IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 1, 2019, accepted September 14, 2019, date of publication September 18, 2019,
date of current version September 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2942214

Trust Evaluation and Covert Communication-Based Secure Content Delivery for D2D Networks: A Hierarchical Matching Approach

XIN SHI[1], DAN WU[1], CHENG WAN[1], MENG WANG[1], AND YU ZHANG[1,2]
[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Sixty-Third Research Institute, National University of Defense Technology, 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 Excellent Young Scholars under Grant BK20170089, and in part by the Jiangsu Provincial Natural Science Fund for Outstanding Young Scholars under Grant BK20180028.

ABSTRACT In this paper, we investigate the secure content delivery issue for device-to-device networks based on the trust evaluation mechanism and covert communication model. Specifically, in order to stimulate the lasting and rational cooperation among mobile devices, we propose a trust evaluation mechanism, where the trust degree between two mobile devices can be obtained through historical assessed values. Simultaneously, a covert communication model is introduced to guarantee the undetectability of content delivery, which helps to stop malicious wardens adopting some coming external attacks. In this way, the availability and dependability of content sharing, as well the confidentiality and integrity of transmitted contents cam be guaranteed. Then, combining security-aware metrics, in terms of trust degree and covert rate, with physical layer transmission performances, in terms of achievable rate and successful delivery probability, we propose the definition of secrecy-aware effective rate to serve as a guidance on the joint optimization issue of content delivery mode selection and resource management, which is formulated as a social welfare maximization problem. To solve the complex problem tactfully, it is decoupled into two subproblems, i.e., mode selection which is a many-to-one matching problem, and resource management which is a one-to-one matching problem. By analyzing the interaction between two issues, a novel hierarchical stable matching algorithm is proposed to obtain three-dimension stable matching results. Its properties, such as stability, convergence, optimality, and complexity, are theoretically analyzed and proved. Finally, extensive numerical results are provided to demonstrate the advantages of our proposed algorithms.

INDEX TERMS Trust evaluation, covert communication, mode selection, resource management, hierarchical matching.

I. INTRODUCTION

A. BACKGROUNDS

With the data traffic in wireless networks growing at an unpredictable rate, device-to-device (D2D) content sharing has attracted wide attention. It can make full use of the limited computing, storage, and transmission capabilities of mobile devices, and then, it can bring significant gains such as high energy efficiency, low latency, and high data rate [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Leandros Maglaras.

Generally, there exist three main categories roles for the mobile devices in a typical D2D content sharing scenario. *i*) Some mobile devices who have content requests are denoted as demanders. *ii*) Some mobile devices who have stored some popular contents previously and can serve as content transmitters for the moment are taken as potential providers. *iii*) Other mobile devices act as ordinary cellular users.

Moreover, to achieve the precision and efficiency of D2D content sharing, content delivery needs to be carefully designed. It focuses on the pairing scheduling between

potential providers and demanders, as well the interference coordination between potential providers and ordinary cellular users. More specifically, the pairing scheduling between potential providers and demanders can be also regarded as the content delivery mode selection issue [2]. Most of the existing literature mainly consider the following two modes, i.e., *i*) base station (BS)-to-device (B2D) delivery mode, where the demander acquires its desired content from the BS directly, and *ii*) D2D delivery mode, where the demander will acquire its desired content from a single potential provider by establishing D2D link. Additionally, we propose a novel multi-device-to-device (MD2D) delivery mode in our previous work [3] to distract the pressures and boost the download speeds, where multiple potential providers deliver contents to a demander in a collaborative way. Moreover, the interference coordination between potential providers and cellular users is well known as the resource management issue and has been widely investigated [4]–[6], which actually consists of power control and radio resource allocation. The former focuses on the process of adjusting power levels for both cellular users and potential providers. The latter aims to make a precise allocation of spectrum resources for D2D pairs.

B. RELATED WORKS AND MOTIVATIONS

Despite the significant gains brought by D2D content sharing, serious concerns on security limit its widespread application. On one hand, due to the lack of central authority, i.e., the BS, it is difficult to guarantee the availability and dependability of content sharing. In other word, the selfishness and self-organization nature will enable the proactivity of mobile devices when acting as demanders, but negativity as potential providers. It will result in the dilemma that there are much more demanders than available potential providers [7]. On the other hand, traditional security issues in cellular networks depend on complex encryption and decryption mechanism, whereas which is not compatible with D2D communications. That is because of the limited computing resources of mobile devices, as well the decentralized and large-scale nature. Thus, the confidentiality and integrity of contents transmitted through D2D links are under serious threats [8]. In this regard, to guarantee the security and efficiency of content delivery for D2D networks, a series of technical questions need to be systematically answered.

Question 1: How to overcome the selfish behaviors such as free-riding for mobile devices, and stimulate the lasting and rational cooperation among them?

Due to the facts that mobile devices are carried by social individuals, their selfishness and limited resources such as energy, storage, and computing capabilities may result in that potential providers are unwilling to participate in the content sharing process. More seriously, selfish behaviors such as free-riding may well occur, which will severely undermine the cooperation among mobile devices. With this regard, a well-designed incentive mechanism is of great significance to guarantee the availability and dependability of content sharing. Most of the existing literature exploit some social metrics such as social similarity [9]–[11], which actually have two main shortcomings. *i*) Subjective consciousness of mobile devices is grossly neglected, which enables to reflect their cooperative intentions more accurately [12]. *ii*) The social metrics based incentive mechanisms will lead to the localization and homogenization of content sharing, i.e., more content sharing will happen among those who have similar social roles [13]. Q. Xu *et al*. in [14], [15] propose a trust evaluation mechanism for multi-homing edge computing-enabled heterogeneous networks. Utilizing its own historical assessed values towards others, rather than social metrics, a mobile device can preliminarily estimate the security features of other devices, which are characterized as trust degrees. In this way, the above shortcomings can be well overcome. Motivated by this, a straightforward trust evaluation mechanism is proposed in this work, which can be exploited to stimulate the lasting and rational cooperations among mobile devices. Besides, an efficient mode selection mechanism is needed to pair potential providers and demanders precisely by making full use of the obtained trust degrees.

Question 2: How to provide the content delivery with a high level of security assurance, so as to prevent the diversified external attacks imposed by a malicious warden?

Due to the more open network structure and lack of centralization, D2D content sharing is more vulnerable to diversified security threats. Traditional physical layer security technique focuses on enhancing the security of transmitted contents [16], whereas it ignores the undetectability of content delivery, which may lead to some external attacks adopted by the malicious wardens, such as eavesdropping and decoding attack, electronic countermeasure, and even physical means [17]. Note that the covert communication is a cutting-edge and emerging physical layer security technique, which can achieve the undetectable wireless transmissions [18]. If a wireless transmission is guaranteed to be undetectable, the malicious warden has no idea whether the content delivery happens or not, and thus, it cannot take further diversified external attacks. Generally, the covert communication can be achieved by exploiting the existence of interference (or noise) so that the warden cannot recognize the targeted signals from the interference (or noise) accurately. B. Bash *et al.* in [19] prove that $O(\sqrt{n})$ bits can be transmitted covertly in n channel uses from an information theoretical perspective, which is well known as the square root law. Then, covert communications under various application scenarios have attracted wide attention, such as relay-aided networks [20], [21] and unmanned aerial vehicle (UAV) enabled wireless transmission scenarios [22]. Unfortunately, there are few researches about the application of covert communications in D2D networks. Our previous work in [23] proposes a novel covert communication model for D2D underlaying cellular networks, where the co-channel interference introduced by spectrum reusing is utilized as the cover of transmitted contents to puzzle the detection at the malicious warden. As thus,

the covert communication model can be exploited to provide content delivery with a high level of security assurance. With this regard, precise co-channel interference coordination is required to guarantee the covert communication between potential providers and demanders, as well meet the quality of service (QoS) requirements of both cellular users and D2D pairs, which can be achieved through efficient resource management mechanisms.

Question 3: How to integrate the trust evaluation and covert communication into the content delivery process, and implement the joint optimization of mode selection and resource management in a concise and interpretable manner?

Recall that the trust evaluation and covert communication work on the mode selection and resource management respectively, and most of the existing literature focus on solving them separately by predetermining the results of the other one [24]–[26]. However, they are tightly coupled, and thus, integrating both the trust evaluation and covert communication into the content delivery process is of great significance. Combining security-aware metrics, in terms of trust degree and covert rate, with physical layer transmission performances, in terms of achievable rate and successful delivery probability (SDP), we propose a novel definition of secrecy-aware effective rate to serve as a guidance on the joint optimization issue of content delivery mode selection and resource management, which is formulated as a social welfare maximization problem.

To solve the complex joint optimization problem, matching theory has attracted our attention. That is mainly because the joint optimization issue is essentially a matching problem among potential providers, demanders, and ordinary cellular users. However, different from most of the two-sided matching problems in the existing literature [27]–[29], the joint issue is a three-dimension matching problem. Thus, how to design a distributed algorithm and obtain a three-dimension stable matching result is a challenge and meaningful work. In this regard, [30] gives us great inspirations, in which the authors investigate the three-dimensional matching graph, and propose a local search based algorithm. Although the stability of the matching results cannot be ensured, it provides us with great idea for solving three-dimension matching problems. In this work, a novel hierarchical matching approach is utilized to solve the joint issue in a concise and interpretable manner, which is proved to converge to a three-dimension stable matching result.

C. CONTRIBUTIONS AND ORGANIZATIONS

The secure content delivery based on trust evaluation and covert communication is investigated for D2D content sharing. The contributions of this work are summarized as the following three-folds.

- Considering the various security threats in D2D content sharing scenarios, we propose the trust evaluation mechanism and covert communication model to guarantee the availability and dependability of content sharing, as well the confidentiality and integrity of transmitted contents. In the former, mobile devices obtain their trust degrees towards others by exploiting their own historical assessed values. In the latter, the co-channel introduced by spectrum reusing is utilized to puzzle the malicious warden, as thus hide the content delivery process.
- By combining security-aware metrics, in terms of trust degree and covert rate, with physical layer transmission performances, in terms of achievable rate and successful delivery probability, the definition of secrecy-aware effective rate is proposed. Guided by this, the joint content delivery mode selection and resource management optimization issue is formulated as a social welfare maximization problem, aiming to achieve both high transmission performance and security assurance.
- To solve the intractable problem in a concise and interpretable manner, it is decoupled into two subproblems, i.e., mode selection which is a many-to-one matching problem, and resource management which is a one-to-one matching problem. Then, a novel hierarchical stable matching algorithm is proposed to obtain a three-dimension stable matching result. Theoretical analyses of its properties such as stability, convergence, and optimality are carried out. Finally, extensive simulation results are provided to demonstrate the advantages and properties of our proposed algorithms.

The remainder of this paper is organized as follows. In Section II, we introduce the network model, along with the trust evaluation mechanism and the covert communication model, so as to define the secrecy-aware effective rate. In Section III, we formulate the joint optimization issue as a social welfare maximization problem, and decouple it into two subproblems. By utilizing a hierarchical matching approach, the joint optimization issue is well solved in Section IV. Extensive simulation results are provided to evaluate the performance of our proposed algorithm in Section V. Section VI concludes this work and introduces our future works.

II. SYSTEM MODEL

A. NETWORK MODEL

Without loss of generality, we investigate the content delivery in a single-cell D2D underlaying cellular network shown as Fig. 1, where some users who carry smart devices are randomly distributed. The potential providers, demanders, and ordinary cellular users are denoted by $\mathcal{P} = \{p_1, \cdots, p_j, \cdots, p_{N_p}\}$, $\mathcal{D} = \{d_1, \cdots, d_i, \cdots, d_{N_d}\}$, and $\mathcal{C} = \{c_1, \cdots, c_n, \cdots, c_{N_c}\}$, where N_p, N_d, and N_c denote the number of potential providers, demanders, and ordinary cellular users, respectively. Moreover, a central BS is accessible for any user within the network, and the BS is connected with the content servers in the cloud thus it can be regarded as an omnipotent provider. In such a single-cell D2D network, three main categories content delivery modes for demanders obtaining their desired contents are considered, i.e., B2D

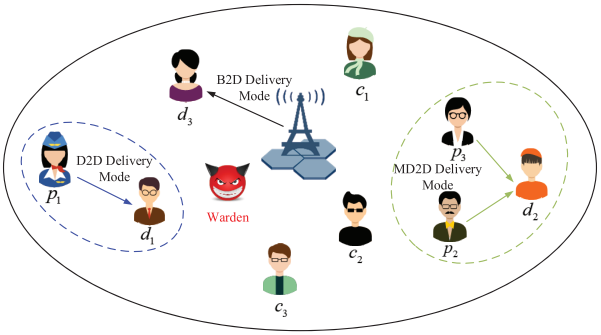


FIGURE 1. Single-cell D2D underlaying cellular network.

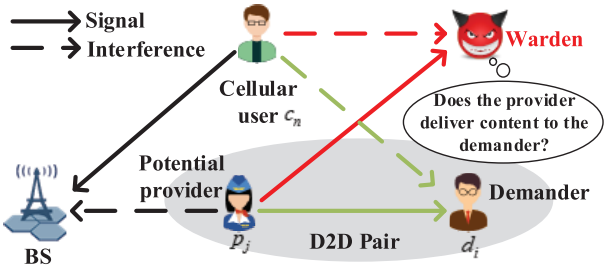


FIGURE 2. Covert communication model.

delivery mode shown as d_3 in Fig. 1, D2D delivery mode shown as p_1 and d_1, and MD2D delivery mode shown as p_2, p_3 and d_2.

More importantly, considering the openness of wireless channels and the lack of central authority in D2D content sharing scenario, it is faced with various security threats. On one hand, the lasting and rational cooperation among mobile devices may be destroyed by some selfish behavior such as free-riding. Thus, the availability and dependability of content sharing is threatened. On the other hand, the malicious warden[1] listens to the environment silently to judge whether the content delivery happens or not. Once it detects the content delivery successfully, further malicious acts will be taken to destroy the content delivery process so that the confidentiality and integrity of contents transmitted through D2D links cannot be guaranteed. In this regard, it is of great significance to provide D2D content sharing with high security assurance.

B. TRUST EVALUATION MECHANISM

Considering the evolution of roles, potential providers, demanders, and ordinary cellular users will transform into each other. In this regard, mobile devices are represented in a general way in this subsection. Specifically, the trust degree of u_k towards $u_{\hat{k}}$, denoted by $T_{u_k \to u_{\hat{k}}}$, is calculated base on the direct trust degree and indirect trust degree, where $u_k, u_{\hat{k}} \in \mathcal{U}, \mathcal{U} = \mathcal{P} \cup \mathcal{D} \cup \mathcal{C}$.

Direct trust degree is based on the assessed value of trust in each time of interaction between two devices, i.e.,

$$DT_{u_k \to u_{\hat{k}}} = \frac{1}{K_{u_k,u_{\hat{k}}}} \sum_{k=1}^{K_{u_k,u_{\hat{k}}}} v^k_{u_k \to u_{\hat{k}}} e^{-\omega(t - t^k_{u_k,u_{\hat{k}}})} \tag{1}$$

where $v_{u_k \to u_{\hat{k}}} \in [0, 1]$ is the assessed trust value of u_k towards $u_{\hat{k}}$ in the *kth* interaction, and the larger $v_{u_k \to u_{\hat{k}}}$, the more u_k trusts $u_{\hat{k}}$, $e^{-\omega(t - t^k_{u_k,u_{\hat{k}}})}$ denotes that the influence of assessed trust value decays with time, where t denotes the current time, $t^k_{u_k,u_{\hat{k}}}$ denotes the time of *kth* interaction, and ω denotes the decay parameter. Indirect trust degree of u_k towards $u_{\hat{k}}$ comes from the direct trust of other individuals in the networks towards $u_{\hat{k}}$ and the credibility degree of u_k towards other individuals, which is defined as

$$Cre_{u_k \to u_{\tilde{k}}} = \frac{DT_{u_k \to u_{\tilde{k}}}}{\sum\limits_{u_{\tilde{k}} \in \mathcal{U}, u_{\tilde{k}} \neq u_k} DT_{u_k \to u_{\tilde{k}}}}. \tag{2}$$

With credibility degree of other individuals, the indirect trust degree of u_k towards $u_{\hat{k}}$ is given by

$$IDT_{u_k \to u_{\hat{k}}} = \sum_{u_{\tilde{k}} \in \mathcal{U}, u_{\tilde{k}} \neq u_k} Cre_{u_k \to u_{\tilde{k}}} DT_{u_{\tilde{k}} \to u_{\hat{k}}}. \tag{3}$$

Based on (1) and (3), the trust degree of u_k towards $u_{\hat{k}}$ is

$$T_{u_k \to u_{\hat{k}}} = \tau_{u_k \to u_{\hat{k}}} DT_{u_k \to u_{\hat{k}}} + (1 - \tau_{u_k \to u_{\hat{k}}}) IDT_{u_k \to u_{\hat{k}}}, \tag{4}$$

where $\tau_{u_k \to u_{\hat{k}}}$ is given by

$$\tau_{u_k \to u_{\hat{k}}} = \frac{K_{u_k,u_{\hat{k}}}}{K_{u_k,u_{\hat{k}}} + \sum\limits_{u_{\tilde{k}} \in \mathcal{U}, u_{\tilde{k}} \neq u_k} Cre_{u_k,u_{\tilde{k}}} K_{u_k,u_{\tilde{k}}}}. \tag{5}$$

As shown in Eq. (5), as the number of interaction between u_k and $u_{\hat{k}}$, i.e., $K_{u_k,u_{\hat{k}}}$ increases, the value of $\tau_{u_k \to u_{\hat{k}}}$ also increases. It illustrates that u_k tends to rely more on his own judgement. Similarly, the trust degree of $u_{\hat{k}}$ towards u_k, i.e., $T_{u_{\hat{k}} \to u_k}$, can be obtained in the same way. Finally, trust degree between u_k and $u_{\hat{k}}$ is a definition that reflects the subjective consciousness of bidirectional conformity, which can be denoted by

$$T_{u_k,u_{\hat{k}}} = \tau_1 T_{u_k \to u_{\hat{k}}} + \tau_2 T_{u_{\hat{k}} \to u_k}, \tag{6}$$

where τ_1 and τ_2 are predetermined tunable parameters with constraint $\tau_1 + \tau_2 = 1$.

C. COVERT COMMUNICATION MODEL

To prevent the external attacks imposed by a malicious warden, the covert communication model in [23] is adopted in this work, where the co-channel interference introduced by uplink spectrum reusing is utilized as the cover of transmitted contents. The covert communication model is shown as Fig. 2. When potential provider p_j reuses the uplink spectrum of cellular user c_n to transmit contents to demander d_i, both the legal demander d_i and the malicious warden suffer from the co-channel interference from c_n.

The malicious warden listens to the environment silently to judge whether the content delivery between p_j and d_i happens

[1] Actually, the model can be extended to the scenario with multiple malicious wardens since each of them is relevant to this scenario of our work.

or not according to the average power of its received signals by utilizing a radiometer as its detector. As thus, a negligible successful detection probability at the warden should be guaranteed, which is the core of the covert communication. For this purpose, the following two-folds are important. *i*) The wireless channels in the network are independent quasi-static Rayleigh fading with equal block length [31], which means that the channel coefficients remain stationary in a block and change randomly and independently in the next block [32]. Thus, in each block, the average power of received signals at the warden will change randomly and independently. *ii*) The uplink spectrum reusing makes the warden suffer from the co-channel interference from c_n. More importantly, the co-channel interference can be changing and even dynamic under block fading wireless channels. Thus, the average power of received signals at the warden is time-varying. In this regard, the co-channel interference from c_n can be utilized to puzzle the detection at the warden.

Denoting $H_{u_k,\hat{u}_k}$ as the commonly used channel gain model between u_k and $u_{\hat{k}}$, $u_k, u_{\hat{k}} \in \mathcal{U} \cup \{Warden\}$, it can be represented as

$$H_{u_k,\hat{u}_k} = \left|h_{u_k,\hat{u}_k}\right|^2 d_{u_k,\hat{u}_k}^{-\alpha}, \tag{7}$$

where $h_{u_k,\hat{u}_k}$ and $d_{u_k,\hat{u}_k}$ denote the channel coefficient and distance between u_k and $u_{\hat{k}}$, α denotes the path loss exponent. Then, the average power of received signals at the warden in a given block, denoted as p_W, can be expressed as

$$p_W = \begin{cases} q_{c_n} H_{c_n,W} + \sigma_W^2, & if\, \mathcal{H}_0, \\ q_{p_j,d_i}^{c_n} H_{p_j,W} + q_{c_n} H_{c_n,W} + \sigma_W^2, & if\, \mathcal{H}_1, \end{cases} \tag{8}$$

where $q_{p_j,d_i}^{c_n}$ denote the transmission power of p_j when it reuses the uplink spectrum of c_n to transmit contents to d_i, q_{c_n} denotes the transmission power of c_n, σ_W^2 denotes the additive white Gaussian noise (AWGN) variance at the warden. $\mathcal{H}_1$ specifies the event that p_j enables to transmit contents to d_i covertly in the current block, and $\mathcal{H}_0$ otherwise. Accordingly, the probabilities of $\mathcal{H}_1$ and $\mathcal{H}_0$ are denoted as $\mathbb{P}_{\mathcal{H}_1}$ and $\mathbb{P}_{\mathcal{H}_0}$. Obviously, $\mathbb{P}_{\mathcal{H}_0} + \mathbb{P}_{\mathcal{H}_1} = 1$.

Recall that the warden judges whether the content delivery happens or not according to the average power of its received signals, i.e., $p_W \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \gamma$, where $\mathcal{D}_1$ and $\mathcal{D}_0$ are denoted as the correspondence to the decisions in favor of hypothesis $\mathcal{H}_1$ and $\mathcal{H}_0$, and γ is a predetermined detection threshold. Actually, there are two types of detection errors at the warden. *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 $\mathbb{P}_{MD} = \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1)$. Then, adopting equal prior probabilities in this work, i.e., $\mathbb{P}_{\mathcal{H}_0} = \mathbb{P}_{\mathcal{H}_1} = 0.5$, we define the detection error rate at the warden as $\varepsilon = \mathbb{P}_{FA} + \mathbb{P}_{MD}$, to characterize its detection performance.

Since the essence of covert communication is to guarantee a negligible successful detection probability at the warden, our purpose is to maintain $\varepsilon \geq 1 - \xi$ even considering some extremely adverse environments, where $\xi \in [0, 1]$ is a predetermined value, denoting the defect of warden's detector. The above inequation is denoted as the covert constraint, and theoretically, it is given as follows Theorem 1.

Theorem 1: When the uplink spectrum of c_n is reused by p_j, the content delivery between potential provider p_j and demander d_i is guaranteed to be covert only if the following constraint is satisfied,

$$\varepsilon^* \geq 1 - \xi, \tag{9}$$

where ε^* denotes the minimal detection error rate at the warden, and is given by $\varepsilon^* = \frac{b}{a-b}(e^{-\frac{\gamma^* - \sigma_W^2}{b}} - e^{-\frac{\gamma^* - \sigma_W^2}{a}}) + 1$. γ^* denotes the optimal detection threshold for the warden, and represented by $\gamma^* = \frac{ab}{a-b}\ln(\frac{b}{a}) + \sigma_W^2$, $a = q_{c_n} d_{c_n,W}^{-\alpha}$, $b = q_{p_j,d_i}^{c_n} d_{p_j,W}^{-\alpha}$.

Proof: The detailed analyses and derivations based on some mathematical methods are given in [23]. ■

Note that when p_j reuses the uplink spectrum of c_n to transmit contents to d_i, if the constraint (9) is satisfied, the content delivery between p_j and d_i can be always guaranteed covert [19], which can be utilized to guarantee the covert communications between potential providers and demanders during the content delivery process. Moreover, the covert rate between p_j and d_i is defined as its achievable rate under constraint (9). For convenience, we will use achievable rate and covert rate interchangeably later in this paper.

D. DEFINITION OF SECRECY-AWARE EFFECTIVE RATE

In the D2D underlaying cellular network, each cellular user is allocated with an orthogonal spectrum to communicate with the BS, and N_c cellular users totally occupy equal part of spectrum with a bandwidth W. Each potential provider is permitted to reuse the uplink spectrum of at most one cellular user to transmit contents to demanders, thus when p_j reuses the uplink spectrum of c_n, the achievable rate between provider p_j and demander d_i is represented as

$$R_{p_j,d_i}^{c_n} = \frac{W}{N_c}\log_2(1 + \frac{q_{p_j,d_i}^{c_n} H_{p_j,d_i}}{q_{c_n} H_{c_n,d_i} + \sigma_{d_i}^2}), \tag{10}$$

where $\sigma_{d_i}^2$ denotes the AWGN variance at demander d_i. Utilizing a binary variable y_{p_j,c_n} to indicate whether p_j reuses the uplink spectrum of c_n ($y_{p_j,c_n} = 1$) or not ($y_{p_j,c_n} = 0$), the achievable rate between p_j and d_i is formulated as

$$R_{p_j.d_i} = \sum_{c_n \in \mathcal{C}} y_{p_j,c_n} R_{p_j,d_i}^{c_n}. \tag{11}$$

Based on (11), the achievable rate for d_i to obtain its desired content f_{d_i} is denoted by

$$R_{d_i} = \sum_{p_i \in \mathcal{P}} \mu_{p_j}^{f_{d_i}} x_{p_j,d_i} R_{p_j.d_i}. \tag{12}$$

where $\mu_{p_j}^{f_{d_i}}$ is a binary variable utilized to indicate whether p_j has the desired content f_{d_i} of d_i in its cache ($\mu_{p_j}^{f_{d_i}} = 1$) or

not ($\mu_{p_j}^{f_{d_i}} = 0$), and x_{p_j,d_i} is a binary variable that indicates whether p_j collaborates with d_i to provide its desired content ($x_{p_j,d_i} = 1$) or not ($x_{p_j,d_i} = 0$).

Meanwhile, when the uplink spectrum of c_n is reused by p_j, the uplink achievable rate of c_n is represented as

$$R_{c_n}^{p_j,d_i} = \frac{W}{N_c}\log_2(1 + \frac{q_{c_n}H_{c_n}}{q_{p_j,d_i}^{c_n}H_{p_j} + \sigma^2}), \tag{13}$$

where H_{c_n} and H_{p_j} denote the channel gains between c_n and the BS, and between p_j and the BS, respectively. σ^2 is the AWGN variance at the BS. Similarly, the uplink achievable rate of c_n can be represented as

$$R_{c_n}=\frac{W}{N_c}\log_2(1+\frac{q_{c_n}H_{c_n}}{\sum\limits_{p_j\in\mathcal{P}}\sum\limits_{d_i\in\mathcal{D}} x_{p_j,d_i}y_{p_j,c_n}q_{p_j,d_i}^{c_n}H_{p_j}+\sigma^2}). \tag{14}$$

Moreover, a certain contact duration between p_j and d_i is required to transmit the content f_{d_i} successfully, which should be at least $s_{f_{d_i}}/R_{d_i}$, where $s_{f_{d_i}}$ denotes the size of content f_{d_i}. Some studies have pointed out that the contact duration between two mobile devices follows the gamma distribution [33], or the exponential distribution [34]. Here, the gamma distribution $\Gamma(\beta, \theta)$ is adopted to model the contact duration between two mobile devices, where β and θ are two parameters that define the shape of the distribution. Assuming that the contact processes among connected pairs are independent, we consider the gamma distributed contact duration T_c with probability density function (PDF) given by

$$g(T_c;\beta,\theta) = \begin{cases} \dfrac{T_c^{\beta-1}}{e^{\frac{T_c}{\theta}}\theta^{\beta}\Gamma(\beta)}, & if\, T_c \geq 0 \\ 0, & if\, T_c < 0. \end{cases} \tag{15}$$

As such, the success delivery probability for d_i obtaining its desired content f_{d_i} from p_j is characterized as

$$P_{p_j,d_i} = \Pr\{T_c \geq \frac{s_{f_{d_i}}}{R_{d_i}}\} = 1 - \frac{\Upsilon(\beta, \frac{s_{f_{d_i}}}{R_{d_i}\theta})}{\Gamma(\beta)}, \tag{16}$$

where $\Upsilon(\beta, \frac{s_{f_{d_i}}}{R_{d_i}\theta})$ is the lower incomplete Gamma function.

Based on the above definitions and analyses, we define the secrecy-aware effective rate for d_i obtaining f_{d_i} as

$$R_{d_i}^{se} = \sum_{p_i\in\mathcal{P}} \mu_{p_j}^{f_{d_i}} x_{p_j,d_i}R_{p_j.d_i}P_{p_j,d_i}T_{p_j,d_i}. \tag{17}$$

The secrecy-aware effective rate is defined by exploiting both security-aware metrics, in terms of trust degree and covert rate, and physical layer transmission performances, in terms of achievable rate and successful delivery probability. In essence, this definition is a joint characterization of both the transmission performance and security assurance, which is utilized to not only stimulate the lasting and rational cooperation between potential providers and demanders, but also provide content delivery with a high security assurance.

III. PROBLEM FORMULATION

In order to maximize the secrecy-aware effective rate defined previously, the overall problem can be formulated as a welfare maximization with multiple constraints, i.e.,

$$\begin{aligned} &\max_{\mathbf{X},\mathbf{Y},\mathbf{Q}} \sum_{d_i\in\mathcal{D}} R_{d_i}^{se} \\ &s.t.\ C_1: \sum_{d_i\in\mathcal{D}} x_{p_j,d_i} \leq 1, \quad \forall p_j \in \mathcal{P} \\ &\quad C_2: \sum_{p_j\in\mathcal{P}} x_{p_j,d_i} \leq quota, \quad \forall d_i \in \mathcal{D} \\ &\quad C_3: \mathbf{X} \in \{0,1\}^{N_p\times N_d} \\ &\quad C_4: \sum_{c_n\in\mathcal{C}} y_{p_j,c_n} \leq 1, \quad \forall p_j \in \mathcal{P} \\ &\quad C_5: \sum_{p_j\in\mathcal{P}} y_{p_j,c_n} \leq 1, \quad \forall c_n \in \mathcal{C} \\ &\quad C_6: \mathbf{Y} \in \{0,1\}^{N_p\times N_c} \\ &\quad C_7: R_{c_n} \geq R_c^{thr}, \quad \forall c_n \in \mathcal{C} \\ &\quad C_8: 0 < q_{p_j,d_i}^{c_n} \leq q^{\max} \\ &\quad C_9: \varepsilon^* \geq x_{p_j,d_i}y_{p_j,c_n}(1-\xi). \end{aligned} \tag{18}$$

In essence, the optimization problem (18) is a joint mode selection and resource management issue. Specifically, $\mathbf{X}$ is defined as a $N_p \times N_d$ matrix, where $[\mathbf{X}]_{j,i} = x_{p_j,d_i}$. According to the values of $\mathbf{X}$, the content delivery mode for $\forall d_i \in \mathcal{D}$ is determined. *i*) If $\sum_{p_j\in\mathcal{P}} x_{p_j,d_i} > 1$, it means that demander d_i obtains its desired contents from multiple potential providers, and thus the content delivery mode for d_i is MD2D mode. *ii*) If $\sum_{p_j\in\mathcal{P}} x_{p_j,d_i} = 1$, it means that d_i obtains its desired contents from a single provider, and accordingly, the content delivery mode for d_i is D2D mode. *iii*) Otherwise, demander d_i will acquire its desired content from the BS, which is called B2D mode. $\mathbf{Y}$ is defined as a $N_p \times N_c$ matrix, where $[\mathbf{Y}]_{j,n} = y_{p_j,c_n}$. The uplink spectrum reusing is determined according to $\mathbf{Y}$, since $y_{p_j,c_n} = 1$ means that provider p_j reuses the uplink spectrum of ordinary cellular user c_n to transmit contents to demanders, and $y_{p_j,c_n} = 0$ otherwise. $\mathbf{Q}$ denotes the power control matrix, where $\mathbf{Q} \in R^{N_p\times N_d\times N_c}$, and $[\mathbf{Q}]_{j,i,n} = q_{p_j,d_i}^{c_n}$.

In the optimization problem (18), C_1 and C_2 mean that each potential provider can serve at most one demander, however, each demander can be served by at most *quota* potential providers simultaneously, where *quota* denotes the maximum number limit. C_4 and C_5 indicate that each potential provider is permitted to reuse the uplink spectrum of at most one cellular user, and the uplink spectrum of one cellular user is permitted to be reused by at most one potential provider. C_3 and C_6 define the two matrices $\mathbf{X}$ and $\mathbf{Y}$. C_7 indicates that the QoS requirements of cellular users should be satisfied, where R_c^{thr} denotes the QoS threshold of cellular users. C_8 is the transmission power range of potential providers, where

$q^{\max}$ denotes the maximum. C_9 denotes the covert constraint, which is derived from (9). If the covert constraint C_9 is satisfied, the content delivery between potential provider p_j and demander d_i is ensured to be covert when the uplink spectrum of c_n is reused.

Obviously, (18) is a complex mixed integer nonlinear programming (MINLP) problem. Moreover, due to the fact that two unknown binary matrices interact with each other, it is naturally a NP-hard problem. Although the problem can be solved through the exhaustive search, the high computational complexity restricts its real application, especially when the scale of network is huge. Essentially, the joint mode selection and resource management issue is a matching problem among the potential providers, demanders, and ordinary cellular users. In order to solve the problem in a tractable manner, we decouple the joint issue into two subproblems, i.e., mode selection and resource management. Specifically, the content delivery mode selection can be formulated as a many-to-one matching problem, and the resource management is formulated as a one-to-one matching problem.

A. SUBPROBLEM 1: TWO-SIDED MANY-TO-ONE MATCHING FOR CONTENT DELIVERY MODE SELECTION

The mode selection issue is a two-sided many-to-one matching problem between provides and demanders, which is formulated as follows. For arbitrary provider $p_j \in \mathcal{P}$, it aims at providing the desired content for demander d_i who has the highest trust degree with itself, i.e.,

$$\begin{aligned} &\max_{\hat{x}_{p_j,d_i}} \sum_{d_i \in \mathcal{D}} \hat{x}_{p_j,d_i} T_{p_j,d_i} \\ &s.t.\ C_1: \sum_{d_i \in \mathcal{D}} \hat{x}_{p_j,d_i} \le 1 \\ &\quad C_2: \hat{x}_{p_j,d_i} \in \{0,1\}, \end{aligned} \tag{19}$$

where $\hat{x}_{p_j,d_i} = 1$ indicates that provider p_j decides to provide demander d_i with its desired content f_{d_i}, and $\hat{x}_{p_j,d_i} = 0$ otherwise. The problem in essence explores the optimal matching of p_j based on its trust degrees, subject to the matching rule that a potential provider can serve at most one demander.

For arbitrary demander $d_i \in \mathcal{D}$, in order to maximize its achievable rate to obtain its desired content f_{d_i}, the matching problem among d_i and all the providers in $\mathcal{D}$ can be formulated as a maximum weighted matching problem, i.e.,

$$\begin{aligned} &\max_{\hat{x}_{d_i,p_j}} \sum_{p_j \in \mathcal{P}} \hat{x}_{d_i,p_j} \mu_{p_j}^{f_{d_i}} R_{p_j,d_i} \\ &s.t.\ C_1: \sum_{p_j \in \mathcal{P}} \hat{x}_{d_i,p_j} \le quota \\ &\quad C_2: \hat{x}_{d_i,p_j} \in \{0,1\}, \end{aligned} \tag{20}$$

where $\hat{x}_{d_i,p_j} = 1$ means that d_i is matched with p_j, and $\hat{x}_{d_i,p_j} = 0$ otherwise. Actually, the above optimization problem means that d_i aims to be matched with at most *quota* potential providers such that it can obtain a high achievable rate for the desired content f_{d_i}.

Note that if and only if $\hat{x}_{p_j,d_i} = \hat{x}_{d_i,p_j} = 1$, it is said that provider p_j and demander d_i are matched together and then $x_{p_j,d_i} = 1$. In this way, the content delivery mode selection matrix $\mathbf{X}$ in (18) can be obtained through solving the two-sided many-to-one matching problem. Moreover, based on (16), it can be seen that the SDP for d_i obtaining its desired content f_{d_i}, i.e., P_{p_j,d_i}, is monotonically increasing with R_{d_i}, the achievable rate of d_i. Thus, the optimization problems (19) and (20) are consistent with the original overall optimization problem (18). However, it is not easy to solve the matching problem separately. As shown in (11), R_{p_j,d_i} is relevant to the resource management matrices $\mathbf{Y}$ and $\mathbf{Q}$. Once the results of resource management change, the content delivery mode selection will change correspondingly.

B. SUBPROBLEM2: TWO-SIDED ONE-TO-ONE MATCHING PROBLEM FOR RESOURCE MANAGEMENT

Similarly, the resource management issue is formulated as a two-sided one-to-one matching problem. For $\forall p_j \in \mathcal{P}$, it would like to choose a c_n to reuse its uplink spectrum to provide the corresponding demander with its desired content. Actually, p_j would like to choose a cellular user c_n to reuse its uplink spectrum which can bring it with high physical domain transmission performance, i.e., achievable rate,

$$\begin{aligned} &\max_{\hat{y}_{p_j,c_n}, q^{c_n}_{p_j,d_i}} \sum_{c_n \in \mathcal{C}} \hat{y}_{p_j,c_n} R^{c_n}_{p_j,d_i}(d_i \in \{d_i | x_{p_j,d_i} = 1\}) \\ &s.t.\ C_1: \sum_{c_n \in \mathcal{C}} \hat{y}_{p_j,c_n} \le 1 \\ &\quad C_2: \hat{y}_{p_j,c_n} \in \{0,1\} \\ &\quad C_3: R^{p_j,d_i}_{c_n}(d_i \in \{d_i | x_{p_j,d_i} = 1\}) \ge R^{thr}_c \\ &\quad C_4: 0 < q^{c_n}_{p_j,d_i}(d_i \in \{d_i | x_{p_j,d_i} = 1\}) \le q^{\max} \\ &\quad C_5: \varepsilon^* \ge \hat{y}_{p_j,c_n}(1-\xi). \end{aligned} \tag{21}$$

In the above optimization problem, $\hat{y}_{p_j,c_n} = 1$ means that p_j reuses the uplink spectrum of c_m, and $\hat{y}_{p_j,c_n} = 0$ otherwise.

Then, for each $c_n \in \mathcal{C}$, the matching problem among itself and all the providers in $\mathcal{P}$ can be formulated as a maximum uplink achievable rate problem based on (13), i.e.,

$$\begin{aligned} &\max_{\hat{y}_{c_n,p_j}} \sum_{p_j \in \mathcal{P}} \hat{y}_{c_n,p_j} R^{p_j,d_i}_{c_n}(d_i \in \{d_i | x_{p_j,d_i} = 1\}, q^{c_n,op}_{p_j,d_i}) \\ &s.t.\ C_1: \sum_{p_j \in \mathcal{P}} \hat{y}_{c_n,p_j} \le 1 \\ &\quad C_2: \hat{y}_{c_n,p_j} \in \{0,1\}, \end{aligned} \tag{22}$$

where $q^{c_n,op}_{p_j,d_i}$ denotes the optimal transmission power of p_j when it reuses the uplink spectrum of c_n to transmit contents to d_i, and it is derived from (21), i.e., $q^{c_n,op}_{p_j,d_i} = \arg \max_{\hat{y}_{p_j,c_n}=1, q^{c_n}_{p_j,d_i}} \sum_{c_n \in \mathcal{C}} \hat{y}_{p_j,c_n} R^{c_n}_{p_j,d_i}(d_i \in \{d_i | x_{p_j,d_i} = 1\})$. Essentially, the optimization problem (22) aims to find the optimal

candidate for c_n in order to maximize its uplink rate with the given $q_{p_j,d_i}^{c_n,op}$, while the uplink spectrum reusing rule should be satisfied.

If and only if $\hat{y}_{p_j,c_n} = \hat{y}_{c_n,p_j} = 1$, we have $y_{p_j,c_n} = 1$, which means that p_j and c_n are matched together. Together with the $q_{p_j,d_i}^{c_n,op}$, resource management matrices $\mathbf{Y}$ and $\mathbf{Q}$ can be obtained. Thus, the resource management issue is solved through the two-sided one-to-one matching problem. However, as shown in (21) and (22), the mode selection matrix $\mathbf{X}$ should be known in advance in order to solve the one-to-one matching problem. As thus, different mode selection results will have influence on the resource management, and meanwhile, different resource management results will impact the mode selection. Due to the interaction of both issues, utilizing traditional matching algorithm is hard to obtain matching results that can satisfy both issues simultaneously. Hence, our purpose is to design a distributed algorithm to obtain a three-dimension stable matching result, i.e., the matching among potential providers, demanders, and ordinary cellular users.

IV. MATCHING THEORY BASED JOINT MODE SELECTION AND RESOURCE MANAGEMENT

A. MODE SELECTION ORIENTED TWO-SIDED STABLE MATCHING

Aiming at achieving the mutual benefit between potential providers and demanders, we introduce a two-sided many-to-one matching game so as to not only solve the optimization problems (19) and (20) in a distributed manner, but also achieve mutual benefit. Mathematically, the matching game between potential providers and demanders is formulated as the tuple $(\mathcal{P}, \mathcal{D}, S_{\mathcal{P}\to\mathcal{D}}, S_{\mathcal{D}}, quota)$. Potential providers $\mathcal{P}$ and demanders $\mathcal{D}$ act as players in the matching game. One demander can be matched with at most *quota* potential providers, and one potential provider can be matched with at most one demander. The preference profiles of potential providers $\mathcal{P}\to\mathcal{D}$ and demanders $\mathcal{D}$ are denoted by $S_{\mathcal{P}\to\mathcal{D}}$ and $S_{\mathcal{D}}$, respectively. $S_{\mathcal{P}\to\mathcal{D}} = \{S_{\mathcal{P}\to\mathcal{D}}(p_j)\}_{p_j\in\mathcal{P}}$ and $S_{\mathcal{D}} = \{S(d_i)\}_{d_i\in\mathcal{D}}$, where $S_{\mathcal{P}\to\mathcal{D}}(p_j)$ and $S(d_i)$ denote the preference profile of provider p_j and demander d_i. Formally, the two-sided many-to-one matching is stated as follows.

Definition 1 (Many-to-One Matching): Given two disjoint finite sets of players $\mathcal{P}$ and $\mathcal{D}$, a many-to-one matching Ω is defined as a function from $\mathcal{P}\cup\mathcal{D}$ to $\mathcal{P}\cup\mathcal{D}$ such that for all $p_j\in\mathcal{P}$ and $d_i\in\mathcal{D}$

i) $\Omega(p_j)\in\mathcal{D}\cup\emptyset$, and $\left|\Omega(p_j)\right|\in\{0,1\}$,

ii) $\Omega(d_i)\in\mathcal{P}\cup\emptyset$, and $|\Omega(d_i)|\le quota$,

iii) $\Omega(p_j)=d_i \Leftrightarrow \Omega(d_i)=p_j$.

Condition *i)* guarantees the constraints C_1 and C_2 in optimization problem (19). Condition *ii)* guarantees the constraints C_1 and C_2 in optimization problem (20). Condition *iii)* implies that if p_j is matched with d_i, then d_i is also matched with p_j, which can be also expressed as if $x_{p_j,d_i} = 1 \Leftrightarrow \hat{x}_{p_j,d_i} = \hat{x}_{d_i,p_j} = 1$.

In order to build the preference profiles for potential providers and demanders, we firstly analyze their individual utilities and then define the preference relation utilized to show their priorities towards potential candidates. Specifically, derived from (19), for each potential provider $p_j\in\mathcal{P}$, its individual utility when matched with d_i is given by

$$u_{p_j}(d_i) = T_{p_j,d_i}, \tag{23}$$

which indicates that the potential provider is more likely to provide contents for the demander who has high trust degree. Similarly, based on (20), the individual utility for each demander d_i when matched with p_j can be expressed as

$$u_{d_i}(p_j) = \mu_{p_j}^{f_{d_i}} R_{p_j,d_i}, \tag{24}$$

which demonstrates that demanders prefer those potential providers who have their desired contents and can bring them with high achievable transmission rate.

Then, we define the preference relation $\succ$ as a reflexive, complete and transitive binary relation between the game players $\mathcal{P}$ and $\mathcal{D}$. Specifically, $\succ_{\mathcal{P}\to\mathcal{D}(p_j)}$ is defined over $\mathcal{D}$ so that for any two potential demanders d_i and $d_{\hat{i}}$, we have $d_i\succ_{\mathcal{P}\to\mathcal{D}(p_j)}d_{\hat{i}} \Leftrightarrow u_{p_j}(d_i) > u_{p_j}(d_{\hat{i}})$. Similarly, $\succ_{d_i}$ is defined over $\mathcal{P}$, and for any two potential provider p_j and $p_{\hat{j}}$ we have $p_j\succ_{d_i}p_{\hat{j}} \Leftrightarrow u_{d_i}(p_j) > u_{d_i}(p_{\hat{j}})$. Moreover, $\succ_{\mathcal{P}\to\mathcal{D}} = \{\succ_{\mathcal{P}\to\mathcal{D}(p_j)}\}_{p_j\in P}$ and $\succ_{\mathcal{D}} = \{\succ_{d_i}\}_{d_i\in\mathcal{D}}$ denote the sets of preference relation of potential providers and demanders, respectively. With the defined preference relation sets $\succ_{\mathcal{P}}$, $\succ_{\mathcal{D}}$ and their individual utilities (23) and (24), all the potential providers and demanders can obtain the preference profiles, i.e., $S_{\mathcal{P}\to\mathcal{D}}$ and $S_{\mathcal{D}}$.

After establishing the preference profiles, the many-to-one matching is solved based on the general assignment algorithm in [35]. Specifically, we propose a mode selection oriented stable matching algorithm (MSA) to solve the mode selection issue in a distributed manner. The pseudo code is summarized in Algorithm 1 and the details are described as follows.

All the potential providers and demanders construct their preference profiles according the preference relations and individual utilities. As thus, the potential providers and demanders interact with each other to implement the matching process. Specifically, in the t-th iteration, for $\forall d_i\in\mathcal{D}$, if d_i has not been matched with *quota* providers and its current preference profile, i.e., $S^{(t)}(d_i)$ is not empty, it will make a proposal to the potential provider who has the highest priority in $S^{(t)}(d_i)$. Then, for $\forall p_j\in\mathcal{P}$, if p_j receives at least one proposal from the demanders and its current preference profile is not empty, i.e., $S_{\mathcal{P}\to\mathcal{D}}^{(t)}(p_j)\neq\emptyset$, it will be matched with the candidate who has the highest priority in $J^{(t)}(p_j)\cup\Omega^{(t)}(p_j)$, where $J^{(t)}(p_j)$ denotes the set of demanders who make proposals to p_j. Finally, both the potential providers and demanders update their preference profiles according to their operations in the current iteration. In this way, the two-sided stable matching Ω can be obtained after limited iterations, as well the mode selection matrix $\mathbf{X}$.

Algorithm 1 Mode Selection Oriented Stable Matching Algorithm (MSA)

Input: Resource management matrices $\mathbf{Y}$ and $\mathbf{Q}$, trust degrees, *quota*, and network topology;
All the potential providers and demanders construct their initial preference profiles $S_{\mathcal{P}\to\mathcal{D}}$ and $S_{\mathcal{D}}$ based on the individual utilities (23) and (24);
Initialization: $t=0$, $\Omega^{(0)}=\emptyset$;
while $t=0$ or $\Omega^{(t)}\neq\Omega^{(t-1)}$ for $t>0$ **do**
  for $d_i\in\mathcal{D}$ **do**
    if $\left|\Omega^{(t)}(d_i)\right|<$ *quota* & $S^{(t)}(d_i)\neq\emptyset$ **then**
      d_i proposes itself to the potential provider who has the highest priority in its current preference profile $S^{(t)}(d_i)$;
    end if;
  end for;
  for $p_j\in\mathcal{P}$ **do**
    if p_j receives at least one proposal from demanders & $S^{(t)}_{\mathcal{P}\to\mathcal{D}}(p_j)\neq\emptyset$ **then**
      All the demanders that propose themselves form a set $J^{(t)}(p_j)$. p_j accepts the proposal of the candidate in $J^{(t)}(p_j)\cup\Omega^{(t)}(p_j)$ who has the highest priority in its current preference profile $S^{(t)}_{\mathcal{P}\to\mathcal{D}}(p_j)$, then rejects others;
    else
      p_j holds its current matching;
    end if;
  end for;
  Potential providers and demanders update their preference profiles;
  $t=t+1$;
end while
Output: The matching Ω and mode selection matrix $\mathbf{X}$.

In order to prove that the matching Ω obtained by utilizing MSA is two-sided stable, we firstly give the definition of two-sided stable matching as follows.

Definition 2 (Two-Sided Stable Matching): A matching Ω is two-sided stable if and only if there exists no blocking pair $\{(p_j,d_i)|p_j\in\mathcal{P},d_i\in\mathcal{D}\}$ that satisfies the following preference relations simultaneously

$$d_i\succ_{\mathcal{P}\to\mathcal{D}(p_j)}\Omega(p_j)\quad and\ p_j\succ_{d_i}\Omega(d_i),\tag{25}$$

where $\Omega(p_j)$ and $\Omega(d_i)$ denote the current matching results of p_j and d_i, respectively.

Theorem 2: The matching Ω obtained from MSA is two-sided stable.

Proof: According to the definition of two-sided stable matching, if Ω is not two-sided stable, there should be a blocking pair $\{(p_j,d_i)|p_j\in\mathcal{P},d_i\in\mathcal{D}\}$ that satisfies $d_i\succ_{\mathcal{P}\to\mathcal{D}(p_j)}\Omega(p_j)$ and $p_j\succ_{d_i}\Omega(d_i)$ simultaneously. According to the preference relation $d_i\succ_{\mathcal{P}\to\mathcal{D}(p_j)}\Omega(p_j)$, potential provider p_j must have made a proposal to the demander d_i which provides it with a higher individual utility compared to $\Omega(p_j)$ in the matching process. However, due to the matching result $\Omega(p_j)\neq d_i$, it can be inferred that d_i prefers $\Omega(d_i)$ than p_j, i.e., $\Omega(d_i)\succ_{d_i}p_j$. Actually, $\Omega(d_i)\succ_{d_i}p_j$ and $p_j\succ_{d_i}\Omega(d_i)$ are incompatible, which demonstrates the inexistence of the blocking pair $\{(p_j,d_i)|p_j\in\mathcal{P},d_i\in\mathcal{D}\}$. In this way, the many-to-one matching Ω resulting from MSA is proved to be two-sided stable. ■

B. RESOURCE MANAGEMENT ORIENTED TWO-SIDED STABLE MATCHING

In order to solve the resource management issue in a distributed way and achieve mutual benefit, we reformulate the matching problem between potential providers and ordinary cellular users as a one-to-one matching game, which is denoted as the tuple $(\mathcal{P},\mathcal{C},S_{\mathcal{P}\to\mathcal{C}},S_{\mathcal{C}})$. Potential providers and cellular users act as players in the game. $S_{\mathcal{P}\to\mathcal{C}}$ and $S_{\mathcal{C}}$ denote the preference profiles of potential providers and cellular users in the one-to-one matching game, respectively. $S_{\mathcal{P}\to\mathcal{C}}=\{S_{\mathcal{P}\to\mathcal{C}}(p_j)\}_{p_j\in\mathcal{P}}$ and $S_{\mathcal{C}}=\{S(c_n)\}_{c_n\in\mathcal{C}}$, where the preference profile of potential provider p_j is denoted as $S_{\mathcal{P}\to\mathcal{C}}(p_j)$, and $S(c_n)$ is the preference profile of cellular user c_n. Then, the two-sided one-to-one matching is formally defined as follows.

Definition 3 (One-to-One Matching): Given two disjoint finite sets of players $\mathcal{P}$ and $\mathcal{C}$, a one-to-one matching Φ is defined as an allocation from $\mathcal{P}\cup\mathcal{C}$ to $\mathcal{P}\cup\mathcal{C}$ such that if $\Phi(p_j)\neq p_j$, then $\Phi(p_j)\in\mathcal{C}$ and if $\Phi(c_n)\neq c_n$, then $\Phi(c_n)\in\mathcal{P}$. $\Phi(p_j)=c_n$ if and only if $\Phi(c_n)=p_j$.

Actually, the constraints C_1 and C_2 in (21) and (22) are ensured due to the essence of one-to-one matching game. Once the matching results is obtained, the resource management issue is solved. For example, if $\Phi(p_j)=c_n$ and $\Phi(c_n)=p_j$, then $y_{p_j,c_n}=\hat{y}_{p_j,c_n}=\hat{y}_{c_n,p_j}=1$. It implies that potential provider p_j reuses the uplink spectrum of cellular user c_n to transmit contents to the corresponding demander. In what follows, we firstly derive the individual utilities of potential providers and cellular users based on the optimization problems (21) and (22). Then, the preference profiles establishment is achieved with the preference relation $\succ$ defined previously. Moreover, we propose a resource management oriented stable matching algorithm based on the Gale-Shapley algorithm in [36] to solve the resource management issue.

Specifically, for $\forall p_j\in\mathcal{P}$, its individual utility when matched with cellular user c_n is denoted by

$$v_{p_j}(c_n)=\max_{\hat{y}_{p_j,c_n}=1,q^{c_n}_{p_j,d_i}}\sum_{c_n\in C}\hat{y}_{p_j,c_n}R^{c_n}_{p_j,d_i}(d_i\in\{d_i|x_{p_j,d_i}=1\}),\tag{26}$$

subject to C_3, C_4, and C_5 in (21). As shown above, the individual utility for potential provider p_j is measured by the achievable rate between it and its corresponding demander, i.e., $d_i\in\{d_i|x_{p_j,d_i}=1\}$ when the uplink spectrum of c_n is reused. By observing (26) and (10), it is obviously that $v_{p_j}(c_n)$ is monotonically increasing with the transmission power of p_j, i.e., $q^{c_n}_{p_j,d_i}$. Thus, the optimal transmission power $q^{c_n,op}_{p_j,d_i}$ can be obtained by utilizing the one-dimensional search, and the

power control matrix $\mathbf{Q}$ can be obtained. The details are given in our previous work [23].

Similarly, $v_{c_n}(p_j)$ denotes the individual utility for c_n when matched with p_j, which is given by

$$v_{c_n}(p_j) = \max_{\hat{y}_{c_n,p_j}=1} \sum_{c_n \in C} \hat{y}_{c_n,p_j} R_{c_n}^{p_j,d_i}(d_i \in \{d_i | x_{p_j,d_i}=1\}, q_{p_j,d_i}^{c_n,op}). \tag{27}$$

In essence, cellular user c_n wants to be matched with the provider who causes little interference, and thus, it can obtain a maximum uplink achievable rate.

Then, combined with the preference relation $\succ_{\mathcal{P}\to\mathcal{C}}$ and $\succ_{\mathcal{C}}$, both the potential providers and cellular users can establish their preference profiles $S_{\mathcal{P}\to\mathcal{C}}$ and $S_{\mathcal{C}}$. Specifically, $\succ_{\mathcal{P}\to\mathcal{C}} = \{\succ_{\mathcal{P}\to\mathcal{C}(p_j)}\}_{p_j\in\mathcal{P}}$ and $\succ_{\mathcal{C}} = \{\succ_{c_n}\}_{c_n\in\mathcal{C}}$. $\succ_{\mathcal{P}\to\mathcal{C}(p_j)}$ is defined over $\mathcal{C}$ so that for two cellular users c_n and $c_{\hat{n}}$, we have $c_n \succ_{\mathcal{P}\to\mathcal{C}(p_j)} c_{\hat{n}} \Leftrightarrow v_{p_j}(c_n) > v_{p_j}(c_{\hat{n}})$. $\succ_{c_n}$ is defined over $\mathcal{P}$, then for any two potential provider p_j and $p_{\hat{j}}$ we have $p_j \succ_{c_n} p_{\hat{j}} \Leftrightarrow v_{c_n}(p_j) > v_{c_n}(p_{\hat{j}})$. After establishing the preference profiles, we propose a resource management oriented stable matching algorithm (RAA) based on the Gale-Shapley algorithm to solve the resource management issue. Specifically, Algorithm 2 summarizes the pseudo code, and the details are explained as follows.

Similarly, all the potential and cellular users obtain their initial preference profiles according to the preference relations and individual utilities (26) and (27). After establishing the preference profiles, the potential providers and cellular users interact with each other to obtain the matching results. Specifically, in the t-th iteration, for $\forall p_j \in \mathcal{P}$, if it has not been matched and its current preference profile $S^{(t)}_{\mathcal{P}\to\mathcal{C}}(p_j)$ is not empty, it will make a proposal to the cellular user who has the highest priority in $S^{(t)}_{\mathcal{P}\to\mathcal{C}}(p_j)$. For $\forall c_n \in \mathcal{C}$, if it receives at least one proposal from the potential providers and its current preference profile is not empty, i.e., $S^{(t)}(c_n) \neq \emptyset$, it will accept the proposal of the candidate in $J^{(t)}(c_n) \cup \Phi^{(t)}(c_n)$ who has the highest priority in $S^{(t)}(c_n)$, and reject to others. Finally, potential providers and cellular users update their preference profiles based on the acceptance or rejection operations in the current iteration. As thus, a two-sided stable matching Φ can be obtained after limited iterations and the resource management matrix $\mathbf{Y}$ is determined.

Note that the matching Φ is two-sided stable if and only if no blocking pair $\{(p_j, c_n) | p_j \in \mathcal{P}, c_n \in \mathcal{C}\}$ exists, where the definition of blocking pair is given as ***Definition 2***.

Theorem 3: The matching Φ resulting from RAA is two-sided stable.

Proof: The proof is similar with ***Theorem 1***. ■

C. HIERARCHICAL STABLE MATCHING

Due to the interaction of both issues, i.e., the process of mode selection needs pre-allocated resources and the resource management also requires the result of mode selection, the matching results Ω and Φ cannot satisfy both issues simultaneously. Thus, we proposed a hierarchical stable matching algorithm (HSMA) by combining the MSA with RAA in order to obtain a three-dimension stable matching result among potential providers, demanders, and cellular users. The pseudo code is given in Algorithm 3. In the HSMA, we decouple the joint mode selection and resource management issue into a many-to-one matching problem (mode selection) and a one-to-one matching problem (resource management), and then the joint issue is performed in an iterative manner so that a three-dimension stable matching result Λ can be obtained.

Specifically, we firstly allocate each $p_j \in \mathcal{P}$ a random cellular user, of which the uplink spectrum is reused. Then, with the given resource management result, potential providers and demanders establish their preference profiles $S_{\mathcal{P}\to\mathcal{D}}$ and $S_{\mathcal{D}}$, and then operate the many-to-one matching process as described in Algorithm 1 to address the mode selection issue. After the mode selection matrix $\mathbf{X}$ is obtained, potential providers and cellular users are able to establish their preference profiles $S_{\mathcal{P}\to\mathcal{C}}$ and $S_{\mathcal{C}}$, then implement the one-to-one matching process as described in Algorithm 2 to handle

Algorithm 2 Resource Management Oriented Stable Matching Algorithm (RAA)

Input: Mode selection matrix $\mathbf{X}$, power control matrix $\mathbf{Q}$, and network topology;
All the potential providers and demanders construct their initial preference profiles $S_{\mathcal{P}\to\mathcal{C}}$ and $S_{\mathcal{D}}$ based on their individual utilities (26) and (27);
Initialization: $t = 0$, $\Phi^{(0)} = \emptyset$;
while $t = 0$ or $\Phi^{(t)} \neq \Phi^{(t-1)}$ for $t > 0$ **do**
  for $p_j \in \mathcal{P}$ **do**
    if p_j has no partner & $S^{(t)}_{\mathcal{P}\to\mathcal{C}}(p_j) \neq \emptyset$ **then**
      p_j makes a proposal to the cellular user who has the highest priority in its current preference profile $S^{(t)}_{\mathcal{P}\to\mathcal{C}}(p_j)$;
    end if;
  end for;
  for $c_n \in \mathcal{C}$ **do**
    if c_n receives at least one proposal from potential providers & $S^{(t)}(c_n) \neq \emptyset$ **then**
      All the potential providers that propose themselves form a set $J^{(t)}(c_n)$. c_n accepts the proposal of the candidate in $J^{(t)}(c_n) \cup \Phi^{(t)}(c_n)$ who has the highest priority in its current preference profile $S^{(t)}(c_n)$, then rejects to others;
    else
      c_n holds its current matching;
    end if;
  end for;
  Potential providers and cellular users update their preference profiles;
  $t = t + 1$;
end while
Output: Φ and $\mathbf{Y}$.

Algorithm 3 Hierarchical Stable Matching Algorithm (HSMA)

1: **Input**: Network topology;
2: ***Step 1: Initialization***
3: For $\forall p_j \in \mathcal{P}$, it is allocated with a random cellular user to reuse the uplink spectrum to transmit contents;
4: ***Step 2: Mode Selection***
5: Potential providers and demanders establish their preference profiles, and then implement the MSA;
6: The matching Ω between potential providers and demanders is obtained, as well the mode selection matrix $\mathbf{X}$;
7: If the matching Ω and the mode selection matrix $\mathbf{X}$ have appeared, change them randomly;
8: ***Step 3: Resource Management***
9: Potential providers and cellular users establish their preference profiles, and then implement the RAA;
10: The matching Φ between potential providers and cellular users can be obtained, as well the resource management matrix $\mathbf{Y}$;
11: If the matching Φ and the resource management matrix $\mathbf{Y}$ have appeared, change them randomly;
12: Repeat ***Step 2-3*** until no blocking tuple exists.
13: **Output**: A three-dimension stable matching Λ.

the resource management issue. Note that if the matching Ω or Φ has appeared in the iterations, it will be changed randomly. Finally, the MSA and RAA are performed in an iterative manner until there exists no blocking tuple in the three-dimension matching Λ. In this way, a three-dimension stable matching result can be obtained and the joint issue is well addressed.

In order to prove that the matching Λ obtained by utilizing our proposed HSMA is three-dimension stable, we define the blocking tuple as follows.

Definition 4 (Blocking Tuple): A tuple $\{(p_j, d_i, c_n)|p_j \in \mathcal{P}, d_i \in \mathcal{D}, c_n \in \mathcal{C}\}$ is a blocking tuple if at least one of the following relations is satisfied

i) $d_i \succ_{\mathcal{P}\to\mathcal{D}(p_j)} \Omega(p_j)$ *and* $p_j \succ_{d_i} \Omega(d_i)$,
ii) $c_n \succ_{\mathcal{P}\to\mathcal{C}(p_j)} \Phi(p_j)$ *and* $p_j \succ_{c_n} \Phi(c_n)$.

Naturally, a matching is three-dimension stable if and only if there exists no blocking tuple. In the next subsection, we will analyze the stability of our proposed HSMA, as well its convergence, optimality, and complexity.

D. PROPERTIES OF THE PROPOSED ALGORITHM

Theorem 4 (Stability): The matching Λ resulting from the HSMA is three-dimension stable.

Proof: Actually, the theorem can be easily proved by utilizing the contradiction method. The matching Λ is said to be three-dimension stable if and only if there exists no blocking tuple. We would like to assume that there exists at least one blocking tuple $\{(p_j, d_i, c_n)|p_j \in \mathcal{P}, d_i \in \mathcal{D}, c_n \in \mathcal{C}\}$ in the matching Λ. Thus, at least one of the following relations is satisfied, i.e., *i)* $d_i \succ_{\mathcal{P}\to\mathcal{D}(p_j)} \Omega(p_j)$ *and* $p_j \succ_{d_i} \Omega(d_i)$, and *ii)* $c_n \succ_{\mathcal{P}\to\mathcal{C}(p_j)} \Phi(p_j)$ *and* $p_j \succ_{c_n} \Phi(c_n)$. However, as shown in the pseudo code of Algorithm 3, the algorithm will last until all the blocking tuples are disjointed from Λ, which conflicts with our assumption. In this regard, it can be proved that there exists no blocking tuple in the matching Λ resulting from the HSMA, and thus it is three-dimension stable. ■

Theorem 5 (Convergence): The proposed HSMA converges to a three-dimension stable matching Λ after limited iterations.

Proof: The convergence of the MSA and RAA can be easily proved due to the nature of deferred acceptance, which is described detailedly as Theorem 2 in [37], and thus we focus on the convergence of our proposed HSMA. It can be seen that Algorithm 3 terminates until there exists no blocking tuple in the matching Λ, and one iteration in the HSMA means that both the MSA and RAA have run once. In order to prevent the algorithm from entering an endless loop, a breaking rule is adopted. That is if the matching result Ω obtained from Step 2 (or Φ obtained from Step 3) has appeared previously, we will change it randomly, which is shown as lines 7 and 11 in Algorithm 3. In this way, the HSMA is guaranteed to have a chance to iterate through all possible matching results until a three-dimension matching Λ is found, i.e., there exists no blocking tuple in the matching. Thus, we demonstrate that the proposed HSMA will converge to a three-dimension stable matching Λ after limited iterations. ■

Theorem 6 (Optimality): The matching Λ obtained from the HSMA is locally optimal for the joint optimization problem.

Proof: In order to prove the theorem, we will demonstrate that *i)* the matching Ω obtained from the MSA is weak Pareto optimal for each demander $d_i \in \mathcal{D}$, and *ii)* the matching Φ resulting from the RAA is weak Pareto optimal for each potential provider $p_j \in \mathcal{P}$. Specifically, based on the definition of Pareto improvement in [38], the proof of *i)* is given as follows. Firstly, we assume that there exists Pareto improvement in the matching Ω, and demander p_j is the improvement for potential provider d_i, i.e., $p_j \succ_{d_i} \Omega(d_i)$. Then, the following two conditions are considered. *i)* p_j has not been matched in the matching Ω, i.e., $\Omega(p_j) = \emptyset$. However, obviously the preference relation $d_i \succ_{\mathcal{P}\to\mathcal{D}(p_j)} \Omega(p_j)$ holds, which means that p_j prefers to be matched with d_i compared to the condition that it has no partner. Thus, $\{(p_j, d_i)|p_j \in \mathcal{P}, d_i \in \mathcal{D}\}$ is actually a blocking pair according to the Definition 2. This contradicts our proposed Theorem 1, and cannot hold. *ii)* p_j has selected another demander $d_{\hat{i}}$ as its partner in the matching Ω, i.e, $\Omega(p_j) = d_{\hat{i}}$. In this regard, due to the preference relation $p_j \succ_{d_i} \Omega(d_i)$, d_i must have proposed to p_j, and p_j rejects the proposal. Thus, we have $d_{\hat{i}} \succ_{\mathcal{P}\to\mathcal{D}(p_j)} d_i$, which demonstrates that p_j and d_i cannot be matched together according to the definition of Pareto improvement. Similarly, the matching Φ resulting from the RAA can be proved to be weak Pareto optimal for each $p_j \in \mathcal{P}$. Hence, we come to the conclusion that the matching Λ obtained from the HSMA is locally optimal for the joint optimization problem. ■

Remark 1 (Complexity): The computational complexity of the HSMA depends on both the MSA and RAA, thus we will analyze the complexity of the two algorithms respectively. In the MSA, the complexity consists of two parts, i.e., preference profiles establishment and many-to-one stable matching. In the preference profiles establishment, each demander ranks all the potential providers in a descending order by utilizing Bubble sort algorithm according to the utilities, and so do the potential providers. The complexity for each demander to establish its preference profile is $O(N_p \log(N_p))$*, and the total complexity for all the demanders to establish preference profiles is* $O(N_d N_p \log(N_p))$*. Similarly, the total complexity for all the potential providers to achieve the preference profiles establishment is* $O(N_d N_p \log(N_d))$*. Hence, the total complexity of preference profiles establishment is* $O(N_d N_p \log(N_d N_p)) \sim O(N_d^2 N_p^2)$*. In the many-to-one stable matching, each demander makes a proposal to its favorable potential providers, and if rejected, it will send a proposal to the next one. Thus, the complexity in the worst case is* $O(N_d(N_p - 1))$ *[39].*

Similarly, the complexity of the RAA consists of two parts, i.e., preference profiles establishment and one-to-one stable matching. The complexity of the former is $O(N_p N_c \log(N_p N_c)) \sim O(N_p^2 N_c^2)$*, and that of the latter is* $O(N_p N_c)$ *under the worst case when the preference profiles of all the potential providers and cellular users are the same [37]. Hence, the total complexity of the HSMA is* $O(N_{loop}(N_d^2 N_p^2 + N_d(N_p - 1) + N_p^2 N_c^2 + N_p N_c)) \sim O(N_{loop} N_p^2 (N_d^2 + N_c^2))$*, where* N_{loop} *is the number of iterations in the HSMA.*

V. PERFORMANCE EVALUATION

In this section, extensive simulation results are given to evaluate the performance of our proposed algorithm. Specifically, we investigate the joint content delivery mode selection and resource management issue in a single-cell D2D underlaying cellular network, where the cell radius is 500m. The related simulation parameters are shown as Table 1 if no special declaration. Also, the AWGN power spectrum density at $\forall d_i \in \mathcal{D}$ is -174dBm/Hz. All the demanders, potential providers, and cellular users are all randomly distributed in the cell. To eliminate the influence of randomness, we have run hundreds of simulations and obtain the average values.

A. CONVERGENCE OF THE PROPOSED ALGORITHM

As analyzed in previous Section IV-D, the convergence of our proposed HSMA depends on both MSA and RAA. Thus, Fig. 3 and 4 are given to demonstrate the convergence of MSA and RAA, respectively. Specifically, Fig. 3 shows the cumulative distribution function (CDF) of number of iterations in MSA until a two-sided stable matching Ω is obtained. With the increasing number of potential providers, the number of iterations grows large due to that demanders have more candidates to be matched, and thus the algorithm needs more time to converge. Despite the increasing N_p, the MSA always converges within limited iterations. Similarly, in Fig. 4, we plot the CDF of number of iterations in RAA under different number of potential providers, which verifies the convergence of the algorithm.

Fig. 5 shows the social welfare versus the number of iterations in the proposed HSMA under different number of potential providers. Note that one iteration in HSMA means that both the MSA and RAA have been run one time. It can be easily seen that with the number of potential providers increasing, the proposed HSMA needs more time to converge. Besides, the social welfare grows with the increasing N_p. This is due to the fact that with more potential providers

TABLE 1. Simulation parameters.

Parameters	Values
Cell radius	500m
Number of demanders N_d	5
Number of potential providers N_p	10
Number of ordinary cellular users N_c	10
System bandwidth W	6MHz
Path loss exponent α	4
Content size $s_{f_{d_i}}$	10-500MB
Transmission power of cellular users q_{c_n}	20dBm
Maximal transmission power of potential providers $q^{\max}$	17dBm
Transmission power of the BS	36dBm
Noise power spectrum density at BS σ^2	-174dBm/Hz
Noise power spectrum density at the warden σ_W^2	-174dBm/Hz
QoS threshold of cellular users R_c^{thr}	1bps/Hz
Two parameters that define the contact duration distribution β and θ	1, 10
Covert communication threshold ξ	0.1
Maximum number of potential providers permitted to serve a demander $quota$	3

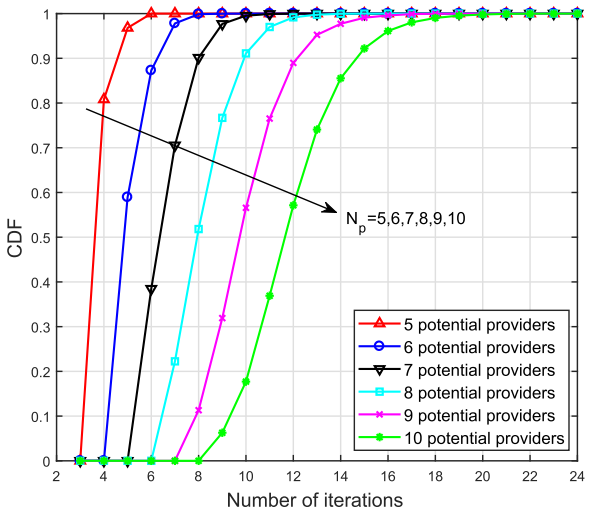


FIGURE 3. Distribution of the number of iterations in MSA.

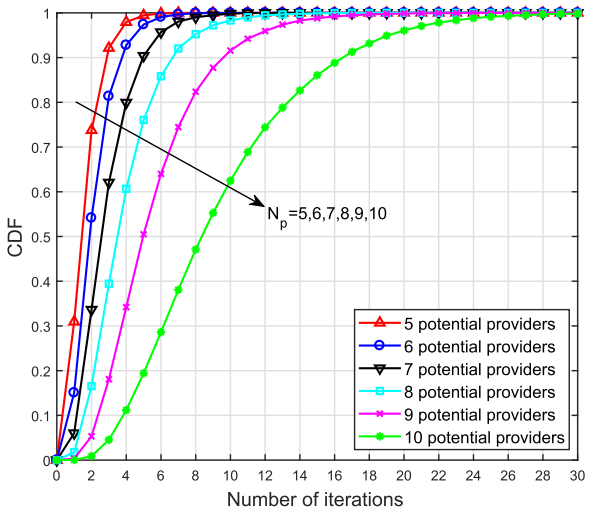


FIGURE 4. Distribution of the number of iterations in RAA.

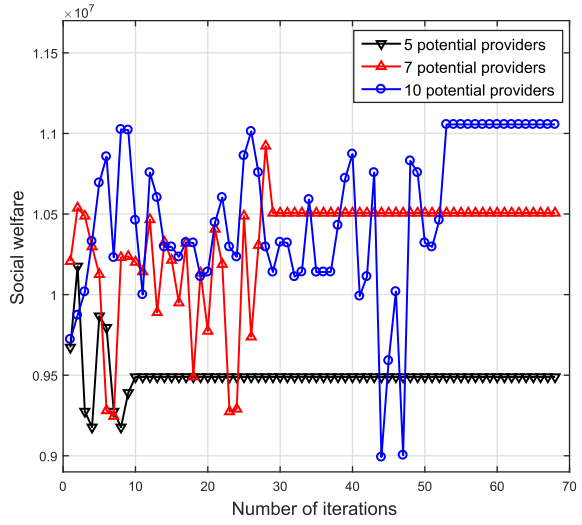


FIGURE 5. Social welfare versus the number of iterations in the proposed HSMA.

joining in the network, the demanders are able to be matched with more potential providers and they may be matched with those who have good link qualities and high trust degrees. In a word, the simulation results demonstrate our proposed Theorem 4.

B. TRADEOFF BETWEEN THE SOCIAL WELFARE AND COMPLEXITY

Fig. 6 plots the social welfare versus the number of potential providers, which demonstrates the tradeoff between the overall performance and the computational complexity of different kinds of algorithms. Specifically, in order to evaluate the performance of our proposed HSMA, we compare it with other four benchmarks, i.e., the exhaustive search, only RAA, only MSA, and random matching. The exhaustive search is widely utilized to obtain a global optimal social welfare with high computational complexity, and always outperform the other algorithms. Our proposed HSMA achieves the joint

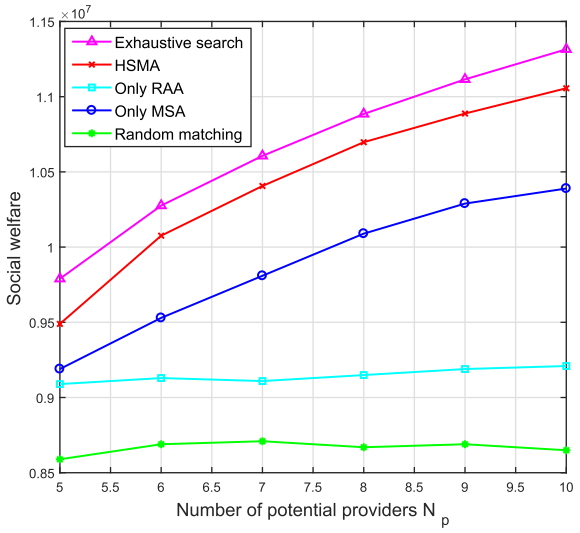


FIGURE 6. Social welfare versus the number of potential providers under different algorithms.

optimization of mode selection and resource management, and thus can reach a near-optimal performance compared to the only RAA, only MSA, and random matching. The only RAA separately solves the resource management issue without considering the mode selection issue, and has been investigated in some existing works, such as [25]. Moreover, the only MSA solves the mode selection issue separately with predetermined resource management strategies, as mentioned in [2]. Obviously, both the only RAA and only MSA perform worse than our proposed HSMA in terms of pursuing high social welfare. In addition, the results of random matching are plotted as a benchmark to evaluate the other algorithms.

As shown in the figure, with the number of potential providers N_p increasing, social welfare in the exhaustive search, the HSMA, and the MSA grows large. The reasons are two-fold. *i*) With the number of potential providers increasing, each demander has more candidates to be matched. Thus, the demander may benefit more from being matched with a more preferred potential provider. *ii*) Due to the increasing number of potential providers N_p, more demanders are able to be served in MD2D mode, i.e., they can be served by multiple potential providers in a collaborative way. In this regard, the increasing number of potential providers improves the social welfare. However, the social welfare in both the RAA and the random matching remains almost unchanged. This is due to the fact that the mode selection issue is not considered in both the two kinds of algorithms. Thus, the increasing number of potential providers shows no effect on the social welfare.

C. SOCIAL WELFARE IN DIFFERENT COMBINATIONS OF CONTENT DELIVERY MODES

Fig. 7 and 8 show the effect of different combinations of content delivery modes on the individual utility of each demander and the social welfare, respectively. Specifically, the

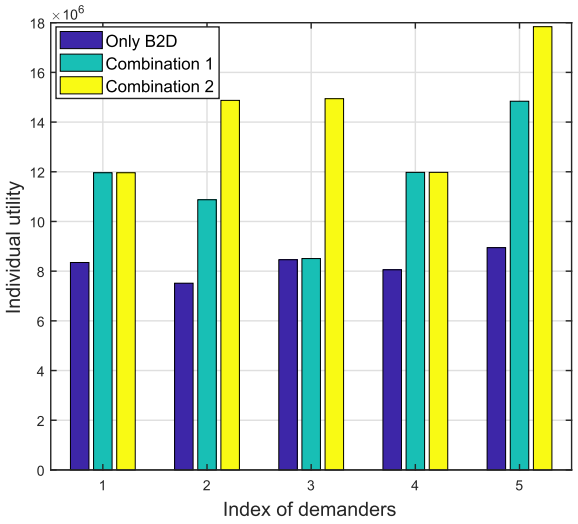


FIGURE 7. Individual utility of each demander under different combinations of content delivery modes.

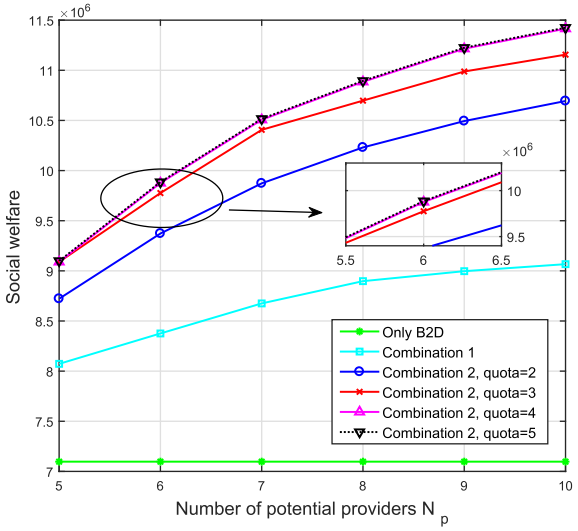


FIGURE 8. Social welfare under different combinations of content delivery modes with different quotas.

combination 1 indicates that the content delivery modes in the current scenario is restricted to B2D mode and D2D mode, the MD2D mode is not permitted in this kind of scenarios. The combination 2 means that B2D, D2D, and MD2D modes coexist in the content delivery scenario. In Fig. 7, there exist 5 demanders and 10 potential providers, and the *quota* is set to be 3. It can be seen from the figure that under combination 1, the demanders are able to establish D2D links with those potential providers who have good link qualities and high trust degrees and obtain their desired contents through D2D mode. Thus, the individual utility of each demander is higher than that in B2D mode. Moreover, under combination 2, some demanders like 2, 3, and 5 could obtain higher individual utilities by introducing the novel MD2D mode because they are served by more potential providers. However, the individual utilities of demander 1 and 4 remain unchanged due to the fact that the number of potential providers are limited, and thus some demanders may have no chance to be served by multiple potential providers.

Further, we investigate the effect of different *quotas* on the social welfare (the *quota* under combination 1 can be regarded as 1), shown as Fig. 8. It can be seen that with the increasing number of potential providers, the growth of social welfare slows down under combination 1 and 2. As mentioned previously, the reasons are two-fold. When number of potential providers N_p is small, the social welfare grows fast due to the interaction of both reasons. However, when N_p grows large enough, one of the reasons no longer plays a role and thus, the growth of social welfare slows down. Specifically, *i*) the demanders may have been matched with their most preferred potential providers, and the increasing number of potential providers will no more change the matching results. *ii*) All the demanders may have been matched with *quota* potential providers, and thus they cannot be matched with more potential providers even if more potential providers join in the network. In this regard, it can be predicted that when N_p grows large enough, both of the reasons will no longer work, and the social welfare remains unchanged. Besides, it can be also seen that when *quota* is large, the social welfares under different *quotas* are the same because compared to the *quota*, N_p restricts demanders from being matched with more potential providers. Actually, the outcome of social welfare is influenced by the interaction of N_p and *quota*.

VI. CONCLUSION

Secure content delivery plays an important role in D2D content sharing networks due to the existence of various security threats. In this work, a trust evaluation mechanism is proposed to stimulate the lasting and rational cooperation between potential providers and demanders. Moreover, the covert communication model is adopted to prevent the content delivery from external attacks. Then, by combining the security-aware metrics, in terms of trust degree and covert rate, with physical layer transmission performances, in terms of achievable rate and successful delivery probability, a novel definition of secrecy-aware effective rate is given to guarantee both the efficiency and security of content delivery. Then, we formulate the joint content delivery mode selection and resource management issue as a social welfare maximization problem. To solve the joint optimization problem in a distributed manner, we decouple it into two subproblem and solve them separately. Finally, considering the interaction of two issues, a novel hierarchical stable matching algorithm is proposed to achieve the joint optimization. Its properties such as stability, convergence, optimality, and complexity are well analyzed. The simulation results demonstrate the advantages of our proposed algorithms. However, the unilateral dominance of traditional matching algorithms remains unsolved. Besides, the covert communication in unlicensed bands still remains unsolved, which will be our future focus.

REFERENCES

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

[2] 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.

[3] D. Wu, L. Zhou, Y. Cai, and Y. Qian, "Optimal content sharing mode selection for social-aware D2D communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 910–913, Dec. 2018.

[4] F. Malandrino, Z. Limani, C. Casetti, and C. F. Chiasserini, "Interference-aware downlink and uplink resource allocation in hetnets with D2D support," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2729–2741, May 2015.

[5] M. Ahmed, Y. Li, Z. Yinxiao, M. Sheraz, D. Xu, and D. Jin, "Secrecy ensured socially aware resource allocation in device-to-device communications underlaying hetnet," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4933–4948, May 2019.

[6] S. Cicaló and V. Tralli, "QoS-aware admission control and resource allocation for D2D communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5256–5269, Aug. 2018.

[7] 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.

[8] 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.

[9] E. Datsika, A. Antonopoulos, N. Zorba, and C. Verikoukis, "Green cooperative device–to–device communication: A social–aware perspective," *IEEE Access*, vol. 4, pp. 3697–3707, 2016.

[10] 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.

[11] M. N. Soorki, W. Saad, M. H. Manshaei, and H. Saidi, "Social community-aware content placement in wireless device-to-device communication networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 8, pp. 1938–1950, Aug. 2019.

[12] C. Zhao, S. Yang, X. Yang, and J. A. McCann, "Rapid, user-transparent, and trustworthy device pairing for D2D-enabled mobile crowdsourcing," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2008–2022, Jul. 2017.

[13] A. Ometov, E. Olshannikova, P. Masek, T. Olsson, J. Hosek, S. Andreev, and Y. Koucheryavy, "Dynamic trust associations over socially-aware D2D technology: A practical implementation perspective," *IEEE Access*, vol. 4, pp. 7692–7702, 2016.

[14] Q. Xu, Z. Su, Q. Zheng, M. Luo, B. Dong, and K. Zhang, "Game theoretical secure caching scheme in multihoming edge computing-enabled heterogeneous networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4536–4546, Jun. 2019.

[15] Q. Xu, Z. Su, and K. Zhang, "Game theoretical secure caching scheme in multi-homing heterogeneous networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[16] 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.

[17] 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.

[18] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 813–816, Jun. 2019.

[19] 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.

[20] 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.

[21] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4089–4102, Aug. 2019.

[22] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint optimization of a UAV's trajectory and transmit power for covert communications," *IEEE Trans. Signal Process.*, vol. 67, no. 16, pp. 4276–4290, Aug. 2019.

[23] 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. 72835–72849, 2019.

[24] J. Jiang, S. Zhang, B. Li, and B. Li, "Maximized cellular traffic offloading via device-to-device content sharing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 1, pp. 82–91, Jan. 2016.

[25] S. Liu, Y. Wu, L. Li, X. Liu, and W. Xu, "A two-stage energy-efficient approach for joint power control and channel allocation in D2D communication," *IEEE Access*, vol. 7, pp. 16940–16951, 2019.

[26] F. Hussain, M. Y. Hassan, M. S. Hossen, and S. Choudhury, "System capacity maximization with efficient resource allocation algorithms in D2D communication," *IEEE Access*, vol. 6, pp. 32409–32424, 2018.

[27] M. Hasan and E. Hossain, "Distributed resource allocation for relay-aided device-to-device communication under channel uncertainties: A stable matching approach," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3882–3897, Oct. 2015.

[28] Y. Gu, Y. Zhang, M. Pan, and Z. Han, "Matching and cheating in device to device communications underlying cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2156–2166, Oct. 2015.

[29] S. M. A. Kazmi, N. H. Tran, W. Saad, Z. Han, T. M. Ho, T. Z. Oo, and C. S. Hong, "Mode selection and resource allocation in device-to-device communications: A matching game approach," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3126–3141, Nov. 2017.

[30] L. Wang, H. Wu, Y. Ding, W. Chen, and H. Vincent Poor, "Hypergraph-based wireless distributed storage optimization for cellular D2D underlays," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2650–2666, Oct. 2016.

[31] 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.

[32] 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.

[33] X. Zhang, Y. Li, Y. Zhang, J. Zhang, H. Li, S. Wang, and D. Wang, "Information caching strategy for cyber social computing based wireless networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 391–402, Jul./Sep. 2017.

[34] B. Wang, Y. Sun, S. Li, and Q. Cao, "Hierarchical matching with peer effect for low-latency and high-reliable caching in social IoT," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 1193–1209, Feb. 2019.

[35] 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.

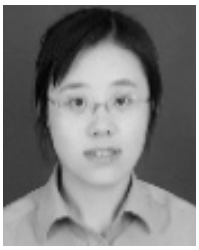
[36] D. Gale and L. S. Shapley, "College admissions and the stability of marriage," *Amer. Math. Monthly*, vol. 69, no. 1, pp. 9–15, Jan. 1962.

[37] 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.

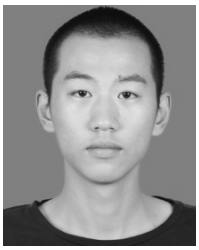
[38] C. Xu, C. Gao, Z. Zhou, Z. Chang, and Y. Jia, "Social network-based content delivery in device-to-device underlay cellular networks using matching theory," *IEEE Access*, vol. 5, pp. 924–937, 2017.

[39] Y. Wu, D. Wu, L. Yang, X. Shi, L. Ao, and Q. Fu, "Matching-coalition based cluster formation for D2D multicast content sharing," *IEEE Access*, vol. 7, pp. 73913–73928, 2019.

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.

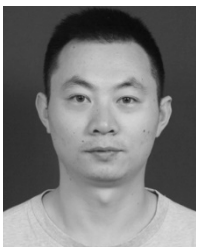


DAN WU received the B.S., M.S., and Ph.D. degrees from the Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2006, 2009, and 2012, respectively. She is currently an Associate Professor with the Army Engineering University of PLA, Nanjing. Her research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



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.

MENG WANG received the B.S. and M.S. degrees in instructional technology from the Nanjing Normal University, Nanjing, China, in 2006 and 2009, respectively. He is currently a Lecturer with the College of Communications Engineering, Army Engineering University of PLA, Nanjing. His current interests include wireless network security, D2D communications, and game theory.



YU ZHANG received the B.S. and M.S. degrees from the PLA University of Science and Technology, Nanjing, China, in 2006 and 2008, respectively. He is currently pursuing the Ph.D. degree in communications and information system with the College of Communications Engineering, Army Engineering University of PLA. He is currently an Associate Researcher with the Sixty-Third Research Institute, National University of Defense Technology. His research interests include electromagnetic spectrum management, cooperative communications, cognitive radio, and physical layer security.