IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 7, 2019, accepted May 25, 2019, date of publication May 29, 2019, date of current version June 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2919453

Resource Allocation for Covert Communication in D2D Content Sharing: A Matching Game Approach

XIN SHI, DAN WU, CHAO YUE, CHENG WAN, AND XINRONG GUAN
College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China

Corresponding author: Dan Wu (wujing1958725@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61671474, in part by the Jiangsu Provincial Natural Science Fund for Outstanding Young Scholars under Grant BK20180028, and in part by the Jiangsu Provincial Natural Science Fund for Excellent Young Scholars under Grant BK20170089.

ABSTRACT Device-to-device (D2D) content sharing, as a promising solution to rapidly growing mobile data traffic, is facing serious security issues. Hence, how to ensure its security is challenging and meaningful work. Covert communication is regarded as an emerging and cutting-edge security technique for its higher level of security and less need for channel state information (CSI), and accordingly, has attracted wide attention. However, it is not easy to directly apply covert communication to D2D content sharing to ensure both security and efficiency. In this paper, a novel covert communication model is constructed in D2D content sharing scenario, where the co-channel interference (CCI) introduced by spectrum reusing is exploited as the cover of contents so that the contents are hidden from the warden. Then, we propose a secure and efficient resource allocation scheme to ensure both security and efficiency of D2D content sharing by addressing the following two issues: 1) In order to guarantee the robustness of our scheme, covert constraints are learned by analyzing the detection performance at the warden, i.e., the security of D2D content sharing is guaranteed even considering some extremely adverse environments. 2) The joint spectrum allocation and power control is modeled as a two-sided matching problem and then reformulated as the one-to-one matching game based on the principle of mutual benefit, in order to ensure the quality of service (QoS) requirements of both D2D pairs and cellular users. Then, covert constraints guaranteed resource allocation algorithm based on Gale–Shapley algorithm is proposed. Its properties such as stability, optimality, convergence, and complexity are analyzed. The extensive simulation results are provided to verify the theoretical analyses and demonstrate the efficiency of our proposed algorithm, which has at least 7.63% performance gain compared with some existing approaches and no more than 4.83% performance loss compared with the exhaustive search.

INDEX TERMS D2D content sharing, covert communication, co-channel interference, resource allocation, matching game.

I. INTRODUCTION

A. BACKGROUND AND RELATED WORKS

Device-to-device (D2D) content sharing is regarded as a proper solution to the rapidly growing mobile data traffic [1], which allows direct communications among multiple smart devices without need for access to the cellular infrastructure designed for long term evolution-advanced (LTE-A) under the 3GPP [2]. By taking full advantage of the caching capacities of the smart devices widely distributed in the network, D2D content sharing can provide sufficient gains in terms of high data rates, low power consumption, and short delays [3]. Unfortunately, D2D content sharing is more vulnerable to the security issues compared with the traditional cellular network because the distributed caching extends the scope of contents sources [4], which increases the possibility of information leakage. More importantly, conventional end-to-end encryption technique is not compatible with D2D content sharing network due to the following facts. 1) Smart devices have limited storage, transmission, and computing capacities for security-related works, and the lack of central authority, i.e., the base station (BS), results in that additional

The associate editor coordinating the review of this manuscript and approving it for publication was Syed Mohammad Zafaruddin.

functionalities must be undertaken by smart devices themselves such as auditing and logging [5]. Thus, they cannot take more care of the complex encryption and decryption. 2) The decentralized and large-scale nature of D2D content sharing makes key management difficult. More critically, the encrypted contents are unique for one certain device and cannot be reused to serve other devices, and then, the benefits of D2D content sharing may well vanish. In this regard, it is an important concern to achieve information confidentiality in D2D content sharing network.

Developing security techniques at the physical layer may lead to enforcing the security of upper layers and thus improve overall D2D networks. Recently, physical layer security, which exploits the wireless channel characteristics to prevent eavesdroppers based on the information theoretic secrecy analysis of Shannon [6], has attracted wide attention. Literature on physical layer security for D2D networks mainly contains *i*) channel state information (CSI) based key extraction [7], *ii*) physical layer security performance analyses [8], *iii*) beamforming design from a physical layer security perspective [9], and *iv*) resource management in order to enhance the physical layer security performances [10]. However, there are two main categories of shortcomings for physical layer security to ensure the information confidentiality. *i*) Authors in most of the existing literature on physical layer security assume previously known CSI of the eavesdropping nodes and secure backhauls, which are difficult to achieve in practical applications. *ii*) Physical layer security only focuses on protecting the transmitted data, but cannot ensure the undetectability of wireless transmission. It will lead to security concerns on monitoring and maintaining privacy, especially in some special scenarios, e.g., the battlefield [11].

To deal with the shortcomings analyzed above, the covert communication is of great potential. As covert communication is an emerging and cutting-edge wireless communication security technique, it aims to ensure the undetectability of a wireless transmission while guaranteeing a negligible successful detection probability by exploiting the average power uncertainty of received signals at a warden [12]. By utilizing the covert communication, a vicious warden cannot detect the transmission so that it has no chance to take subsequent malicious acts, e.g., eavesdropping and decoding attack, denial of service (DoS) attack, and electronic countermeasure [13]. More importantly, covert communication can be achieved with unknown or imperfect CSI of warden's monitoring channels [14]–[16], which makes it more consistent with practical applications. Besides, covert communication is quite compatible with D2D content sharing scenarios due to the existing co-channel (CCI) interference introduced by spectrum reusing in D2D underlaying cellular networks. In general, a wireless transmission is ensured to be covert due to the existence of noise (or interference) so that the warden cannot distinguish the targeted message from the noise (or interference) accurately. In this regard, the CCI introduced inevitably by spectrum reusing can be efficiently exploited to ensure the security of D2D content sharing based on covert communication, i.e., utilizing the CCI as the cover of the contents transmitted through D2D links.

Bash *et al*. in [17] present that $O(\sqrt{n})$ bits can be sent from the transmitter to the receiver covertly in n channel uses for the first time, known as the square root law. Bloch [18] investigates the covert communication over noisy channels, and develops an alternative coding scheme based on the principle of channel resolvability. Then, this work is extended to various channel models such as binary symmetric channels [19], discrete memoryless channels [20], multiple access channels [21], and multi-input multi-output (MIMO) additive white Gaussian noise (AWGN) channels [22]. Researchers focus on the performance analyses of covert communications in different kinds of scenarios, for example, wireless relay networks [16], [23], [24], full-duplex receiver scenarios [25], [26], and noise backgrounds [27], [28]. However, the covert communication has not been investigated in D2D content sharing scenarios.

In most of the existing literature, the warden decides whether there is a wireless transmission or not according to the average power of its received signals. If the average power of its received signals is continuously changing with uncertainty, it will be difficult for the warden to make a correct decision. In this regard, it is of great significance for the CCI being able to puzzle the warden. However, it is a challenging work to achieve covert communication in D2D content sharing scenarios due to the following facts. *i*) Considering the differentiated detection abilities of wardens, it is not easy to always make the CCI distort a warden's perception of the occurrence of D2D content sharing. Thus, it is a crucial issue to ensure the robustness of covert communication in D2D content sharing scenarios even considering some extremely adverse environments. *ii*) Spectrum reusing introduces the CCI to both the D2D pairs and the cellular users, which has a negative impact on the quality of service (QoS) of them. More importantly, the QoS performances of the D2D pairs and the cellular users are opposites because one side acts as a jammer to the other side. Thus, it is necessary to purse a high-efficiency resource allocation scheme by ensuring the mutual benefit and between the D2D pairs and the cellular users, as well as the QoS requirements of both sides.

B. CONTRIBUTIONS

Motivated by the above discussion, we construct a novel covert communication model in D2D content sharing scenario, then propose a secure and efficient resource allocation scheme, so as to ensure both the security and efficiency for D2D content sharing. To the best of our knowledge, this is the first attempt to solve the joint spectrum allocation and power control problem from a covert communication perspective for D2D content sharing. In brief, we conclude our main contributions as the following three-folds:

- A novel covert communication model is constructed in D2D underlaying cellular network, to ensure the security of D2D content sharing from an information theory perspective. The content transmitted through D2D links is hidden from the warden by exploiting the CCI introduced by spectrum reusing as its cover. Theoretically, we analyze the detection performance at the warden, consisting of the false alarm (FA) and miss detection (MD) rates, which are derived under block fading wireless channels.
- In order to ensure the robustness of our scheme, the covert constraints are learnt to guarantee the security of D2D content sharing even considering some extremely adverse environments by deriving the closed-form expressions of the optimal detection threshold and minimal detection error rate at the warden. Then, the joint spectrum allocation and power control problem with covert constraints is formulated as a two-sided matching problem based on the principle of mutual benefit for the purpose of achieving high-efficiency resource allocation.
- Aiming at solving the two-sided matching problem in a tractable manner, we model it as a two-sided *one-to-one* matching game and propose a covert constraints guaranteed resource allocation algorithm based on Gale-Shapley algorithm. It includes two phases, i.e., preference profiles establishment and stable matching. The power control issue is transformed into the former, and the spectrum allocation problem is solved in process of the latter. Moreover, the properties of our proposed algorithm are analyzed, such as stability, convergence, optimality and complexity. Finally, extensive numerical results verify the correctness of our theoretical analyses and demonstrate the efficiency of our proposed algorithm.

C. ORGANIZATIONS

The remainder of this paper is organized as follows. Section II presents the system model consisting of network model, covert communication model in D2D content sharing and problem overview. In Section III, we analyze the detection performance at the warden and propose covert constraints to guarantee the security of D2D content sharing. In Section IV, we model the joint spectrum allocation and power control problem as a two-sided matching problem and reformulate it as an *one-to-one* matching game. Then, a covert constraints guaranteed resource allocation algorithm based on Gale-Shapley algorithm is proposed, followed by the properties analyses. Finally, extensive simulation results are given in Section V, and this work is concluded in Section VI.

II. SYSTEM MODEL AND PROBLEM OVERVIEW

A. NETWORK MODEL

We investigate the D2D content sharing in a D2D underlaying cellular network. Without loss of generality, M active regular cellular users and N D2D pairs are randomly located in a single cell. The M regular cellular users together form $\mathcal{C} = \{C_1, \cdots, C_m, \cdots, C_M\}$. The N D2D pairs comprise $\mathcal{D} = \{D_1, \cdots, D_n, \cdots, D_N\}$. Each D2D pair consists of a D2D content provider (DP) and a D2D content requester (DR). Specifically, the former enables to make the most of its limited caching capacity to store some popular contents. Once it receives a content request from the latter, and it does temporally not retrieve contents for itself, it can serve as a transmitter to send the desired contents to the latter by constructing D2D link between them. Then, these DPs and DRs comprise $\mathcal{DP} = \{DP_1, \cdots, DP_n, \cdots, DP_N\}$ and $\mathcal{DR} = \{DR_1, \cdots, DR_n, \cdots, DR_N\}$, respectively. Here, we employ the contents cache policy in [29] to identify which content is stored by each $DP_n \in \mathcal{DP}$, and the provider-requester pairing scheme in [30] to form the D2D pairs.

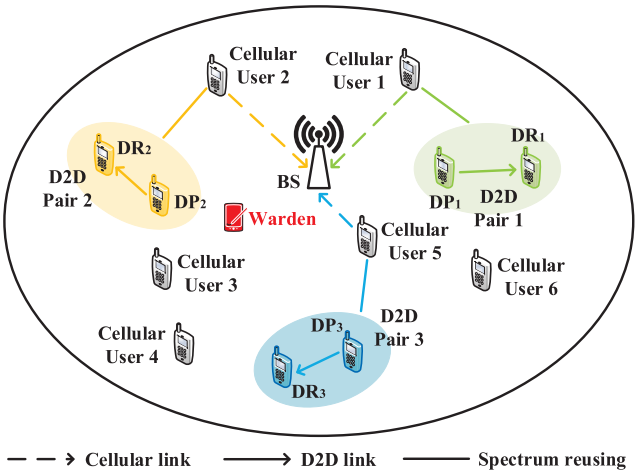


FIGURE 1. Single-cell D2D underlaying cellular network.

Due to the openness nature of wireless channels, the content sharing between each D2D pair is faced with security threats. Without loss of generality, there exists a warden randomly distributed in the network, who could be a malicious competitor or adversary. More seriously, it silently listens to the communication environment and tries to detect any transmission between each $DP_n \in \mathcal{DP}$ and its corresponding DR_n. In order to address the issue, we introduce the covert communication, and its basic goal is to establish shadow wireless transmission networks [31], where the content sharing between each D2D pair should be kept covert to guarantee the security of the transmission. As shown in Fig. 1, there are three D2D pairs and six cellular users, all of which are randomly distributed. At this time, a warden intends to detect the content sharing of each D2D pair according to the average power of its received signals.[1]

Recall that an effective way to enable the end-to-end covert communication is to introduce interference to confuse the detection at the warden. Fortunately, in D2D underlaying

[1]The detection at the warden can be easily achieved by utilizing a radiometer, i.e., a power detector, as its detector [32].

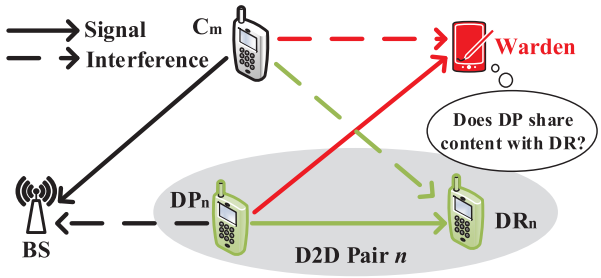


FIGURE 2. Covert communication model in D2D content sharing.

cellular network, more than M orthogonal spectrum resources are available for all the cellular users and each of them occupies one to communicate with the BS. Then, each D2D pair is permitted to reuse the uplink spectrum resource of at most one cellular user for content sharing to enhance spectral efficiency. In this regard, the additional CCI will inevitably be introduced. Fig. 1 illustrates an example of uplink spectrum reusing, where different colors are utilized to represent the uplink spectrum reusing results. For example, D2D pair D_3 reuses the uplink spectrum of cellular user C_5. As a result, DR_3 suffers from the CCI from cellular user C_5, and simultaneously, the BS receives the CCI from DP_3. In this way, we will try to efficiently utilize such additional CCI to form the covert communication in D2D content sharing scenario, so as to prevent security threats brought by the warden.

Remark 1: Although we just consider a scenario with a single warden, our work can be extended to the scenario with multiple wardens, in which the detections at these wardens are independent. It means that the scenario with multiple wardens can be separated into multiple independent single-warden scenarios, and each of them is relevant to this scenario of our work.

B. COVERT COMMUNICATION MODEL IN D2D CONTENT SHARING

Fig. 2 is presented to show the covert communication model in the D2D content sharing scenario. Specifically, when DP_n wants to share contents with DR_n by D2D communication, they form D2D pair D_n, and a D2D link between them is constructed by reusing the uplink spectrum of cellular user C_m. Simultaneously, the warden listens to the communication environment silently to judge whether the content sharing between DP_n and DR_n happens or not according to the average power of its received signals. As such, we should ensure a negligible successful detection probability at the warden, which is the essence of covert communication. To this end, on one hand, all the wireless channels in the covert communication model are independent quasi-static Rayleigh fading with equal block length [23], which means that the channel coefficients remain stationary in a block and change randomly and independently in the next block [33]. Actually, the Rayleigh fading channel model can describe the shortwave channels reflected by the ionosphere and troposphere, as well as the built-up urban environment, where there exists no line of sight (LOS) link. The channel model is practical and quite compatible with the D2D content sharing scenarios. Then, the average power of received signals at the warden changes randomly in each block. On the other hand, and perhaps most importantly, the spectrum reusing makes DR_n and the warden suffer from the CCI caused by C_m. Moreover, the CCI can be changing and even dynamic under block fading channels, which makes the average power of received signals at the warden more uncertain. In other words, we can utilize the CCI caused by cellular user C_m to achieve the covert communication for D2D content sharing between DP_n and DR_n. We denote h_{DP_n,DR_n}, h_{C_m,DR_n}, $h_{DP_n,W}$ and $h_{C_m,W}$ as the channel coefficients from DP_n to DR_n, C_m to DR_n, DP_n to the warden and C_m to the warden, respectively. These channel coefficients are circularly symmetric complex Gaussian with zero mean and unit variance [15].

During the content sharing, when DP_n shares contents with DR_n, the signal sent by DP_n is denoted by $\mathbf{s}_{DP_n} = [s^1_{DP_n}, s^2_{DP_n}, \cdots, s^l_{DP_n}]$, where l is the number of channel uses. Then, let $\mathcal{H}_1$ specify the event that DP_n enables to share contents with DR_n covertly, and accordingly, DP_n will share contents with DR_n covertly at a probability $\mathbb{P}_{\mathcal{H}_1}$. Otherwise, $\mathcal{H}_0$ specifies that DP_n does not share contents with DR_n covertly, and the probability of this is $\mathbb{P}_{\mathcal{H}_0}$. Obviously, $\mathbb{P}_{\mathcal{H}_0} + \mathbb{P}_{\mathcal{H}_1} = 1$. Note that, the probabilities $\mathbb{P}_{\mathcal{H}_0}$ and $\mathbb{P}_{\mathcal{H}_1}$ are statistical data and can be adjusted by DP_n. In addition, C_m sends signals to the BS all the time during DP_n needs to share contents with DR_n, and the signal sent by C_m is denoted by $\mathbf{s}_{C_m} = [s^1_{C_m}, s^2_{C_m}, \cdots, s^l_{C_m}]$. Both DP_n and C_m employ zero mean Gaussian signals with variances [34], that is, the transmission power of DP_n and C_m, which are denoted by $p^{C_m}_{D_n}$ and p_{C_m}, respectively. Then, the received signal at DR_n is denoted by $\mathbf{r}^{C_m,D_n}_{DR_n} = [r^{C_m,D_n,1}_{DR_n}, r^{C_m,D_n,2}_{DR_n}, \cdots, r^{C_m,D_n,l}_{DR_n}]$, which is given by Eq. (1), as shown at the top of the next page. Here, α is the path-loss exponent. d_{C_m,DR_n} denotes the distance between C_m and DR_n, and d_{DP_n,DR_n} denotes the distance between DP_n and DR_n, $\mathbf{n}_{DR_n}$ is the AWGN at DR_n, with a variance of $\sigma^2_{DR_n}$. Similarly, the received signal at the warden is denoted as $\mathbf{r}^{C_m,D_n}_{W} = [r^{C_m,D_n,1}_{W}, r^{C_m,D_n,2}_{W}, \cdots, r^{C_m,D_n,l}_{W}]$, which is given by Eq. (2), as shown at the top of the next page. Here, $d_{C_m,W}$ denotes the distance between C_m and the warden, and $d_{DP_n,W}$ denotes the distance between DP_n and the warden, $\mathbf{n}_W$ is the AWGN at the warden with a variance of σ^2_W. In this way, the purpose of covert communication can be characterized as guaranteeing the successful detection at the warden a sufficient small probability by making the average power of received signals at the warden, i.e., $\mathbf{r}^{C_m,D_n}_{W}$ changing with uncertainty. More importantly, once we can achieve the covert communication for D2D content sharing, we can gain a series of advantages such as anti-eavesdropping, privacy preservation and anti-jamming.

C. PROBLEM OVERVIEW

Note that, although the covert communication could provide D2D content sharing with a high level of security by ensuring the undetectability of the content sharing between

$$\mathbf{r}_{DR_n}^{C_m,D_n} = \begin{cases} \sqrt{p_{C_m}} h_{C_m,DR_n} d_{C_m,DR_n}^{-\alpha/2} \mathbf{s}_{C_m} + \mathbf{n}_{DR_n}, & if\ \mathcal{H}_0, \\ \sqrt{p_{D_n}^{C_m}} h_{DP_n,DR_n} d_{DP_n,DR_n}^{-\alpha/2} \mathbf{s}_{DP_n} + \sqrt{p_{C_m}} h_{C_m,DR_n} d_{C_m,DR_n}^{-\alpha/2} \mathbf{s}_{C_m} + \mathbf{n}_{DR_n}, & if\ \mathcal{H}_1, \end{cases} \tag{1}$$

$$\mathbf{r}_{W}^{C_m,D_n} = \begin{cases} \sqrt{p_{C_m}} h_{C_m,W} d_{C_m,W}^{-\alpha/2} \mathbf{s}_{C_m} + \mathbf{n}_{W}, & if\ \mathcal{H}_0, \\ \sqrt{p_{D_n}^{C_m}} h_{DP_n,W} d_{DP_n,E}^{-\alpha/2} \mathbf{s}_{DP_n} + \sqrt{p_{C_m}} h_{C_m,W} d_{C_m,W}^{-\alpha/2} \mathbf{s}_{C_m} + \mathbf{n}_{W}, & if\ \mathcal{H}_1, \end{cases} \tag{2}$$

each $DP_n \in \mathcal{DP}$ and DR_n, the following challenges should be addressed to ensure such advantages. *i*) The core of covert communication is to tactfully exploit the CCI generated by the cellular users to ensure the undetectability of the content sharing between each DP_n and DR_n. Although resource management is regarded as an efficient way to interference management, it is not easy to always make the generated CCI distort a warden's perception of the occurrence of the D2D content sharing. This is due to the fact that detection abilities of different kinds of wardens vary widely. Hence, we should guarantee the robustness of covert communication in D2D content sharing scenario, even considering some extremely adverse cases. *ii*) Both of the D2D pairs and the cellular users suffer from the interference due to spectrum reusing. Also, both sides have different QoS requirements, and more importantly, it is unfair to ensure the QoS performance of either side, and even, it is unacceptable to benefit one side at the expense of the other side. Hence, we should pursue a resource allocation resolution based on the principle of mutual benefit, so as to optimize the QoS performances of both sides. To this end, a secure and efficient resource allocation scheme is required. That is, we quantificationally analyze the detection performance at the warden, and further learn the covert constraints to guarantee the security of content sharing (Please see Section III). Guided by these results, we propose a matching game based resource allocation scheme to achieve the joint optimization of spectrum allocation and power control, which does not only guarantee the covert communication in D2D content sharing, but also ensure the QoS requirements of both the D2D pairs and the cellular users based on the mutual benefit principle (Please see Section IV).

III. GUARANTEE OF COVERT COMMUNICATION IN D2D CONTENT SHARING

In this section, considering the proposed covert communication model in D2D content sharing, we analyze the detection performance at the warden and obtain the closed-form expressions of optimal detection threshold and minimal detection error rate. Then, we learn the covert constraints to guarantee the robustness of our proposed secure and efficient resource allocation scheme even considering the worst case that the warden is able to adjust its detection threshold to minimize its detection error rate.

A. DETECTION PERFORMANCE AT THE WARDEN

In order to guarantee the robustness of the covert communication in D2D content sharing scenario, we analyze the detection performance at the warden. Specifically, the warden judges whether DP_n shares contents with DR_n covertly based on the average power of its received signals. According to [35], by exploiting the Neyman-Pearson criterion, the optimal decision rule for the warden to minimize its probability of detection error is the likelihood ratio test, that is,

$$\frac{p_W}{l} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \gamma, \tag{3}$$

where $p_W = \sum_{i=1}^{l} \left| r_W^{C_m,D_n,i} \right|^2$ denotes the total power received by the warden in a given block, $i = 1, 2, \cdots, l$ is the index of each channel use, and γ is a predetermined detection threshold, $\mathcal{D}_0$ and $\mathcal{D}_1$ correspond to the decisions in favour of hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Actually, there are two types of detection errors. *i*) False alarm occurs with a probability $\mathbb{P}_{FA}$ if the warden mistakenly decides $\mathcal{D}_1$ while $\mathcal{H}_0$ is true. *ii*) Miss detection appears with a probability $\mathbb{P}_{MD}$ if the warden mistakenly decides $\mathcal{D}_0$ while $\mathcal{H}_1$ is true. Obviously, we have $\mathbb{P}_{FA} = \mathbb{P}(\mathcal{D}_1|\mathcal{H}_0)$ and $\mathbb{P}_{MD} = \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1)$.

Lemma 1: The false alarm and miss detection rates at the warden are given by

$$\mathbb{P}_{FA} = \begin{cases} e^{-\frac{x}{a}}, & for\ x \geq 0, \\ 1, & for\ x < 0, \end{cases} \tag{4}$$

$$\mathbb{P}_{MD} = \begin{cases} -\frac{a}{a-b} e^{-\frac{x}{a}} + \frac{b}{a-b} e^{-\frac{x}{b}} + 1, & for\ x \geq 0\ and\ a \neq b, \\ 1 - e^{-\frac{x}{a}} - e^{-\frac{x}{b}}, & for\ x \geq 0\ and\ a = b, \\ 0, & for\ x < 0, \end{cases} \tag{5}$$

respectively, where $x = \gamma - \sigma_W^2$, $a = \frac{p_{C_m}}{d_{C_m,W}^{\alpha}}$, $b = \frac{p_{D_n}^{C_m}}{d_{DP_n,W}^{\alpha}}$.

Proof: According to Eqs. (2) and (3), the expressions of FA probability and MD probability can be shown as

$$\begin{aligned} \mathbb{P}_{FA} &= \mathbb{P}(\mathcal{D}_1|\mathcal{H}_0) = \mathbb{P}(\frac{p_W}{l} > \gamma|\mathcal{H}_0) \\ &= \mathbb{P}[(\sigma_W^2 + p_{C_m}|h_{C_m,W}|^2 d_{C_m,W}^{-\alpha}) \frac{\mathcal{X}_l^2}{l} > \gamma], \end{aligned} \tag{6}$$

and

$$\begin{aligned} \mathbb{P}_{MD} &= \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1) = \mathbb{P}(\frac{p_W}{l} < \gamma|\mathcal{H}_1) \\ &= \mathbb{P}[(\sigma_W^2 + p_{C_m}|h_{C_m,W}|^2 d_{C_m,W}^{-\alpha} \\ &\quad + p_{D_n}^{C_m}|h_{DP_n,W}|^2 d_{DP_n,W}^{-\alpha}) \frac{X_{2l}^2}{l} < \gamma], \end{aligned} \tag{7}$$

$$\varepsilon = \begin{cases} (\mathbb{P}_{\mathcal{H}_0} - \frac{a}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x}{a}} + \frac{b}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x}{b}} + \mathbb{P}_{\mathcal{H}_1}, & for\ x \geq 0\ and\ a \neq b \\ \mathbb{P}_{\mathcal{H}_1} + (1 - 3\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x}{a}}, & for\ x \geq 0\ and\ a = b \\ \mathbb{P}_{\mathcal{H}_0}, & for\ x < 0 \end{cases}. \tag{12}$$

where $\mathcal{X}_l^2$ and $\mathcal{X}_{2l}^2$ are chi-squared random variables with l and $2l$ degrees of freedom, respectively. Then we replace them by 1 since we consider a sufficient large number of channel uses, i.e., $l \to \infty$, based on the Lebesgue's Dominated Convergence Theorem in [36]. Recall that the wireless channels in the network are subject to independent quasi-static Rayleigh fading and the channel coefficients are circularly symmetric complex Gaussian with zero mean and unit variance. Thus, Eq. (4) can be obtained by

$$\begin{aligned} \mathbb{P}_{FA} &= \mathbb{P}(g_1 > \frac{x}{a}) \\ &= \begin{cases} e^{-\frac{x}{a}}, & for\ x \geq 0, \\ 1, & for\ x < 0, \end{cases} \end{aligned} \tag{8}$$

where $g_1 = |h_{C_m,W}|^2$. Eq. (7) can be rewritten as

$$\begin{aligned} \mathbb{P}_{MD} &= \mathbb{P}(p_{C_m}|h_{C_m,W}|^2 d_{C_m,W}^{-\alpha} \\ &\quad + p_{D_n}^{C_m}|h_{DP_n,W}|^2 d_{DP_n,W}^{-\alpha} < \gamma - \sigma_W^2) \\ &= \mathbb{P}(ag_1 + bg_2 < x). \end{aligned} \tag{9}$$

where $g_2 = |h_{DP_n,E}|^2$. Obviously, $\mathbb{P}_{MD} = 0$ when $x < 0$, since a, b, g_1 and g_2 are no less than 0. Then, when $x \geq 0$, the distribution function of $ag_1 + bg_2$ is given by

$$\begin{aligned} &\mathbb{P}(ag_1 + bg_2 < x) \\ &= \int_{g_1}\int_{g_2} f(g_1, g_2)dg_1dg_2 \\ &= \int_0^{\frac{x}{a}} dg_1 \int_0^{\frac{x-ag_1}{b}} f(g_1, g_2)dg_2 \\ &= \int_0^{\frac{x}{a}} dg_1 \int_0^{\frac{x-ag_1}{b}} e^{-g_1}e^{-g_2}dx_2 \\ &= -\int_0^{\frac{x}{a}} e^{-g_1}(e^{-\frac{x-ag_1}{b}} - 1)dg_1 \\ &= \begin{cases} -\frac{a}{a-b}e^{-\frac{x}{a}} + \frac{b}{a-b}e^{-\frac{x}{b}} + 1, & for\ a \neq b, \\ 1 - e^{-\frac{x}{a}} - e^{-\frac{x}{b}}, & for\ a = b, \end{cases} \end{aligned} \tag{10}$$

which leads to the desired results in Eq. (5). ■

Given prior probabilities $\mathbb{P}_{\mathcal{H}_0}$ and $\mathbb{P}_{\mathcal{H}_1}$, we define the detection error rate at the warden to characterize its detection performance, i.e.,

$$\varepsilon = \mathbb{P}_{\mathcal{H}_0}\mathbb{P}_{FA} + \mathbb{P}_{\mathcal{H}_1}\mathbb{P}_{MD}, \tag{11}$$

which is derived from the formula of total probability. By submitting Eqs. (4) and (5) into (11), we can obtain the expression of ε as Eq. (12), as shown at the top of this page. Considering different kinds of wardens, their abilities to access useful information to help them make correct judgements vary widely. Thus, in order to guarantee the robustness of our proposed scheme, we focus on the worst case that the warden is able to access all the useful information such as locations and transmission power of both cellular users and D2D pairs, along with the prior probabilities $\mathbb{P}_{\mathcal{H}_0}$ and $\mathbb{P}_{\mathcal{H}_1}$. As thus, the warden could adjust its detection threshold γ to the optimal value γ_{op} so as to minimize its detection error rate, denoted by $\varepsilon_{\min}$. In this regard, we are committed to find γ_{op} and $\varepsilon_{\min}$ and ensure the covert communication between DP_n and DR_n in such extremely adverse environment.

Theorem 1: The optimal detection threshold γ_{op} for the warden is

$$\gamma_{op} = \begin{cases} \gamma^*, & for\ x \geq 0\ and\ a \neq b, \\ \sigma_W^2, & for\ x \geq 0\ and\ a = b\ and\ \mathbb{P}_{\mathcal{H}_1} < \frac{1}{3}, \\ nonexistent\ \gamma, & otherwise, \end{cases} \tag{13}$$

where $\gamma^* = \frac{ab}{b-a}\ln[(\frac{b}{a}-1)\frac{\mathbb{P}_{\mathcal{H}_0}}{\mathbb{P}_{\mathcal{H}_1}}+1]+\sigma_W^2$. The corresponding minimal detection error rate $\varepsilon_{\min}$ at the warden is denoted by

$$\varepsilon_{\min} = \begin{cases} \varepsilon^*, & for\ x \geq 0\ and\ a \neq b, \\ 1 - 2\mathbb{P}_{\mathcal{H}_1}, & for\ x \geq 0\ and\ a = b\ and\ \mathbb{P}_{\mathcal{H}_1} < \frac{1}{3}, \\ \mathbb{P}_{\mathcal{H}_1}, & for\ x \geq 0\ and\ a = b\ and\ \mathbb{P}_{\mathcal{H}_1} \geq \frac{1}{3}, \\ \mathbb{P}_{\mathcal{H}_0}, & for\ x < 0, \end{cases} \tag{14}$$

where ε^* is represented by

$$\varepsilon^* = (\mathbb{P}_{\mathcal{H}_0} - \frac{a}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{\gamma^*-\sigma_W^2}{a}} + \frac{b}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{\gamma^*-\sigma_W^2}{b}} + \mathbb{P}_{\mathcal{H}_1}. \tag{15}$$

Proof: Given the expression of the detection error rate ε shown as Eq. (12), we consider the following optimization problem to find the optimal detection threshold γ_{op} for the warden, i.e.,

$$\min_{\gamma}\ \varepsilon. \tag{16}$$

Then, we prove Theorem 1 in the following cases.

Case 1: When $x < 0$, ε is always a constant $\mathbb{P}_{\mathcal{H}_0}$. It can be easily seen that γ_{op} is nonexistent.

Case 2: When $x \geq 0$ and $a = b$, the expression of ε is an exponential function and the coefficient $1 - 3\mathbb{P}_{\mathcal{H}_1}$

determines the value of γ_{op}. Specifically, when $1-3\mathbb{P}_{\mathcal{H}_1}>0$, i.e., $\mathbb{P}_{\mathcal{H}_1}<\frac{1}{3}$, ε is a strictly increasing function. Thus, $\gamma_{op}=\sigma_W^2$. Otherwise, when $1-3\mathbb{P}_{\mathcal{H}_1}\leq 0$, i.e., $\mathbb{P}_{\mathcal{H}_1}\geq\frac{1}{3}$, ε is decreasing so that γ_{op} is nonexistent.

Case 3: When $x\geq 0$ and $a\neq b$, for obtaining γ_{op}, we calculate the following equation

$$F(x)=\frac{\partial\varepsilon}{\partial x}=(-\frac{1}{a}\mathbb{P}_{\mathcal{H}_0}+\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x}{a}}-\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x}{b}}=0. \tag{17}$$

After some simplification, we have the result that $x^*=\frac{ab}{b-a}\ln[(\frac{b}{a}-1)\frac{\mathbb{P}_{\mathcal{H}_0}}{\mathbb{P}_{\mathcal{H}_1}}+1]$ is the unique extreme point of the function ε. Note that in this expression of x^*, the values of the four parameters, i.e., a, b, $\mathbb{P}_{\mathcal{H}_0}$, and $\mathbb{P}_{\mathcal{H}_1}$ are supposed to satisfy the relational expression, $\frac{b}{a}>1-\frac{\mathbb{P}_{\mathcal{H}_1}}{\mathbb{P}_{\mathcal{H}_0}}$, which is achievable because DP_n can adjust its transmission power freely. Then, we need to prove that x^* is a minimum, which can be proved if the following two inequations are satisfied simultaneously

$$F(x^*-\Delta)<0, \tag{18}$$
$$F(x^*+\Delta)>0, \tag{19}$$

under the condition that $F(x^*)=0$, where $\Delta>0$. Eqs. (18) and (19) can be transformed to

$$(-\frac{1}{a}\mathbb{P}_{\mathcal{H}_0}+\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x^*}{a}}e^{\frac{\Delta}{a}}<\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x^*}{b}}e^{\frac{\Delta}{b}}, \tag{20}$$
$$(-\frac{1}{a}\mathbb{P}_{\mathcal{H}_0}+\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x^*}{a}}e^{-\frac{\Delta}{a}}>\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x^*}{b}}e^{-\frac{\Delta}{b}}, \tag{21}$$

respectively. Here, taking Eq. (20) as an example, the proof is given in the following two subcases.

Subcase 1: When $a>b>0$, by using $F(x^*)=0$, we have the following result

$$(-\frac{1}{a}\mathbb{P}_{\mathcal{H}_0}+\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x^*}{a}}=\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x^*}{b}}>0. \tag{22}$$

Moreover, since $0<e^{\frac{\Delta}{a}}<e^{\frac{\Delta}{b}}$, Eq. (20) is true in Subcase 1.

Subcase 2: When $0<a<b$, by using $F(x^*)=0$, we have the following result

$$(-\frac{1}{a}\mathbb{P}_{\mathcal{H}_0}+\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1})e^{-\frac{x^*}{a}}=\frac{1}{a-b}\mathbb{P}_{\mathcal{H}_1}e^{-\frac{x^*}{b}}<0. \tag{23}$$

Moreover, since $e^{\frac{\Delta}{a}}>e^{\frac{\Delta}{b}}>0$, Eq. (20) is true in Subcase 2.

Thus, Eq. (18) is proved. Similarly, Eq. (19) can be proved, and we reach the conclusion that x^* is a minimum of ε, i.e., $\gamma_{op}=\frac{ab}{b-a}\ln[(\frac{b}{a}-1)\frac{\mathbb{P}_{\mathcal{H}_0}}{\mathbb{P}_{\mathcal{H}_1}}+1]+\sigma_W^2$. Finally, based on the above discussion, the optimal detection threshold γ_{op} is given in Theorem 1, and the minimal detection error rate ε_{min} can be obtained by submitting Eq. (13) into (12). ■

B. COVERT CONSTRAINTS

Given $\varepsilon_{\min}$ by Theorem 1, we focus on how to ensure that the content sharing between DP_n and DR_n is covert even in the worst case. Formally, according to [23], we propose the covert constraints to guarantee the security of content sharing between DP_n and DR_n, when D_n reuses the uplink spectrum of C_m, which is illustrated by Theorem 2.

Theorem 2: When the uplink spectrum of C_m is reused by D_n, the content sharing between DP_n and DR_n is guaranteed to be covert only if the following constraint is satisfied, i.e.,

$$\varepsilon^*\geq\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}-\xi, \tag{24}$$

where ε^* is given by Eq. (15), and $\xi\in[0,1]$ denotes the equipment defect of the detector, i.e., a radiometer.

Proof: According to [23], when D2D pair D_n reuses the uplink spectrum of C_m, the D2D content sharing between DP_n and DR_n is ensured to be covert if the following inequation is satisfied, i.e.,

$$\varepsilon_{min}\geq\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}-\xi. \tag{25}$$

Here, ε_{min} is obtained by Eq. (14) in Theorem 1. Specifically, when $x<0$, it can be easily seen that $\mathbb{P}_{\mathcal{H}_0}\geq\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}>\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}-\xi$, since $\xi\geq 0$. When $x\geq 0$ and $a=b$ and $\mathbb{P}_{\mathcal{H}_1}\geq\frac{1}{3}$, similarly, $\mathbb{P}_{\mathcal{H}_1}\geq\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}>\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}-\xi$. When $x\geq 0$ and $a=b$ and $\mathbb{P}_{\mathcal{H}_1}<\frac{1}{3}$, Eq. (25) is equivalent to $1-2\mathbb{P}_{\mathcal{H}_1}\geq 2\mathbb{P}_{\mathcal{H}_1}-\xi$. Moreover, it can be transformed to $\mathbb{P}_{\mathcal{H}_1}\leq\frac{1+\xi}{3}$, which is always true since $\mathbb{P}_{\mathcal{H}_1}<\frac{1}{3}$ and $\xi\geq 0$. When $x\geq 0$ and $a\neq b$, it is a sufficient condition for Eq. (25) that $\varepsilon^*\geq\min\{\mathbb{P}_{\mathcal{H}_0},\mathbb{P}_{\mathcal{H}_1}\}-\xi$. ■

As shown in the formulas above, the instantaneous channel state information of warden's monitoring channels is unnecessary in order to guarantee the covert communication between D2D pairs, which further demonstrates the advantage of the covert communications.

IV. MATCHING GAME BASED RESOURCE ALLOCATION

In this section, we address the issue of resource allocation in D2D content sharing, i.e., the joint issue of spectrum allocation and power control, to achieve the following two goals: *i*) The process of sharing the contents between each DP_n and DR_n should be covert. More importantly, the robustness of covert communication should be guaranteed, especially considering some extremely adverse environments. *ii*) The basic QoS requirements of both the D2D pairs and the cellular users should be satisfied simultaneously. Obviously, from the perspective of D2D pairs, they have their own priorities. Once a D2D pair determines to reuse the uplink spectrum of a cellular user, it is actually matched with this cellular user. Similarly, from the perspective of cellular users, they have their own priorities. Once a cellular user determines to share its uplink spectrum with a D2D pair, it is actually matched with this D2D pair. Hence, we will model the issue of spectrum allocation and power control as a two-sided matching

problem. Obviously, it is not easy to earn the benefit from matching with each other in a tractable manner.

Considering the matching game can bring both of the D2D pairs and the cellular users with mutual benefit in a distributed manner, we will further model the two-sided matching problem as an *one-to-one* matching game and transform the power control into the preference establishment of this matching game. As such, a covert constraints guaranteed resource allocation algorithm based on the Gale-Shapley algorithm in [37] is proposed, and we analyze its properties, such as stability, convergence, optimality, complexity, and scalability.

A. TWO-SIDED MATCHING PROBLEM FORMULATION

Once D2D pair D_n is matched with cellular user C_m, D_n will reuse the uplink spectrum of C_m. Then, as shown in Eq. (1), DR_n suffers from the CCI caused by C_m. Thus, the signal to interference plus noise ratio (SINR) of the D2D link between DP_n and DR_n is denoted by

$$\eta_{D_n}^{C_m} = \frac{p_{D_n}^{C_m} \left|h_{DP_n,DR_n}\right|^2 d_{DP_n,DR_n}^{-\alpha}}{p_{C_m} \left|h_{C_m,DR_n}\right|^2 d_{C_m,DR_n}^{-\alpha} + \sigma_{DR_n}^2}. \tag{26}$$

Then, we define the normalized achievable rate of the D2D link between DP_n and DR_n under constraint (24) as the covert rate of D2D pair D_n. Without special declaration, R_{D_n,C_m}^{cov} refers to the covert rate of D2D pair D_n when it is matched with C_m, represented by

$$R_{D_n,C_m}^{cov} = \log_2(1 + \eta_{D_n}^{C_m}(p_{D_n}^{C_m})), \tag{27}$$

where $p_{D_n}^{C_m} \in \mathbf{p}_{D_n}^{C_m}$, and $\mathbf{p}_{D_n}^{C_m}$ denotes the solution set of $p_{D_n}^{C_m}$ that satisfies the covert constraint (24). At the same time, the BS suffers from the CCI generated by DP_n, and thus the uplink SINR of cellular user C_m is denoted by

$$\eta_{C_m}^{D_n} = \frac{p_{C_m} \left|h_{C_m}\right|^2 d_{C_m}^{-\alpha}}{p_{D_n}^{C_m} \left|h_{DP_n}\right|^2 d_{DP_n}^{-\alpha} + \sigma^2}, \tag{28}$$

where h_{C_m} and d_{C_m} denote the channel coefficients and distance from C_m to the BS, similarly, h_{D_n} and d_{D_n} denote the distance from D_n to the BS, and σ^2 is the AWGN variance at the BS. Then, the normalized achievable uplink rate of C_m can be obtained by

$$R_{C_m,D_n} = \log_2(1 + \eta_{C_m}^{D_n}). \tag{29}$$

Denoting two $M \times N$ matrices $\mathbf{y}$ and $\mathbf{z}$ as the matching decisions of D2D pairs $\mathcal{D}$ and cellular users $\mathcal{C}$, respectively. $[\mathbf{y}]_{m,n} = y_{C_m,D_n}$ and $[\mathbf{z}]_{m,n} = z_{C_m,D_n}$. Specifically, both y_{C_m,D_n} and z_{C_m,D_n} are binary variables. $y_{C_m,D_n} = 1$ indicates that D_n would like to reuse the uplink spectrum of C_m, and $y_{C_m,D_n} = 0$, otherwise. Similarly, $z_{C_m,D_n} = 1$ denotes that C_m prefers D_n to reuse its uplink spectrum, and $z_{C_m,D_n} = 0$. Otherwise. $\mathbf{p_D}$ denotes the set of transmission power adopted by $\forall DP_n \in \mathcal{DP}$ when matched with $\forall C_m \in \mathcal{C}$, where $\mathbf{p_D} \in \mathbb{R}^{M\times N}$, $[\mathbf{p_D}]_{m,n} = p_{D_n}^{C_m}$.

For each D2D pair $D_n \in \mathcal{D}$, the matching problem among itself and all the cellular users in $\mathcal{C}$ is formulated as a maximum covert rate matching problem based on Eq. (27), i.e.,

$$\max_{\mathbf{y},\mathbf{p_D}} \sum_{C_m\in C} y_{C_m,D_n} R_{D_n,C_m}^{cov}(p_{D_n}^{C_m}), \tag{30a}$$

$$s.t.\ y_{C_m,D_n} \in \{0,1\}, \quad \forall C_m \in \mathcal{C}, \tag{30b}$$

$$\sum_{C_m\in\mathcal{C}} y_{C_m,\ D_n} \le 1, \tag{30c}$$

$$0 < p_{D_n}^{C_m} \le p_D^{\max}, \quad \forall C_m \in \mathcal{C}, \tag{30d}$$

$$R_{C_m,D_n} \ge R_C^{thr}, \quad \forall C_m \in C, \tag{30e}$$

$$\varepsilon^* \ge \min\{\mathbb{P}_{\mathcal{H}_0}, \mathbb{P}_{\mathcal{H}_1}\} - \xi, , \quad \forall C_m \in \mathcal{C}. \tag{30f}$$

In essence, the optimization problem in (30) is a joint spectrum allocation and power control problem for D2D pair D_n, in which the covert rate of D_n is maximized by determining the optimal cellular user and transmission power of DP_n while some constraints are satisfied. Specifically, constraints (30b) and (30c) ensure that a D2D pair can be matched with at most one cellular user, i.e., it can reuse the uplink spectrum of at most one cellular user. The transmission power range is given by (30d), which indicates that the transmission power of DP_n should be no more than $p_D^{\max}$. Constraint (30e) guarantees the basic QoS requirements of cellular users, where R_C^{thr} is the QoS threshold. The covert constraint between DP_n and DR_n is given by (30f) to guarantee the robustness of our scheme, which is equivalent to Eq. (24).

Similarly, for each cellular user $C_m \in \mathcal{C}$, the matching problem among itself and all the D2D pairs in $\mathcal{D}$ can be modeled as a maximum uplink rate matching problem based on Eq. (31), i.e.,

$$\max_{\mathbf{z}} \sum_{D_n\in\mathcal{D}} z_{C_m,D_n} R_{C_m,D_n}(p_{D_n}^{C_m,op}), \tag{31a}$$

$$s.t.\ z_{C_m,D_n} \in \{0,1\}, \quad \forall D_n \in \mathcal{D}, \tag{31b}$$

$$\sum_{D_n\in\mathcal{D}} z_{C_m,D_n} \le 1, \tag{31c}$$

where $p_{D_n}^{C_m,op}$ is the optimal transmission power adopted by DP_n when it is matched with C_m, which is derived from the optimization problem in (30), i.e., $p_{D_n}^{C_m,op} = \arg\max_{y_{C_m,D_n}=1, p_{D_n}^{C_m}} \sum_{C_m\in C} y_{C_m,D_n} R_{D_n,C_m}^{cov}(p_{D_n}^{C_m})$. In essence, the optimization problem in (31) investigates the optimal matching for cellular user C_m to maximize its achievable uplink rate with a given $p_{D_n}^{C_m,op}$, subject to the spectrum reusing rule that the uplink spectrum of C_m can be reused by at most one D2D pair, denoted by constraints (31b) and (31c). Besides, as illustrated from the objective function of optimization problem (31), the cellular users tend to share their uplink spectrum with the D2D pairs. This is due to the fact that cellular users may benefit from spectrum reusing because incentive mechanisms exist among the cellular users and the

D2D pairs, for instance, monetary incentives [38] and social relationship incentives [39].

Note that, it is difficult to find a solution that satisfies both the optimization problems in (30) and (31) due to the following facts: *i*) Optimization problem in (30) is a mixed integer nonlinear programming (MINLP) problem [40], which contains both binary variable y_{C_m,D_n} and continuous variable $p_{D_n}^{C_m}$. Such an optimization problem may be solved through exhaustive search, but high computation complexity limits its application, especially when the number of cellular users and D2D pairs in the network is large. *ii*) More importantly, solving one of the two optimization problems in (30) and (31) separately has an impact on the other, and thus the decisions of D2D pairs and cellular users may contradict with each other, which leads to an unstable and unsatisfying matching results. To deal with these challenges, we will introduce an *one-to-one* matching game model to reduce the complexity and reach a stable resource allocation result in a decentralized way.

B. MATCHING GAME MODELING AND PREFERENCE ESTABLISHMENT

In order to find a solution that satisfies both the optimization problems in (30) and (31), we introduce a two-sided *one-to-one* matching game to reach a stable matching result. In terms of mathematical expression, we formulate the two-sided *one-to-one* matching game as the tuple $(\mathcal{D}, \mathcal{C}, \mathcal{S}_\mathcal{D}, \mathcal{S}_\mathcal{C})$. Specifically, D2D pairs and cellular users act as players. Each D2D pair will be matched with at most one cellular user, and vice versa. $\mathcal{S}_\mathcal{D}$ and $\mathcal{S}_\mathcal{C}$ denote the preference profiles of D2D pairs $\mathcal{D}$ and cellular users $\mathcal{C}$, respectively. $\mathcal{S}_\mathcal{D} = \{S(D_n)\}_{D_n\in\mathcal{D}}$ and $\mathcal{S}_\mathcal{C} = \{S(C_m)\}_{C_m\in\mathcal{C}}$, where $S(D_n)$ denotes the preference profile of D2D pair D_n and $S(C_m)$ denotes the preference profile of cellular user C_m. Formally, based on the concepts of matching theory in [41], the notion of *one-to-one matching* is given as follows:

Definition 1 (One-to-One Matching): A one-to-one matching μ is defined as an allocation from $\mathcal{C}\bigcup\mathcal{D}$ to $\mathcal{C}\bigcup\mathcal{D}$, which is denoted by $\mu : \mathcal{C}\bigcup\mathcal{D} \to \mathcal{C}\bigcup\mathcal{D}$. For $C_m \in \mathcal{C}$, $\mu(C_m) = \mathcal{D}\bigcup\{C_m\}$ and for $D_n \in \mathcal{D}$, $\mu(D_n) = \mathcal{C}\bigcup\{D_n\}$. $\mu(C_m) = D_n$ if and only if $\mu(D_n) = C_m$.

Once the matching μ is obtained, the spectrum allocation issue is solved. Taking D_n and C_m as an example, if $\mu(C_m) = D_n$ and $\mu(D_n) = C_m$, we have $y_{C_m,D_n} = z_{C_m,D_n} = 1$, which indicates that D2D pair D_n reuses the uplink spectrum of cellular user C_m. Note that, the spectrum reusing rule shown in constraints (30b), (30c), (31b) and (31c) is actually satisfied during the matching process, which is due to the essence of *one-to-one* matching game. In what follows, the individual utilities of D2D pairs and cellular users are given firstly deriving from the optimization problems in (30) and (31), respectively. Then, by combining the individual utilities with the preference relation defined later, the preference profiles establishment process is implemented. Moreover, the power control problem is solved during the preference profile establishment process.

Specifically, for each $D_n \in \mathcal{D}$, when matched with C_m, its individual utility v_{C_m,D_n} is given by

$$v_{C_m,D_n} = \max_{y_{C_m,D_n}=1, p_{D_n}^{C_m}} \sum_{C_m\in\mathcal{C}} y_{C_m,D_n} R_{D_n,cov}^{C_m}(p_{D_n}^{C_m}), \quad (32)$$

subject to (30d), (30e) and (30f). By observing Eq. (32), it can be easily seen that v_{C_m,D_n} is monotone increasing with $p_{D_n}^{C_m}$. Thus DP_n can obtain an optimal individual utility by adopting a maximum transmission power $p_{D_n}^{C_m,op}$ that satisfies the above three constraints, i.e.,

$$p_{D_n}^{C_m,op} = \max\{p_D^{\max}, p_1^{\max}, p_2^{\max}\}, \quad (33)$$

where $p_1^{\max}=\frac{1}{|h_{DP_n}|^2 d_{DP_n}^{-\alpha}}(\frac{p_{C_m}|h_{C_m}|^2 d_{C_m}^{-\alpha}}{2^{R_C^{thr}}-1}-\sigma^2)$ denotes the maximum $p_{D_n}^{C_m}$ that satisfies (30e), and $p_2^{\max} = \max_{p_{D_n}^{C_m}\in\mathbf{p}_{D_n}^{C_m}} p_{D_n}^{C_m}$ denotes the maximum $p_{D_n}^{C_m}$ that satisfies (30f), which can be solved by some mathematical tools, such as one-dimensional search, gradient descent algorithm, etc. Note that the $p_{D_n}^{C_m,op}$ derived from Eq. (33) satisfies with the covert constraints, and thus the successful detection probability at the warden is low. In this way, the covert communication between DP_n and DR_n is guaranteed.

Similarly, u_{C_m,D_n} denotes the individual utility of $C_m \in \mathcal{C}$ when matched with D_n, given by

$$u_{C_m,D_n} = \max_{z_{C_m,D_n}=1, p_{D_n}^{C_m,op}} \sum_{D_n\in\mathcal{D}} z_{C_m,D_n} R_{C_m}^{D_n}(p_{D_n}^{C_m,op}). \quad (34)$$

The intuition of u_{C_m,D_n} is that cellular user C_m wants to maximize its achievable uplink rate.

Then, we define the preference relation $\succ$, which is used to show the priorities. Note that $\succ_\mathcal{D} = \{\succ_{D_n}\}_{D_n\in\mathcal{D}}$ and $\succ_\mathcal{C} = \{\succ_{C_m}\}_{C_m\in\mathcal{C}}$ denote, respectively, the sets of preference relations of D2D pairs and cellular users, which can be obtained by individual utilities. Formally, the notion of the preference relation is described as follows [42]:

Definition 2 (Preference Relation $\succ$): A preference relation $\succ$ is a reflexive, complete and transitive binary relation between the players in $\mathcal{C}$ and $\mathcal{D}$. Specifically, a strict preference relation $\succ_{D_n}$ is defined over the set $\mathcal{C}$ such that for any two cellular users, i.e., C_m and $C_{\hat{m}}$, we have

$$C_m \succ_{D_n} C_{\hat{m}} \Leftrightarrow v_{C_m,D_n} > v_{C_{\hat{m}},D_n}. \quad (35)$$

Similarly, a strict preference relation $\succ_{C_m}$ is defined over the set $\mathcal{D}$ such that for any two cellular users, i.e., D_n and $D_{\hat{n}}$, we have

$$D_n \succ_{C_m} D_{\hat{n}} \Leftrightarrow u_{C_m,D_n} > u_{C_m,D_{\hat{n}}}. \quad (36)$$

With the preference relation sets $\succ_\mathcal{D}$, $\succ_\mathcal{C}$ and individual utilities, $D_n \in \mathcal{D}$ and $C_m \in \mathcal{C}$ are able to build their preference profiles. Specifically, each $D_n \in \mathcal{D}$ employs $\succ_\mathcal{D}$ to rank all the cellular users in a descending order to form its preference profile $S(D_n)$. Similarly, each $C_m \in \mathcal{C}$ employs $\succ_\mathcal{C}$ to rank all the D2D pairs in a descending order to form its preference profile $S(C_m)$. Absolutely, $S(D_n)$ and $S(C_m)$ can be obtained by utilizing some sorting algorithms, such as Bubble sort.

C. ALGORITHM IMPLEMENTATION

In this subsection, we propose a distributed matching algorithm by exploiting the Gale-Shapley algorithm to obtain a stable *one-to-one* matching result used for spectrum allocation and an optimal power control strategy for pursuing a maximal sum covert rate of D2D pairs. Then, the covert constraints guaranteed resource allocation algorithm based on Gale-Shapley algorithm is summarized in Algorithm 1 and described in detail as follows.

The algorithm consists of two parts, i.e., preference profiles establishment and stable matching, and the power control issue is transformed into the former. During the preference profiles establishment (lines 2-8), each $D_n \in \mathcal{D}$ obtains its optimal transmission power $p_{D_n}^{C_m,op}$ when matched with C_m by Eq. (33). Then, individual utilities v_{C_m,D_n} and u_{C_m,D_n} are calculated by D2D pairs and cellular users according to Eqs. (32) and (34), respectively. With the preference relation, the preference profiles are established by Bubble sort algorithm. During the stable matching process (lines 9-32), the Gale-Shapley algorithm is adopted, which is also known as deferred acceptance algorithm [43]. Specifically, in the $t-$th iteration, each $D_n \in \mathcal{D}$ firstly proposes itself to the cellular user belonging to $\mathcal{C}$ who has the highest priority in the current preference profile of D_n, i.e., $S^{(t)}(D_n)$. Then, for each $C_m \in \mathcal{C}$, the D2D pairs that propose themselves to C_m in the $t-$th iteration form a set $J^{(t)}(C_m)$. Simultaneously, C_m determines a D2D pair belonging to $J^{(t)}(C_m)$ who has the highest ranking from $S^{(t)}(C_m)$, denoted by $D_{\tilde{n}}$ for convenience. If $D_{\tilde{n}} \succ_{C_m} \mu^{(t)}(C_m)$, C_m will select $D_{\tilde{n}}$ to replace its current partner. Otherwise, the matching result $\mu^{(t+1)}(C_m)$ remains unchange. Finally, all the D2D pairs and cellular users update their preference profiles based on the acceptance and rejection operations in the $t-$th iteration. After limited iterations, the stable matching results can be obtained, indicated by μ.

In order to implement Algorithm 1, at the beginning of each block, each $DP_n \in \mathcal{DP}$ and $C_m \in \mathcal{C}$ broadcast pilots so that their channel knowledge can be estimated due to the channel reciprocity according to [44]. Then, each $D_n \in \mathcal{D}$ and $C_m \in \mathcal{C}$ obtain their preference profiles according to their utilities by exploiting Bubble sort locally. After that, D2D pairs and cellular users interact with each other to obtain a stable matching result. Actually, D2D pairs just send acknowledgements like handshakes, and the corresponding cellular users respond to the proposals by selecting actions of acceptance or rejection. In this way, the proposed algorithm is implemented in a distributed and self-organizing manner without participation of the BS. Note that, the related factors are updated periodically, and the corresponding frequency is a predetermined value by the given length of each block. Thus, the algorithm can be implemented with the low storage cost.

D. PROPERTIES OF PROPOSED ALGORITHM

In this subsection, we propose the properties of the covert constraints guaranteed resource allocation algorithm and prove them. Firstly, the notion of stable matching is given according to [30]. Then, we prove the stability, convergence and optimality of the proposed algorithm. Finally, the complexity and scalability of the proposed algorithm are analyzed.

Definition 3 (Stable Matching): A matching μ is called stable, if and only if there does not exist a blocking pair $\{(D_n, C_m) | D_n \in \mathcal{D}, C_m \in \mathcal{C}\}$ that satisfies the following

Algorithm 1 Covert Constraints Guaranteed Resource Allocation Algorithm

1: **Initialization**: $t = 0$, $\mu^{(0)} = \emptyset$;
2: **for** $D_n \in \mathcal{D}$ **do**
3: Calculate $p_{D_n}^{C_m,op}$ for each $C_m \in \mathcal{C}$ according to (33), and store them in $\mathbf{p_D}$;
4: Obtain v_{C_m,D_n} with each $C_m \in \mathcal{C}$ according to (32) and sort all the $C_m \in \mathcal{C}$ in a descending order according to v_{C_m,D_n}, then obtain its initial preference profile $S^0(D_n)$;
5: **end for**;
6: **for** $C_m \in \mathcal{C}$ **do**
7: Obtain u_{C_m,D_n} with each $D_n \in \mathcal{D}$ according to (34), then sort all the $D_n \in \mathcal{D}$ in a descending order according to u_{C_m,D_n} to obtain its initial preference profile $S^0(C_m)$;
8: **end for**;
9: **while** $t = 0$ or $\mu^{(t)} \neq \mu^{(t-1)}$ for $t > 0$ **do**
10: **for** $D_n \in \mathcal{D}$ **do**
11: **if** D_n has not found a partner & $S^{(t)}(D_n) \neq \emptyset$ **then**
12: Propose itself to the cellular user who has the highest priority in its current preference profile $S^{(t)}(D_n)$;
13: **end if**;
14: **end for**;
15: **for** $C_m \in \mathcal{C}$ **do**
16: **if** C_m receives more than one proposal & $S^{(t)}(C_m) \neq \emptyset$ **then**
17: All the D2D pairs that propose themselves to C_m form a set $J^{(t)}(C_m)$;
18: Determine a D2D pair $D_{\tilde{n}}$ in $J^{(t)}(C_m)$, who has the highest priority from $S^{(t)}(C_m)$;
19: **if** $D_{\tilde{n}} \succ_{C_m} \mu^{(t)}(C_m)$ **then**
20: Accept $D_{\tilde{n}}$ as partner and reject $\mu^{(t)}(C_m)$, i.e., $\mu^{(t+1)}(C_m) = D_{\tilde{n}}$;
21: $J^{(t)}(C_m) = J^{(t)}(C_m) \backslash \{D_{\tilde{n}}\} \bigcup \mu^{(t)}(C_m)$;
22: **else**
23: Reject the proposal of $D_{\tilde{n}}$, i.e., $\mu^{(t+1)}(C_m) = \mu^{(t)}(C_m)$;
24: **end if**;
25: **for** $D_n \in J^{(t)}(C_m)$ **do**
26: $S^{(t+1)}(C_m) = S^{(t)}(C_m) \backslash \{D_n\}$;
27: $S^{(t+1)}(D_n) = S^{(t)}(D_n) \backslash \{C_m\}$;
28: **end for**;
29: **end if**;
30: **end for**;
31: $t = t + 1$;
32: **end while**
33: **Output**: μ.

constraints at the same time

$$C_m \succ_{D_n} \mu(D_n) \text{ and } D_n \succ_{C_m} \mu(C_m), \tag{37}$$

where $\mu(D_n)$ and $\mu(C_m)$ denote the current matching results of D_n and C_m, respectively.

Proposition 1 (Stability): The matching μ resulting from Algorithm 1 is stable.

Proof: According to Definition 3, if μ is not stable, there exists at least one blocking pair (D_n, C_m), $\mu(D_n) \neq C_m$, $C_m \succ_{D_n} \mu(D_n)$ and $D_n \succ_{C_m} \mu(C_m)$. Due to the preference relation $C_m \succ_{D_n} \mu(D_n)$, in the matching process, D2D pair D_n must have proposed itself to the cellular user C_m which can provide a higher individual utility than $\mu(D_n)$. Then, it can be inferred from the matching result $\mu(D_n) \neq C_m$ that C_m prefers $\mu(C_m)$ than D_n, i.e., $\mu(C_m) \succ_{C_m} D_n$. Actually, the condition $\mu(C_m) \succ_{C_m} D_n$ cannot hold when $D_n \succ_{C_m} \mu(C_m)$, which means that the blocking pair formed by C_m and D_n is not existent. Similarly, it can be proved that $C_m \succ_{D_n} \mu(D_n)$ and $\mu(C_m) \neq D_n$ are incompatible. Thus, the matching μ resulting from Algorithm 1 is stable. ■

Proposition 2 (Convergence): The proposed Algorithm 1 can converge to a stable matching result μ.

Proof: As described above, in the $t-$th iteration, D2D pair D_n propose itself to the cellular user C_m who is the highest priority of its current preference profile $S^{(t)}(D_n)$ and has not yet rejected D_n. Then, after the $t-$th iteration, D_n will not propose itself to C_m any more regardless of whether C_m accept or reject it in the $t-$th iteration. The analysis above implies that with the number of iterations t increasing, the preference profile of each $D_n \in \mathcal{D}$, i.e., $S^{(t)}(D_n)$ keeps decreasing. In this wise, the number of iterations is no more than the number of cellular users M. By combining the above conclusion with *Proposition 1*, we come to that the proposed Algorithm 1 converges to a stable matching result μ after limited iterations. ■

Proposition 3 (Optimality): The resulting matching μ is weak Pareto optimal for each D2D pair $C_m \in \mathcal{C}$.

Proof: By exploiting the notion of Pareto improvement proposed in [41], the proof of *Proposition 3* is given as follows. Assuming that there exists Pareto improvement for matching μ and cellular user C_m ($C_m \neq \mu(D_n)$) is the improvement for D2D pair D_n, we have $C_m \succ_{D_n} \mu(D_n)$. Then, we consider the following two conditions. *i*) C_m has not been matched in matching μ, i.e., $\mu(C_m) = \emptyset$. It is obvious that C_m prefers to select D_n as its partner, i.e., $D_n \succ_{C_m} \mu(C_m)$. Thus, (D_n, C_m) is a blocking pair for matching μ based on Definition 3. This contradicts *Proposition 1*. *ii*) C_m has been matched with $D_{\hat{n}}$ in matching μ, i.e., $\mu(C_m) = D_{\hat{n}}$. Due to the deferred acceptance property of our proposed algorithm, D_n would propose to C_m. However, C_m rejects the proposal of D_n so that they cannot form a pair later, which contradicts our assumption. Accordingly, *Proposition 3* is proved. ■

Remark 2 (Complexity): The complexity of Algorithm 1 consists of two parts, i.e., preference profiles establishment and stable matching. In order to establish the preference profiles in the single-cell network with N D2D pairs and M cellular users, each D2D pair ranks all the cellular users in a descending order according to the utilities by exploiting Bubble sort algorithm, and so do the cellular users. For each D2D pair, the complexity of preference establishment is $O(M \log(M))$. Thus, the total complexity of establishing the preference profiles for all the D2D pairs is $O(MN \log(M))$. Similarly, the total complexity of establishing the preference profiles for all the cellular users is $O(MN \log(N))$. Thus, the total complexity of preference profiles establishment is $O(MN \log(MN))$. In the process of stable matching, the worst case is when the preference profiles of all the D2D pairs for all the cellular users are the same [30]. The number of iterations is no more than N, and at each iteration, there are at most M cellular users to make proposals. Hence, the complexity of two-sided stable matching is $O(MN)$.

Remark 3 (Scalability): Similar to the scalability problems in [30], [45], considering a large scale network, two aspects of scalability problems should be taken into consideration. i) The signaling overhead and information exchanging increase as the scale of network grows large. ii) Some D2D pairs and cellular users may have more than one best matching candidates. In other words, there may exist two cellular users C_m and $C_{\hat{m}}$ that $v_{C_m,D_n} = v_{C_{\hat{m}},D_n}$. To address the first problem, a simple way is to delete the D_n and C_m that cannot be involved in a stable matching. $S(D_n)$ and $S(C_m)$ are consistent if deleting C_m from $S(D_n)$ represents that D_n is also removed from $S(C_m)$ [45]. To address the latter problem, a tie-breaking rule is proposed for the purpose of helping D_n and C_m make their decisions. Our algorithm employs "first come, first served" based on [30] as the tie-breaking rule.

TABLE 1. Simulation Parameters.

Parameters	values
Number of D2D Pairs N	5
Number of cellular users M	5
Path loss α	4
Transmission power of cellular users p_{C_m}	20dBm
Maximal transmission power of D2D providers $p_D^{\max}$	17dBm
Noise power at BS σ^2	-174dBm
Noise power at the warden σ_W^2	-174dBm
QoS requirement of cellular users R_C^{thr}	1bps/Hz
Probability of D2D providers sending a covert message $\mathbb{P}_{\mathcal{H}_1}$	0.8
Covert communication threshold ξ	0.1

V. SIMULATION RESULTS AND ANALYSIS

In this section, we provide extensive numerical results to verify the correctness of Lemma 1 and Theorem 1 and the properties of our proposed algorithm such as convergence and optimality. The related parameter settings are shown in Table 1 without special declarations. Also, the BS can cover an area of radius 100m. The noise power at $\forall DR_n \in \mathcal{DR}$ is -174dBm. The N D2D pairs and M cellular users are all

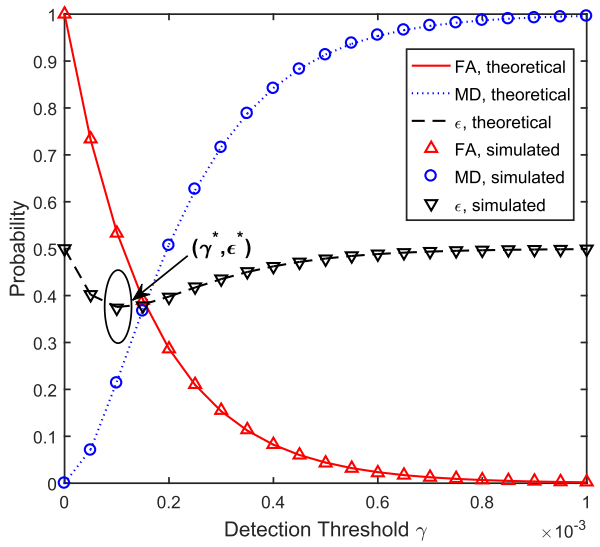


FIGURE 3. The detection performance of the warden versus detection threshold γ, when $p_{D_n}^{C_m} = 17dBm$, $d_{C_m,W} = d_{DP_n,W} = 5m$, $\mathbb{P}_{\mathcal{H}_0} = \mathbb{P}_{\mathcal{H}_1} = 0.5$.

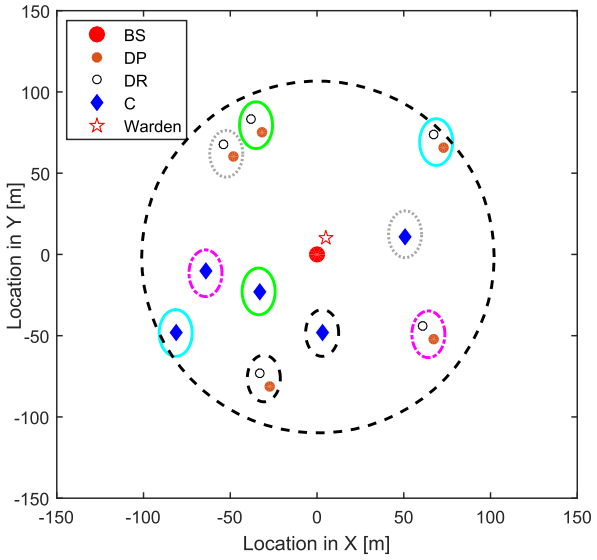


FIGURE 4. A snapshot of the matching results with an example network topology, where $M = N = 5$.

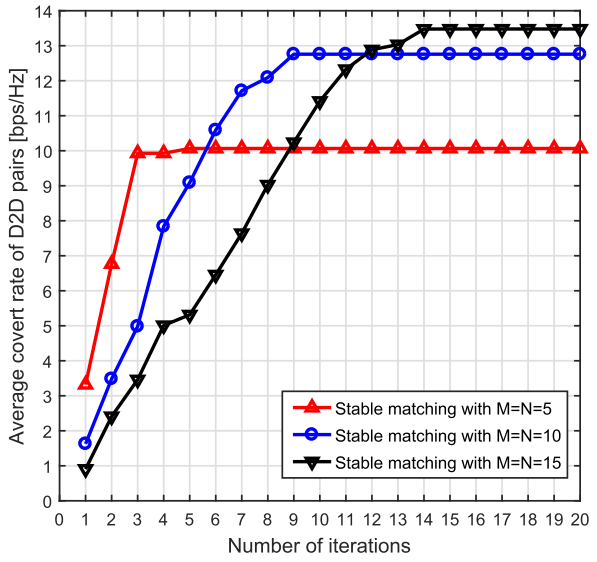


FIGURE 5. Average covert rate of D2D pairs versus the number of iterations, when $M = N = 5, 10, 15$.

distributed randomly in the single-cell network. Note that in the simulations, we compare our proposed algorithm with other three kinds of approaches in [40], i.e., random power with stable matching, optimal power with random matching, and random power with random matching. In particular, in the first and third algorithms, we allocate the transmission power of DP_n randomly in the range of $(0, p_{D_n}^{C_m,op}]$. While in the second and third approaches, D2D pairs and cellular users are matched randomly. Moreover, we compare our proposed algorithm with the exhaustive search to evaluate its efficiency. In order to eliminate the impact of randomness and obtain statistical average values, we have run hundreds of simulations.

In Fig. 3, we investigate the probabilities of FA, MD and detection error rate ε versus the detection threshold γ in a given covert communication model where the related parameters are presented in the caption. It can be seen that the simulation results are well fit with the theoretical results, which verifies the correctness of Lemma 1 and Theorem 1. In particular, $\mathbb{P}_{FA}$ is a monotonically decreasing function with respect to γ while $\mathbb{P}_{MD}$ is monotonically increasing. Mathematically, this is due to the monotonicity of exponential function. Then, detection error rate ε is derived from $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$, which is decreasing first and then increasing. When γ is small, $\mathbb{P}_{FA}$ plays a crucial role in the detection error rate ε because the warden mistakenly identifies an interference signal as a desired signal. As γ increases, on the contrary, the warden mistakenly identifies a desired signal as an interference signal, thus $\mathbb{P}_{MD}$ plays a key role in the detection performance at the warden. Hence there exists a minimum value of ε shown as $(\gamma^*, \varepsilon^*)$ in the figure, which can be derived from Eqs. (13) and (14) mathematically. Actually, the values of γ^* and ε^* are related to the parameters such as $p_{D_n}^{C_m}$, $d_{C_m,W}$ $d_{DP_n,W}$, $\mathbb{P}_{\mathcal{H}_0}$, and $\mathbb{P}_{\mathcal{H}_1}$. In this work, we focus on deriving the closed-form expressions of γ^* and ε^*, and based on which, the covert constraints are proposed as Eq. (24). Then, the constraints are satisfied in process of preference profiles establishment, and thus the low successful detection probability at the warden is guaranteed. As a result, the covert communications between D2D pairs are guaranteed.

Fig. 4 represents a snapshot of the network topology with spectrum reusing results. Each D2D pair and the cellular user whose uplink spectrum is reused by the D2D pair are circled using the same color. It can be seen that the spectrum reusing results does not just depend on the distance between D2D pairs and cellular users due to the fact that block fading wireless channels are considered in the network. Fig. 5 verifies the convergence of the proposed algorithm in three network

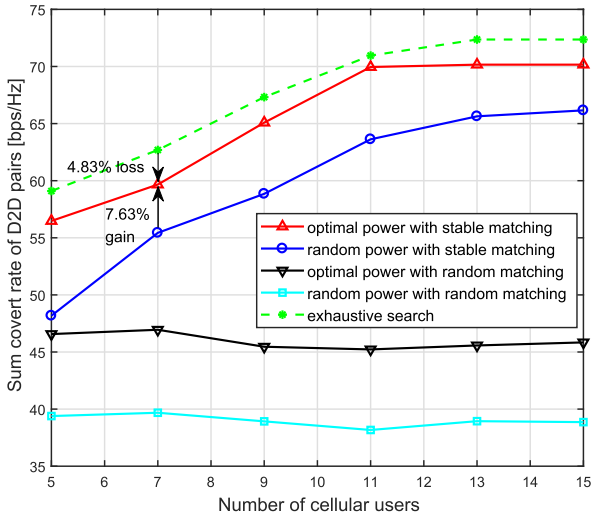


FIGURE 6. Sum covert rate of D2D pairs versus the number of cellular users M.

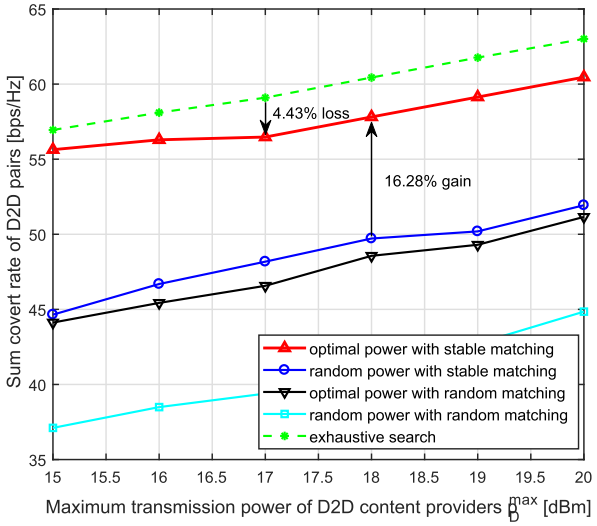


FIGURE 7. Sum covert rate of D2D pairs versus the maximum transmission power of D2D content providers $p_D^{\max}$.

topologies of different sizes, i.e., $M = N = 5, 10, 15$. The numbers of iterations are 5, 9, 14, respectively. Although the number of iterations is increasing while the network grows in size, it is no more than the number of cellular users M, as analyzed in *Proposition 2*. Besides, it can be seen from Fig. 5 that the average covert rate of D2D pairs increases while the size of network grows large. This is due to the fact that each D2D pair has more selected objects, that is, each D2D pair is able to select the cellular user who could bring a higher individual utility v_{C_m,D_n} to reuse its uplink spectrum. However, the average covert rate of D2D pairs improves slowly with the growing network scale when the network scale is large enough. It is because that each D2D pair has selected a preferred enough cellular user.

In Fig. 6-9, we investigate the performance of the proposed algorithm with some other existing approaches versus some vital parameters. As shown in these figures, the exhaustive

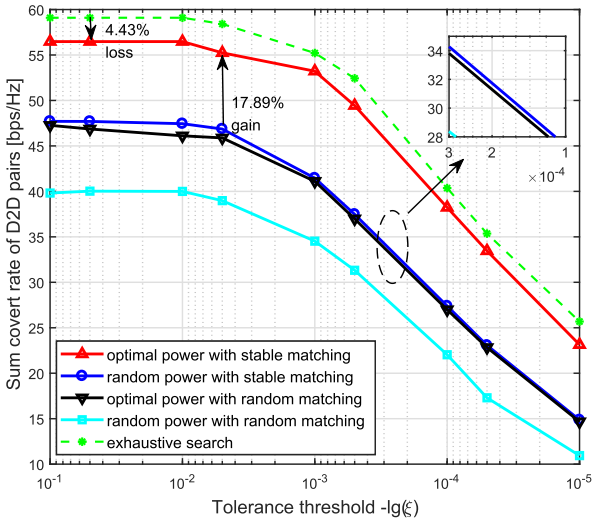


FIGURE 8. Sum covert rate of D2D pairs versus the covert constraints threshold ξ.

search is always the optimal while the random power with random matching algorithm is always the worst. Our proposed algorithm performs near-optimal, and has no more than 4.83% performance loss compared with the exhaustive search under different simulation parameters, which further demonstrates its efficiency. Besides, our proposed algorithm has significant performance gain compared with the other three baselines, which is at least 7.63%.

Specifically, Fig. 6 shows the sum covert rate of D2D pairs versus the number of cellular users M. The sum covert rates of D2D pairs in the proposed algorithm and random power with stable matching algorithm grow bigger with the number of cellular users increasing. The reason is that each D2D pair has more selected objects i.e., cellular users, as the number of cellular users increases, so that each D2D pair is more likely to be matched with a cellular user who could bring it with a higher individual utility v_{C_m,D_n}. However, the sum cover rates of D2D pairs in the two algorithms using random matching approaches are almost invariable because the randomness of random matching makes the increasing number of cellular users meaningless.

Fig. 7 shows the sum cover rate of D2D pairs versus the maximum transmission power of D2D content providers $p_D^{\max}$. Actually, as the maximum transmission power of D2D providers increases, the sum covert rates of D2D pairs in all the algorithms grow bigger. This is due to the fact that D2D providers may adjust its transmission power $p_{D_n}^{C_m}$ to a larger value based on Eq. (33). Meanwhile, covert rate R_{D_n,C_m}^{cov} is monotonically increasing with transmission power $p_{D_n}^{C_m}$ according to Eqs. (26) and (27). Thus, a higher sum covert rate of D2D pairs could be obtained with the maximum transmission power of D2D content providers $p_D^{\max}$ increasing. In the following numerical results, the parameters have impact on the sum covert rate of D2D pairs indirectly by affecting the transmission power of D2D providers $p_{D_n}^{C_m}$.

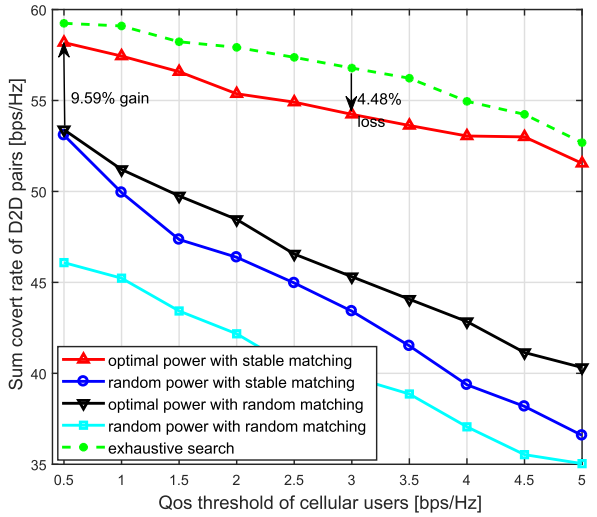


FIGURE 9. Sum covert rate of D2D pairs versus the QoS threshold of cellular users R_C^{thr}.

Fig. 8 shows the sum rate of D2D pairs versus the covert constraints threshold ξ. In order to observe the relationship between them clearly, logarithmic coordinate $-\lg(\xi)$ is adopted in this figure. It can be seen that with the covert constraints threshold ξ decreasing, the sum covert rates of D2D pairs decrease. Because a tighter threshold ξ limits the range of transmission power $p_{D_n}^{C_m}$ according to (30e), which indicates a smaller $p_2^{\max}$ in Eq. (33). Hence, we come to the results that the sum covert rate of D2D pairs decreases with the covert constraints threshold ξ decreasing.

Fig. 9 shows the sum covert rate of D2D pairs versus the QoS threshold of cellular users R_C^{thr}. As shown in the figure, the sum rates of D2D pairs decrease with the QoS threshold of cellular users R_C^{thr} increasing. It is due to the fact that R_C^{thr} is monotonically decreasing with transmission power $p_{D_n}^{C_m}$ based on Eqs. (28) and (29). Thus a larger R_C^{thr} leads to a tight range of $p_{D_n}^{C_m}$, i.e., a smaller $p_1^{\max}$ in Eq. (33). Hence, we come to the results that the sum covert rate of D2D pairs decreases with the QoS threshold of cellular users threshold R_C^{thr} increasing.

VI. CONCLUSIONS

In this paper, a novel secure and efficient resource allocation scheme for covert communication in D2D content sharing scenario is proposed to ensure both the security and efficiency of D2D content sharing. Specifically, the covert communication in D2D content sharing is achieved with the assistance of cellular users by utilizing the CCI introduced by spectrum reusing under block fading wireless channels. We present the false alarm rate and miss detection rate at the warden, and from which the total detection error rate at the warden is derived. To guarantee the robustness of our scheme, the optimal detection threshold and minimal detection error rate at the warden are given in closed-form expressions. Base on the above analyses, the covert constraints are learnt to ensure the security of D2D content sharing. Then, we formulate the joint spectrum allocation and power control problem as a two-sided matching problem to maximize the sum covert rate of D2D pairs in the network while guaranteeing the covert constraints. In order to solve it in a tractable manner, we model it as an *one-to-one* matching game, and a covert constraints guaranteed resource allocation algorithm based on Gale-Shapley algorithm is proposed to solve the matching game, followed by its properties analyses, such as stability, optimality, convergence, and complexity. Finally, extensive simulation results are given to verify our theoretical analyses and the properties of the proposed algorithm. Moreover, we investigate the impact of some key parameters like the number of cellular users, QoS threshold of cellular users, maximum transmission power of D2D providers and covert constraints threshold on the sum covert rate of D2D pairs.

REFERENCES

[1] L. Zhou, D. Wu, J. Chen, and Z. Dong, "When computation hugs intelligence: Content-aware data processing for industrial IoT," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1657–1666, Jun. 2018.
[2] V. W. S. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge University Press, 2017.
[3] D. Wu, L. Zhou, Y. Cai, and Y. Qian, "Collaborative caching and matching for d2d content sharing," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 43–49, Jun. 2018.
[4] D. Wu, L. Zhou, and Y. Cai, "Social-aware rate based content sharing mode selection for D2D content sharing scenarios," *IEEE Trans. Multimedia*, vol. 19, no. 11, pp. 2571–2582, Nov. 2017.
[5] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.
[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[7] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for device-to-device communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 336–340.
[8] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5766–5777, Jul. 2018.
[9] M. Zhang and Y. Liu, "Secure beamforming for untrusted MISO cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4861–4872, Jul. 2018.
[10] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.
[11] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a Poisson field of interferers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6005–6017, Sep. 2018.
[12] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46–52, Dec. 2018.
[13] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[14] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
[15] S. Yan, B. He, Y. Cong, and X. Zhou, "Covert communication with finite blocklength in AWGN channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[16] 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 Commun. Lett.*, vol. 8, no. 1, pp. 317–320, Feb. 2019.
[17] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on awgn channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[18] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[19] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 2945–2949.

[20] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[21] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2229–2233.

[22] X. Wang, Y. Liu, X. Lu, S. Lv, Z. Shi, and L. Sun, "CovertMIMO: A covert uplink transmission scheme for MIMO systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

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

[24] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[25] J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert communications with a full-duplex receiver over wireless fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

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

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

[28] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.

[29] Y. Long, D. Wu, Y. Cai, and J. Qu, "Joint cache policy and transmit power for cache-enabled D2D networks," *IET Commun.*, vol. 11, no. 16, pp. 2498–2506, Nov. 2017.

[30] D. Wu, L. Zhou, Y. Cai, H.-C. Chao, and Y. Qian, "Physical–social-aware D2D content sharing networks: A provider–demander matching game," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7538–7549, Aug. 2018.

[31] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

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

[33] Q. Wu, Y. Xu, J. Wang, L. Shen, J. Zheng, and A. Anpalagan, "Distributed channel selection in time-varying radio environment: Interference mitigation game with uncoupled stochastic learning," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4524–4538, Nov. 2013.

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

[35] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*. New York, NY, USA: Springer, 2008.

[36] A. Browder, *Mathematical Analysis: An Introduction*. New York, NY, USA: Springer-Verlag, 1996.

[37] S. Bayat, Y. Li, L. Song, and Z. Han, "Matching theory: Applications in wireless communications," *IEEE Signal Process. Mag.*, vol. 33, no. 6, pp. 103–122, Nov. 2016.

[38] L. Pu, X. Chen, J. Xu, and X. Fu, "D2D fogging: An energy-efficient and incentive-aware task offloading framework via network-assisted D2D collaboration," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3887–3901, Dec. 2016.

[39] C. Yi, S. Huang, and J. Cai, "An incentive mechanism integrating joint power, channel and link management for social-aware D2D content sharing and proactive caching," *IEEE Trans. Mobile Comput.*, vol. 17, no. 4, pp. 789–802, Apr. 2018.

[40] Z. Zhou, C. Gao, C. Xu, T. Chen, D. Zhang, and S. Mumtaz, "Energy-efficient stable matching for resource allocation in energy harvesting-based device-to-device communications," *IEEE Access*, vol. 5, pp. 15184–15196, 2017.

[41] C. Xu, C. Gao, Z. Zhou, Z. Chang, and Y. Jia, "Social network-based content delivery in device-to-device underlay cellular networks using matching theory," *IEEE Access*, vol. 5, pp. 924–937, 2017.

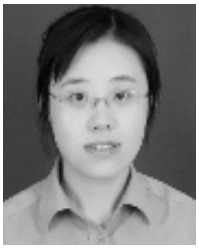
[42] J. Zhao, Y. Liu, K. K. Chai, Y. Chen, and M. Elkashlan, "Joint subchannel and power allocation for NOMA enhanced D2D communications," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 5081–5094, Nov. 2017.

[43] D. Gale and L. S. Shapley, "College admissions and the stability of marriage," *Amer. Math. Monthly*, vol. 69, no. 1, pp. 9–15, Jan. 1962.

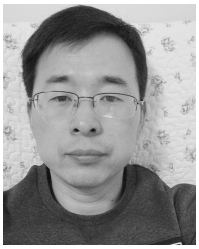
[44] X. Chen, Z. Zhang, H.-H. Chen, and H. Zhang, "Enhancing wireless information and power transfer by exploiting multi-antenna techniques," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 133–141, Apr. 2015.

[45] Z. Zhou, K. Ota, M. Dong, and C. Xu, "Energy-efficient matching for resource allocation in D2D enabled cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5256–5268, Jun. 2017.

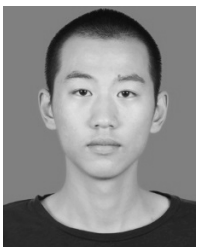
XIN SHI received the B.S. degree in electronic engineering from Peking University, China, in 2017. He is currently pursuing the M.S. degree with the College of Communications Engineering, Army Engineering University of PLA, Nanjing, China. His current research interests include D2D communications, resource management, content security, and game theory.



DAN WU received the B.S., M.S., and Ph.D. degrees from the Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2006, 2009, and 2012, respectively. She is currently an Associate Professor with the Army Engineering University of PLA, Nanjing. Her research interests include resource allocation and management, game theory, cooperative communications, and wireless sensor networks.



CHAO YUE received the B.S. and M.S. degrees from the PLA University of Science and Technology, Nanjing, China, in 2000 and 2007, respectively. He is currently a Lecturer with the College of Communications Engineering, Army Engineering University of PLA, Nanjing. His research interests include resource allocation and management, electronic design, and wireless communications.



CHENG WAN received the B.S. degree from the South China University of Technology, China, in 2018. He is currently pursuing the M.S. degree with the College of Communications Engineering, Army Engineering University of PLA. His current research interests include D2D communications, covert communications, content security, and resource management.

XINRONG GUAN received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2009 and 2014, respectively. His current research interests include physical layer security, wireless key generation, cooperative communications, and cognitive radio networks.