Matching Theory Based Physical Layer Secure Transmission Strategy for Cognitive Radio Networks

ZHOU TIAN\(^{1,}\) , SHEN YI\(^{1,}\) , PAN ZHIWEN\(^{1,2,3,}\) (Member, IEEE), LIU NAN\(^{2,}\) (Member, IEEE), AND YOU XIAOHU\(^{2,3,}\) (Fellow, IEEE)

\(^{1}\)School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China
\(^{2}\)National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
\(^{3}\)Purple Mountain Laboratories, Nanjing 211100, China

Corresponding author: Pan Zhiwen (pzw@seu.edu.cn)

This work was supported in part by the National Key Research and Development Project under Grant 2018YFB1802402.

ABSTRACT In this paper, a cooperative secure transmission strategy is proposed for cognitive radio networks (CRNs) comprising of multiple primary users (PUs), multiple secondary users (SUs) and malicious eavesdroppers. Specifically, we construct the utility functions for primary users and secondary users that try to achieve the transmission opportunities, and optimization problem aiming at maximizing the aggregated throughput of network is formulated. Then, distributed primary users-secondary users matching algorithm is proposed to solve the optimization problem, and the final cooperative secure transmission strategy is obtained. Simulation results show that our proposed strategy outperforms existing schemes.

INDEX TERMS Cognitive radio networks, cooperative secure transmission, matching theory.

I. INTRODUCTION

Cognitive radio network (CRN), which allows the primary users to share the spectrum with secondary users without impairing the quality of service (QoS) of primary users, is a promising scheme to improve the spectrum utilization efficiency [1].

Information security is a critically important issue in cognitive radio networks (CRNs). Physical layer security, which exploits the intrinsic randomness of wireless channel to enhance the security, is developed, and user cooperation technology is widely recognized as one of the essentials for physical layer security [2]–[6].

However, in CRNs, both primary users (PUs) and secondary users (SUs) are selfish, they are not willing to cooperate with each other actively. To incent cooperation motivation for non-altruistic users, spectrum leasing technique, which allows primary users to abalienate their own spectrum access time or some economic benefits for secondary users’ assistance service, is an effective solution.

Numerous works so far focus on using spectrum leasing technique to enhance physical layer security in CRNs [7]–[16]. A primary privacy preserving scheme with joint information and power transfer is developed in [7], where a single primary user (PU) pair, a single secondary user (SU) pair and a single secondary user (SU) jammer is considered. Wang and Ren [8] propose a secure transmission scheme for the CRN with a single SU pair equipped with multiple antennas. References [9]–[12] investigate secure communication issue for CRNs where the selection of helpers and resource-allocation problems are simultaneously studied. All these existing works [7]–[12], however, deal with network with a single PU pair, and cannot be directly extended to more practical scenario with multiple primary users. In contrast to the single PU pair scenarios considered in aforementioned literatures, the CRNs with multiple PU pairs and multiple jammers are investigated in [13]–[16]. In [13], [14], the authors investigate the problem of helper assignment and resource allocation issues for a CRN based on auction theory. Their auction-theory based algorithm has some nice economic properties, but is not efficient, which means many PUs cannot obtain help from SUs. In [15], a scheme for trustworthy friendly jammer selection is designed for a centralized cooperative cognitive radio network. Authors in [16] study the problem of physical layer security in an unmanned aerial vehicle (UAV) enabled cognitive radio network.
However, [15] and [16] adopt complex centralized methods, which are not suitable for the scenarios with a large number of users.

To address the above-mentioned issues, matching theory based distributed scheme for the CRN with multiple heterogeneous users is advantageous. Some distributed and flexible methods based on matching theory are proposed to address the joint optimization issues of jammer selection and resource allocation for physical layer security [17]–[20]. They prove that by utilizing matching theory, network users can make independent and rational strategic decisions, high-efficiency and low-complexity algorithms can be developed to model collaboration among many users. However, to the best of our knowledge, there is no literature on distributed matching mechanism to address the secure communication issue in CRNs with multiple non-altruistic PUs, SUs, and eavesdroppers.

Thus, in this article, a distributed matching algorithm is proposed to facilitate secure data transmission for multiple PU-base station (BS) links from malicious eavesdroppers through the assistance of multiple SUs. Under this framework, the primary users and secondary users are assumed to be selfish entities, who only pay attention to their own interests. To improve secrecy rates, primary users are willing to provide a certain amount of spectrum access time to secondary users in exchange for secure communication. We construct utility functions for primary users and secondary users based on secrecy rate and transmission rate respectively and maximize the sum of utilities of all PUs and SUs, and eavesdroppers.

Thus, in this article, a distributed matching algorithm is proposed to facilitate secure data transmission for multiple PU-base station (BS) links from malicious eavesdroppers through the assistance of multiple SUs. Under this framework, the primary users and secondary users are assumed to be selfish entities, who only pay attention to their own interests. To improve secrecy rates, primary users are willing to provide a certain amount of spectrum access time to secondary users in exchange for secure communication. We construct utility functions for primary users and secondary users based on secrecy rate and transmission rate respectively and maximize the sum of utilities of all PUs and SUs, and eavesdroppers.

The rest of the paper is organized as follows. System model is presented in section II. Section III introduces the proposed optimization problem formulation. Subsequently, we present a distributed algorithm to solve this problem in sections IV. Numerical results are provided in section V, followed by conclusions in section VI.
Cooperative jamming. As shown in Fig. 3, SU provides cooperative jamming assistance to confuse eavesdroppers during the assisting part. Meanwhile, PU is transmitting information to BS simultaneously (interference caused by SU also affects BS).

In our model, PU\(m\) would not like to share the spectrum to SU\(n\) unless its minimum secrecy rate requirement \(R_{mn}^{\text{min}}\) can be satisfied by SU\(n\)’s assistance, and SU\(n\) is willing to help PU\(m\) only when it can obtain a transmission opportunity which can satisfy its minimum transmission rate requirement \(R_{n}^{\text{min}}\).

Assume Rayleigh fading channels are for all the users including the eavesdroppers, and the channel-state information (CSI) remains constant within a coherent slot within some time. Moreover, the CSI of all the users is available (including eavesdropper’s CSI). The channel coefficient from PU\(m\) to BS is denoted by \(h_{m,b}\). Similarly, we have \(h_{m,k}, h_{m,n}, h_{n,b}, h_{n,k}\) and \(h_{n,D_{n}}\). The channel coefficient is assumed to follow the complex zero mean Gaussian distribution.

When overheard by multiple eavesdroppers simultaneously and no assistance from SUs, PU\(m\) can achieve the following the secrecy rate

\[
y_{m}^{D} = \left[ \log_{2} \left( 1 + \frac{P_{m} |h_{m,b}|^2}{\sigma^2} \right) - \log_{2} \left( 1 + \max_{k \in E} \left( \frac{P_{m} |h_{m,k}|^2}{\sigma^2} \right) \right) \right]^{+} (1)
\]

which denotes the secrecy rate for PU\(m\) by direct transmission, where \([x]^+ = \max\{0, x\}\), \(P_{m}\) denotes the transmit power of PU\(m\), and \(\sigma^2\) is the variance of additive white Gaussian noise (AWGN).

The primary secrecy rate of PU\(m\) with SU\(n\)’s cooperative relaying, \(y_{m}^{C}(n)\), can be expressed as

\[
y_{m}^{C}(n) = (1 - \alpha_{m,n}) \cdot \left[ R_{m,b}^{C} (n) - \max_{k \in E} \left( R_{m,k}^{C} (n) \right) \right]^{+} (2)
\]

where \(1 - \alpha_{m,n}\) fraction is for the assisting phase, and \(R_{m,b}^{C} (n)\) and \(R_{m,k}^{C} (n)\) are the expected rate of PU-BS channel and that of PU-eavesdropper channel by involving SU\(n\)’s cooperative transmission, respectively. Under AF protocol, according to [21], \(R_{m,b}^{C} (n)\) and \(R_{m,k}^{C} (n)\) can be expressed as:

\[
R_{m,b}^{C} (n) = \frac{1}{2} \log_{2} \left( 1 + \frac{P_{m} |h_{m,b}|^2}{\sigma^2} + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} \right) (3)
\]

\[
R_{m,k}^{C} (n) = \frac{1}{2} \log_{2} \left( 1 + \frac{P_{m} |h_{m,k}|^2}{\sigma^2} + \frac{P_{n} |h_{n,k}|^2}{\sigma^2} + \frac{P_{n} |h_{n,k}|^2}{\sigma^2} \right) (4)
\]

where \(P_{n}\) denotes the transmit power of SU\(n\), primary secrecy rate for PU\(m\) with SU\(n\)’s cooperative jamming, \(y_{m}^{J}(n)\), is

\[
y_{m}^{J}(n) = (1 - \alpha_{m,n}) \cdot \left[ R_{m,b}^{J} (n) - \max_{k \in E} \left( R_{m,k}^{J} (n) \right) \right]^{+} (5)
\]

where \(R_{m,b}^{J} (n)\) and \(R_{m,k}^{J} (n)\) are the expected rate of PU-BS channel and that of PU-eavesdropper channel by involving SU\(n\)’s cooperative jamming, respectively:

\[
R_{m,b}^{J} (n) = \log_{2} \left( 1 + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} \right) (6)
\]

\[
R_{m,k}^{J} (n) = \log_{2} \left( 1 + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} \right) (7)
\]

Transmission rate of SU\(n\) in the rewarding part, \(R_{n}(m)\), is

\[
R_{n}(m) = \alpha_{m,n} \cdot \log_{2} \left( 1 + \frac{P_{n} |h_{n,b}|^2}{\sigma^2} \right) (8)
\]

To measure the interests of primary users and secondary users, we construct the utility functions based on the defined secrecy rate with cooperation and corresponding transmission rate.

The utility function for secondary user SU\(n\) while providing friendly assistance for primary user PU\(m\) is defined as

\[
u_{m,n}^{SU} (\alpha_{m,n}) = R_{n}(m) (9)
\]

For primary user PU\(m\) with the assistance of secondary user SU\(n\), the utility function denoted by \(U_{m,n}^{PU} (\alpha_{m,n})\) is given by

\[
u_{m,n}^{PU} (\alpha_{m,n}) = max \{ y_{m}^{C} (n) , y_{m}^{J} (n) \} (10)
\]

II. PROBLEM FORMULATION

In this section, a matching function is defined to indicate the matching state of users, and the optimization problem we aim to address is obtained.

Specifically, the matching state represents whether a user has formed a cooperative relationship with any other user. Based on the matching states of all users and the corresponding utility functions, the optimization problem that tries to maximize sum utility of the overall network is formulated.

A. MATCHING FUNCTION DEFINITION

To facilitate the establishment of the optimization problem, it is helpful to give some definitions.

A matching function is first defined as follows:

\[
\Phi : \{ \text{PU}_{m} : m \in \mathcal{P} \cup \{0\} \} \bigcup \{ \text{SU}_{n} : n \in \mathcal{S} \cup \{0\} \} \rightarrow \{ \text{PU}_{m} : m \in \mathcal{P} \cup \{0\} \} \bigcup \{ \text{SU}_{n} : n \in \mathcal{S} \cup \{0\} \} (11)
\]

For all PU\(m\), \(m \in \mathcal{P}\) and \(SU_{n}, n \in \mathcal{S}\):

\[
\Phi (\text{PU}_{m}) = \text{SU}_{0} \Rightarrow P_{0} = 0, \alpha_{m,0} = 0 \quad (12)
\]

\[
\Phi (\text{SU}_{n}) = \text{PU}_{0} \Rightarrow P_{0} = 0, \alpha_{n,0} = 0 \quad (13)
\]

\[
\Phi (\text{PU}_{m}) \in \{ \text{SU}_{n} : n \in \mathcal{S} \cup \{0\} \} \quad (14)
\]
Note that there is a virtual primary user and a virtual secondary user in this matching function. Any primary user matching with the virtual secondary user with zero power and zero \( \alpha \) represents that no secondary user will cooperate with this primary user. Then it follows that the utility for this primary user is equal to its secrecy rate by direct transmission. This corresponds to item (12) of the proposed definition.

If one secondary user is matched with the virtual primary user with zero power zero \( \alpha \), it does not provide assistance service for any primary user, then it follows that the utility for this secondary user is zero. This corresponds to item (13) of proposed definition.

The item (14) and (15) indicate that one primary user is matched to one single secondary user or the virtual secondary user and one secondary user is matched to one single primary user or the virtual primary user, respectively. And item (16) suggests that \( PU_m \) is matched to \( SU_n \) with \( \alpha_{m,n} \) and meanwhile \( SU_n \) is matched to \( PU_m \) with \( \delta_{m,n} \). Moreover, only the virtual primary user and virtual secondary user can be matched with multiple users.

According to established matching function, the matching identifier \( \lambda_{m,n} \) is defined as follows:

\[
\lambda_{m,n} = \begin{cases} 
1, & \text{if } \Phi(SU_n) = (PU_m, \alpha_{m,n}) \text{ for } m \in \mathcal{P}, n \in \mathcal{S} \\
1, & \text{if } \Phi(SU_n) = (PU_m, \alpha_{m,n}) \text{ for } m = 0, n \in \mathcal{S} \\
1, & \text{if } \Phi(PU_m) = (SU_n, \alpha_{m,n}) \text{ for } m \in \mathcal{P}, n = 0 \\
0, & \text{otherwise.}
\end{cases}
\]  

(17)

**B. OBJECTIVE AND OPTIMIZATION PROBLEM**

The objective is to maximize the security performance of the network and allocate enough spectrum access time to secondary users for their own transmission.

Social welfare of the network is defined as the utilities of all primary users and secondary users

\[
SW = \sum_{m \in \mathcal{P} \cup \{0\}} \sum_{n \in \mathcal{S} \cup \{0\}} \lambda_{m,n} \left[ U_{m,n}^{PU}(\alpha_{m,n}) + U_{m,n}^{SU}(\alpha_{m,n}) \right]
\]  

(18)

Then, the optimization problem is

\[
\max \sum_{m \in \mathcal{P} \cup \{0\}} \sum_{n \in \mathcal{S} \cup \{0\}} \lambda_{m,n} \left[ U_{m,n}^{PU}(\alpha_{m,n}) + U_{m,n}^{SU}(\alpha_{m,n}) \right]
\]

s.t. \( 1 \geq \alpha_{m,n} \geq 0, \forall m \in \mathcal{P}, \forall n \in \mathcal{S} \) 

(20)

\( \sum_{n \in \mathcal{S}} \lambda_{m,n} \leq 1, \forall m \in \mathcal{P} \) 

(21)

\( \sum_{m \in \mathcal{P}} \lambda_{m,n} \leq 1, \forall n \in \mathcal{S} \) 

(22)

Specifically, constraint (20) guarantees that each \( \alpha_{m,n} \) is between 0 and 1, constraint (21) means that one primary user will be matched with only one secondary user, while constraint (22) implies that each secondary user can be matched with only one primary user.

**III. PROPOSED DISTRIBUTED ALGORITHM**

Since above optimization problem is NP-hard, distributed primary users-secondary users matching algorithm bargaining \( \alpha \) between primary users and secondary users is proposed.

In general, all the secondary users keep broadcasting the acceptable \( \alpha \) for providing assistance service, and each primary user will determine whether to send a request for assistance to secondary users based on every \( \alpha \) from secondary users. Then secondary users will decide whether to change their current match and adjust the acceptable \( \alpha \) according to the amount of requests received. This algorithm will last until no primary users send a request.

The details of the algorithm are illustrated in Algorithm 1. Specifically, The DPSMA includes an initialization stage in step 1, followed by several rounds of iteration. Moreover, a requester set \( W \) is defined to record whether no primary user sends a request.

**Step 1-(Initialization):** Each secondary user \( SU_n, n \in \mathcal{S} \) calculates its acceptable \( \alpha_{m,n}^f \) to serve primary user \( PU_m, \forall m \in \mathcal{P} \) in the iteration \( t (t = 1) \).

**Step 2-(PUs Demand for SUs):** Each secondary user \( SU_n, n \in \mathcal{S} \) announces its corresponding acceptable \( \alpha_{m,n}^f \) to all the primary users, which form a set \( \alpha_n^f = \{ \alpha_{m,n}^f | \forall m \in \mathcal{P} \} \). Then, each unmatched primary user \( PU_m, \forall m \in \mathcal{P} \) determines the best match set \( \Omega_m(b_m) \), which is denoted by

\[
\Omega_m(b_m) = \begin{cases} 
\arg \max_{n \in \mathcal{S}} U_{m,n}^{PU}(\alpha_{m,n}^f), & \text{if } U_{m,n}^{PU}(\alpha_{m,n}^f) \\
\geq U_{m,n}^{PU}(\alpha_{m,n}^f) \text{ and } U_{m,n}^{SU}(\alpha_{m,n}) \\
0, & \text{otherwise}
\end{cases}
\]  

(23)

where \( b_m^f = \{ \alpha_{m,n}^f | \forall n \in \mathcal{S} \} \). The best match set for \( PU_m \) contains the indices of secondary users who can provide the maximum utility. If the best match set is not empty, the primary user will send a request for assistance to the random one secondary user whose index is in the best match set. Denote the request from \( PU_m \) to \( SU_n \) by \( g_{m,n}^f \),

\[
g_{m,n}^f = \begin{cases} 
1, & \text{if } PU_m \text{ sends a request to } SU_n \\
0, & \text{otherwise}
\end{cases}
\]  

(24)

**Step 3-(SUs Decision Making):** Based on the amount of received requests from primary users, each secondary user \( SU_n, n \in \mathcal{S} \) decides to change its match and obtains its acceptable \( \alpha \) in the iteration \( t + 1 \).

(Step 3-1) If the secondary user is not matched and receives no requests from primary users after increasing its acceptable \( \alpha \), the secondary user will match with the random one who sends a request to it in the iteration \( t - 1 \).
TABLE 1. Simulation parameters.

| Parameter                  | Value |
|----------------------------|-------|
| Power of PUs               | 1 W   |
| Power of SUs               | 1 W   |
| Noise power                | 1 mW  |
| Length of one slot         | 1 s   |
| Bandwidth for all channels | 1 MHz |
| Path-loss exponent         | 2     |
| Fixed length \(r\)         | 0.2   |

(Step 3-2) If the secondary user receives multiple requests from primary users, the secondary user will increase its acceptable \(\alpha\) with the fixed length \(r\) in iteration \(t+1\) and match with the virtual primary user.

(Step 3-3) If the secondary user receives a request from only one primary user and is not matched, the secondary user will match with this primary user. If the secondary user receives a request from only one primary user and is matched with any other primary user, the secondary user will match with the virtual primary user.

Step 4-(End of the Algorithm): If no primary user sends a request, the algorithm will end. Otherwise, the algorithm will go back to step 2 and enter the iteration \(t+1\).

The above DPSMA provides a distributed algorithm for iteratively solving our formulated optimization problem.

An exact analysis of overhead and complexity is difficult, due to the dependency on a number of system parameters, such as secondary users’ minimum acceptable \(\alpha\), the fixed length \(r\) and the number of primary users and secondary users. We can however, find an expression for the upper bound on the maximum signaling overhead.

**Theorem 1:** The signaling overhead of the DPSMA is upper bounded by \(C_{\text{max}} = c \times N_{\text{max}}\), where \(c\) is the signaling overhead for any user sending a request or reply to another user, \(N_{\text{max}}\) is the maximum sum of requests and replies from all users, and

\[
N_{\text{max}} = \frac{N + F + N M}{r} \max_{m \in S} \left(\alpha_n^{\text{MAX}} - \alpha_n^{\text{min}}\right)
\]

where \(\alpha_n^{\text{MAX}} = \max \left(\alpha_{m,n} | U_{m,n}\right)\), \(F = \min \{N, M\}\) and \(\alpha_n^{\text{min}} = \min \alpha_n^{j,k}\).

**Proof:** See Appendix A.

**Theorem 2:** The complexity of the proposed algorithm is \(O(N + F + NM)\).

**Proof:** See Appendix B.

IV. SIMULATION RESULTS

In this section, we show the performance of the proposed distributed primary users-secondary users matching algorithm through numerical simulations. In particular, we model the cognitive radio network as a square region \([100m \times 100m]\). The base station is located in the center of the area at \([50m, 50m]\), and 4 eavesdroppers locate at \([0m, 0m]\), \([0m, 100m]\), \([100m, 0m]\), \([100m, 100m]\), respectively. Other simulation parameters are listed in Table 1.

We assume that the number of PUs is 20, and PUs’ minimum secrecy rate requirements \(\eta_{m}^{\text{min}}\) are randomly and uniformly distributed within \([0, \eta_{m}^{\text{MAX}}]\), and SUs’ minimum transmission rate requirements are randomly and uniformly distributed within \([0, \max R]\). \(\eta_{m}^{\text{MAX}} = \max R = 0.2\).

Aggregated throughput of the network and the channel utilization ratio are employed as performance metrics. The aggregated throughput contains the secrecy rates of all the
PUs who can attain their minimum secrecy rate requirements and the transmission rates of all the SUs who obtain the transmission time. Channel utilization ratio $k$ is defined as

$$k = \frac{m_{PU_{satisfied}}}{M_{PU_{all}}}$$

where $m_{PU_{satisfied}}$ is the number of primary users whose minimum secrecy rate requirement can be satisfied and $M_{PU_{all}}$ is the number of all primary users in the network.

**A. SIMULATIONS IN CRNs WITH ONE-TIME PAIRING**

First, we show the performance of DPSMA in CRNs with one-time pairing. For a CRN, multiple PUs and SU pairs are randomly distributed in the considered area. The proposed DPSMA is compared with four schemes, i.e., baseline scheme, the DASI in [14], and two kinds of maximum weighted matching (MWM) schemes based on [22].

- For baseline scheme, PUs execute secure transmission directly if their minimum secrecy rate requirements could be satisfied without the assistance of secondary users.
- For DASI, in order to compare with our proposed DPSMA, we set the maximum transmitting energy per slot for all SUs be equal to the transmitting power of our proposed DPSMA.
- MWM schemes include MWM-PU scheme and MWM-SU scheme. In MWM-PU scheme, we set all secondary users participate in the matching according to their minimum required rates. Correspondingly, the secrecy rates that they can provide for primary users through cooperation will reach the maximum. Thus, the maximum matching such that sum of all primary users’ secrecy rates is maximum can be found. In MWM-SU scheme, we set all primary users participate in the matching according to their minimum required secrecy rates. Correspondingly, the rates that they can provide for secondary users through cooperation will reach the maximum. Thus, the maximum matching such that sum of all secondary users’ rates is maximum can be found. Generally, these two schemes focus on maximizing the interests of primary users and the interests of secondary users, respectively.

Fig. 4 and Fig. 5 show the aggregated throughput of the network and the channel utilization ratio versus the power of secondary users of our proposed DPSMA, DASI, MWM schemes and the baseline scheme, respectively.

In Fig. 4 and Fig. 5, on one hand we can observe that DPSMA outperforms DASI, MWM-PU scheme, and the baseline scheme since the baseline scheme does not consider cooperation between primary users and secondary users. Although DASI and MWM-PU scheme employs multiuser cooperation techniques, DASI sacrifices too many pairs that should be winners, and MWM-PU scheme only consider maximizing the interests of primary users. However, on the premise of protecting the interests of all users, our proposed strategy allows users to freely negotiate and pair with each other in a distributed way. Then, compared with DASI and MWM-PU scheme, more primary users and secondary users can be matched together reasonably, leading to a significant increase in aggregated throughput and channel utilization ratio. Then, our proposed strategy always achieves better performance than these three schemes.

On the other hand, we can observe that DPSMA suffers degradations over MWM-SU scheme for the aggregated throughput. The reason of the degradation is that to maintain rationality of our proposed scheme, DPSMA always focuses on the interests of all users.

In Fig. 6 and Fig. 7, we show the aggregated throughput of the network and the channel utilization ratio versus the number of secondary users of our proposed DPSMA, DASI, MWM schemes and the baseline scheme, respectively. For all schemes except the baseline scheme, it is obvious that the throughput and channel utilization ratio increase as the...
number of SUs increases, for the reason that high density of SU leads to the high probability of PU-SU matching success. Moreover, due to the reasons similar to those in Fig. 4 and Fig. 5, we can see that DPSMA significantly improves the system performance comparing with DASI, MWM-PU scheme, and the baseline scheme.

B. SIMULATIONS IN CRNs WITH MULTIPLE-TIME PAIRING

Next, we show the performance of DPSMA with multiple-time pairing in a CRN as considered in [14], which is a CRN with discrete time duration \([0, T] = \{0, 1, \ldots, t, \ldots, T\}\) that consists of multiple time slots. Primary users join in the network at the beginning and remain in the network until the end during which they aim to perform secure transmission. For secondary users, they join and leave the network in a stochastic way, and all secondary users are patient for its traffic requirement, i.e., it is satisfied to transmit at any time slot when its remaining time is enough. In this part, we consider the short-term spectrum rental scenario, where the secondary users intend to obtain the channel usage for one time slot.

We assume that 500 secondary users join the network, and the secondary users arrive in the network following Poisson process, with probability density function \(f(x) = \lambda e^{-\lambda x}\), where \(\lambda > 0\) denotes the arrival intensity of secondary users per time slot. The arrival intensity varies from 100 to 5 i.e., secondary users’ interarrival time \((1/\lambda)\) varies from 0.01 to 0.2. The simulation continues until all 500 secondary users have joined the network. In addition to the baseline scheme and MWM schemes, we compare DPSMA with an ideal dynamic auction scheme called d-DASI in [14]. In this ideal scheme, all the arriving secondary users join the auction directly and remain in the auction until their departure time. Furthermore, the time length of each secondary user remains in the network is randomly distributed within \([0, \delta]\), where \(\delta\) is the maximum waiting time length and we set \(\delta = 8\). Both the arrival time and the time length they remain in the network are rounded to the nearest integral.

Fig. 8 and Fig. 9 show the average aggregated throughput and average channel utilization ratio versus the secondary users’ interarrival time, respectively. It is obvious that both the channel utilization ratio and aggregated throughput decrease when the interarrival time increases, since small arrival intensity leads to the low density of secondary users in the CRN, which results in the small opportunities for cooperation between primary users and secondary users. Furthermore, we can see that DPSMA improves the system performance more significantly in CRNs through multiple-time pairing than one-time pairing. Compared with the other schemes except MWM-SU scheme, since those secondary users remain in the network are more likely to be matched
reasonably by DPSMA, which can provide good match result with higher probability.

V. CONCLUSION
In this paper, a matching theory based distributed algorithm is proposed to address the secure communication issue in CRNs containing multiple PUs, SUs and eavesdroppers. Utility functions for both primary users and secondary users is defined. Then, the network throughput maximization problem is formulated and solved by proposed DPSMA. Simulation results show the performance gain of the proposed scheme.

APPENDIX A
PROOF OF THEOREM 1
Following the DPSMA, the primary users and secondary users communicate with each other as follows: in DPSMA-Step 2-(1) all the secondary users announce their acceptable \( \alpha \) to all the primary users, and thus there are \( \alpha \) requests. Note that in the first iteration of the DPSMA, the secondary users will achieve their minimum acceptable \( \alpha_{\text{min}} \) requests, \( n \in S \) to the primary users.

After receiving the secondary users’ acceptable \( \alpha \) in DPSMA-Step 2-(3), in the worst case scenario, all the primary users will send a request to the secondary users and thus there are \( N \) requests at most. In DPSMA-Step 3-(1)-1), some secondary users will accept the bids and thus there are \( F \) replies at most. In DPSMA-Step 3-(1)-2), some primary users will cancel their requests, and thus there are \( N \) replies at most. The proof thus follows by noting that the maximum sum of requests and replies from all users at each iteration is \( N + F + NM \).

And from DPSMA-Step 3-(2), \( SU_n, n \in S \) will increase its acceptable \( \alpha \) if it receives more than one request. The maximum possible acceptable \( \alpha \) that the primary users can send for \( SU_n \) is \( \alpha_{\text{MAX}} \). So if \( SU_n, n \in S \), increases its acceptable \( \alpha \) to \( \alpha_{m,n} = \alpha_{\text{MAX}} + r \), no \( PU_m, m \in P \) will send a request to it. In the worst case scenario, each \( PU_m, m \in P \) will not send any request at most after \( (1/r)(\alpha_{\text{MAX}} - \alpha_{\text{min}}) \) iterations. Thus the maximum number of iterations such that all the primary users will not send any request is \( (1/r)\max_{n \in S}(\alpha_{\text{MAX}} - \alpha_{\text{min}}) \).

APPENDIX B
PROOF OF THEOREM 2
For our proposed algorithm, the proof follows by noting that the complexity is proportional to the total number of times the primary users communicate with the secondary users, given in (25).

REFERENCES
[1] S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.
[2] Y. Chen, T. Zhang, Y. Liu, and X. Qiao, “Physical layer security in NOMA-enabled cognitive radio networks with outdated channel state information,” IEEE Access, vol. 8, pp. 159480–159492, 2020.
[3] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, “Generative adversarial network assisted power allocation for cooperative cognitive covert communication system,” IEEE Commun. Lett., vol. 24, no. 7, pp. 1463–1467, Jul. 2020.
[4] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, “Secure transmission design in HARQ assisted cognitive NOMA networks,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2528–2541, Jan. 2020.
[5] P. Yan, Y. Zou, X. Ding, and J. Zhu, “Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems,” IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5115–5128, May 2020.
[6] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, and J. Wang, “Security-reliability tradeoff analysis for underlay cognitive two-way relay networks,” IEEE Trans. Wireless Commun., vol. 18, no. 12, pp. 6030–6042, Dec. 2019.
[7] D. Wang, F. Zhou, and V. C. M. Leung, “Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks,” IEEE Trans. Cognit. Commun. Netw., vol. 6, no. 2, pp. 683–693, Jun. 2020.
[8] D. Wang and P. Ren, “Energy-efficient primary security provisioning for the full-duplex cognitive radio networks,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1–6.
[9] 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.
[10] F. Aghfah, A. Shamshoohara, L. Nijjla, and C. Kamhoua, “A reputation-based Stackelberg game model to enhance secrecy rate in spectrum leasing to selfish IoT devices,” in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2018, pp. 312–317.
[11] X. Liu, K. Zheng, L. Fu, X. Liu, X. Wang, and G. Dai, “Energy efficiency of secure cognitive radio networks with cooperative spectrum sharing,” IEEE Trans. Mobile Comput., vol. 18, no. 2, pp. 305–318, Feb. 2019.
[12] X. Wang, Y. Ji, H. Zhou, and J. Li, “A nonmonetary QoS-aware auction framework toward secure communications for cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 65, no. 7, pp. 5611–5623, Jul. 2016.
[13] X. Wang, Y. Ji, H. Zhou, and J. Li, “DASI: A truthful double auction mechanism for secure information transfer in cognitive radio networks,” in Proc. 12th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON), Jun. 2015, pp. 19–27.
[14] X. Wang, Y. Ji, H. Zhou, and J. Li, “Auction-based frameworks for secure communications in static and dynamic cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2658–2673, Mar. 2017.
[15] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, “A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 68, no. 4, pp. 3500–3512, Apr. 2019.
[16] N. Tang, H. Tang, B. Li, and X. Yuan, “Cognitive NOMA for UAV-enabled secure communications: Joint 3D trajectory design and power allocation,” IEEE Access, vol. 8, pp. 159968–159978, 2020.
[17] X. Shi, D. Wu, C. Wan, M. Wang, and Y. Zhang, “Trust evaluation and covert communication-based secure content delivery for D2D networks: A hierarchical matching approach,” IEEE Access, vol. 7, pp. 134838–134853, 2019.

[18] 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.

[19] B. Wang, Y. Sun, H. M. Nguyen, and T. Q. Duong, “A novel socially stable matching model for secure relay selection in D2D communications,” IEEE Wireless Commun. Lett., vol. 9, no. 2, pp. 162–165, Feb. 2020.

[20] Y. Wang and L. Wang, “Matching theory-based cooperative secure transmission strategy for social-aware D2D communications,” IEEE Trans. Veh. Technol., vol. 68, no. 8, pp. 8000–8011, Aug. 2019.

[21] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

ZHOU TIAN received the bachelor’s degree in communication engineering from the Nanjing University of Posts And Telecommunications, Nanjing, China, in 2018. He is currently pursuing the master’s degree with Southeast University. His research interests include physical layer security and D2D communications.

SHEN YI received the B.S. degree in telecommunication engineering from Southwest Petroleum University, Chengdu, China, in 2011, and the M.S. degree from the Guilin University of Electronic Technology, Guilin, China, in 2014. He is currently pursuing the Ph.D. degree in cyber science and engineering with Southeast University, Nanjing, China. From September 2014 to December 2016, he was a Lecturer with Tongren University, Tongren, China. His research interests include physical layer security and UAV communications.

PAN ZHIWEN (Member, IEEE) has been an Associate Professor with the National Mobile Communications Research Laboratory, Southeast University, since 2000, where he has been a Professor since 2004. From 2000 to 2001, he was involved in the research and standardization of 3G, and since 2002, he has been involved in the investigations on key technologies for IMT-A and 5G. He has published more than 50 articles recently and holds more than 50 patents. His research interests include self-organizing networks, wireless networking, and radio transmission technology for wireless communications.

LIU NAN (Member, IEEE) received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2001, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 2007. From 2007 to 2008, she was a Postdoctoral Scholar with the Wireless Systems Lab, Department of Electrical Engineering, Stanford University. In 2009, she became a Professor with the National Mobile Communications Research Laboratory, School of Information Science and Engineering, Southeast University, Nanjing, China. Her research interests include network information theory for wireless networks, SON algorithms for next-generation cellular networks, and energy-efficient communications. She is currently an Associate Editor of China Communications.

YOU XIAOHU (Fellow, IEEE) has been with the National Mobile Communications Research Laboratory, Southeast University, since 1990, where he was a Professor and a Chair Professor of the Cheung Kong Scholars Program, and served as the Director for the Laboratory. He has contributed more than 50 IEEE journal articles and two books in the areas of adaptive signal processing, neural networks, and their applications to communication systems, and holds more than 80 patents. His research interests include mobile communication systems, signal processing and its applications, wireless and mobile communication systems, and modern digital signal processing. He was the Premier Foundation Investigator of the China National Science Foundation. From 1999 to 2002, he was a Principal Expert of the C3G Project, responsible for organizing China’s 3G mobile communications research and development activities. From 2001 to 2006, he was a Principal Expert of the National 863 Future Project. Since 2010, he has been the Section Chair of the IEEE Nanjing Section. He served as the General Co-Chair for the 2014 IEEE WCNC.