference, i.e., self-interference at BS and UR working over full-duplex operation, and mutual interference between the cellular and D2D links. The hardware requirements of the DCS are required as follows. The chips (e.g., RS-485) or protocols (e.g., SCAN, LEGO) are needed to support full-duplex operations at BS and UR. Another is that the radiometer needs to be equipped at BS for detecting covert communication. Additionally, the omnidirectional antenna is deployed at BS and D2D users, respectively. Some parameters used are set as $P_{th} = 1\times e^{-10}$ W, $\sigma_r^2 = 1 \times e^{-10}$ W, $\sigma_e^2 = 1 \times e^{-10}$ W, $\sigma_d^2 = 1 \times e^{-10}$ W, $\sigma_s^2 = 1 \times e^{-10}$ W, $\alpha = 4$, $P_r^{\max} = 1$ W, $R_s = 0.1$ Mbits/s, $R_c = 0.01$ Mbits/s, $d_{s,r} = 100$ m, $d_{r,e} = 500$ m, $d_{r,d} = 100$ m, $d_{r,r} = 50$ cm and $\phi = 1\times e^{-9}$ unless otherwise specified. Additionally, simulation results are provided to compare with the theory results.

6.1 Secrecy Rate

Under the cellular and D2D modes, we investigate the impacts of transmit powers at BS and UR on the secrecy rate, respectively. Regarding the cellular mode, we explore how the secrecy rate $\mathbf{C}_s^c$ varies with the transmit power P_s of BS. For the scenario of $d_{s,d} = \{80, 100, 120\}$ m and $d_{s,e} = 500$ m, simulation and theory results are presented in Fig. 2. We can see from Fig. 2 that these two results match well, which validates our secrecy rate modeling under the cellular mode. Fig. 2 illustrates that $\mathbf{C}_s^c$ monotonously increases as P_s increases. This can be interpreted as follows. According to the definition of secrecy rate, we know that $\mathbf{C}_s^c$ is proportional to the following three variables: the probability of selecting cellular mode, the probability of transmission without secrecy outage, and the instantaneous secrecy rate. Since the values of these three variables increase with the increase of P_s, $\mathbf{C}_s^c$ also increases. Another observation from Fig. 2 indicates that for each fixed setting of P_s, $\mathbf{C}_s^c$ decreases as the distance $d_{s,d}$ between BS and UE increases. This is because the increase of $d_{s,d}$ leads to the decrease of the values of these three variables.

We proceed to examine the impact of the secrecy transmit power P_r on the secrecy rate under the D2D mode with the settings of $P_c = 0$ W when H_0 is true, $P_c = 0.01$ W when H_1 is true, $d_{s,e} = 500$ m, $d_{s,d} = \{200, 300\}$ m, $\varepsilon = 0.1$ and $\xi = 0.9$. As shown in Fig. 3, the theory and simulation results also match well under the underlay mode and overlay mode. We can observe from Fig. 3 that as P_r increases, the secrecy rate first increases and then decreases under the underlay mode, while it monotonously increases under the overlay mode. This phenomenon can be explained as follows. For the underlay mode, the increase of P_r has two-fold effects on the secrecy rate. It can increase the values of these three variables mentioned above, which leads to the increase of the secrecy rate. Meanwhile, it can also increase the negative effect of the self-interference on UR and thus reduce the secrecy rate. When P_r is relatively small, the positive effect dominates the negative one. Thus, the secrecy rate increases with the increase of P_r. When P_r further increases, the negative effect dominates the positive one, and thus P_r decreases. On the other hand, since there does not exist the negative effect of the self-interference on UR under the overlay mode, the secrecy rate keeps a monotonous increase as P_r increases. The insight from the phenomenon is that, in practice, we need to carefully set the secrecy transmit power P_r of UR for achieving the largest secrecy rate under the underlay mode.

Another observation from Fig. 3 shows that for a given P_r, the secrecy rate under both modes increases with the increase of $d_{s,d}$. The reasons behind the phenomena can be explained as follows. For the underlay mode, the increase of $d_{s,d}$ decreases the interference at UE through direct link from BS, which increases the SINR at UE, and thus increases the secrecy rate. For the overlay mode, the increase of $d_{s,d}$ leads to the increase of the probability $1 - P_{ms}$ of selecting D2D mode, which increases the average secrecy rates $\mathbf{C}_s^{o0}$ and $\mathbf{C}_s^{o1}$ according to their definitions in the Theorem 7 and Theorem 8. Thus, the secrecy rate $\mathbf{C}_s^o$ under the overlay mode increases according to (62). We can also see from Fig. 3 that the secrecy rate under the overlay mode is always larger than that under the underlay mode when $d_{s,d} = 200$ m, while when $d_{s,d} = 300$ m, the secrecy rate under overlay mode is less than that under the underlay mode for the relatively small secrecy transmit power P_r of UR. We can have an insight that when the distance $d_{s,d}$ between source and destination is small, we can adopt the overlay mode to

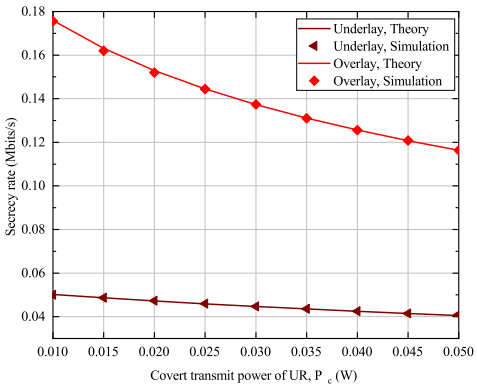

Fig. 4: Secrecy rate vs. P_c under D2D mode.

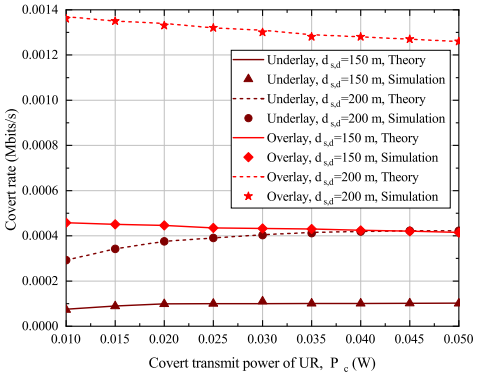

Fig. 6: Covert rate vs. P_c under D2D mode.

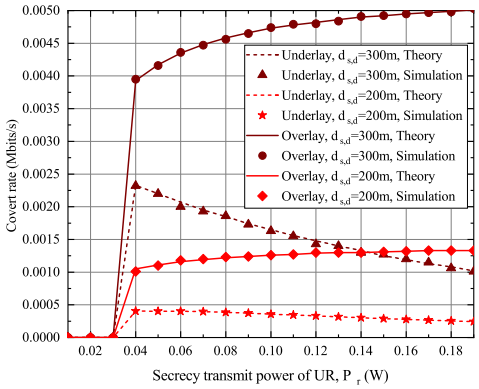

Fig. 5: Covert rate vs. P_r under D2D mode.

achieve better performance. When $d_{s,d}$ is large, the impacts of P_r on the secrecy rate are different under the overlay and underlay modes, and thus P_r should be carefully tuned to achieve better performance.

We continue to explore the impact of the covert transmit power P_c of UR on the secrecy rate under the D2D mode when H_1 is true. We summarize in Fig. 4 how the secrecy rate varies with P_c for the setting of $P_r = 0.15$ W, $d_{s,e} = 500$ m, $d_{s,d} = 200$ m, $\varepsilon = 0.1$ and $\xi = 0.9$. We can see from Fig. 4 that as P_c increases, the secrecy rates decrease under both the underlay and the overlay modes. This is due to the fact that the covert transmission interferes with the secure transmission, which leads to the decrease of the secrecy rates.

6.2 Covert Rate

To explore the impact of secrecy transmit power P_r of UR on the covert rate, we summarize in Fig. 5 how the covert rate varies with P_r under the underlay and overlay modes for the setting of $P_c = 0.01$ W, $d_{s,e} = 500$ m, $d_{s,d} = \{200, 300\}$ m, $\varepsilon = 0.1$ and $\xi = 0.9$. The theory results are entirely consistent with our simulation results, which indicates the correctness of the covert rate modelling. We can see from Fig. 5 that as P_r increases, the covert rate first remains at zero, then increases and finally decreases under the underlay mode, while the covert rate first remains at zero, and then increases under the overlay mode. This is due to the following reasons. According to the definition of covert rate, we know that it is proportional to the probability of transmission without secrecy outage and that of transmission without covert outage under the underlay and overlay modes. As P_r is relatively small, secrecy outage occurs such that the covert rates are zero under these two modes. Note that since the secrecy transmission interferes with the covert transmission, the increase of P_r has two-fold effects on the covert rate. It can increase the probability of transmission without secrecy outage leading to the increase of covert rate. Meanwhile, it can also decrease the probability of transmission without covert outage leading to the decrease of covert rate. As P_r increases, the positive effect dominates the negative one and thus the covert rate increases under the overlay mode. Under the underlay mode, the positive effect first dominates the negative one. However, due to the increase of the self-interference effect, the negative effect then dominates the positive one. Thus, the covert rate first increases and then decreases as P_r increases underlay the underlay mode. We can find an optimal P_r to maximize the covert rate under the underlay mode.

Finally, we study the impact of covert transmit power P_c of UR on the covert rate. For the setting of $P_r = 0.15$ W, $d_{s,e} = 500$ m, $d_{s,d} = \{150, 200\}$ m and $\varepsilon = 0.4$ and $\xi = 0.9$, we can observe from Fig. 6 that as P_c increases, the covert rate increases under the underlay mode, while decreases under the overlay mode. This can be explained as follows. Under the underlay mode, the secrecy outage probability is proportional to the received covert signal at UE, and the self-interference at UR from covert signal and secrecy signal transmissions. However, since the covert transmit power P_c is very small relative to the secrecy transmit power, the secrecy outage probability mainly depends on the self-interference from the secrecy signal transmission. Thus, increasing P_c has very little effect on the secrecy outage probability. But it can increase the probability of transmission without covert outage, which leads to the increase of the covert rate. Regarding the overlay mode without the self-interference effect, the secrecy outage probability mainly depends on the received covert signal at UE such that a

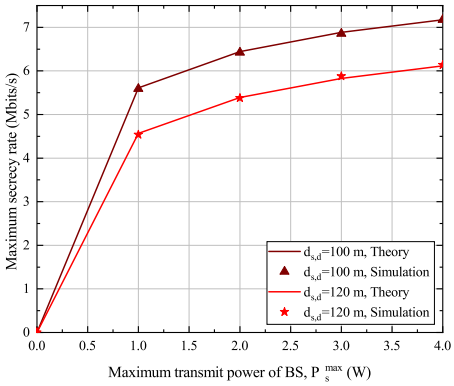

Fig. 7: Maximum secrecy rate vs. $P_s^{\max}$ under the cellular mode.

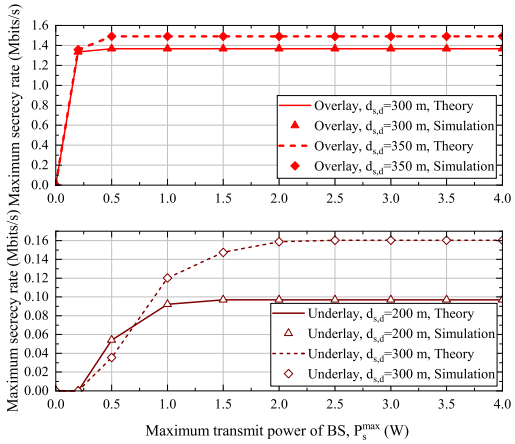

Fig. 8: Maximum secrecy rate vs. $P_s^{\max}$ under the D2D mode.

small increase of P_c can also result in a significant increase of the secrecy outage probability, which leads to the decrease of the covert rate.

6.3 Performance Optimization

To explore the impact of the maximum transmit power $P_s^{\max}$ at BS on the maximum secrecy rate $\mathbf{C}_s^{c*}$ under the cellular mode, we summarize in Fig. 7 how $\mathbf{C}_s^{c*}$ varies with the maximum transmit power $P_s^{\max}$ for the setting of $d_{s,e} = 500$ m, and $d_{s,d} = \{100, 120\}$ m. We can observe from Fig. 7 that $\mathbf{C}_s^{c*}$ increases with the increase of $P_s^{\max}$. This is because $\mathbf{C}_s^{c}$ increases with P_s, the optimal transmit power at BS is $P_s^{\max}$ for achieving the maximal secrecy rate, which results in the increase of maximum secrecy rate with the maximum transmit power $P_s^{\max}$. The observation implies that the maximum value of the maximum transmit power $P_s^{\max}$ of BS can achieve the maximum secrecy rate under the cellular mode.

As shown in Fig. 8, we continue to explore the impact of the maximum transmit power $P_s^{\max}$ at BS on the maximum secrecy rate under the D2D mode with the setting of $P_c = 0$ W when H_0 is true, $P_c = 0.05$ W when H_1 is true, $P_r = 0.45$ W, $d_{s,e} = 500$ m, $\varepsilon = 0.1$, $\xi = 0.9$, $d_{s,d} = \{200, 300\}$ m and $d_{s,d} = \{300, 350\}$ m. We can observe from Fig. 8 that as $P_s^{\max}$ increases, the maximum secrecy rates first increase and then remain unchanged under both the underlay and overlay modes. This is due to the following reasons. We know that P_s increases, $\mathbf{C}_s^u$ and $\mathbf{C}_s^o$ first increase up to maximum values and then decrease. Thus, as $P_s^{\max}$ is relatively small which is lower than the optimal P_s, the maximum values of $\mathbf{C}_s^u$ and $\mathbf{C}_s^o$ increase with $P_s^{\max}$. As $P_s^{\max}$ continues to increase, $\mathbf{C}_s^u$ and $\mathbf{C}_s^o$ achieve maximum values and thus remain unchanged with the increase of $P_s^{\max}$. This means that there exists an optimal $P_s^{\max}$ to achieve the maximum value of the maximum secrecy rate.

7 Conclusion

This paper investigated the joint covert and secure communications in DCSs. We first derived some basic results in terms of the maximum detection probability at BS, and then provided theoretical modelling for secrecy and covert rates under the cellular and D2D modes. We further explored the optimal transmit power control for the secrecy and covert rate maximization from the perspective of BS and UR, respectively. The results in this paper indicate that in comparison with the separate cellular and D2D modes, a suitable mode selection for the UE can significantly improve the secrecy rate and covert rate from the perspective of BS and UR. An optimal power control at BS and UR can also achieve maximum secrecy rate and maximum covert rate under each mode. Therefore, suitable mode selection and optimal power control are crucial to enhance the system performances for supporting various applications with different security requirements. An interesting work in our future research is to consider more practical issues such as channel fading, interference, mobility, and multiple antennas.

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] I. Budhiraja, N. Kumar, and S. Tyagi, "Ishu: Interference reduction scheme for D2D mobile groups using uplink NOMA," *IEEE Transactions on Mobile Computing*, 2021.

[3] M. Hmila, M. Fernandez-Veiga, M. R. Perez, and S. Herreria-Alonso, "Distributed energy efficient channel allocation in underlay multicast D2D communications," *IEEE Transactions on Mobile Computing*, 2020.

[4] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[5] B. Yang, T. Taleb, Y. Fan, and S. Shen, "Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks," *IEEE Network*, vol. 35, no. 2, pp. 104–111, 2021.

[6] B. Yang, T. Taleb, G. Chen, and S. Shen, "Covert communication for cellular and X2U-enabled UAV networks with active and passive wardens," *IEEE Network*, vol. 36, no. 1, pp. 166–173, 2022.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] B. Yang, T. Taleb, Z. Wu, and L. Ma, "Spectrum sharing for secrecy performance enhancement in D2D-enabled UAV networks," *IEEE Network*, vol. 34, no. 6, pp. 156–163, 2020.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[17] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[18] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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*, vol. 69, no. 9, pp. 6198–6212, 2021.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

[33] ——, "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.

[34] C. Wang, Z. Li, H. Zhang, D. W. K. Ng, and N. Al-Dhahir, "Achieving covertness and security in broadcast channels with finite blocklength," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7624–7640, 2022.

[35] C. Wang, Z. Li, and D. W. Kwan Ng, "Optimal joint beamforming and jamming design for secure and covert URLLC," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–7.

[36] U. Altun and E. Basar, "RIS enabled secure communication with covert constraint," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*, 2021, pp. 685–689.

[37] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Covertness and secrecy study in untrusted relay-assisted D2D networks," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 17–30, 2023.

[38] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 128–137, 2015.

[39] 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.

[40] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[41] 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.

[42] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE transactions on information forensics and security*, vol. 10, no. 10, pp. 2095–2107, 2015.

[43] "Matlab program for simulation," 2023. [Online]. Available: https://pan.baidu.com/s/16VKQwwDdeiQVoB2ppcmmeQ?pwd=mvgz

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. And she received the Ph.D. degree with the School of Computer Science and Technology, Xidian University, Xian, China, in 2022. She is currently an associate researcher with the Hangzhou Institute of Technology, Xidian University, Hangzhou, China. Her research interest focuses on the covert communication.

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 Nov. 2020 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 received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xian, 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 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. Jiangs 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 received the BE degree in information engineering with distinction and the MSc and PhD degrees in information sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a full professor with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum. He is the founder and director of the MOSA!C Lab. Between 2018 and 2023, he was a full professor at the Center for Wireless Communications, University of Oulu, Oulu, Finland. Between 2014 and 2021, he was a professor with the School of Electrical Engineering, Aalto University, Finland. Prior to that, he was working as senior researcher and 3GPP standards expert with NEC Europe Ltd., Heidelberg, Germany. Before joining NEC and till Mar. 2009, he worked as a assistant professor with the Graduate School of Information Sciences, Tohoku University, Japan, in a lab fully funded by KDDI, the second largest mobile operator in Japan. From Oct. 2005 till Mar. 2006, he worked as research fellow with the Intelligent Cosmos Research Institute, Sendai, Japan. His research interests lie in the field of telco cloud, network softwarization and network slicing, AI-based software defined security, immersive communications, mobile multimedia streaming, and next generation mobile networking. He has been also directly engaged in the development and standardization of the Evolved Packet System as a member of 3GPP's System Architecture working group 2. He served as the general chair of the 2019 edition of the IEEE Wireless Communications and Networking Conference (WCNC19) held in Marrakech, Morocco. He was the guest editor in chief of the IEEE JSAC Series on Network Softwarization and Enablers. He was on the editorial board of IEEE Transactions on Wireless Communications, IEEE Wireless Communications Magazine, IEEE Journal on Internet of Things, IEEE Transactions on Vehicular Technology, IEEE Communications Surveys and Tutorials, and a number of Wiley journals. Till Dec. 2016, he served as chair of the Wireless Communications Technical Committee.