IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2019, accepted March 5, 2019, date of publication March 18, 2019, date of current version April 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2905581

An Extensive Game-Based Resource Allocation for Securing D2D Underlay Communications

OLEKSII RUDENKO[1], YUHONG LIU[2], CHENWEI WANG[3], AND SUSANTO RAHARDJA[1], (Fellow, IEEE)

[1]School of Marine Science and Engineering, Northwestern Polytechnic University, Xi'an 710000, China
[2]Department of Computer Engineering, Santa Clara University, Santa Clara, CA 95053, USA
[3]DOCOMO Innovations Inc., Palo Alto, CA 94304, USA

Corresponding author: Susanto Rahardja (susantorahardja@ieee.org)

The work of S. Rahardja was supported in part by the Overseas Expertise Introduction Project for Discipline Innovation (111 Project: B18041).

ABSTRACT Device-to-device (D2D) communication has been increasingly attractive due to its great potential to improve cellular communication performance. While resource allocation optimization for improving the spectrum efficiency is of interest in the D2D-related work, communication security, as a key issue in the system design, has not been well investigated yet. Recently, a few studies have shown that D2D users can actually serve as friendly jammers to help enhance the security of cellular user communication against eavesdropping attacks. However, only a few studies considered the security of D2D communications. In this paper, we consider the secure resource allocation problem, particularly, how to assign resources to cellular and the D2D users to maximize the system security. To solve this problem, we propose an extensive game-based algorithm aiming at strengthening the security of both cellular and the D2D communications via system resource allocation. Finally, the simulation results show that the proposed method is able to efficiently improve the overall system security when compared to existing studies.

INDEX TERMS D2D communication, extensive game, secrecy capacity, security, resource allocation.

I. INTRODUCTION

For a past decade, the cellular communication has gained more popularity and it still attracts increasing attention nowadays. New technologies and applications are demanded to support content distribution, video streaming, relaying, cellular offloading and much more [1]. These technologies require low energy consumption, efficient spectrum usage and high throughput. Device-to-device (D2D) communications, which enable direct communications between pairs of devices within certain physical distances, has been recognized as a promising solution to improve spectrum efficiency and network throughput [1], [2].

Although introducing D2D communications into cellular network is beneficial [3], it also brings many security challenges to the network and the users. First, the security management in D2D communications may be completely distributed when the Base Station (BS) is not involved, leading to a high communication and management overhead [4]. Second, compared to standalone cellular communications, mobile users involved in D2D communications may have very limited capacity for security related computations [5]. As a result, conventional cryptographic based solutions cannot be applied directly due to their heavy computational costs and lightweight security solutions are required. However, in the past few years, security in D2D communications has not been studied extensively.

Recently, a few studies have been proposed to utilize physical layer interference to protect the cellular communications against eavesdropping attacks, in which one or multiple malicious users aim to collect private information transmitted between legitimate users by listening to their communication channels [5], [6]. The interference issue introduced by the resource sharing between Cellular Users (CUs) and D2D Users (DUs) has already attracted attentions in many previous studies [7]–[14]. However, most prior works assumed such interference to be harmful, as it would affect cellular communications and reduce the link budget. Nevertheless, from the aspect of the physical layer security, creating additional interference in the channel by allowing DUs to access the cellular band will also disturb malicious eavesdroppers from listening to the channel [15]. As a result, a secure non-zero rate transmission between legitimate users can be ensured by means of analyzing and adjusting physical parameters of wireless channels among mobile users, without involving heavy cryptographic computations.

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

For this line of research, the key problem is to allocate radio resources among DUs and CUs so that the interference is managed in a way that the physical layer security level is maximized [15]–[17]. Specifically, the security level is quantified as Secrecy Capacity (SC), which is defined as the maximum rate of trustworthy data to be transmitted in the cellular channel in the presence of malicious eavesdroppers [18]–[20]. Among the limited prior works along this research direction [15]–[17] , most of them only considered DUs as friendly jammers that help CUs to achieve their maximum SC. However, the SC of these DUs was not considered in the optimization formulation. In addition, most of these studies assumed the BS to perform all computation for allocating resources for CUs and DUs, which would be time-consuming and computationally heavy.

In this work, we aim to ensure the efficient communication security for both cellular users and D2D underlay communications in a cooperative way. Our main contributions are summarized as follows.

1. In the proposed algorithm, the SC of both DUs and CUs has been considered, leading to an increase of the system overall security. Specifically, this work models the resource allocation problem as an optimization problem, which aims to maximize the SC of both CUs and DUs. The proposed optimization problem is resolved by designing an extensive game between CUs and DUs.
2. This extensive game allows users to concurrently make their own matching decisions in a distributed way with minimum involvement of the BS. Moreover, by avoiding repetitive attempts to match the same pair of CUs and DUs, and having successfully matched users exit the game, the proposed game achieves high efficiency in matching, leading to low computation and communication overheads.
3. Comprehensive experiments have been designed and conducted. Four different resource allocation algorithms are compared with the proposed one. Experiment results show that the proposed algorithm consistently achieves higher total secrecy capacity and less number of matching iterations.

II. RELATED WORK

In this section, we mainly discuss related works in two categories: resource allocation and physical layer security.

A. RESOURCE ALLOCATION

In this line of research, existing studies mainly focus on resource optimization and ignore the security aspect. Therefore, they treat interference caused by D2D as a negative factor and aim to minimize the interference between CUs and DUs in their models. For example, the authors in [8] propose an interference graph-based resource allocation (InGRA) method, which solves the NP-hard matching problem within polynomial time by adopting the interference level as the weight of graph edges between CUs and DUs. In [9], the authors propose to allocate resources through an auction game, where the cellular channels and DUs are considered as bidders and goods respectively. The results show positive dynamics in system throughput. Other studies are also proposed with different assumptions. For example, in [21], the authors propose a Graph based Two-step Resource Allocation (GTRA) algorithm in the scenario of full duplex (FD) mode. In [22], the authors investigate resource allocation in D2D underlay communications with Rayleigh fading channels by assuming that only the statistical channel state information (CSI) is known. Their proposed solution, based on Hungarian algorithm, tends to maximize the ergodic sum rates under transmitting power and outage constraints.

These works inspire us to leverage bipartite graph matching to model the resource allocation problem, however, their major goal is to improve system performance, such as spectrum efficiency, throughput and transmitting power efficiency, etc., by minimizing interference introduced by D2D underlay communications. Different from these works, our proposed work mainly aims to maximize legitimate users' (including both CUs and DUs) secrecy capacity by utilizing such interference.

B. PHYSICAL LAYER SECURITY

With the concept of wiretap channel first proposed in [20], where the authors prove that wiretap channel can be another version of the main channel to facilitate two users to communicate securely without the need of private key exchanges, many physical layer security studies [6], [15]–[17], [20], [23]–[27] have been proposed to not decreasing the interference between cellular and D2D users but, on the contrary, using it to mitigate the negative impact of eavesdropper. In particular, the concept of SC is also first introduced in [20]. Then many studies have been proposed to improve CUs' SC by considering DUs as friendly jammers. For example, [23] aims to improve the SC of CUs by modeling the matching between CUs and DUs as a weighted bipartite graph and addressing it through the Kuhn-Munkres (KM) algorithm. In [26], the authors also propose to improve the SC of CUs by matching them with DUs while considering the trade-off between the power consumption and security. In [27] authors consider a scenario of a dynamic spectrum overlay, where they improve security performance of primary users (may be treated as CUs) against malicious eavesdropping with the help of friendly jamming from secondary users (may be treated as DUs) in form of Stackelberg game model.

Very recently, two studies have been proposed to consider the security of both CUs and DUs. In [25], the authors aim to maximize the secure transmission rate for both CUs and DUs. However, their proposed scheme can match at most one pair in each iteration, leading to high iteration number and long convergence time. The authors in [24] aim to maximize the SC of both CUs and DUs in heterogeneous networks, which consist of high-power nodes (HPN) and low-power nodes (LPN). However, their application scenario (i.e. the heterogeneous networks) is very specific.

Different from [24], [25], in this work, we propose to have CUs and DUs form cooperation groups in a regular cellular network in a completely distributed way with minimum involvement of the BS. In addition, the proposed scheme is carefully designed to minimize the number of matching iterations to achieve high efficiency.

Among other physical layer security papers, few recent works [28], [29] proposed methods to solve the sum secrecy rate maximization (SSRM) problem in presence of the malicious eavesdropper. In [28], authors consider a scenario of a multiple-input multiple-output multiple-eavesdropper (MIMOME) wiretap channel with artificial noise and D2D underlay communication. Their proposed method solves the SSRM problem with QoS constraints guarantee. Further in [29], these authors changed their initial scenario to multiple-input single-output (MISO) with multiple selective eavesdropper. They used successive convex approximation method to maximize the worst-case minimum secrecy rate.

As a summary, these studies discussed above show that regardless of different system model assumptions, proper resource allocation between CUs and DUs can significantly improve the total cellular network performance and security. But as more constraints are considered in the optimization problem, it often requires much higher computational complexity to solve the problem. In this work, we propose an extensive game based scheme that maximizes the system overall SC in a distributed way with high efficiency.

III. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

In this paper, we consider a single-cell wireless network where the BS is equipped with N antennas, and serves N CUs using N orthogonal channels via zero-forcing beamforming.[1] In this network, there are M pairs of DUs, which can access the BS via the uplink transmissions/channels in the underlay mode, and a malicious eavesdropper that overhears information in *all* channels [23], [25], as shown in Figure 1. Please note that for convenience purpose, we use one DU to indicate a pair of D2D users (i.e. one transmitter and one receiver). In this paper, we assume block-fading channels for all the users, including the eavesdropper, where the channel-state information (CSI) remains constant within a coherent block/slot within some time. Moreover, the CSI of all the users is available at the BS [23].

In the cellular network, since the uplink transmission is less loaded than the downlink transmission, sharing uplink channels with D2D users is widely assumed, e.g., [23], [25]. Also, in this paper, we assume that each user, including CUs, DUs and the eavesdropper, is equipped with a single antenna, e.g., [23]. If the users are equipped with multiple antennas as well, then the resulting analysis would be much complicated as multiplexing in the spatial domain can also be

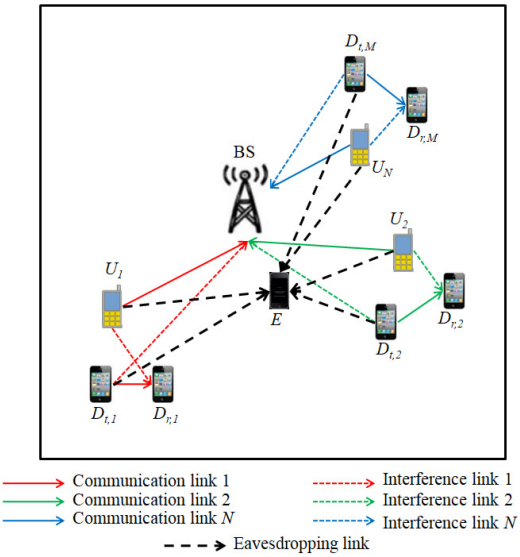

FIGURE 1. System model representation.

exploited. In addition, allowing each CU to share its uplink channels with multiple DUs, and thus serving more DUs might increase the sum-throughput of the system. However, it introduces extra interference to cellular uplink communications and other D2D communications. Thus, in this paper, we assume only one-to-one matching between CUs and DUs, meaning that a CU shares its uplink channel with no more than one DU, and also one DU cannot access multiple CUs uplink channels at every time.[2]

The malicious eavesdropper tends to retrieve sensitive data from one or multiple users in the network, including both CUs and DUs. However, legitimate users do not know the exact target of the eavesdropper. This leads to the worst case scenario, where all users have to consider the possibility of eavesdropper listening to their channels for the security purpose.[3] Also, if the eavesdropper is active and listens to any channel, the BS can detect its location and then share such information with all the other users in the system.

Next, we show the channel models and rate expressions that are used in this paper. We denote CUs, DUs and the eavesdropper as U_i, D_j and E, respectively, where $i = 1, 2, \ldots, N$ and $j = 1, 2, \ldots, M$. In addition, the transmit power of U_i and D_j is denoted by P_{U_i} and P_{D_j}, respectively. Moreover, for the D2D pair D_j, we use $D_{t,j}$ and $D_{r,j}$ to represent its transmitter and receiver, respectively. Note

[1] If the number of CUs is less than N, the analysis made in this paper still applies in a similar manner but the effective channel from each CU to the BS would become a vector rather than a scalar

[2] In fact, the analysis made in this paper can be extended to address the multiple-to-multiple matching problem by allowing unmatched DUs to continue proposing to CUs that have already been successfully matched. However, determining the optimal combinations of multiple DUs to share the same channel may lead to significantly higher computational complexity. Therefore, we leave this problem to our future work

[3] In the case that multiple eavesdroppers are present and without collaboration with one another, the problem can be decoupled into multiple independent sub-problems where in each sub-problem only one eavesdropper is present. Then the overall system SC is the sum of that of each user, which is the minimum SC against different eavesdroppers

that when the BS with N antennas serves N CUs simultaneously via zero-forcing beamforming to form N parallel interference-free channels, the resulting effective CSI, represented by h, for each user is a scalar, which can be calculated by the product of the *actual* $1 \times N$ channel vector and the $N \times 1$ beamforming vector. In this paper, we assume that each effective channel h follows the Rayleigh fading, i.e., $h \sim \mathcal{CN}(0, d^{-\alpha/2})$, where d represents the distance between the transmitter and the receiver, and α represents the propagation path-loss factor.

For a CU that does not share its spectrum with any DU, its channel capacity is given by:

$$C_{U_i} = \log_2(1 + \text{SNR}_{U_i,B}) = \log_2\left(1 + \frac{|h_{U_i,B}|^2 P_{U_i}}{\sigma^2}\right), \quad (1)$$

where $|h_{U_i,B}|^2$ is the channel gain from CU U_i to the BS and σ^2 is the variance of the additive white Gaussian noise. If the malicious eavesdropper E listens to a cellular user U_i's uplink channel, then the regular wiretap channel's capacity is:

$$C^E_{U_i} = \log_2\left(1 + \frac{|h_{U_i,E}|^2 P_{U_i}}{\sigma^2}\right), \quad (2)$$

where $|h_{U_i,E}|^2$ is the channel gain from CU U_i to eavesdropper E.

Finally, we introduce the channel secrecy capacity (SC) calculation as follows. Specifically, for a CU who does not share its channel with any DU, the SC can be computed as [23]

$$SC_{U_i} = [C_{U_i} - C^E_{U_i}]^+ = \left[\log_2\left(1 + \frac{|h_{U_i,B}|^2 P_{U_i}}{\sigma^2}\right) - \log_2\left(1 + \frac{|h_{U_i,E}|^2 P_{U_i}}{\sigma^2}\right)\right]^+, \quad (3)$$

where $[\cdot]^+ \triangleq \max(\cdot, 0)$. On the other hand, when a DU D_j shares the channel of CU U_i, it helps the CU U_i to increase its SC by generating extra interference to eavesdropper. Because of treating this extra interference as noises, e.g., [21]–[25], we obtain the following SC for U_i:

$$SC_{U_i,D_j} = \left[\log_2\left(1 + \frac{|h_{U_i,B}|^2 P_{U_i}}{\sigma^2 + |h_{D_{t,j},B}|^2 P_{D_j}}\right) - \log_2\left(1 + \frac{|h_{U_i,E}|^2 P_{U_i}}{\sigma^2 + |h_{D_{t,j},E}|^2 P_{D_j}}\right)\right]^+, \quad (4)$$

where $|h_{D_{t,j},B}|^2$ and $|h_{D_{t,j},E}|^2$ are the channel gains from D_j transmitter to the BS and to the eavesdropper E, respectively. Additionally, based on the chosen channel after the matching process [25], the SC for D_j can be calculated as:

$$SC_{D_j,U_i} = \left[\log_2\left(1 + \frac{|h_{D_{t,j},r}|^2 P_{D_j}}{\sigma^2 + |h_{U_i,D_{r,j}}|^2 P_{U_i}}\right) - \log_2\left(1 + \frac{|h_{D_{t,j},E}|^2 P_{D_j}}{\sigma^2 + |h_{U_i,E}|^2 P_{U_i}}\right)\right]^+, \quad (5)$$

where $|h_{D_{t,j},r}|^2$ is the channel gain for the D2D, from $D_{t,j}$ (i.e. the transmitter) to $D_{r,j}$ (i.e. the receiver), and $|h_{U_i,D_{r,j}}|^2$ is the channel gain from CU U_i to $D_{r,j}$.

B. PROBLEM FORMULATION

We define an $N \times M$ matrix $K = [k_{i,j}]$, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, M$, where $k_{i,j}$ is a binary value indicating whether U_i is matched with D_j. We set $k_{i,j} = 1$ if U_i and D_j are matched to share the same channel, or $k_{i,j} = 0$ otherwise. Then we formulate the problem of resource allocation as the maximization of the total system SC:

$$\max_K \sum_{i=1}^{N} k_{i,j}(SC_{U_i,D_j} + SC_{D_j,U_i}) + (1 - k_{i,j})SC_{U_i},$$
$$\text{s.t.} \begin{cases} \sum_{i=1}^{N} k_{i,j} \le 1, & 1 \le i \le N, \\ \sum_{j=1}^{M} k_{i,j} \le 1, & 1 \le j \le M, \\ k_{i,j} \in \{0, 1\}, & 1 \le i \le N, \quad 1 \le j \le M. \end{cases} \quad (6)$$

The first constraint $\sum_{i=1}^{N} k_{i,j} \le 1$ indicates that each CU can only share its channel with no more than one DU. Similarly, the second constraint $\sum_{j=1}^{M} k_{i,j} \le 1$ indicates that each DU can only join no more than one CU's channel at a certain time.

This maximization problem can be solved in a centralized way (i.e. at the BS side). However, as this problem is NP-hard [25], the centralized approach will cause heavy computation at the BS side. Therefore, we propose to approximate the original problem by having each individual CU and DU maximize their own SC through an extensive game matching process. In particular, as we assume the BS knows the CSI of all users, it will share the information with related CUs and DUs. That means, each CU can calculate its own SC for matching with any specific DU. Similarly, each DU can calculate its own SC for matching with any specific CU. With such information, CUs and DUs will be able to launch the proposed matching process in a distributed way.

IV. AN EXTENSIVE GAME BASED RESOURCE ALLOCATION OPTIMIZATION

To address the maximization problem discussed above, in this section, we further formulate it as a matching problem in a bipartite graph. In addition, we propose to resolve the problem by launching an extensive game between CUs and DUs in the system.

A. CONSTRUCTING A BIPARTITE GRAPH

The bipartite graph is a graph consisting of two sets of vertices, where edges only exist between two vertices from different sets. Particularly in our problem, as shown in Figure 2, we consider two different sets containing cellular users and D2D users separately, and aim to find the best matches

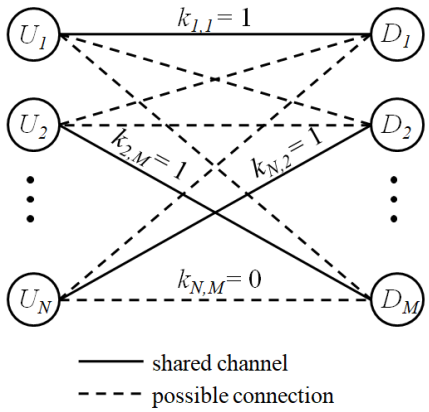

FIGURE 2. Bipartite graph representation.

between these two sets so that the overall system SC can be maximized.

In particular, let us have a set $\boldsymbol{U}$ containing all the CUs such that $U_i \in \boldsymbol{U}$, $i = 1, 2, \ldots, N$, and a set $\boldsymbol{D}$ containing all the DUs such that $D_j \in \boldsymbol{D}$, $j = 1, 2, \ldots, M$. Then a bipartite graph is created with vertices from set $\boldsymbol{U}$ and set $\boldsymbol{D}$. As illustrated in Figure 2, if a cellular user U_i shares its uplink channel with a D2D user D_j, there will be an edge between these two vertices. Recall that we have defined an $N \times M$ matrix binary $K = [k_{i,j}]$, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, M$, to indicate whether a specific edge exists between any two vertices. This bipartite graph will have $N * M$ edges at maximum. If channel is shared between specific U_i and D_j (solid line), the corresponding $k_{i,j}$ equals to 1, otherwise, the edge represents the possible connection for 2 specific users (dashed line) and in that case $k_{i,j}$ equals to 0.

B. AN EXTENSIVE GAME BETWEEN CELLULAR USERS AND D2D USERS

To address the best matching problem in the bipartite graph discussed above, we introduce an extensive game based matching strategy between CUs and DUs. Different from the classic strategic game, which often underestimates the sequential order of players' actions, the extensive game explicitly takes the sequential structure of players' decision making process into considerations [30] and thus allows us to study the cases where each player's decision can change along the events when other players' actions change.

In particular, the simplest extensive game involves two players, both of whom have their own interests/preferences (i.e. payoff) and interact with each other in multiple rounds (i.e. time points). At each time point, only one player needs to make an action. For both of the two players, if the payoff of performing an action is higher than that of performing any of all other actions, this action will be chosen and performed. Different from the classic strategic game, the players in an extensive game may have different orders to perform actions, and each of their actions may influence the other one's later actions, leading to different possible action sequences. Therefore, we need to specify the set of all sequences of actions that can possibly occur, as well as the player who performs an action at each time point in each sequence (i.e. the orders of actions). The game will reach the Nash equilibrium if none of these two players can perform another action, other than the one chosen, to further increase his/her payoff when the other player does not change his/her action.

In our problem, in order to find the best matches between CUs and DUs, we propose to design an extensive game among all the cellular and D2D users. Specifically, we propose to have the D2D users initiate the game as they are eager to share the celluar channels. Therefore, at the first time point, each DU has N different action options as requesting for channel access from $U_1, U_2, U_3, \ldots U_N$, respectively. To simply explain the game design, we use an arbitrary pair of CU (i.e. U_i) and DU (i.e. D_j) as an example to discuss the game process between them, as shown in Figure 3. Please note that the similar process may occur between any pairs of CU and DU at the same or different time points. To focus only on the interactions between D_j and U_i, we simply consider D_j's possible actions as either sending request to U_i or not (i.e. sending request to any other CUs). Among different action options, D_j will take the action with the highest payoff. Assuming that if sharing the channel of U_i would bring the highest payoff for D_j, consequently D_j will take the action as sending request to U_i. Then at the next time point, U_i needs to decide whether to accept the request from D_j or not. Please note that at this time point, U_i may receive multiple requests from different DUs. Similarly, among different requests, U_i will accept the one with the highest payoff for itself. If U_i accepts D_j's request, they will form a match and quit the game. Otherwise, D_j will mark U_i as "rejected" to ensure not sending repeated requests to U_i again, and then sends request to some other CU instead. As shown in Figure 3, this process between each pair of a CU and a DU can be modeled in the form of a tree.

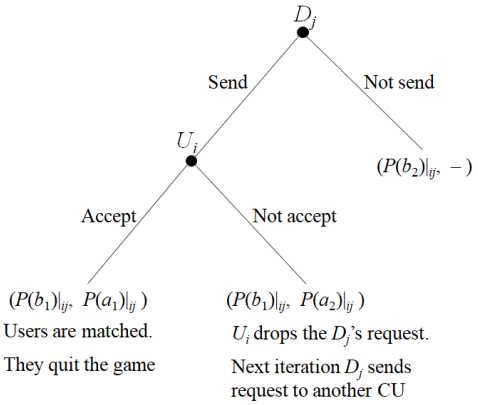

FIGURE 3. Example of an extensive game between an arbitrary pair of CU and DU.

In this work, we denote the two actions of a CU, accept or not accept a request from a specific DU, as a_1 and a_2 respectively, and the two actions of a DU, send or not send request to a specific CU as b_1 and b_2 respectively. Then the

payoff of each action is marked as $P(a_1)$, $P(a_2)$, $P(b_1)$, $P(b_2)$, respectively. A DU D_j will send the request to U_i, if $P(b_1)|_{ij}$ is higher than $P(b_2)|_{ij}$, where $P(b_2)|_{ij}$ represents the highest payoff for D_j if it sends request to any other CUs in the system. Then the given U_i may accept the request if $P(a_1)|_{ij} > P(a_2)|_{ij}$, where $P(a_2)|_{ij}$ represents the highest payoff for U_i if it accepts any other requests that has been received from other DUs *at the same time point*. Otherwise, the request will be rejected. Then this iteration is done, resulting in either a successful or an unsuccessful match between U_i and D_j. The CUs (or DUs) that are not successfully matched with any other DUs (or CUs) will participate in the next matching iteration.

C. CALCULATION OF THE GAME PAYOFF

Specifically, we calculate the payoff for each action in Figure 3 as follows. For U_i, the payoff of the action a_1 is its SC improvement (i.e. gain G_{ij}) introduced by allowing D_j to share its channel, when compared to its original SC with no DUs sharing its channel:

$$P(a_1)|_{ij} = G_{ij} = SC_{U_i,D_j} - SC_{U_i}. \tag{7}$$

The payoff of action a_2 is its maximum SC improvement if it accepts the request from any other DUs that wants to share its channel at a given moment τ (e.g. at the current iteration):

$$P(a_2)|_{ij} = \max_m \ (G_{im})|_\tau, \quad m \neq j, \tag{8}$$

where m represents the indices of the non-matched DUs.

For D_j, the payoff of action b_1 is its SC when it is allowed to access the channel of U_i:

$$P(b_1)|_{ij} = SC_{D_j,U_i}. \tag{9}$$

The payoff of action b_2 is player D_j's maximum SC that can be achieved when connecting with any other possible non-matched CUs:

$$P(b_2)|_{ij} = \max_n (SC_{D_j,U_n})\ |_{\sum_m k_{n,m}=0}, \quad n \neq i. \tag{10}$$

In addition, for all the payoff values we implement the following function:

$$P(X)|_{ij} = \max(P(X)|_{ij}, 0), \tag{11}$$

where X denotes the possible actions of both U_i and D_j, $\max(P(X)|_{ij}, 0)$ is the maximum value between $P(X)|_{ij}$ and 0. It indicates that a user's payoff will be set as 0 if it is negative. Then we define the **condition of matching** as follows.

Definition 1: **Condition of Matching**: If and only if $P(a_1)|_{ij} > P(a_2)|_{ij}$, $P(b_1)|_{ij} > P(b_2)|_{ij}$, and at the same time $P(a_1)|_{ij} > 0$, users U_i and D_j are matched and the corresponding value in matrix K is set as 1 (i.e. $k_{i,j} = 1$).

D. AN ITERATIVE MATCHING PROCESS

In this section, we summarize the detailed procedure of the proposed algorithm, which is an iterative matching process. In particular, the input values for the algorithm are SC_{U_i}, SC_{D_j,U_i} and SC_{U_i,D_j} for all $i = 1, 2, \ldots, N, j = 1, 2, \ldots, M$, which can either be obtained by the CUs and DUs themselves or be provided by the BS. Please note that each CU (or DU) only needs to know its own SC for matching or not matching with any specific DU (or CU). They do not have to know the SC for other users. Then the CUs and DUs will launch an extensive game to match each other. Specifically, the matching is done through iterations, where each iteration contains two time points (i.e. steps) in the extensive game.

Procedure 1 Optimization Algorithm Procedure (DU side)

1: Find the input values of SC_{D_j,U_i} for all $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, M$
2: Take a non-matched D_j as an example, where $j = 1, 2, \ldots, M$ //the further actions are taken by all D_j at the same time
3: Find $\max_{i=1}^{N}(SC_{D_j,U_i})|_{\sum_m k_{i,m}=0}$
4: **if** The corresponding U_i is already marked as sent **then**
5: Exclude it from current iteration
6: Recalculate $\max_{i=1}^{N}(SC_{D_j,U_i})|_{\sum_m k_{i,m}=0}$
7: **end if**
8: The given D_j sends the request to the corresponding U_i. This U_i is marked as sent
9: Find the specific $P(b_1)|_{ij}$ and $P(b_2)|_{ij}$

In step 1, all the non-matched DUs will launch the game by deciding which CU to send the request to. For each non-matched $D_j|_{\sum_n k_{n,j}=0}$, it calculates its maximum payoff (i.e. SC) when matching with any of the non-matched CUs as $\max_{i=1}^{N}(SC_{D_j,U_i})|_{\sum_m k_{i,m}=0}$. After that each D_j sends only one request to the corresponding CU that may enable its maximum payoff (e.g. U_i), and marks this CU as "sent". Please note that this will guarantee that the second part of the matching condition (i.e. $P(b_1)|_{ij} > P(b_2)|_{ij}$) is satisfied. The procedure is shown in the Procedure 1.

In step 2, CUs will make their decisions about accepting or rejecting requests that they have received in step 1. Please note that it is possible for some CUs to not receive any requests, indicating that all the DUs decide to perform b_2 in their one-to-one game with these CUs at this iteration. In this case, these CUs, which are not matched with any DU, will have to perform a_2 to all DUs. On the other hand, CUs, that receive one or several requests, make their decisions by calculating $P(a_1)|_{ij}$ and $P(a_2)|_{ij}$ and check if the first and the third parts of the matching condition (i.e. $P(a_1)|_{ij} > P(a_2)|_{ij}$ and $P(a_1)|_{ij} > 0$) are satisfied. If yes, U_i will accept the request from D_j and reject all other requests. This way, U_i and D_j will be matched and leave the game. The value of $k_{i,j}$ will be set as 1. Other DUs that are not matched will wait for the next iteration.

In the next iteration, only the non-matched CUs and DUs will continue participating the game. The DUs will expand their extensive game tree by sending a request to another non-matched CU. Please note that a CU receiving one or

Procedure 2 Optimization Algorithm Procedure (CU side)

Find the input values of SC_{U_i} and SC_{U_i,D_j} for all $i = 1, 2, \ldots, N, j = 1, 2, \ldots, M$
$b_{match} =$ true
while $b_{match} ==$ true **do**
  Take a non-matched U_i as an example. //the further actions are taken by all U_i at the same time
  if U_i received at least one request from any D_j **then**
    for each requested D_j **do**
      Find $P(a_1)|_{ij}$ and $P(a_2)|_{ij}$
      if The condition of matching takes place **then**
        $k_{i,j}$ is set to 1
        The given U_i and D_j are added to the matrix K. Both of users finish the game.
      end if
    end for
  end if
  if No more matches are established **then**
    $b_{match} =$ false
  end if
end while

multiple requests will always choose the best one to match and leave the game, unless none of the requests can result in a positive payoff. As a result, if a DU has sent request to a specific CU already but got rejected, it will not send any further requests to the same CU again. Such design can help us greatly reduce repetitive negotiation steps. The proposed algorithm stops when no further matching can be found. The procedure of step 2 is shown in the Procedure 2.

E. ANALYSIS OF COMPUTATIONAL COMPLEXITY

Compared to other schemes, one of the main advantages of the proposed algorithm is that the resource allocation process is done in a distributed way. It means that the BS does not perform heavy computations. Instead, these computations are performed simultaneously by each individual CU and DU. Specifically, for each DU, before sending matching requests to CUs, it needs to calculate and rank its possible SCs when matching with each CU. The computational complexity of such process is $O(N)$. Moreover, this value is fixed and doesn't depend on the algorithm's iterations number. On the other hand, for each CU, after it receives at least one request from DUs, it needs to compare its possible SCs when matching with each of the requesting DUs. In the extreme case, a CU may receive requests from all DUs, which requires $O(M)$ SC calculations. Such extreme case may only occur when all the D2D pairs are located densely and close to one CU, which is very rare. The average computational complexity of that process is $O(M/N)$ per one iteration, if we assume that DUs and CUs are uniformly located in the cell. Please note that, if a CU receives multiple valid requests, it will choose one to match and quit the game, leading to no further computation. Otherwise, if a CU receives no request in one iteration, it does not need to perform any computation but continues participating in the next iteration. Thus, the total computational complexity for both CU and DU is $O(N + M/N)$ on average per one iteration, and the overall computational complexity of the proposed algorithm is $O(N + M)$. That is the extreme case that occurs when the algorithm needs to be run N iterations in order to match the last CU.

Meanwhile, the computational complexity of KM algorithm in [23] is $O(NM^2)$, since the BS performs all the computations. The computational capacity of the secrecy-based scheme in [25] is $O(N)$ for CU side and $O(MN)$ for DU side. In other words, the overall computation complexity of that algorithm is $O(N + MN)$. Given that, our proposed algorithm has the lowest computational complexity and can be implemented easily into the cellular network.

V. SIMULATION

A. EXPERIMENT SETUP

To evaluate the results of the proposed algorithm, simulation in MATLAB is performed. In particular, we model the cellular network as a square region [1000m × 1000m], where both the horizontal and vertical axes range from 0m to 1000m. The base station is located in the center of the area at [500m, 500m]. We assume that the eavesdropper prefers to stay close to the center for better signal reception, and therefore simulate its location as a uniformly distributed random variable with 50m radius away from the BS. Cellular and D2D users are randomly placed inside the cellular area with a uniform distribution (as random placement is the standard way of simulation in wireless communications). Specifically, for each D2D user pair, the transmitter's location is determined first, and the receiver's location is then determined at a random location with a fixed radius from the transmitter. The signal propagation for all the links is simulated using Rayleigh fading model with Additive White Gaussian Noise (AWGN) with zero mean. Other simulation parameters are listed in Table 1.

TABLE 1. Simulation parameters.

The power of CU's transmitter (P_{U_i})	10 dBm
The power of D2D transmitter (P_{D_j})	10 dBm
D2D pair distance	10m - 20 m
Noise power (σ^2)	-70 dBm
Propagation loss factor (α)	2 - 4
Number of experiments	100

B. COMPARISON SCHEMES

The proposed resource sharing algorithm is compared to four algorithms. The first one, named random assignment, represents a naive solution that randomly assigns DUs to CUs. Please note, even for this random assignment algorithm, the matching between a pair of DU and CU may fail if such match leads to negative SC for either the CU or DU. Furthermore, two state-of-the-art researches are also implemented for comparison. One is the KM algorithm proposed in [23], where the authors propose to build a weighted bipartite graph

and use the CU's SC values as the weights for each matching edge. The other one is a secrecy-based access control scheme proposed in [25]. Although the authors in that paper also consider the coalition formation game, we only focus on the access control scheme, since it uses one-to-one matching.

In addition, the proposed algorithm is also compared to the Gale-Shapley (GS) algorithm, which is a well-known algorithm to address the stable marriage problem [31]. This algorithm wasn't applied for resource sharing in D2D communication before, but it was applied for that in other fields, for example in [32]. The stable marriage problem aims to identify a stable matching between nodes from two different sets, with each node's matching preferences given, which is very similar to our problem. However, these two algorithms are very different in the following aspects. First, the GS algorithm is mainly effective when the two sets have exactly the same number of nodes, which is not the case in most of our scenarios. Second, the GS algorithm assumes that all nodes would rather be paired with an arbitrary node than not paired, even if the paired node ranks the lowest on their preference list. However, in our scenario, a CU may not want to pair with a DU if such pairing makes its SC value negative. Third, the computational complexity of the GS algorithm can be very high since even the paired nodes will not leave the game but stay to participate in the future matching in case they can find a better partner. It may lead to significantly larger number of iterations. In order to compare the proposed algorithm with the GS algorithm, we have slightly revised the GS algorithm so that it takes into account the value of SC, and there will be no matching of users in case of a negative SC. Such revisions will help the GS algorithm perform better in our scenario.

VI. EXPERIMENT RESULTS

In this section, we evaluate the performance of the proposed scheme mainly based on the total system secrecy capacity, the ratio of successfully matched CUs and their cumulative distribution over iterations.

A. TOTAL SYSTEM SECRECY CAPACITY

We have conducted three sets of experiments to evaluate the total system secrecy capacity achieved by different algorithms under the influence of various environmental settings. Specifically, we have investigated the impact of (1) the number of CUs, DUs and their ratio, (2) the propagation loss factor, and (3) the distance between each D2D pair, in three sets of experiments respectively.

1) IMPACT OF USERS NUMBER

In the first set of experiments, we dynamically adjust the number of CUs and DUs while fixing the propagation loss factor and the distance between each D2D pair as 3m and 20m, respectively. The results are shown in Figure 4.

In Figure 4, there are four subplots, representing cellular network with fixed number of CUs as 10, 20, 30 and 40, respectively. The five curves in each subplot represent the proposed resource allocation algorithm (PA), the KM algorithm in [23] (KM), the secrecy-based access control scheme in [25] (SB), the Gale-Shapley algorithm (GS), and the random assignment algorithm (RA), respectively.

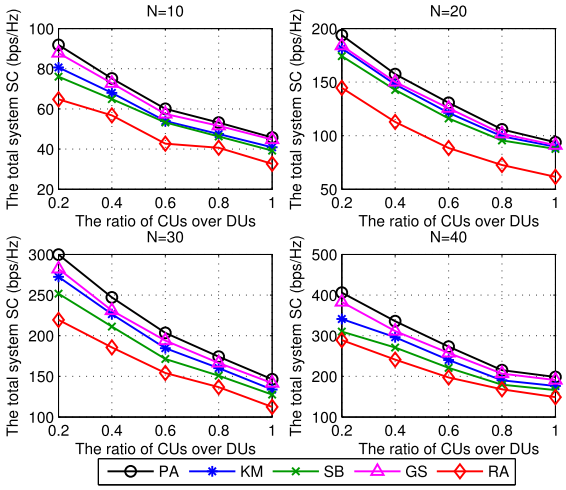

FIGURE 4. Total system secrecy capacity at different number of CUs.

From Figure 4, we can observe consistent trend across all the four subplots. That is, when the number of CUs is fixed, the decrease of the ratio of CUs over DUs (i.e. the increase of DUs in the system) leads to higher system SC. This validates the effectiveness of improving system SC by introducing D2D communications. In addition, the proposed scheme achieves the highest overall system SC when compared to other schemes. This is because the proposed scheme aims to maximize the SC for the entire cellular network. Competing algorithms, specifically, KM and SB, on the contrary, match DUs with CUs only if that results in maximal SC for CUs. The random assignment scheme yields the worst SC among all schemes as it does not consider SC at all during its matching process. Moreover, these curves are not linearly decreasing with the decrease of DUs, because when the CU/DU ratio is decreased, on average, each CU has fewer options when choosing the best DU to match, leading to a slight drop of the system SC.

2) IMPACT OF PROPAGATION LOSS FACTOR

In this set of experiments, we aim to evaluate the dependency of the total system SC on the propagation loss factor α for different algorithms at the fixed number of CUs and DUs. The results are shown in Figure 5.

In Figure 5, the x-axis represents the propagation loss factor α, and the y-axis represents the total system secrecy capacity. As we can see from the Figure 5, increasing the propagation loss factor from 2 to 3 leads to the increase of the total system SC up to its maximum value for all the five resource sharing algorithms. The further increase of α leads to the decrease of the total system SC. This is due to the achievement of an optimal system status when considering both the information communication among legitimate users and the information that can be retrieved by the eavesdropper.

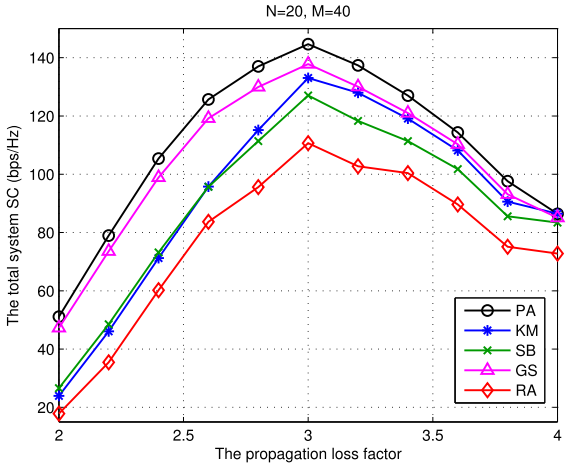

FIGURE 5. Total system secrecy capacity at different α.

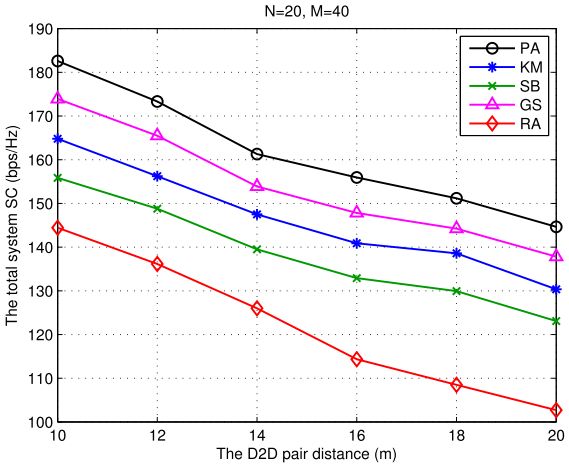

FIGURE 6. Total system secrecy capacity at different D2D pair distance.

More specifically, when α is larger, the propagation medium is worse, leading to higher information propagation loss between legitimate users (i.e. from CU to BS, or from D2D transmitter to D2D receiver), which on the other hand, also prevents eavesdroppers from retrieving more information. When α is smaller, the propagation medium is closer to free space, which does not only help information propagate freely between legitimate users, but also benefits the eavesdropper in terms of retrieving more information. In our experiments, the optimal system SC is achieved when $\alpha = 3$. Regardless of the propagation loss factor value, the proposed scheme always outperforms the other algorithms in terms of overall system SC. Such results demonstrate consistent effectiveness of the proposed scheme in different environments.

3) IMPACT OF D2D USERS DISTANCE

In the third set of experiments, we evaluate the dependency of the total system secrecy capacity on the D2D pair distance for different algorithms, when there are $N = 20$ and $M = 40$ users in the network and the propagation loss factor is 3. The results are shown in Figure 6.

As we can see from the Figure 6, increasing the D2D pair distance leads to the decrease of the total system secrecy capacity, as the DU transmitter and its receiver become more distant from each other. Nevertheless, regardless of the D2D pair distance value, the proposed algorithm always achieves higher total system SC when compared to other resource sharing algorithms.

B. RATIO OF SUCCESSFULLY MATCHED CELLULAR USERS

In addition to the overall system secrecy capacity, we also investigate the ratio of matched CUs when different schemes are applied. In Figure 7, we illustrate the ratio of successfully matched CUs when the number of DUs in the cellular network increases.

From Figure 7, we can observe that these five schemes achieve similar ratio of matched pairs, especially when the total number of DUs is large. When the DU number is small, indicating less choices for CUs, the KM algorithm outperforms all other schemes and achieves the highest ratio of matched CUs. Compared to the KM algorithm, although the proposed scheme achieves less number of matched CUs, its high overall SC indicates that the matching mechanism is more efficient. That is, the matched CUs and DUs can achieve higher overall SC. Please note that even the random assignment algorithm cannot match all CUs because any matching that leads to negative SC will be rejected.

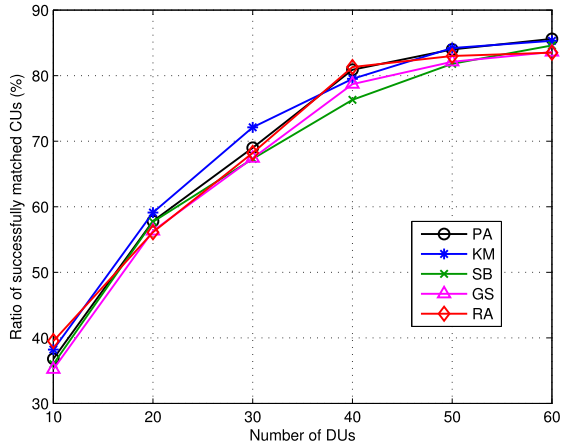

FIGURE 7. Ratio of successfully matched CUs at $N = 10$.

C. CUMULATIVE DISTRIBUTION OF SUCCESSFULLY MATCHED CELLULAR USERS OVER ITERATIONS

In this set of experiments, we investigate the cumulative distribution of successfully matched CUs along the iteration number they were matched at, i.e. what is the increase in successfully matched CUs per each iteration of the algorithm. We set number of CUs as 20 and number of DUs as 100. The experiments results are shown in Figure 8.

As can be seen from Figure 8, the proposed algorithm is very efficient in terms of iterations number, as it could match most of the CUs during first 3 iterations. Similarly, the GS

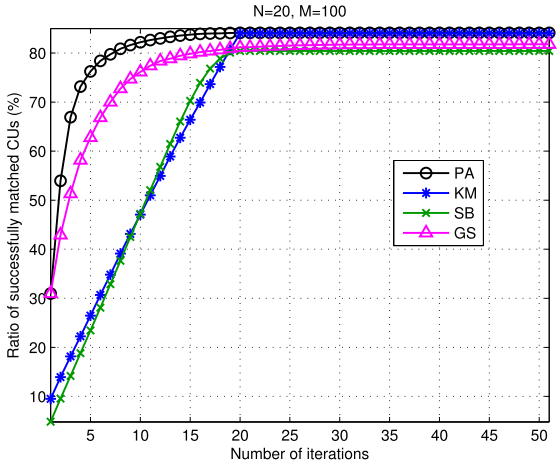

FIGURE 8. Cumulative distribution of successfully matched CUs.

algorithm can also match user pairs efficiently in the first few iterations. However, the GS algorithm completes all the matching at the 51st iteration, as it attempts to find the best DU for every CU, which leads to the case that even paired CUs and DUs can stay in the system to participate in the later matching iterations. Furthermore, the other two algorithms (i.e. the KM algorithm and the secrecy-based access control algorithm) show approximately the same number of matched CUs per iteration, that is one per iteration on average, resulting in more iterations to finish the matching algorithm. Compared to these two algorithms, the proposed algorithm can match several CUs during one iteration, because the DUs can send requests simultaneously and several of them can be matched at the same time.

VII. CONCLUSION

In this paper, we formulate the secure resource allocation between CUs and DUs as an optimization problem, which is resolved through an extensive game-based scheme. The simulation results show that introducing D2D users into a cellular network can significantly increase the system secrecy capacity, and the proposed algorithm outperforms the four different comparison schemes. Several interesting works could be investigated in future work. For example, how to characterize the secrecy capacity of the system in the presence of D2D communications in more complex scenarios, such as devices with multi-antennas, full-duplex mode channel sharing, dynamic transmit power adjustment, multiple-to-multiple users matching. Also, when CUs, DUs or the eavesdropper has high mobility, how to extend this work is worthy of further investigation.

REFERENCES

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

[2] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[3] M. C. Erturk, S. Mukherjee, H. Ishii, and H. Arslan, "Distributions of transmit power and SINR in device-to-device networks," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 273–276, Feb. 2013.

[4] 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. 29, no. 2, pp. 1054–1079, 2nd Quart., 2016.

[5] M. Wang and Z. Yan, "Security in D2D communications: A review," *IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 1199–1204.

[6] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu, and C. Zhao, "Device-to-device communications: The physical layer security advantage," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 1606–1610.

[7] B. Kaufman, J. Lilleberg, and B. Aazhang, "Spectrum sharing scheme between cellular users and ad-hoc device-to-device users," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1038–1049, Mar. 2013.

[8] R. Zhang *et al.*, "Interference graph-based resource allocation (InGRA) for D2D communications underlaying cellular networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3844–3850, Aug. 2015.

[9] C. Xu *et al.*, "Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 348–358, Sep. 2013.

[10] T. Peng, Q. Lu, H. Wang, S. Xu, and W. Wang, "Interference avoidance mechanisms in the hybrid cellular and device-to-device systems," in *Proc. IEEE PIMRC*, Sep. 2009, pp. 617–621.

[11] C. Xu, L. Song, Z. Han, Q. Zhao, X. Wang, and B. Jiao, "Interference-aware resource allocation for device-to-device communications as an underlay using sequential second price auction," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 445–449.

[12] S. Xu, H. Wang, T. Chen, Q. Huang, and T. Peng, "Effective interference cancellation scheme for device-to-device communication underlaying cellular networks," in *Proc. IEEE 72nd Veh. Technol. Conf.-Fall*, Sep. 2010, pp. 1–5.

[13] P. Janis, V. Koivunen, C. Ribeiro, J. Korhonen, K. Doppler, and K. Hugl, "Interference-aware resource allocation for device-to-device radio underlaying cellular networks," in *Proc. IEEE 69th Veh. Technol. Conf. VTC Spring*, Apr. 2009, pp. 1–5.

[14] M. Jung, K. Hwang, and S. Choi, "Joint mode selection and power allocation scheme for power-efficient device-to-device (D2D) communication," in *Proc. IEEE 75th Veh. Technol. Conf. (VTC Spring)*, May 2012, pp. 1–5.

[15] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

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

[17] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. 11th IEEE Singapore Int. Conf. Commun. Syst.*, Nov. 2008, pp. 974–979.

[18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[19] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[20] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[21] L. Ren, M. Zhao, X. Gu, and L. Zhang, "A two-step resource allocation algorithm for D2D communication in full duplex cellular network," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–7.

[22] L. Wang, H. Tang, H. Wu, and G. Stüber, "Resource allocation for D2D communications underlay in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1159–1170, Feb. 2017.

[23] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2319–2324.

[24] K. Zhang, M. Peng, P. Zhang, and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1822–1834, Feb. 2017.

[25] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.
[26] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.
[27] Y. Yao, W. Zhou, B. Kou, and Y. Wang, "Dynamic spectrum access with physical layer security: A game-based jamming approach," *IEEE Access*, vol. 6, pp. 12052–12059, 2018.
[28] W. Mei, Z. Chen, and J. Fang, "Sum secrecy rate optimization for MIMOME wiretap channel with artificial noise and D2D underlay communication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.
[29] W. Mei, Z. Chen, J. Fang, and B. Fu, "Secure D2D-enabled cellular communication against selective eavesdropping," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.
[30] M. J. Osborne *et al.*, *An Introduction to Game Theory*, vol. 3. New York, NY, USA: Oxford Univ. Press, 2004.
[31] 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.
[32] Y. Liu, L. Zhang, F. Tao, and L. Wang, "Resource service sharing in cloud manufacturing based on the Gale–Shapley algorithm: Advantages and challenge," *Int. J. Comput. Integr. Manuf.*, vol. 30, nos. 4–5, pp. 420–432, May 2017.

OLEKSII RUDENKO received the B.Eng. degree in mobile communication and the M.Eng. degree in technologies and facilities of telecommunication from the Odessa National Academy of Telecommunication n.a. A. S. Popov, in 2014 and 2016, respectively. He is currently pursuing the Ph.D. degree in information and communication engineering with Northwestern Polytechnical University (NPU). Up to date, together with I. Strelkovskaya and E. Lysiuk, he has published a paper Usage of Cubic Spline-Interpolation for Voice Signal Recovery in Vocoder Radiocommunication Systems for local 5th International Scientific-Practical Conference on Infocommunications: Present and Future, Odessa, Ukraine, in 2015. His research interests include wireless communications and informational security.

YUHONG LIU received the B.S. and M.S. degrees from the Beijing University of Posts and Telecommunications, in 2004 and 2007, respectively, and the Ph.D. degree from the University of Rhode Island, in 2012. She is currently an Assistant Professor with the Department of Computer Engineering, Santa Clara University. With expertise in trustworthy computing and cyber security, her research interests include developing trust models and applying them on emerging applications, such as online social media, cyber-physical systems, and cloud computing. Her work on securing online reputation systems received the Best Paper Award at the IEEE International Conference on Social Computing, in 2010, (acceptance rate = 13%). She was a recipient of the 2013 University of Rhode Island Graduate School Excellence in Doctoral Research Award. She also received the Best Paper Award at the 9th International Conference on Ubi-Media Computing (UMEDIA 2016).

CHENWEI WANG received the B.Eng. degree in information engineering and the M.S. degree in communications and information systems from the Beijing University of Posts and Telecommunications, China, in 2005 and 2008, respectively, and the Ph.D. degree in electrical and computer engineering from the University of California at Irvine, Irvine, USA, in 2012. His industry experience includes intern positions of Research Engineer at Nokia Siemens Networks, Beijing, China, in 2008, and DoCoMo USA Labs, Palo Alto, CA, USA, in 2010. Since 2013, he has been a Research Engineer and then a Senior Research Engineer at DoCoMo Innovations Inc., Palo Alto. His research interests include information theory, wireless communications and networks, machine learning, and data analytics. He was a recipient of the 2017 IEEE GLOBECOM Best Paper Award, the 2016 IEICE Best Tutorial Paper Award, the 2014 IEEE Signal Processing Society Young Author Best Paper Award, and also a recipient of the honor of the IEEE Communications Letters Exemplary Reviewer, in 2011 and 2014.

SUSANTO RAHARDJA (F'11) received the B.Eng. degree from the National University of Singapore, and the M.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, all in electronic engineering.

He is currently a Chair Professor with Northwestern Polytechnical University (NPU) under the Thousand Talent Plan of People's Republic of China. He attended the Stanford Executive Programme at the Graduate School of Business, Stanford University, USA. He has contributed to the development of a series of audio compression technologies, such as Audio Video Standards AVS-L, AVS-2 and ISO/IEC 14496-3:2005/Amd.2:2006, and ISO/IEC 14496-3:2005/Amd.3:2006 in which some have been licensed to several companies. He has more than 15 years of experience in leading research team for media related research that cover areas in signal processing (audio coding and video/image processing), media analysis (text/speech, image, and video), media security (biometrics, computer vision, and surveillance), and sensor networks. He has published more than 300 papers. He holds more than 70 patents worldwide out of which 15 are U.S. patents. His research interests include multimedia, signal processing, wireless communications, discrete transforms, and signal processing algorithms and implementation.

Dr. Rahardja was a recipient of several honors, including the IEE Hartree Premium Award, the Tan Kah Kee Young Inventors' Open Category Gold Award, the Singapore National Technology Award, the A*STAR Most Inspiring Mentor Award, a Finalist of the 2010 World Technology & Summit Award, the Nokia Foundation Visiting Professor Award, and the ACM Recognition of Service Award. He was a Conference Chair of 5th ACM SIGGRAPHASIA, in 2012, and the APSIPA 2nd Summit and Conference, in 2010 and 2018, as well as other conferences in ACM, SPIE, and IEEE. He was an Associate Editor of the IEEE TRANSACTIONS ON AUDIO, SPEECH AND LANGUAGE PROCESSING and the IEEE TRANSACTIONS ON MULTIMEDIA and a Senior Editor of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING. He is currently serving as an Associate Editor for the *Journal of Visual Communication and Image Representation* (Elsevier), the IEEE TRANSACTIONS ON MULTIMEDIA, and the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS.