Secure Communication in OFDMA-Based Cognitive Radio Networks: An Incentivized Secondary Network Coexistence Approach

Mohammad Reza Abedi, Nader Mokari, Mohammad Reza Javan, *Member, IEEE*, and Halim Yanikomeroglu, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a secure cooperative communications scheme for orthogonal frequency-division multiple-access (OFDMA) cognitive radio networks (CRNs), where a primary base station (PBS) wants to transmit information to some distant primary users (PUs) in the presence of a set of passive eavesdroppers. In our model, the transmission is performed in two consecutive time slots; in the first time slot, the PBS transmits while the secondary users (SUs) and the eavesdroppers listen. In the second time slot, the SUs transmit while the PUs, the secondary base station (SBS), and the eavesdroppers listen. We consider two schemes for eavesdropping; in the first scheme, the eavesdroppers listen to transmissions from the PBS to the SUs, and in the second scheme, we assume that the eavesdroppers apply the maximal ratio combining approach on the received signals in the first and second time slots for the primary network. In the proposed model, the SUs are allowed to use the licensed spectrum of the PUs, as long as they help the PUs to satisfy their secrecy rate requirement. We assume a frame-based transmission where each frame is divided into two consecutive time slots of equal duration. In the first time slot, the PBS transmits while the SUs and the eavesdroppers listen. In the second time slot, the selected SUs relay the PBS information to the distant PUs. Meanwhile, the SUs use the remaining resources to transmit their own information to the SBS while the eavesdroppers listen to this transmission. We formulate our proposed schemes as an optimization problem and solve it by dual Lagrange approach. We evaluate our proposed scheme in various situations using simulations and show the efficiency of the proposed scheme. An important aspect of the proposed paradigm is that replacing the conventional average interference threshold constraint by the primary secrecy rate constraint does not only decrease the secondary average secrecy rate with respect to the conventional case but can actually provide significantly higher secondary average secrecy rate as well.**

***Index Terms*—Average secrecy rate, cognitive radio network (CRN), decode-and-forward (DF) relay, eavesdropping, power allocation.**

Manuscript received June 19, 2015; revised February 14, 2016; accepted March 29, 2016. Date of publication April 21, 2016; date of current version February 10, 2017. The review of this paper was coordinated by Prof. H.-H. Chen.

M. R. Abedi and N. Mokari are with the Electrical and Computer Engineering Department, Tarbiat Modares University, Tehran 11365 9363, Iran.

M. R. Javan is with the Department of Electrical Engineering, Shahrood University of Technology, Shahrood 36199 95161, Iran (e-mail: javan@shahroodut.ac.ir).

H. Yanikomeroglu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2016.2555946

I. Introduction

A. Motivations and Related Work

Scarcity of the available spectrum makes its efficient use very desirable. Cognitive radio [1] is an important concept, which improves the efficiency of using the available bandwidth by dynamically exploiting the idle spectrum and adapting its transmission parameters [2], [3].

Cooperative cognitive radio networks (CCRNs) have attracted much attention where secondary users (SUs) are allowed to access the spectrum owned by primary users (PUs) for their cooperation to PUs to enhance PUs' transmission quality [4]–[12]. In [4], a spectrum leasing of a primary network (PN) to an *ad hoc* secondary network (SN) for the help it may receive from the SN is considered. In their scheme, the transmission time is divided into three phases where, in the first two phases, the PN and the SN cooperate to improve the transmission quality of the PN, whereas in the third phase, cooperating SUs are allowed to access the network for their own transmission. In [5], a cooperative scheme is proposed in which SUs help PUs by working as amplify-and-forward (AF) relays. In their scheme, a fraction of subcarriers are allocated for relaying the PU's information, and the remaining are used by the SU for its own transmission as a reward for its cooperation. In [6], a cooperative scheme is considered in which, using spatial multiplexing and beamforming, the secondary base station (SBS) works as a relay to transmit primary base station (PBS) information to the cell-edge users while it transmits its own information to the SUs.

In [7], a cooperative communications scenario is proposed in which the PU leases a portion of its resources both in time and frequency as a reward to cooperating SUs who relay the primary information. They modeled their scheme as a noncooperative game where SUs compete by controlling their transmit power. In [8], a cooperative scenario is considered in which the frequency band is divided into two separate bands. In one band, the SU helps the PU by relaying its information while the other SU uses another band to transmit its information. In [9], a cooperative communication scenario is considered where the SU assigns a fraction of its transmit power budget for the primary transmission to compensate the effect of its induced interference on the PU. The SU then applies superposition coding to eliminate the PU's interference. In [10], a cooperative relay selection scheme for CRNs is proposed. In their scheme, several SUs exist, each of which can be a potential relay for PUs. They considered a slotted transmission where a fraction of time is assigned for cooperation between the PUs and the selected SU and the remaining is assigned to the cooperating SU for its own transmission. In [11], a cooperative scheme is proposed in which the available subcarriers are assigned to the SUs by the PUs for their help to improve the PUs' communications. In their model, the transmission time is divided into two parts where, in the first part, the SUs help the primary system by working as relays, and as a reward, the cooperating SUs gain access to the network resources in the second part for their own transmission. In [12] a full-duplex cooperative communication is proposed in which the SU helps information transmission of the PU to be improved by working as a decode-and-forward (DF) relay and sending the PU's information on some of the available subcarriers. In turn, the cooperating SU gains access to the remaining subcarriers for its own transmission.

As the wireless channel is a broadcast channel, the information transmission over it can be accessed by unauthorized users. Physical layer security [13] can be seen as an effective approach that makes secure communications feasible in numerous ways such as cooperative communications [14], [15] and cooperative jamming [16]. In addition to spectral efficiency, CCRNs can also be seen as an efficient model to improve secure communications [17]–[21]. In [17], a cooperative communications scenario with friendly jamming for secrecy rate improvement is considered. In their model, noncooperative terminals are tempted into cooperation with the legitimate party by producing jamming signal and gain access to the network resources as the reward for their help. They modeled their scheme in a game-theoretic framework. In [18], two schemes are proposed for spectrum access in CRNs. In the first scheme, two SUs help the PU by working as a cooperating relay and a cooperating jammer. As a reward, a fraction of time is allocated to the SUs for their own transmission. In the second scheme, a set of SUs help the PU to improve its secrecy rate via beamforming and, as a reward, gain access to the network for a fraction of time to transmit their own information. In [19], secure communications with an untrusted cognitive radio is considered. An information-theoretic framework to study the situation when this cooperation is beneficial to both PUs and SUs is provided. In [20], a spectrum leasing scheme with the aim to maximize the secrecy rate of the PN while satisfying the data rate requirement of the SN is proposed. In their model, the SU produces interference to the eavesdropper via a well-designed beamformer. In turn, the SN is allowed to use the network resources. In [21], a communications model is considered in which the security of both the PU's and SU's transmissions is taken into account. In their model, the cross interference from the PU on the SU and from the SU to the PU is viewed as helpful in improving their secrecy rate. In [22], the problem of resource allocation in orthogonal frequency-division multiple-access (OFDMA) two-way AF relay networks in the presence of an eavesdropper is considered. The proposed joint resource allocation problem aims to maximize the secrecy capacity for legitimate sources subject to limited power budget and orthogonal subcarrier allocation constraints.

B. Contributions

In this paper, we consider the problem of resource allocation in Long-Term Evolution (LTE) systems, which provides both cognitive radio and relaying scheme capabilities. Cooperative cognitive system can be useful for the following objectives in LTE systems.

1) It can be used to improve the coverage and capacity in mobile radio systems through the extension of existing LTE/LTE-Advanced technologies.
2) It leads to innovative concepts for joint spectrum utilization in multi-operator cellular systems. Moreover, proposed schemes can provide new cognitive services within LTE/LTEAdvanced radio systems.
3) Physical-Layer Secrecy can be used in the LTE System.

We propose a new cooperative communication scheme for CRNs. In our model, we assume that there exists a PN in which the PBS wants to communicate to distant PUs securely in the presence of a set of passive eavesdroppers. In addition, there exists an SN where SUs want to transmit information to an SBS. However, as the PN owns the resources, the SN can gain access to it at the expense of cooperation with the PN. More precisely, the PN makes use of the help from the SUs, which work as DF relays to relay PBS signals to distant PUs. As a reward, the SUs gain access to the resources licensed by the PN, if any remains, for their own transmission. In our scheme, we assume that, in addition to the PN, the SN is also required to securely communicate as the eavesdroppers listen to the information transmission by the SUs.

We assume that the legitimate transmitters, i.e., the PBS and the SUs, know the channel distribution information (CDI) of the legitimate channels, i.e., channels from the PBS to the SUs, from the SUs to the SBS, and from the SUs to the PUs. In addition, in our proposed scheme, instead of the channel state information (CSI) of channels from the PBS to the eavesdroppers and from the SUs to the eavesdroppers, only the CDI of these channels is available. Such an assumption is of practical interest because the eavesdropper is passive and acquiring its CSI is hard. On the other hand, CDI can be obtained simply by estimating the path loss (which includes distance-dependent attenuation and shadowing). In practice, the large-scale channel variations are slow, and their estimations are easier than estimating the fast-fading fluctuations.[1] In this paper, we use the kernel density estimation (KDE) and its robust counterpart [23], [24] as tools to assess the effect of CDI imperfection on the resource-allocation performance. Although our focus in this paper is on the effect of CDI estimation error on the performance of average resource-allocation problems, this work can provide grounds to analyze the effect of imperfect CDI in other applications relying on CDI.

[1]Indeed, it can be assumed that the CDI for the users over a relatively small geographical area follows the same distribution as they locate near each other. This way, channel distributions of legitimate users and those of the eavesdropper can be assumed to be independent and identically distributed (i.i.d.). Hence, by knowing the CDI of legitimate channels, we also get to know that of the eavesdropper. In addition, if the users are distributed within a larger geographical area, we can divide this area into small regions and consider previous assumptions for CDI in each region.

We formulate our proposed schemes as an optimization problem in which the aim is to maximize the average secrecy rate of the SUs while the PN is required to achieve a minimum amount of average secrecy rate and solve it in a similar way to [25]–[27]. We consider two schemes for eavesdropping the primary transmission; in the first scheme, the eavesdroppers listen to the transmissions from the PBS to the SUs, and in the second scheme, we assume that the eavesdroppers apply the maximal ratio combining (MRC) approach on the received signals in the first and second time slots for the PN. In addition, we assume individual average transmit power constraints for the PBS and each SU. We solve the optimization problem using the dual Lagrange approach where we determine which SU should work as a relay, perform subcarrier paring for the first and second hops of relaying transmission, and obtain the average transmit power assigned to the subcarriers by the PBS and the SUs. We finally evaluate the efficiency of our proposed schemes using simulations in various situations. Simulation results show that, compared with the exhaustive search method, the proposed strategy can achieve almost optimal performance. In addition, simulation results indicate that, in terms of the secondary average secrecy rate, the proposed setup outperforms the conventional setup where the average interference temperature constraint is used. An important aspect of the proposed paradigm is that the proposed setup does not only decrease the secondary average secrecy rate with respect to the conventional case but can also provide significantly higher secondary average secrecy rate. As a case study, the proposed system model can be applied in an LTE-based model. LTE is an emerging technology provided by the Third-Generation Partnership Project (3GPP) in which new features such as relaying scheme and cognitive radio have been considered for the future of this generation system.

A summary of comparisons of our scheme with other existing schemes is listed as follows.

- In this paper, we propose a new secure cooperative communication scheme for CRNs that provides both cognitive radio and relaying scheme capabilities.
- Unlike the existing studies that require both CSI and CDI, in our proposed scheme, instead of the CSI of channels from the PBS to the eavesdroppers and from the SUs to the eavesdroppers, only the CDI of these channels is required.
- To the best our knowledge, there is no work that investigates CDI imperfection on the resource allocation in secure cooperative communications. To do this, we use the KDE and its robust counterpart as tools to assess the effect of CDI imperfection on the resource-allocation performance.

This paper is organized as follows. In Section II, we introduce our system model and formulate the resource-allocation problem. We solve our optimization problem in Section III. The effect of CDI imperfection on the proposed schemes is studied in Section IV, and practical issues of our scheme are given in Section V. Simulation results are presented in Section VII, and conclusions are given in Section VIII.

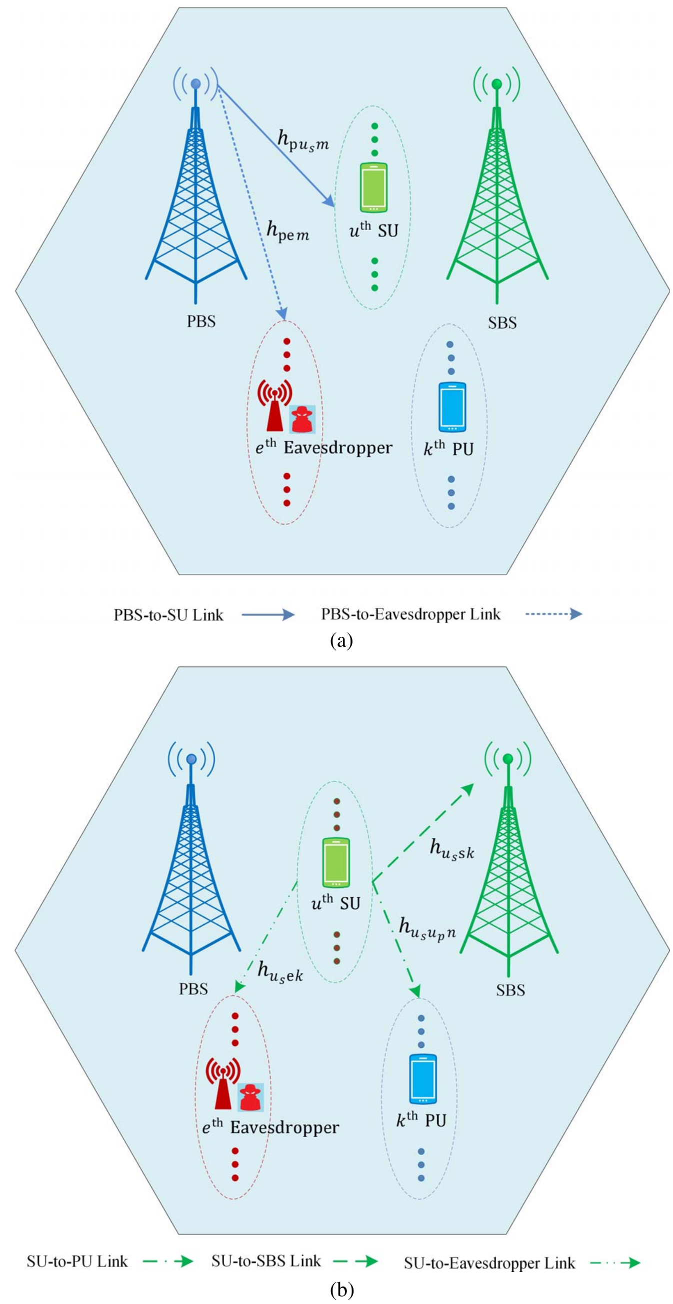


Fig. 1. System model. (a) First hop. (b) Second hop.

II. System Model and Problem Formulation

A. System Model

We consider a CRN in which there exists one OFDMA PN and one OFDMA SN, as shown in Fig. 1. We assume that there exists a set of malicious users in the network, each of which eavesdrops the information transmission in the network independently, i.e., they do not cooperate to use their signals to improve their eavesdropping rate. We denote the set of PUs by $\mathcal{U}_p = \{1, \ldots, U_p\}$, where U_p is the number of PUs; that of SUs by $\mathcal{U}_{\acute{s}} = \{1, \ldots, U_{\acute{s}}\}$, where $U_{\acute{s}}$ is the number of SUs; that of subcarriers by $\mathcal{N} = \{1, \ldots, N\}$, where N is the number of subcarriers in the network; and that of eavesdroppers by

$\mathcal{E} = \{1, \ldots, E\}$, where E is the number of eavesdroppers.[2] The SUs are divided into two sets: one set denoted by $\mathcal{U}_{\rm cs} = \{1, \ldots, U_{\rm cs}\}$, which includes cooperating secondary users (CSUs), which are selected to assist the PBS, and the remaining SUs, which transmit their own information, i.e., $\mathcal{U}_s = \mathcal{U}_{\acute{s}} / \mathcal{U}_{\rm cs}$. We assume that the operation of both networks is governed and controlled by a central network controller (CNC), which has full knowledge of the network parameters of the legitimate receivers, e.g., CSI of the legitimate receivers. It is assumed that the CSI of the eavesdroppers is not available at the CNC. In addition, we assume that the CNC allocates the subcarriers orthogonally, i.e., there exists no intracell interference and cross interference between the PN and the SN. Moreover, we assume that all nodes, i.e., users, BSs, and eavesdroppers, are equipped with a single antenna and perform half-duplex communications. The SN has access to the bandwidth owned by the PN at the expense of helping the PN to satisfy its average secrecy rate constraint. This is done by CSUs working as DF relays for the PBS. We assume that the PUs are far from the PBS such that the PBS can only transmit information to them with the help of CSUs, i.e., no direct transmission can be performed. Therefore, the available resources to the SN, which are the average transmit power of the SUs and N subcarriers, are divided into two groups: one group dedicated by the SN to help the PN and the remaining resources, if any, which can be used by the SN for its own transmission. We assume a frame-based transmission protocol in which the time duration of each frame, i.e., T, is divided into two consecutive time slots of equal duration. In the first time slot, the PBS transmits information while the SUs and the eavesdroppers listen. In the second time slot, the selected SUs work as DF relays for the PBS, i.e., they decode the received information from the PBS in the first time slot, re-encode it, and transmit the information to the PUs in the second time slot. We call these subcarriers the secondary subcarriers used for PBS. If there remains any other subcarrier, SUs at the same time in the second time slot transmit their own information to the SBS. We call these subcarriers the secondary subcarriers used by SBS. We assume that, in the second time slot, the eavesdroppers listen to information transmission of SUs on these subcarriers. We use the notation subcarrier pair (SP) (m, n) to denote that subcarrier m is used in the first time slot by the PN and subcarrier n is used in the second time slot by the SN for primary transmission.

B. Problem Formulation

Let us define the normalized channel (power) gains $g^m_{b_p u_{\rm cs}} = |h^m_{b_p u_{\rm cs}}|^2 / (\delta^m_{u_s})^2$, $g^n_{u_{\rm cs} u_p} = |h^n_{u_{\rm cs} u_p}|^2 / (\delta^n_{u_p})^2$, $g^k_{u_s b_s} = |h^k_{u_s b_s}|^2 / (\delta^k_{b_s})^2$, $g^m_{b_p e} = |h^m_{b_p e}|^2 / (\delta^m_e)^2$, and $g^k_{u_s e} = |h^k_{u_s e}|^2 / (\delta^k_e)^2$, where $h^m_{b_p u_{\rm cs}}$, $h^n_{u_{\rm cs} u_p}$, $h^k_{u_s b_s}$, $h^m_{b_p e}$, and $h^k_{u_s e}$ denote the channel coefficients between the PBS and CSU $u_{\rm cs}$ over subcarrier m, between CSU $u_{\rm cs}$ and PU u_p over subcarrier n, between SU u_s and the SBS over subcarrier k, between the PBS and eavesdropper e over subcarrier m, and between SU u_s and eavesdropper e over subcarrier k, respectively. In addition, $(\delta^m_{u_{\rm cs}})^2$, $(\delta^n_{u_p})^2$, $(\delta^k_{b_s})^2$, and $(\delta^m_e)^2$ are the power of the additive white Gaussian noise at $u_{\rm cs}$, u_p, b_s, and eavesdropper e, respectively. Let $p^m_{b_p u_{\rm cs}}$, $p^n_{u_{\rm cs} u_p}$, and $p^k_{u_s b_s}$ denote the transmit power level assigned by the PBS on subcarrier m to CSU $u_{\rm cs}$ in the first time slot, the transmit power level assigned by CSU $u_{\rm cs}$ to PU u_p on subcarrier n in the second slot, and the transmit power level assigned by SU u_s for its transmission to the SBS on subcarrier k in the second time slot, respectively. Suppose that the PBS wants to transmit some information to PU u_p using SP (m, n) with the help of SU u_s.

The instantaneous transmission rate between the PBS and CSU $u_{\rm cs}$ over subcarrier m in the first time slot is given by

$$R^m_{b_p u_{\rm cs}} = \frac{1}{2} \log \left(1 + g^m_{b_p u_{\rm cs}} p^m_{b_p u_{\rm cs}} \right), \tag{1}$$

and the rate between CSU $u_{\rm cs}$ and PU u_p over subcarrier n in the second time slot is given by

$$R^n_{u_{\rm cs} u_p} = \frac{1}{2} \log \left(1 + g^n_{u_{\rm cs} u_p} p^n_{u_{\rm cs} u_p} \right). \tag{2}$$

Therefore, the transmission rate with which the PBS can send information to PU u_p with the help of CSU $u_{\rm cs}$ over SP (m, n) is given by

$$R^{mn}_{u_{\rm cs} u_p} = \min \left(R^m_{b_p u_{\rm cs}}, R^n_{u_{\rm cs} u_p} \right). \tag{3}$$

In addition, the rate between SU u_s and the SBS over subcarrier k in the second time slot is given by

$$R^k_{u_s b_s} = \frac{1}{2} \log \left(1 + g^k_{u_s b_s} p^k_{u_s b_s} \right). \tag{4}$$

On the other hand, the instantaneous rate at which eavesdropper e receives the information from the PBS in the first time slot over subcarrier m is given by

$$R^m_{b_p e} = \frac{1}{2} \log \left(1 + g^m_{b_p e} p^m_{b_p u_s} \right), \tag{5}$$

and the rate at which eavesdropper e receives information from SU u_s in the second slot over subcarrier k is given by

$$R^k_{u_s e} = \frac{1}{2} \log \left(1 + g^k_{u_s e} p^k_{u_s b_s} \right). \tag{6}$$

We assume that the eavesdroppers listen to the transmission of the PBS to the PU only in the first time slot and listens to the transmission of the SU to the SBS in the second time slot. Therefore, the secrecy rate that is achievable by the PBS in the transmission to PU u_p through CSU $u_{\rm cs}$ using SP (m, n) is given by [28]

$$\begin{aligned} S^{mn}_{u_{\rm cs} u_p} &= \min_{e \in \mathcal{E}} \left[R^{mn}_{u_{\rm cs} u_p} - R^m_{b_p e} \right]^+ \\ &= \left[\min \left(R^m_{b_p u_{\rm cs}}, R^n_{u_{\rm cs} u_p} \right) - \max_{e \in \mathcal{E}} \left(R^m_{b_p e} \right) \right]^+, \end{aligned} \tag{7}$$

[2]In some cases, the eavesdroppers are a certain number of the network's users, and thus, we know the number of eavesdroppers.

and the secrecy rate of SU u_s in the transmission to the SBS over subcarrier k in the second time slot is given by

$$S^k_{u_s b_s} = \min_{e\in\mathcal{E}} \left[R^k_{u_s b_s} - R^k_{u_s e}\right]^+ = \left[R^k_{u_s b_s} - \max_{e\in\mathcal{E}}(R^k_{u_s e})\right]^+. \quad (8)$$

We can assume that the eavesdroppers apply the MRC approach on the received signals in the first and second time slots for each PU. Consider the communication between the PBS and PU u_p through CSU $u_{\rm cs}$ over SP (m,n). Suppose that eavesdropper e uses the MRC scheme to combine the signals it receives in the first and second time slots. Therefore, the signal-to-noise ratio at eavesdropper e is given by

$$\gamma^{mn}_{e,c} = p^m_{b_p u_{\rm cs}} g^m_{b_p e} + p^n_{u_{\rm cs} u_p} g^k_{u_{\rm cs} e}. \quad (9)$$

Therefore, the secrecy rate that is achievable by the PBS in the transmission to PU u_p through CSU $u_{\rm cs}$ using SP (m,n) in the MRC scheme can be obtained by replacing $R^m_{b_p e}$ with $R^{mn}_{b_p u_{\rm cs} e} = \log_2(1+\gamma^{mn}_{e,c})$ in (7). In this paper, we provide the solution of the non-MRC scheme and investigate in detail, and it is obvious that the solution of the MRC scheme can be solved in a similar way.

Remark 1: In (7) and (8), we defined the ultimate secrecy rate as the minimum secrecy rate between the source and the destination over all eavesdroppers, which is the maximum rate at which eavesdroppers cannot decode information transmission between the source and the destination. Such a definition is commonly used in the literature, e.g., [14], [29], and [30].

Remark 2: In the literature, for relay-assisted networks, when an adversary user, i.e., eavesdropper, exists, several models were considered for the information transmission eavesdropping. In general, the eavesdropper can adopt MRC, in which signals received in several phases, i.e., from the source and from the relays, are combined [31]. In another model, rather than combining the signals received from the channels in different phases, the maximum value of their corresponding capacities, i.e., between channels in the first and second time slots, is considered as an upper bound on the achievable rate of the eavesdropper [32]. In addition, in some models, such as [14] and [33], only the data rate at which the eavesdropper can listen in one phase is considered. In our paper, for the PN, we assume that the eavesdropper only listens to the PBS in the first time slot. Since the relays (SUs) are spread over the coverage area, focusing in the first hop, the eavesdropper can be more harmful as it could be close to the PBS.

Let $\rho^{mn}_{u_{\rm cs} u_p} \in \{0,1\}$ be an assignment factor indicating that the subcarrier pair (m,n) is used for the transmission between the PBS and PU u_p through CSU $u_{\rm cs}$. In addition, we define the variable $\eta^k_{u_s} \in \{0,1\}$ as an assignment factor, which indicates that subcarrier k is used by SU u_s for the transmission to the SBS. The objective of our proposed resource-allocation scheme is to maximize the total average secrecy rate of the SUs, while the average secrecy rate constraint of each PU and the individual average power constraints for the PBS and each SU are satisfied. Therefore, the proposed secure resource-allocation problem with the help of a trusted SN is formulated as follows:

$$\max_{\mathbf{p},\boldsymbol{\rho},\boldsymbol{\eta}} \mathbb{E}\left\{\sum_{u_s\in\mathcal{U}_s}\sum_{n\in\mathcal{N}} \varpi_{u_s}\eta^n_{u_s} S^n_{u_s b_s}\right\} \quad (10a)$$

$$\text{S.t.:}\ \mathbb{E}\left\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}} \rho^{mn}_{u_{\rm cs}u_p} S^{mn}_{u_{\rm cs}u_p}\right\} \ge \bar{R}^{\rm SP}_{u_p}, \quad \forall\, u_p\in\mathcal{U}_p, \quad (10b)$$

$$\mathbb{E}\left\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}} \rho^{mn}_{u_{\rm cs}u_p} p^m_{b_p u_{\rm cs}}\right\} \le \bar{P}^{\max}_P, \quad (10c)$$

$$\mathbb{E}\left\{\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}} \left(\rho^{mn}_{u_{\acute{s}}u_p} p^n_{u_{\acute{s}}u_p} + \eta^n_{u_{\acute{s}}} p^n_{u_{\acute{s}}b_{\acute{s}}}\right)\right\} \le \bar{P}^{\max}_{u_{\acute{s}}} \quad \forall\, u_{\acute{s}}\in\mathcal{U}_{\acute{s}}, \quad (10d)$$

$$\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{n\in\mathcal{N}} \rho^{mn}_{u_{\rm cs}u_p} = 1, \qquad \forall\, m\in\mathcal{N}, \quad (10e)$$

$$\sum_{u_s\in\mathcal{U}_s}\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}} \left(\rho^{mn}_{u_{\rm cs}u_p} + \eta^n_{u_s}\right) = 1, \quad \forall\, n\in\mathcal{N}, \quad (10f)$$

where $\mathbf{p}$ is the transmit power vector consisting of all the transmit power variables, i.e., $p^m_{b_p u_{\rm cs}}$, $p^n_{u_{\rm cs}u_p}$, and $p^n_{u_s b_s}$, $\boldsymbol{\rho}$ is the vector consisting of assignment variables $\rho^{mn}_{u_{\rm cs}u_p}$, and $\boldsymbol{\eta}$ is the vector consisting of assignment variables $\eta^n_{u_s}$. $0 \le \varpi_{u_s} \le 1$ is a coefficient reflecting fairness consideration. We included the fairness consideration based on the notion of proportional fairness using a priority coefficient, i.e., ϖ_{u_s}, for each user u_s, in the weighted total secrecy rate objective function in (10). These priority coefficients allow us to establish a relative priority for each user, e.g., a larger value of ϖ_{u_s} means that higher priority is given to user u_s and *vice versa*. In the preceding optimization problem, (10b) is the total secrecy rate constraint for each PU, (10c) is the power constraint of the PBS, (10d) is the power constraint for each SU, and (10e) and (10f) indicate that, in each time slot, each subcarrier should be used once.

Problem (10) is difficult to solve because it is a mixed-integer nonlinear problem, which is a combinatorial optimization and NP-hard problem. The optimization problem in (10) is a mixed nonconvex and combinatorial optimization problem. The nonconvexity comes from the constraint (10b), and the combinatorial nature comes from the integer constraint for user selection. The problem (10) stays nonconvex even if we fix or relax the integer variables to continuous variables. In the following, we propose a new approach to solve the problem (10).

C. Structure of Preferred Solutions

In this paper, we provide the solution of the non-MRC scheme in detail and note that, by a similar approach to the non-MRC scheme, the solution of the MRC scheme can be obtained. Among all optimal solutions of the optimization problem (10), we are interested in those that we call energy conservative solutions. In these solutions, there exists a relation between the transmit power of subcarrier m and the transmit power of subcarrier n in SP (m, n). To introduce these solutions, we need the following lemma.

Lemma 1: Let $p^{mn}_{b_p u_{\rm cs} u_p}$ be defined as the total transmit power consumed in the transmission from the PBS to PU u_p through CSU $u_{\rm cs}$ by SP (m, n), i.e.,

$$p^{mn}_{b_p u_{\rm cs} u_p} = p^m_{b_p u_{\rm cs}} + p^n_{u_{\rm cs} u_p}. \tag{11}$$

Then, the value of $S^{mn}_{u_{\rm cs} u_p}$ in (7) is maximized when

$$g^m_{b_p u_{\rm cs}} p^m_{b_p u_{\rm cs}} = g^n_{u_{\rm cs} u_p} p^n_{u_{\rm cs} u_p}. \tag{12}$$

Proof: Let $p^m_{b_p u_{\rm cs}}$ and $p^n_{u_{\rm cs} u_p}$ be the transmit power variables that satisfy (11) and maximize (7). It should be noted that it is not possible to have $R^m_{b_p u_{\rm cs}} < R^n_{u_{\rm cs} u_p}$. Otherwise, we can borrow some power from $p^n_{u_{\rm cs} u_p}$ and add it to $p^m_{b_p u_{\rm cs}}$ while maintaining the inequality $R^m_{b_p u_{\rm cs}} < R^n_{u_{\rm cs} u_p}$. This way, the value of $S^{mn}_{u_{\rm cs} u_p}$ in (7) increases as it is an increasing function of $p^m_{b_p u_{\rm cs}}$. On the other hand, it is also not possible to have $R^m_{b_p u_{\rm cs}} > R^n_{u_{\rm cs} u_p}$. Otherwise, we can borrow some power from $p^m_{b_p u_{\rm cs}}$ and add it to $p^n_{u_{\rm cs} u_p}$ while maintaining the inequality $R^m_{b_p u_{\rm cs}} > R^n_{u_{\rm cs} u_p}$. This way, the value of $S^{mn}_{u_{\rm cs} u_p}$ in (7) increases as it is an increasing function of $p^n_{u_{\rm cs} u_p}$ and a decreasing function of $p^m_{b_p u_{\rm cs}}$. Therefore, $R^m_{b_p u_{\rm cs}} = R^n_{u_{\rm cs} u_p}$ must be held such that the secrecy rate is maximized and the optimal transmit power variables $p^n_{u_{\rm cs} u_p}$ and $p^m_{b_p u_{\rm cs}}$ must satisfy (12). ■

Lemma 1 applies to the optimization problems in which we have a total transmit power constraint rather than the individual power constraints. However, this lemma leads us to a group of optimal solutions, which we call energy conservative solutions.

Let $\mathbf{p}^*$ be an optimal solution of the optimization problem (10), and let us consider a subcarrier pair (m, n). If there exists a subcarrier k that can be used in the SN transmission, then it is not possible to have $R^m_{b_p u_{\rm cs}} < R^n_{u_{\rm cs} u_p}$. Otherwise, we can borrow some power from $p^n_{u_{\rm cs} u_p}$ and use this amount of power for secondary transmission, i.e., we can increase the objective function. However, if all subcarriers in the second time slot are used for primary transmission, it is possible that, at optimal solution, we have $R^m_{b_p u_{\rm cs}} < R^n_{u_{\rm cs} u_p}$. On the other hand, at the optimal solution, it is possible to have $R^m_{b_p u_{\rm cs}} > R^n_{u_{\rm cs} u_p}$ since the transmit power in the first time slot, i.e., $p^m_{b_p u_{\rm cs}}$, only affects the secrecy rate constraint of the PN. This means that, in our optimization problem, for an optimal solution, the equality in (12) may not hold. Note that, when $R^m_{b_p u_{\rm cs}} > R^n_{u_{\rm cs} u_p}$, we can decrease the value of $p^m_{b_p u_{\rm cs}}$ without changing the value of the objective function, which means that we can save energy while maintaining the optimality. On the other hand, for the optimal solutions $R^m_{b_p u_{\rm cs}} < R^n_{u_{\rm cs} u_p}$, we can decrease the value of $p^n_{u_{\rm cs} u_p}$ while maintaining the optimality. This means that, in this case. we can also save some energy.

Definition 1: Let $\mathbf{p}^*_1$ be a solution of the optimization problem (10). We say that $\mathbf{p}^*_1$ is an energy conservative solution if, for any other solution $\mathbf{p}^*_2$, we have $\mathbf{1}^T \mathbf{p}^*_1 \le \mathbf{1}^T \mathbf{p}^*_2$, where $\mathbf{1}$ is a vector all of whose elements are one, and $[\cdot]^T$ is the vector transpose.

Using Lemma 1 and Definition 1, one can realize that, in our optimization problem, for the energy conservative solutions, the equality in (12) always holds. Therefore, in our optimization problem, we look for the energy conservative solutions by imposing the constraint (12). Let $p^{mn}_{b_p u_{\rm cs} u_p}$, $p^m_{b_p u_{\rm cs}}$, and $p^n_{u_{\rm cs} u_p}$ satisfy (11) and (12). They also satisfy the following:

$$p^m_{b_p u_{\rm cs}} = \frac{g^n_{u_{\rm cs} u_p}}{g^m_{b_p u_{\rm cs}} + g^n_{u_{\rm cs} u_p}} p^{mn}_{b_p u_{\rm cs} u_p}, \tag{13}$$

$$p^n_{u_{\rm cs} u_p} = \frac{g^m_{b_p u_{\rm cs}}}{g^m_{b_p u_{\rm cs}} + g^n_{u_{\rm cs} u_p}} p^{mn}_{b_p u_{\rm cs} u_p}. \tag{14}$$

In this case, the value of $R^{mn}_{u_{\rm cs}, u_p}$ in (3) is given by

$$R^{mn}_{u_{\rm cs} u_p} = \frac{1}{2} \log_2 \left(1 + \frac{g^m_{b_p u_{\rm cs}} g^n_{u_{\rm cs} u_p}}{g^m_{b_p u_{\rm cs}} + g^n_{u_{\rm cs} u_p}} p^{mn}_{b_p u_{\rm cs} u_p} \right). \tag{15}$$

Therefore, the secrecy rate that is achievable by DF relaying through CSU $u_{\rm cs}$ and SP (m, n) is given by

$$\begin{aligned} S^{mn}_{u_{\rm cs} u_p} &= \left[R^{mn}_{u_{\rm cs} u_p} - \max_{e \in \mathcal{E}} (R^m_{b_p e}) \right]^+ \\ &= \left[\frac{1}{2} \log_2 \left(1 + \frac{g^m_{b_p u_{\rm cs}} g^n_{u_{\rm cs} u_p}}{g^m_{b_p u_{\rm cs}} + g^n_{u_{\rm cs} u_p}} p^{mn}_{b_p u_{\rm cs} u_p} \right) \right. \\ &\quad \left. - \frac{1}{2} \log_2 \left(1 + \max_{e \in \mathcal{E}} (g^m_{b_p e}) p^m_{b_p u_{\rm cs}} \right) \right]^+ . \end{aligned} \tag{16}$$

Remark 4: Although, for the DF relay networks, the optimality of equality of the data rates in the first and second time slots has been shown, e.g., [34]–[37], our model differs from them as we consider secrecy rate and individual transmit power constraints rather than the total transmit power constraint. In our optimization problem (10), the optimal solution may not satisfy this equality condition. However, we showed that there are optimal solutions that satisfy this equality condition called energy conservative solutions.

III. Solution Based on Dual Approach

A. Transmit Power Allocation

Here, we consider the non-MRC scheme and provide the solution for this problem. The solution to the proposed optimization problem depends on the distributions of the channel power gains. In the following, we focus on the Rayleigh fading scenario, which means that the channel power gains are exponentially distributed. The average secrecy rate of SU u_s in the transmission to the SBS over subcarrier n in the second time slot is given by [38]

$$\begin{aligned} \mathbb{E}\left\{ S^n_{u_s b_s} \right\} &= \mathbb{E} \left\{ \left[\frac{1}{2} \log_2 (1 + g^n_{u_s b_s} p^n_{u_s b_s}) \right. \right. \\ &\qquad \left. \left. - \frac{1}{2} \log_2 (1 + \tilde{g}^n_{u_s e} p^n_{u_s b_s}) \right]^+ \right\} \\ &= \int_0^\infty \int_0^{g^n_{u_s b_s}} \left(\frac{1}{2} \log_2 (1 + g^n_{u_s b_s} p^n_{u_s b_s}) \right. \\ &\qquad \left. - \frac{1}{2} \log_2 (1 + \tilde{g}^n_{u_s e} p^n_{u_s b_s}) \right) \\ &\qquad \times f_{\tilde{g}^n_{u_s e}} (\tilde{g}^n_{u_s e}) f_{g^n_{u_s b_s}} (g^n_{u_s b_s}) d\tilde{g}^n_{u_s e} dg^n_{u_s b_s}, \end{aligned} \tag{17}$$

where $\tilde{g}^n_{u_s e} = \max_{e \in \mathcal{E}} \{ g^n_{u_s e} \}$, and $f_{\tilde{g}^n_{u_s e}} (\tilde{g}^n_{u_s e})$ is the probability density function (pdf) of the random variable $\tilde{g}^n_{u_s e}$.

In addition, the average secrecy rate that is achievable by DF relaying through SU u_s and SP (m,n) is given by [38]

$$\mathbb{E}\left\{S^{mn}_{u_{\rm cs}u_p}\right\} = \mathbb{E}\left\{\left[\frac{1}{2}\log_2\left(1+\frac{g^m_{b_pu_{\rm cs}}g^n_{u_{\rm cs}u_p}}{g^m_{b_pu_{\rm cs}}+g^n_{u_{\rm cs}u_p}}p^{mn}_{b_pu_{\rm cs}u_p}\right)\right.\right.$$
$$\left.\left.-\frac{1}{2}\log_2\left(1+\frac{\tilde{g}^m_{b_pe}g^n_{u_{\rm cs}u_p}}{g^m_{b_pu_{\rm cs}}+g^n_{u_{\rm cs}u_p}}p^{mn}_{b_pu_{\rm cs}u_p}\right)\right]^+\right\}, \quad (18)$$

where $\tilde{g}^m_{b_pe} = \max_{e\in\mathcal{E}}\{g^m_{b_pe}\}$.

Comparing (18) with (17), we can consider the relay channel as the wiretap channel with the direct channel gain $\hat{g}^{mn}_{b_pu_{\rm cs}u_p} = g^m_{b_pu_{\rm cs}}g^n_{u_{\rm cs}u_p}/(g^m_{b_pu_{\rm cs}}+g^n_{u_{\rm cs}u_p})$ and the eavesdropper channel gain $\hat{g}^{mn}_{b_pu_{\rm cs}u_pe} = \tilde{g}^m_{b_pe}g^n_{u_{\rm cs}u_p}/(g^m_{b_pu_{\rm cs}}+g^n_{u_{\rm cs}u_p})$. However, note that the equivalent channel gains $\hat{g}^{mn}_{b_pu_{\rm cs}u_p}$ and $\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}$ are not independent. Therefore, we can rewrite (18) as follows:

$$\mathbb{E}\left\{S^{mn}_{u_{\rm cs}u_p}\right\} = \int_0^{\infty}\int_0^{\hat{g}^{mn}_{b_pu_{\rm cs}u_p}}\left[\frac{1}{2}\log_2\left(1+\hat{g}^{mn}_{b_pu_{\rm cs}u_p}p^{mn}_{b_pu_{\rm cs}u_p}\right)\right.$$
$$\left.-\frac{1}{2}\log_2\left(1+\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}p^{mn}_{b_pu_{\rm cs}u_p}\right)\right]$$
$$\times f(\hat{g}^{mn}_{b_pu_{\rm cs}u_p},\hat{g}^{mn}_{b_pu_{\rm cs}u_pe})d\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}d\hat{g}^{mn}_{b_pu_{\rm cs}u_p}, \quad (19)$$

where $f(\hat{g}^{mn}_{b_pu_{\rm cs}u_p},\hat{g}^{mn}_{b_pu_{\rm cs}u_pe})$ is the joint pdf of the random variables $\hat{g}^{mn}_{b_pu_{\rm cs}u_p}$ and $\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}$.

The Lagrange function of the optimization problem (10) is given by

$$L(\mathbf{p},\boldsymbol{\theta},\boldsymbol{\lambda}) = \mathbb{E}\left\{\sum_{u_s\in\mathcal{U}_s}\sum_{n\in\mathcal{N}}S^n_{u_sb_s}\right\}$$
$$+\sum_{u_p\in\mathcal{U}_p}\theta_{u_p}\left(\mathbb{E}\left\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}}S^{mn}_{u_{\rm cs}u_p}\right\}-\bar{R}^{\rm SP}_{u_p}\right)$$
$$+\lambda_0\left(\bar{P}^{\max}_P-\mathbb{E}\left\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}}p^m_{b_pu_{\rm cs}}\right\}\right)$$
$$+\sum_{u_{\acute{s}}\in\mathcal{U}_{\acute{s}}}\lambda_{u_{\acute{s}}}\left(\bar{P}^{\max}_{u_{\acute{s}}}-\mathbb{E}\left\{\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}}\right.\right.$$
$$\left.\left.\times\left(p^n_{u_{\acute{s}}u_p}+p^n_{u_{\acute{s}}b_s}\right)\right\}\right), \quad (20)$$

where $\boldsymbol{\theta} = [\theta_1,\ldots,\theta_{u_p},\ldots,\theta_{U_p}]$, θ_{u_p} for $u_p = 1,\ldots,U_p$ is the Lagrange multiplier corresponding to the secrecy rate constraint of PU u_p (10b), $\boldsymbol{\lambda} = [\lambda_0,\lambda_1,\ldots,\lambda_{u_{\acute{s}}},\ldots,\lambda_{U_{\acute{s}}}]$, λ_0 is the Lagrange multiplier corresponding to PBS power constraint (10c), and $\lambda_{u_{\acute{s}}}$ for $u_{\acute{s}} = 1,\ldots,U_{\acute{s}}$ is the Lagrange multiplier corresponding to transmit power constraint of SU $u_{\acute{s}}$ (10d). Note that, in (20), we use the variable $p^{mn}_{b_pu_{\rm cs}u_p}$ instead of the variables $p^n_{u_{\rm cs}u_p}$ and $p^m_{b_pu_{\rm cs}}$ by using (13) and (14). Therefore, $\mathbf{p}$ is the vector of the transmit power variables, which can be alternatively denoted by $\mathbf{p} = [\mathbf{p}^{\rm sp},\mathbf{p}^s]$, where $[\mathbf{p}^{\rm sp}]$ is a vector whose elements are $p^{mn}_{b_pu_{\rm cs}u_p}$, and $\mathbf{p}^s$ is a vector whose elements are $p^n_{u_sb_s}$.

Using (20), a dual function can be obtained as follows:

$$g(\boldsymbol{\theta},\boldsymbol{\lambda}) = \max_{\mathbf{p}} L(\mathbf{p},\boldsymbol{\theta},\boldsymbol{\lambda}). \quad (21)$$

To solve (21), we take the derivatives of (21) with respect to $p^{mn}_{b_pu_{\rm cs}u_p}$ and write $\partial L(\mathbf{p},\boldsymbol{\theta},\boldsymbol{\lambda})/\partial p^{mn}_{b_pu_{\rm cs}u_p} = 0$, which can be rewritten as

$$\frac{\theta_{u_p}}{2}\left\{\int_0^{\infty}\int_0^{\hat{g}^{mn}_{b_pu_{\rm cs}u_p}}\right.$$
$$\times\left[\frac{\hat{g}^{mn}_{b_pu_{\rm cs}u_p}}{1+\hat{g}^{mn}_{b_pu_{\rm cs}u_p}p^{mn}_{b_pu_{\rm cs}u_p}}-\frac{\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}}{1+\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}p^{mn}_{b_pu_{\rm cs}u_p}}\right]$$
$$\left.\times f(\hat{g}^{mn}_{b_pu_{\rm cs}u_p},\hat{g}^{mn}_{b_pu_{\rm cs}u_pe})d\hat{g}^{mn}_{b_pu_{\rm cs}u_pe}d\hat{g}^{mn}_{b_pu_{\rm cs}u_p}\right\}$$
$$-\frac{\lambda_0g^n_{u_su_p}+\lambda_{u_s}g^m_{b_pu_s}}{g^m_{b_pu_s}+g^n_{u_su_p}} = 0, \quad (22)$$

where $F_{\tilde{g}^m_{b_pe}}(\cdot)$ is the cumulative density function (CDF) of the random variable $\tilde{g}^m_{b_pe}$.

Similarly, we take the derivatives of (21) with respect to $p^n_{u_sb_s}$ and write $\partial L(\mathbf{p},\boldsymbol{\theta},\boldsymbol{\lambda})/\partial p^n_{u_sb_s} = 0$, which can be rewritten as

$$\frac{g^n_{u_sb_s}F_{\tilde{g}^n_{u_se}}(g^n_{u_sb_s})}{1+g^n_{u_sb_s}p^n_{u_sb_s}}-\int_0^{g^n_{u_sb_s}}\frac{\tilde{g}^n_{u_se}}{1+\tilde{g}^n_{u_se}p^n_{u_sb_s}}f_{\tilde{g}^n_{u_se}}(\tilde{g}^n_{u_se})d\tilde{g}^n_{u_se}$$
$$-\lambda_{u_s} = 0, \quad (23)$$

where $\tilde{g}^n_{u_se} = \max_{e\in\mathcal{E}}\{g^n_{u_se}\}$. In general, no closed-form solution to power allocation is known. However, we can find $p^{mn}_{b_pu_{\rm cs}u_p}$ and $p^n_{u_sb_s}$ based on efficient algorithms yielding numerical solutions of (22) and (23), respectively.

B. Subcarrier Allocation

Now, we perform subcarrier allocation, i.e., we find the value of assignment variables $\rho^{mn}_{u_{\rm cs}u_p}$ and $\eta^n_{u_s}$. In doing so, based on (21) and using the average transmit power values $p^{mn}_{b_pu_{\rm cs}u_p}$ and $p^n_{u_sb_s}$ obtained in the previous subsection, we first define the following functions:

$$\psi^{mn1}_{u_{\rm cs}u_p} = \theta_{u_p}\mathbb{E}\left\{S^{mn}_{u_{\rm cs}u_p}\right\}-\lambda_0\mathbb{E}\left\{p^m_{b_pu_{\rm cs}}\right\}-\lambda_{u_{\rm cs}}\mathbb{E}\left\{p^n_{u_{\rm cs}u_p}\right\}, \quad (24)$$
$$\psi^{n2}_{u_s} = \mathbb{E}\left\{S^n_{u_sb_s}\right\}-\lambda_{u_s}\mathbb{E}\left\{p^n_{u_sb_s}\right\}, \quad (25)$$

where $p^m_{b_pu_{\rm cs}}$ and $p^n_{u_{\rm cs}u_p}$ can be obtained from (13) and (14), respectively.

Suppose that the PBS wants to communicate with PU u_p over SP (m,n) with the help of CSU $u_{\rm cs}$ as a relay. For each subcarrier m in the first time slot, we find the best CSU $u_{\rm cs}$, PU u_p, and the pairing subcarrier n as

$$\phi^{m1}(u^*_{\rm cs},u^*_p,n^*) = \max_{u_{\rm cs}\in\mathcal{U}_s,u\in\mathcal{U}_p,n\in S_{\mathcal{N}}}\psi^{mn1}_{u_{\rm cs}u_p}, \quad (26)$$

where $S_{\mathcal{N}}$ is the set of available subcarriers for the second time slot. We declare that the subcarrier m^* in the first time slot is paired with subcarrier n^* in the second time slot where the transmission is performed to PU u_p^* through relay u_s^* if we have

$$m^* = \underset{m \in S_{\mathcal{M}}}{\arg\max}\, \phi^{m1}(u_{\rm cs}^*, u_p^*, n^*), \tag{27}$$

where $S_{\mathcal{M}}$ is the set of subcarriers available for the first time slot.

On the other hand, suppose that SU u_s wants to transmit information to the SBS. For each subcarrier n in the second time slot, we find the best SU u_s as

$$\phi^{n2}(u_s^*) = \max_{u_s \in \mathcal{U}_s} \psi_{u_s}^{n2}, \tag{28}$$

and find the best subcarrier in the second time slot as

$$n^* = \underset{m \in S_{\mathcal{M}}}{\arg\max}\, \phi^{m2}(u_s^*). \tag{29}$$

Next, by obtaining tuples $(u_{\rm cs}^*, u_p^*, m^*, n^*)$ and (u_s^*, n^*), we obtain the corresponding values of $\psi_{u_{\rm cs}^* u_p^*}^{m^* n^* 1}$ and $\psi_{u_s^*}^{n^* 2}$ from (24) and (25), respectively. Now, we decide that $\rho_{u_{\rm cs}^* u_p^*}^{m^* n^*} = 1$ if $\psi_{u_{\rm cs}^* u_p^*}^{m^* n^* 1} \geq \psi_{u_s^*}^{n^* 2}$, and hence, we set $\eta_{u_s^*}^{n^*} = 0$. On the other hand, we set $\eta_{u_s^*}^{n^*} = 1$ if $\psi_{u_{\rm cs}^* u_p^*}^{m^* n^* 1} < \psi_{u_s^*}^{n^* 2}$, and hence, we set $\rho_{u_{\rm cs}^* u_p^*}^{m^* n^*} = 0$.

C. Dual Problem

So far, we have obtained the value of the average transmit power vector $\mathbf{p}$ and the assignment variables $\boldsymbol{\rho}$ and $\boldsymbol{\eta}$; based on this the dual function $g(\boldsymbol{\theta}, \boldsymbol{\lambda})$ can be obtained. To find the optimal values of dual variables $\boldsymbol{\theta}$ and $\boldsymbol{\lambda}$, we should solve the corresponding dual optimization problem given by

$$(\boldsymbol{\theta}^*, \boldsymbol{\lambda}^*) = \underset{\boldsymbol{\theta} \succeq \mathbf{0}, \boldsymbol{\lambda} \succeq \mathbf{0}}{\arg\max}\, g(\boldsymbol{\theta}, \boldsymbol{\lambda}). \tag{30}$$

Lemma 1: The dual problem $g(\boldsymbol{\theta}, \boldsymbol{\lambda})$ in (30) can be solved using, e.g., the subgradient method or the ellipsoid method, which requires the subgradient of $g(\boldsymbol{\theta}, \boldsymbol{\lambda})$ with respect to $\boldsymbol{\theta}$, $\boldsymbol{\lambda}$. The corresponding subgradients are given by

$$\begin{bmatrix} \mathbb{E}\left\{\sum_{u_{\rm cs} \in \mathcal{U}_{\rm cs}} \sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}} S_{u_{\rm cs} 1}^{mn}\right\} - \bar{R}_1^{\rm SP} \\ \vdots \\ \mathbb{E}\left\{\sum_{u_{\rm cs} \in \mathcal{U}_{\rm cs}} \sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}} S_{u_{\rm cs} U_p}^{mn}\right\} - \bar{R}_{U_p}^{\rm SP} \\ \bar{P}_P^{\max} - \mathbb{E}\left\{\sum_{u_{\rm cs} \in \mathcal{U}_{\rm cs}} \sum_{n \in \mathcal{N}} p_{b_p u_{\rm cs}}^m\right\} \\ \bar{P}_1^{\max} - \mathbb{E}\left\{\sum_{u_p \in \mathcal{U}_p} \sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}}\Big) p_{1 u_p}^n + p_{1 b_s}^n\Big)\right\} \\ \vdots \\ \bar{P}_{U_{\acute{s}}}^{\max} - \mathbb{E}\left\{\sum_{u_p \in \mathcal{U}_p} \sum_{m \in \mathcal{N}} \sum_{n \in \mathcal{N}}\Big) p_{U_{\acute{s}} u_p}^n + p_{U_{\acute{s}} b_s}^n\Big)\right\} \end{bmatrix}. \tag{31}$$

Using Lemma 1, we update the dual variables $\boldsymbol{\phi} = [\boldsymbol{\theta}, \boldsymbol{\lambda}^T]^T$ based on the ellipsoid method. We show our proposed secure resource-allocation scheme in Fig. 2. Based on Algorithm 1, power allocation (Step 2) and subcarrier allocation (Step 3) are repeated until the stopping criterion (Step 5) is fulfilled.

Algorithm 1: Iterative algorithm for finding the transmit powers $p_{b_{\rm p} u_{\rm s} u_{\rm p}}^{mn}, p_{u_{\rm s} b_{\rm s}}^{n}$ and subcarrier allocation based on the ellipsoid method

s1. Initialization: $\boldsymbol{\phi} = [\boldsymbol{\theta}, \boldsymbol{\lambda}^T]^T \leftarrow \boldsymbol{\phi}(0)$, $\boldsymbol{\Sigma} \leftarrow \boldsymbol{\Sigma}(0)$, Set tolerance τ and $\varrho = U^{\rm s} + 2$
s2. If $\boldsymbol{\phi} \prec 0$ for some entries $i \in \mathcal{I}$;
  s2.1. Set $\boldsymbol{d} = \sum_{i \in \mathcal{I}} \boldsymbol{z}_i (\boldsymbol{z}_i$ is i^{th} canonical basis)
  s2.2 Otherwise, Find $p_{b_{\rm p} u_{\rm s} u_{\rm p}}^{mn}$ and $p_{u_{\rm s} b_{\rm s}}^{n}$ using (22) and (23)
  s2.3. Update the variable $p_{b_{\rm p} u_{\rm s}}^{m}$ using (13)
  s2.4. Update the variable $p_{u_{\rm s} u_{\rm p}}^{n}$ using (14)
s3. Perform subcarrier allocation, i.e.,
  s3.1. Set $S_{\mathcal{M}} = \{1, \ldots, N\}$, $S_{\mathcal{N}} = \{1, \ldots, N\}, \boldsymbol{\eta} = \mathbf{0}$, and $\boldsymbol{\rho} = \mathbf{0}$
  s3.2. For each $m \in S_{\mathcal{M}}$ compute $\phi^{m1}(u_{\rm s}^*, u_{\rm p}^*, n^*)$ using (26)
  s3.3. Compute m^* from (27) and form the tuple $(u_{\rm s}^*, u_{\rm p}^*, m^*, n^*)$
  s3.4. For each $n \in S_{\mathcal{N}}$ compute $\phi^{n2}(u_{\rm s}^*)$ using (28)
  s3.5. Compute n^* from (29) and form the tuple $(u_{\rm s}^*, n^*)$
  s3.6. Set $\rho_{u_{\rm s}^* u_{\rm p}^*}^{m^* n^*} = 1$ and $\eta_{u_{\rm s}^*}^{n^*} = 0$ if $\psi_{u_{\rm s}^* u_{\rm p}^*}^{m^* n^* 1} \geq \psi_{u_{\rm s}^*}^{n^* 2}$
  s3.7. Set $\rho_{u_{\rm s}^* u_{\rm p}^*}^{m^* n^*} = 0$ and $\eta_{u_{\rm s}^*}^{n^*} = 1$ if $\psi_{u_{\rm s}^* u_{\rm p}^*}^{m^* n^* 1} < \psi_{u_{\rm s}^*}^{n^* 2}$
  s3.8. Set $S_{\mathcal{M}} = S_{\mathcal{M}} - \{m^*\}$and $S_{\mathcal{N}} = S_{\mathcal{N}} - \{n^*\}$ if $\rho_{u_{\rm s}^* u_{\rm p}^*}^{m^* n^*} = 1$
  s3.9. Set $S_{\mathcal{N}} = S_{\mathcal{N}} - \{n^*\}$ if $\eta_{u_{\rm s}^*, n^*} = 1$
  s3.10. If $S_{\mathcal{N}} \neq \emptyset$ go to s3.1
s4. Perform the ellipsoid update:
  s4.1. $\boldsymbol{d} \leftarrow \boldsymbol{d} / \sqrt{\boldsymbol{d}^T \boldsymbol{\Sigma}}$
  s4.2. $\boldsymbol{\phi} \leftarrow \boldsymbol{\phi} - \boldsymbol{\Sigma} / (\varrho + 1)$
  s4.3. $\boldsymbol{\Sigma} \leftarrow \frac{\varrho^2}{\varrho^2 - 1}(\boldsymbol{\Sigma} - \frac{2}{\varrho + 1} \boldsymbol{\Sigma} \boldsymbol{d} \boldsymbol{d}^T \boldsymbol{\Sigma})$
s5. If $\sqrt{\boldsymbol{d}^T \boldsymbol{\Sigma}} < \tau$, go to Step s6, otherwise, go to step 2
s6. end

Fig. 2. Algorithm for solving the proposed optimization problem using dual approach.

IV. Channel Distribution Information Imperfection

Now, we investigate the effect of imperfect CDI on the performance of the proposed system. To set up a comparison framework, we first evaluate the performance on the proposed framework assuming the availability of perfect CDI. To simulate the case with imperfect CDI, we consider an actual scenario where the corresponding CDI is assumed to be obtained based on the received noisy samples from the channel and may thus be imperfect. We then evaluate the performance based on the resulting imperfect CDI. There are two categories of CDI estimation: parametric and nonparametric. In the former, the distribution is assumed known, and one only needs to estimate the corresponding parameters, e.g., mean and variance, to find the pdf similar to the case of [39]. Here, to be not confined to a specific distribution, we consider the latter case in which the distribution is totally unknown and should be estimated based on the received samples from the channel. Histogram estimation (HE) is perhaps the handiest method among nonparametric estimation schemes. However, the resulting density is discrete and is not in a closed form. Therefore, more advanced methods such as KDE have been proposed in the literature, which are preferred over HE [40]. KDE can estimate the density pretty well based on a reasonable number of samples when the samples are noise free. In reality, the measured channel coefficients may contain some noisy or irrelevant data as well. In this case, a robust density estimation method has to be applied that can provide a good estimation, even in the presence of contaminated samples.

A. CDI Estimation Methods: Nonparametric

1) Kernel Density Estimation: One of the most well-known nonparametric density estimation methods is KDE [40]. Let $\{\mathbf{x}_1, \ldots, \mathbf{x}_Z : \mathbf{x}_i \in \mathbb{R}^d\}$ be a set of observations for estimating a random vector (RV) $\mathbf{x}$ with density $f(\mathbf{x})$, where Z is the number of observation vectors. Moreover, each $\mathbf{x}_i = (x_{i1}, \ldots, x_{id})$, $i = 1, \ldots, Z$ is a sequence of d data in the vector $\mathbf{x}_i$. The kernel density estimate of $f(\mathbf{x})$, which is also called the Parzen window estimate, is a nonparametric estimate given by $\hat{f}_{\mathrm{KDE}}(\mathbf{x}) = (1/Z)\sum_{i=1}^{Z} k_\delta(\mathbf{x}, \mathbf{x}_i)$, where $k_\delta(\mathbf{x}, \mathbf{x}_i)$ is the kernel function. The most commonly used kernel function is a Gaussian kernel $k_\delta(\mathbf{x}, \mathbf{x}_i) = (1/\sqrt{2\pi}\delta)^d \exp(-(\|\mathbf{x} - \mathbf{x}_i\|^2/2\delta^2))$, where the smoothing parameter δ is referred to as the bandwidth. The kernel bandwidth δ is set as the median distance of a training point $\mathbf{x}_i$ to its nearest neighbor.

2) Robust Kernel Density Estimation: The need for a robust KDE arises when analyzing contaminated data. Contaminated data refer to data consisting of realizations from both a nominal or a "clean" distribution in addition to outlying or anomalous measurements. The robust KDE (RKDE) [23], [24] has the form $\hat{f}_{\mathrm{RKDE}}(\mathbf{x}) = \sum_{i=1}^{Z} w_i k_\delta(\mathbf{x}, \mathbf{x}_i)$, where $k_\delta(\mathbf{x}, \mathbf{x}_i)$ is a kernel function, and $w_i \,\forall\, i$, are nonnegative weights that sum to one, i.e., $\sum_{i=1}^{Z} w_i = 1$. The RKDE can be implemented based on the iteratively reweighed least square (IRWLS) algorithm in which the main goal is to find the optimal value of $\omega_i \,\forall\, i$.

The IRWLS algorithm can be implemented in five steps as follows.

Step 1: First, initialize $w_i^{(0)}$ such that $\hat{\mathbf{\Pi}}^{(1)}$ is the geometric median of $\Phi(\mathbf{x}_i)$, i.e., $\hat{\mathbf{\Pi}}^{(1)} = \arg\min_{\mathbf{\Pi}\in\mathcal{H}} \sum_{i=1}^{Z} \rho(\|\Phi(\mathbf{x}_i) - \mathbf{\Pi}\|)$, where $\mathbf{\Pi} = \sum_{j=1}^{Z} w_j \Phi(\mathbf{x}_j)$, and ρ is a robust loss function. Well-known examples of robust loss functions, which are denoted by $\rho(x)$, are Huber's or Hampel's functions (see [23] for details).

Step 2: Set $\| \Phi(\mathbf{x}_i) - \mathbf{\Pi}^{(\varrho)} \|^2 = \langle \Phi(\mathbf{x}_i) - \mathbf{\Pi}^{(\varrho)}, \Phi(\mathbf{x}_i) - \mathbf{\Pi}^{(\varrho)}\rangle = \langle \Phi(\mathbf{x}_i), \Phi(\mathbf{x}_i)\rangle - 2\langle \Phi(\mathbf{x}_i), \mathbf{\Pi}^{(\varrho)}\rangle + \langle \mathbf{\Pi}^{(\varrho)}, \mathbf{\Pi}^{(\varrho)}\rangle$, where ϱ is the iteration number. Since $\mathbf{\Pi}^{(\varrho)} = \sum_{j=1}^{Z} w_j^{(\varrho-1)} \Phi(\mathbf{x}_j)$, we have $\langle \Phi(\mathbf{x}_i), \Phi(\mathbf{x}_i)\rangle = k_\delta(\mathbf{x}_i, \mathbf{x}_i)$, $\langle \Phi(\mathbf{x}_i), \mathbf{\Pi}^{(\varrho)}\rangle = \sum_{j=1}^{Z} w_j^{(\varrho-1)} k_\delta(\mathbf{x}_i, \mathbf{x}_j)$, and $\langle \mathbf{\Pi}^{(\varrho)}, \mathbf{\Pi}^{(\varrho)}\rangle = \sum_{j=1}^{Z}\sum_{l=1}^{Z} w_j^{(\varrho-1)} w_l^{(\varrho-1)} k_\delta(\mathbf{x}_j, \mathbf{x}_l)$.

Step 3: Update $\tilde{w}_i^{(\varrho)}$ as $\tilde{w}_i^{(\varrho)} = \psi(\| \Phi(\mathbf{x}_i) - \mathbf{\Pi}^{(\varrho)} \|)/\| \Phi(\mathbf{x}_i) - \mathbf{\Pi}^{(\varrho)} \|$, where $\psi(x) = d\rho(x)/dx$.

Step 4: To get the value of $w_i^{(\varrho)}$, normalize $\tilde{w}_i^{(\varrho)}$ as $w_i^{(\varrho)} = \tilde{w}_i^{(\varrho)} / \sum_{i=1}^{Z} \tilde{w}_i^{(\varrho)}$.

Step 5: If the algorithm converges, $\hat{\mathbf{\Pi}} = \sum_{i=1}^{Z} w_i^{(\varrho)} \Phi(\mathbf{x}_i)$. Otherwise, let $\varrho = \varrho + 1$ and go to Step 2. The estimated density is obtained as $\hat{f}_{\mathrm{RKDE}}(\mathbf{x}) = \langle \Phi(\mathbf{x}), \hat{\mathbf{\Pi}}\rangle = \langle \Phi(\mathbf{x}), \sum_{i=1}^{Z} w_i^{(\varrho)} \Phi(\mathbf{x}_i)\rangle = \sum_{i=1}^{Z} w_i^{(\varrho)} \langle \Phi(\mathbf{x}), \Phi(\mathbf{x}_i)\rangle = \sum_{i=1}^{Z} w_i^{(\varrho)} k_\delta(\mathbf{x}, \mathbf{x}_i)$.

B. CDI Estimation Methods: Parametric

In the parametric method, the pdf is assumed to have a known distribution with unknown parameters of distribution. The parameters of the assumed pdf can be estimated either using maximum-likelihood (ML) estimation or Bayesian estimation [41]. In our case, an exponential distribution of the form $f(x) = (1/\bar{x})\exp(x/\bar{x})$ is used, where the parameter $\bar{x}$ is the mean and can be estimated either using Bayesian or ML estimation. Using the $\acute{Z}$ training samples $\mathcal{X} = \{x_1, x_2, \ldots, x_{\acute{Z}}\}$, the mean is given by ML estimation as $\hat{\bar{x}} = (1/\acute{Z})\sum_{i=1}^{\acute{Z}} x_i$, where $\hat{\bar{x}}$ is the estimated mean.

V. Practical Considerations

A. Analysis of Duality Gap

When solving an optimization problem using dual approach, one important thing must be taken into consideration: duality gap. The analysis provided here is based on the so-called time-sharing property, which is first introduced in [42]. Consider an optimization problem of the form

$$\max_{\boldsymbol{x}} \sum_{n=1}^{N} f_n(\boldsymbol{x}_n) \tag{32a}$$

$$\text{S.t.}: \sum_{n=1}^{N} h_n(\boldsymbol{x}_n) \le \boldsymbol{P}, \tag{32b}$$

where $\boldsymbol{x}_n \in \mathbb{R}^U$; $\boldsymbol{x} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N]$; $f_n : \mathbb{R}^U \to \mathbb{R}$; $h_n : \mathbb{R}^U \to \mathbb{R}^L$; and $\mathbb{R}^U$ and $\mathbb{R}^L$ are real U vectors ($U \times 1$ matrices) and real L vectors ($L \times 1$ matrices), respectively. In general, $f_n(\boldsymbol{x}_n)$ is not concave, and $h_n(\boldsymbol{x}_n)$ is not convex. Let $\boldsymbol{x}_n^*$ and $\boldsymbol{y}_n^*$ be the optimal solutions of the optimization problem (32a) with $\boldsymbol{P} = \boldsymbol{P}_x$ and $\boldsymbol{P} = \boldsymbol{P}_y$, respectively. We say that this optimization problem satisfies the time-sharing property if, for any $\boldsymbol{P}_x$ and $\boldsymbol{P}_y$ and for any $0 \le \nu \le 1$, there always exists a feasible solution $\boldsymbol{z}_n$ such that $\sum_{n=1}^{N} h_n(\boldsymbol{z}_n) \le \nu\boldsymbol{P}_x + (1-\nu)\boldsymbol{P}_y$, and $\sum_{n=1}^{N} f_n(\boldsymbol{z}_n) \ge \nu f_n(\boldsymbol{x}_n^*) + (1-\nu) f_n(\boldsymbol{y}_n^*)$. In [42, Th. 1], it was shown that if an optimization problem of the form (32a) satisfies the time-sharing property, it has a zero duality gap. Consider the optimization problem (10) whose optimization variables are $\boldsymbol{p}$ and $\boldsymbol{\rho}$. We stack these variable into variable $\boldsymbol{x} = [\boldsymbol{p}\boldsymbol{\rho}]$. Note that, for two constraints limit vectors $\boldsymbol{P_x}$ and $\boldsymbol{P_y}$, we need to construct $\nu\boldsymbol{P_x}$ and $(1-\nu)\boldsymbol{P_y}$ and find their corresponding optimal solutions $\boldsymbol{x}_n^{\nu^*}$ and $\boldsymbol{y}_n^{(1-\nu^*)}$. Although the optimal value of variable $\boldsymbol{p}$ in $\boldsymbol{x}_n^{\nu^*}$ and $\boldsymbol{y}_n^{(1-\nu^*)}$ can be any nonnegative value, the optimal value of each component of $\boldsymbol{\rho}$ must be either 0 or 1, which makes constructing $\nu\boldsymbol{P}_x$ and $(1-\nu)\boldsymbol{P}_y$ impossible as (10e) and (10f) mean that any subcarrier should be allocated once, but $\nu\boldsymbol{P}_x$ and $(1-\nu)\boldsymbol{P}_y$ mean that a fraction of the subcarrier should be assigned. To show the time-sharing property, we may do in the same way as in [42] and [43]. We divide each subcarrier n into N_n adjacent subchannels, each undergoing the same channel condition since they are adjacent. Now, we can construct $\boldsymbol{z}_n$ such that, for the ν portion of the total subchannels in each subcarrier, it takes its entries from $\boldsymbol{x}_n^*$ and, for the $(1-\nu)$ portion, it takes its entries from $\boldsymbol{y}_n^*$. With this construction, it is easy to show that $\sum_{n=1}^{N} h_n(\boldsymbol{z}_n) \approx \nu\boldsymbol{P}_x + (1-\nu)\boldsymbol{P}_y$ and that $\sum_{n=1}^{N} f_n(\boldsymbol{z}_n) \approx \nu f_n(\boldsymbol{x}_n^*) + (1-\nu) f_n(\boldsymbol{y}_n^*)$. As the number of subchannels tends to infinity, the approximation will be more precise. This means that the time-sharing property is satisfied by optimization problem (10), and the duality gap tends to zero as the number of subcarriers goes to infinity.

B. Feasibility of the Optimization Problem

Now, we consider the feasibility of the optimization problem (10). Note that the constraints (10b)–(10d) affect the feasibility of the optimization problem (10). To proceed further, we consider the following optimization problem:

$$\max_{\mathbf{p},\boldsymbol{\rho},\boldsymbol{\eta}} \mathbb{E}\left\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}}\rho^{mn}_{u_{\rm cs}u_p}S^{mn}_{u_{\rm cs}u_p}\right\} \tag{33a}$$

$$\text{S.t.: (10c)}-\text{(10f)}. \tag{33b}$$

We denote the optimal value of (33a) by $\bar{R}^{\rm SP}_{\max}=\mathbb{E}\{\sum_{u_{\rm cs}\in\mathcal{U}_{\rm cs}}\sum_{u_p\in\mathcal{U}_p}\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}}\rho^{mn}_{u_{\rm cs}u_p}S^{mn}_{u_{\rm cs}u_p}\}$. Therefore, if the value of $\bar{R}^{\rm SP}$ in (10b) is higher than $\bar{R}^{\rm SP}_{\max}$, the optimization problem (10) will be infeasible. Note that, as stated in Section V-A, the duality gap vanishes as the number of subcarriers tends to infinity; in that situation, the feasibility statements here will be valid.

C. Conventional Underlay Approach

In this paper, our objective is to maximize the average secrecy rate of the SUs subject to guaranteeing a given average secrecy rate for PUs. However, in the conventional case, such maximization is subject to the average interference threshold constraint, i.e., $\mathbb{E}\{\sum_{u_s\in\mathcal{U}_s}\eta^n_{u_s}p^n_{u_sb_s}g^n_{u_su_p}\}\le\bar{\Gamma}^n_{u_p}, \forall n\in\mathcal{N}, u_p\in\mathcal{U}_p$, where $g^n_{u_su_p}$ is the interference channel power gain between SU u_s and PU u_p, and $\bar{\Gamma}^n_{u_p}, \forall n\in\mathcal{N}, u_p\in\mathcal{U}_p$ is the average interference threshold for PU u_p on subcarrier n. The optimization problem in a conventional underlay system is formulated as the maximization of a sum average rate of all SUs subject to SU average transmitted power and secondary to primary average interference constraints, i.e.,

$$\max_{\mathbf{p},\boldsymbol{\eta}} \mathbb{E}\left\{\sum_{u_s\in\mathcal{U}_s}\sum_{n\in\mathcal{N}}\eta^n_{u_s}S^n_{u_sb_s}\right\} \tag{34a}$$

$$\text{S.t.: } \mathbb{E}\left\{\sum_{n\in\mathcal{N}}\eta^n_{u_s}p^n_{u_sb_s}\right\}\le\bar{P}^{\max}_{u_s}, \qquad \forall u_s\in\mathcal{U}_s, \tag{34b}$$

$$\mathbb{E}\left\{\sum_{u_s\in\mathcal{U}_s}\eta^n_{u_s}p^n_{u_sb_s}g^n_{u_su_p}\right\}\le\bar{\Gamma}^n_{u_p}, \qquad \forall n\in\mathcal{N}, u_p\in\mathcal{U}_p, \tag{34c}$$

$$\sum_{u_s\in\mathcal{U}_s}\eta^n_{u_s}=1, \qquad \forall n\in\mathcal{N}. \tag{34d}$$

The preceding problem can be solved via dual decomposition method. We associate dual variables λ_{u_s} with constraints (34b) and $\vartheta^n_{u_s}$ with constraints (34c).

D. Signaling Overhead

The transmitters should know about their power and subcarrier assignments. Hence, prior to each downlink phase, the signaling information has to be transmitted. We assume that a separate signaling phase is introduced prior to the downlink phase. During this signaling phase, the signaling information is transmitted on all subcarriers using a predefined modulation/coding combination (which can transmit $b_{\rm sig}$ bits per symbol).

TABLE I
SIGNALING OVERHEAD

Approach	Conventional approach	Proposed approach	No. of bits for each variable
Variables	$p^n_{u_sb_s}$	$p^m_{b_pu_{\rm cs}}, p^n_{u_{\rm cs}u_p}, p^n_{u_sb_s}$	6
	$\eta^n_{u_s}, h^n_{u_sb_s}, h^n_{u_{\rm cs}u_p}$	$\eta^n_{u_s}, \rho^{mn}_{u_{\rm cs}u_p}, h^m_{b_pu_{\rm cs}}, h^n_{u_{\rm cs}u_p}, h^n_{u_sb_s}$	6
	$\lambda_{u_s}, \vartheta^n_{u_s}$	$\lambda_0, \lambda_{u_s}, \theta_{u_p}$	3

Denote the number of OFDM symbols required for the transmission of the signaling information by ς. We assume that, for the signaling phase and the downlink phase, a total of S symbols is available. The less the time consumed for the transmission of the signaling information is, the more time is available for the payload transmission. The value of ς depends on the binary representation of the assignments. The basic information unit describing an assignment consists of three factors: power allocation, subcarrier assignment, and Lagrange multipliers [44]. Table I illustrates the required information exchange between the different entities of the network for solving the optimization problem with the conventional approach and the proposed iterative algorithm. It is shown that the conventional approach results in a significant reduction in signaling overhead compared with the proposed approach, particularly when the number of users in the network is large.

VI. Other Allocation Schemes

Treating some optimization variables separately, we provide a number of suboptimal subcarrier and power allocation strategies for the proposed scheme that have low complexity.

A. Equal Power Allocation Scheme

Here, we assume that the power is equally distributed on the subcarriers at each node. When equal power allocation (EPA) strategy is adopted, each subcarrier m or n has the same power, i.e., $[p^m_{u_sb_s}]^i=\bar{P}^{\max}_P/N, \forall i=1,\dots,N$, $[p^n_{u_su_p}]^i=\bar{P}^{\max}_{u_s}/N$, $\forall i=1,\dots,N$, and $[p^n_{u_sb_s}]^i=\bar{P}^{\max}_{u_s}/N, \forall i=1,\dots,N$, where N is the number of subcarriers. In other words, regardless of the channel state for each subcarrier, EPA equally allocates each node power to the subcarrier in two time slots; thus, the performance of adopting EPA cannot do better than our proposed allocation.

B. Greedy Subcarrier Allocation Scheme

Here, we propose a suboptimal algorithm with low complexity for subcarrier allocation. In the first hop, for each subcarrier m and each link, i.e., from the PBS to $u^{\rm th}_{\rm cs}$, we consider $h^m_{b_pu_{\rm cs}}, \forall u\in\mathcal{U}, m\in\mathcal{N}$, and we follow a greedy scheme [45]. In other words, the subcarrier m is assigned to the link that has the maximum value of $h^m_{b_pu_{\rm cs}}$. More precisely, the allocation is performed by $u^*_{\rm cs}=\arg\max_{u_{\rm cs}}h^m_{b_pu_{\rm cs}}$. In the second hop, for each subcarrier n and each link, i.e., from $u^{\rm th}_s$ to the SBS and from $u^{\rm th}_{\rm cs}$ to $u^{\rm th}_p$, we consider $h^n_{u_sb_s}, \forall u_s\in\mathcal{U}_s, n\in\mathcal{N}$ and $h^n_{{\rm cs}u_p}, \forall u_p\in\mathcal{U}_p, n\in\mathcal{N}$, respectively. Then, the subcarrier n is assigned to the link that has the maximum value $h^n_{u_sb_s}$ or $h^n_{u_{\rm cs}u_p}$, i.e., $(u^*_s, u^*_p)=\arg\max_{u_s,u_p}\min(h^n_{u_sb_s}, h^n_{u_{\rm cs}u_p})$.

TABLE II
COMPUTATIONAL COMPLEXITY

Approach	Dual problem complexity	Subcarrier allocation complexity	Total complexity
Conventional approach	$O\left(\frac{(NU_s)(U_s+NU_p)^2}{\delta^2}\right)$	$O(NU_s)$	$O\left(\frac{(NU_s)^2(U_s+NU_p)^2}{\delta^2}\right)$.
Proposed approach	$O\left(\frac{(U_s+U_p+1)(NU_s)^2}{\delta^2}\right)$	$O(2NU_s(1+NU_p))$	$O\left(\frac{2(1+NU_p)(U_s+U_p+1)(NU_s)^3}{\delta^2}\right)$.

C. Computational Complexity

Here, we analyze the complexity of the proposed optimal scheme. The computational complexity of the proposed optimal scheme is mainly determined by the complexity of solving the dual problem. The complexity of the ellipsoid method is polynomial in the number of dual variables and optimization variables. Considering the individual power constraint for the SUs and the sum power constraint for the PBS and the sum rate constraint for the PN, the number of the dual variables is obtained as $U_{\acute{s}} + U_p + 1$. Indeed, by considering optimal power allocation for each PU on each subcarrier, the number of the power optimization variables can be found as $NU_{\acute{s}}$.

The number of iterations required to achieve δ-optimality, i.e., $g - g^* < \delta$, is on the order of $O(1/\delta^2)$. Hence, the required iteration number does not depend on the number of variables. Therefore, the complexity related to the ellipsoid method is $O((U_{\acute{s}} + U_p + 1)(NU_{\acute{s}})^2/\delta^2)$ [46], [47]. The complexity of the ellipsoid method for the conventional scheme is polynomial in the number of dual variables and optimization variables. Considering the individual power constraint for SUs and the individual interference threshold constraints for each PU on each subcarrier, the number of the dual variables is obtained as $U_{\acute{s}} + NU_p$. In addition, by considering optimal power allocation for each PU on each subcarrier, the number of the power optimization variables can be determined as $NU_{\acute{s}}$. Therefore, the complexity related to the ellipsoid method for the conventional scheme is $O((NU_{\acute{s}})(U_{\acute{s}} + NU_p)^2/\delta^2)$ [46], [47].

The order of the subcarrier allocation complexity for each step, i.e., (26)–(29), is $O(N^2U_{\acute{s}}U_p)$, $O(N^2U_{\acute{s}}U_p)$, $O(NU_{\acute{s}})$, and $O(NU_{\acute{s}})$, respectively. Therefore, the total order of the complexity for subcarrier allocation is $O(2NU_{\acute{s}}(1 + NU_p))$. Thus, the total computational complexity is on the order of $O(2NU_{\acute{s}}(1 + NU_p)(U_{\acute{s}} + 2)^2)$. The complexity related to subcarrier allocation for the conventional scheme is $O(NU_{\acute{s}})$. Thus, the total computational complexity is on the order of $O(NU_{\acute{s}}(U_{\acute{s}}+NU_p)^2)$. The computational complexity is shown in Table II, with reference [47].

VII. SIMULATION RESULTS

Now, we evaluate the performance of the proposed scheme using simulations. The channels of the subcarriers are i.i.d. subject to Rayleigh fading. We assume equal noise power at the relay, the destination, and the eavesdropper nodes, i.e., $\sigma_p^2 = \sigma_s^2 = \sigma_e^2$. We also assess the performance of the proposed schemes assuming imperfect CDI. We also determine the number of observation data required to reach a performance close to that of perfect CDI. The nominal data can be generated using exponential distribution, and for generating the outlier data, we use Gaussian RV generation function with zero mean and unit variance, i.e., $\mathcal{N}(0, 1)$. For generating a random variable that has no explicit formula for inverse CDF, we use the acceptance/rejection method described in [24]. In our case, for both interference and secondary channels, the actual density $g(x)$ is assumed exponential with rate 1. The simulation parameters are listed in Table III.

TABLE III
SIMULATION SETUP

Number of realization	1000
Bandwidth	10 MHz
Average path loss	35.3+37.6 log(d)
Fading model	Rayleigh
Total number of subcarrier	64
Shadowing	Log-normal with 0-dB mean, and 8-dB standard deviation
Cell radius	1 km

A. Effect of the Number of Eavesdroppers on the Secrecy Rate of Secondary and Primary Networks

Fig. 3(a) depicts the total secrecy rate of the PN versus the number of PUs u_p, for different numbers of eavesdroppers E. As shown, by increasing the number of PUs, the total secrecy rate of the PN increases. It is shown in Fig. 3(a) that the total secrecy rate of the PN when the eavesdroppers use MRC is less than the case where MRC is not used. This is because, adopting MRC, the eavesdroppers can gather more information from legitimate users compared with the case when MRC is not used.

Fig. 3(b) depicts the total secrecy rate of the SN versus the number of SUs u_s for different numbers of eavesdroppers E. As shown, by increasing the number of SUs, the total secrecy rate of the SN increases. Note that increasing the number of eavesdroppers decreases the total secrecy rate since the eavesdroppers benefit from the increased multiuser diversity.

B. Effect of the Maximum Transmit Power

Fig. 4(a) depicts the total secrecy rate of the SN as a function of the maximum transmit power of the SUs. As shown, the increase in the maximum transmit power of the SUs results in an enhanced performance increasing in terms of the total secrecy rate of the SN. Fig. 4(a) shows the efficiency of the proposed resource-allocation algorithm. An exhaustive search method is employed to locate the optimal resource allocations for maximizing the total secrecy rate. From Fig. 4(a), we can find that our proposed algorithm achieves a performance very close to that of the exhaustive search method.

C. Effect of the Number of Secondary Users on the Secrecy Rate of the Primary Network

In Fig. 4(b), the total secrecy rate of the SN is plotted as functions of the total number of PUs U_p for different values of the minimum required secrecy rate of the PN, i.e., $\bar{R}_{u_p}^{\mathrm{SP}} = 2$, 4, 6, 8 bit/s/Hz, $\forall\, u_p \in \mathcal{U}_p$. This figure shows that increasing the number of PUs decreases the total secrecy rate of the SN.

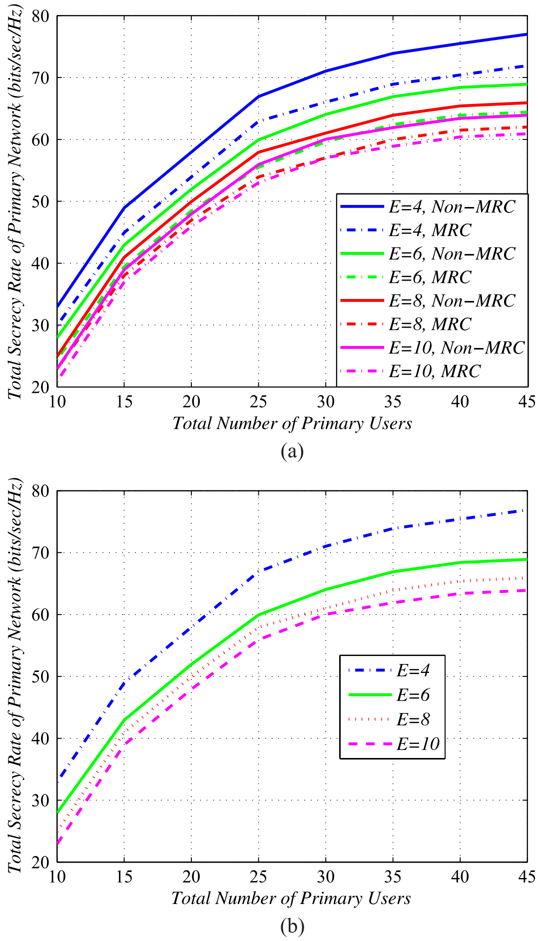


Fig. 3. (a) Total secrecy rate of the PN versus total number of PUs U_p, for different numbers of eavesdroppers E, for the non-MRC and MRC schemes. System parameters: $N = 128$, $U_s = 10$, $P_P^{\max} = 30$ dBm, $P_{u_s}^{\max} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}_{u_p}^{\text{SP}} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$. (b) Total secrecy rate of the SN versus total number of SUs U_s, for different numbers of eavesdroppers E, for the proposed scheme. System parameters: $N = 128$, $U_p = 10$, $P_P^{\max} = 30$ dBm, $P_{u_s}^{\max} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}_{u_p}^{\text{SP}} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$.

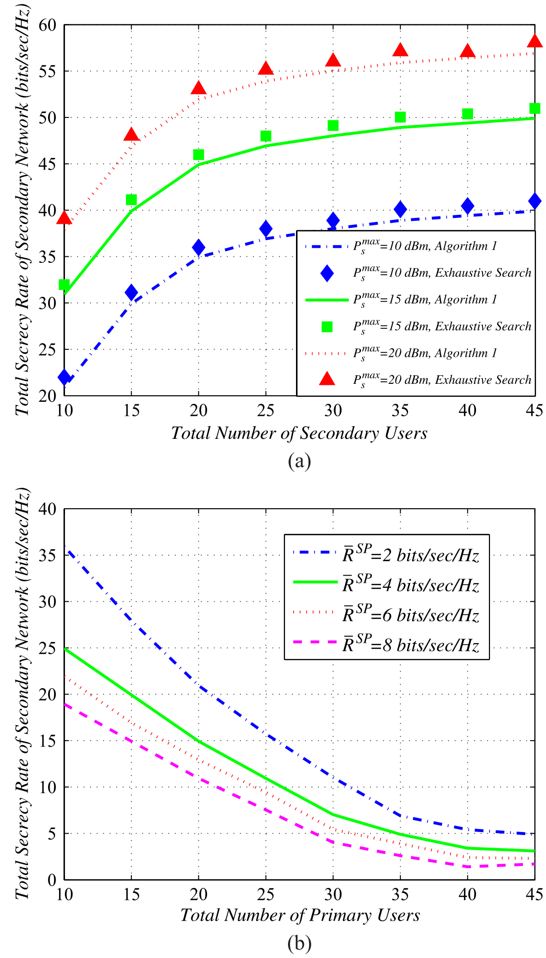


Fig. 4. (a) Total secrecy rate of the SN versus total number of SUs U_s, for different values of the maximum transmitted power at the SU, $P_{u_s}^{\max} = P_s^{\max}, \forall u_s \in \mathcal{U}_s$, for the proposed scheme. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P_P^{\max} = 30$ dBm, $\bar{R}_{u_p}^{\text{SP}} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$. (b) Total secrecy rate of the SN versus total number of PUs U_p, for different values of the minimum required secrecy rate of the PN, i.e., $\bar{R}_{u_p}^{\text{SP}}, \forall u_p \in \mathcal{U}_p$ for the proposed scheme. System parameters: $N = 128$, $U_s = 10$, $E = 4$, $P_P^{\max} = 30$ dBm, $P_{u_s}^{\max} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$.

D. Performance Comparison Between the Proposed Paradigm and the Conventional Underlay Approach

In conventional cognitive radio, maximizing the total secrecy rate of the SN is subject to the interference threshold constraint. Meanwhile, it is important to see whether using the new constraint causes the total secondary secrecy rate to decrease compared with the conventional case. To be able to make a fair comparison, we consider the following framework. For both scenarios, we assume that the CSI value corresponding to any transmitter and receiver pair is equal for both cases. The CSI values are picked up randomly from a normalized Rayleigh distribution. For a given set of CSI values, we fix the interference threshold and solve the conventional problem. We then obtain the maximized secondary secrecy rate. For such a setting, we also obtain the resulting primary secrecy rate. In Fig. 5(a), we have reported the values of the resulting primary secrecy rates versus the number of PUs for different values of interference threshold, i.e., $\Gamma_{u_p}^n = \Gamma$, $\forall n \in \mathcal{N}$, $\forall u_p \in \mathcal{U}_p$. Now, for different values of the primary secrecy rate reported in Fig. 5(b), we solve the proposed problem and obtain the corresponding secondary secrecy rate. We define η as the ratio of the secondary secrecy rate of the proposed scheme to that of the conventional scheme. In Fig. 5(b), we have plotted η versus the number of SUs. As shown in Fig. 5(b), the value of η is always greater than or equal to 1, implying that the new constraint always provides a superior secondary secrecy rate. In other words, we have been able to maintain the secrecy rate of the PU, and yet, such a benefit has come at no cost to the secondary secrecy rate. Moreover, as shown in Fig. 5(a), increasing the amount of tolerable interference threshold may cause the secrecy rate of the PU to decrease significantly. In such cases, changing the interference threshold constraint to the one that we proposed can guarantee a desired primary secrecy rate while providing a secondary secrecy rate equal or better than the conventional case. This is the benefit of considering both the PN and the SN simultaneously in a unified framework.

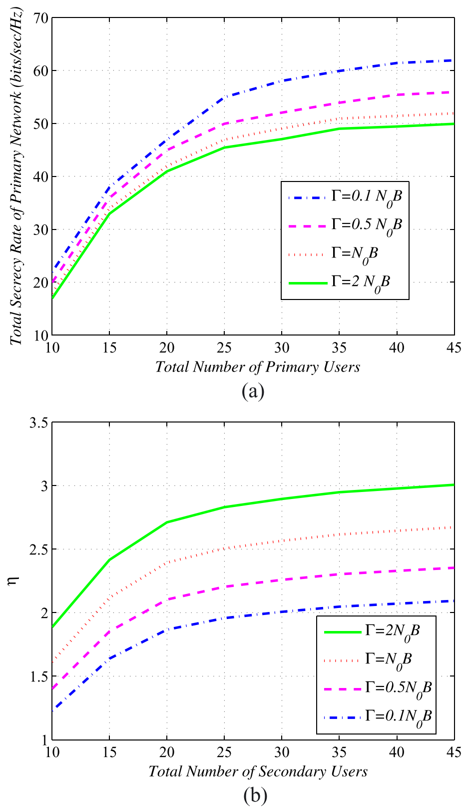


Fig. 5. (a) Total secrecy rate of the PN versus total number of PUs U_p, for different values of interference threshold, $\Gamma^n_{u_p} = \Gamma, \forall n \in \mathcal{N}, u_p \in \mathcal{U}_p$, for the conventional scheme. System parameters: $N = 128$, $U_s = 10$, $E = 6$, $P^{\max}_P = 30$ dBm, $P^{\max}_{u_s} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}^{\rm SP}_{u_p} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$. (b) Comparison of the total secrecy rate of the SN of the proposed paradigm and the conventional underlay approach versus the total number of SUs U_s, for different values of interference threshold, $\Gamma^n_{u_p} = \Gamma, \forall n \in \mathcal{N}, u_p \in \mathcal{U}_p$. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P^{\max}_P = 30$ dBm, $P^{\max}_{u_s} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}^{\rm SP}_{u_p} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$.

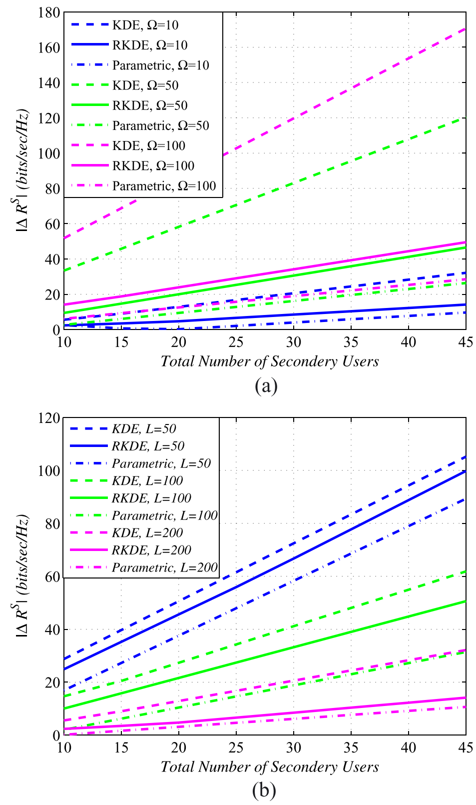


Fig. 6. (a) Difference between the total secrecy rate of the SUs based on the perfect and estimated CDI, $|\Delta R^S|$ versus the total number of SUs $\mathcal{U}_s$ for parametric and nonparametric (KDE, RKDE) estimation methods, and different numbers of outlier data, $\Omega^n_{u_s} = \Omega, \forall u_s \in \mathcal{U}_s, n \in \mathcal{N}$. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P^{\max}_P = 30$ dBm, $P^{\max}_{u_s} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}^{\rm SP}_{u_p} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$, $L^n_{u_s} = 200, \forall u_s \in \mathcal{U}_s, n \in \mathcal{N}$. (b) Difference between the total secrecy rate of the SU based on the perfect and estimated CDI, $|\Delta R^S|$ in $\mathcal{O}^{CN}$ versus the total number of SUs, $\mathcal{U}_s$, for parametric and nonparametric (KDE, RKDE) estimation methods, and different numbers of nominal data, $L^n_{u_s} = L, \forall u_s \in \mathcal{U}_s, n \in \mathcal{N}$. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P^{\max}_P = 30$ dBm, $P^{\max}_{u_s} = 15$ dBm, $\forall u_s \in \mathcal{U}_s$, $\bar{R}^{\rm SP}_{u_p} = 2$ bit/s/Hz, $\forall u_p \in \mathcal{U}_p$, $\Omega^n_{u_s} = 20, \forall u_s \in \mathcal{U}_s, n \in \mathcal{N}$.

E. Evaluation of the Impact of the Number of Nominal and Noisy Data on the Performance

We define $|\Delta R^S|$ as the absolute value of the difference between the total secrecy rate of the SN obtained based on the perfect and estimated CDI. The number of nominal data, i.e., $L^n_{u_s}$, is set to 200 for all cases.

1) Impact of the Number of Outlier Data: Fig. 6(a) shows $|\Delta R^S|$ versus the total number of SUs for different numbers of outlier data, i.e., $\Omega^n_{u_s} = \Omega$, $\forall u_s$, $\forall n$, where $L^n_{u_s} = 200$, $\forall u_s$, $\forall n$. As shown in the figure, the value of $|\Delta R^S|$ is close to zero for the RKDE method with $\Omega^n_{u_s} = \Omega = 10$, $\forall u_s, \forall n$. As Ω increases, $|\Delta R^S|$ increases, implying the divergence from the actual pdf. It is also observed that the value of $|\Delta R^S|$ for KDE is far away from zero and the performance degrades faster compared with that of RKDE as Ω increases.

2) Impact of the Number of Nominal Data: Fig. 6(b) shows the difference between the total secrecy rate of the SN obtained based on perfect and estimated CDI, i.e., $|\Delta R^S|$, as a function of the total number of SUs for different numbers of nominal data for cognitive networks, respectively. In Fig. 6(b), $\Omega^n_{u_s} = \Omega = 20$, $\forall u_s$, $\forall n$, and $L^n_{u_s} = L$, $\forall u_s$, $\forall n$. As shown in the figure, for $L = 10$, both the KDE and RKDE methods perform very poorly. As L increases, the performance of both methods improves, and for $L = 200$, the total secrecy obtained based on RKDE is very close to that of perfect CDI for the conventional network. There is a gap between the aforementioned total secrecy rate for the same reason as indicated in the previous subsection. To reduce this gap, we have to increase L.

3) Effect of Priority Coefficient on Fairness: Here, we study the impact of ϖ_{u_s} on the performance of the proposed scheme. We consider the case where two SUs exist in the network with $\varpi_1 = 1 - \varpi_2$. Fig. 7(a) demonstrates that, when $\varpi_1 = 1$, user 1 has a higher priority and user 2 cannot obtain any secrecy rate and vice versa. For $\varpi_1 = 0.5$, both users have the same priority. By adjusting $\varpi_1 = 1 - \varpi_2$, the priority and fairness between these users change.

4) Comparison of the Performance of the Proposed Schemes: In Fig. 7(b), we compare the performance of the proposed (optimal) solution with the schemes in Section VI. We observe that the optimal proposed solution gives a significantly higher total secrecy rate (better performance) than that of the other schemes. In addition, it can be also seen that increasing

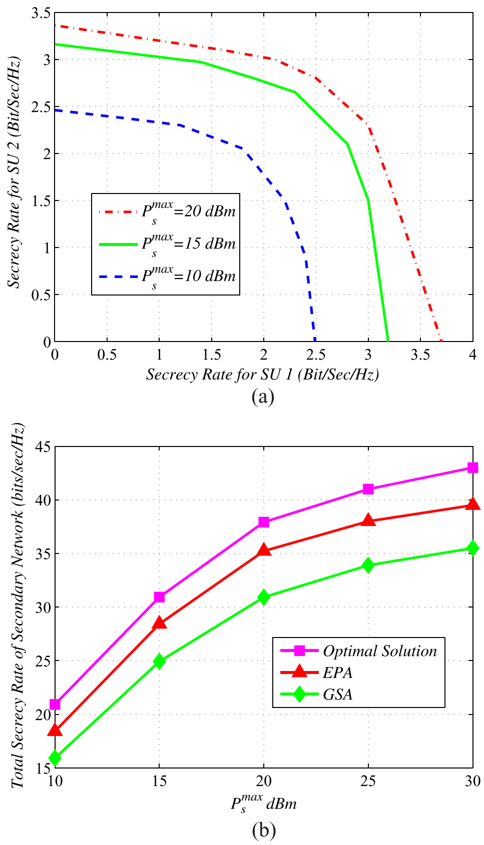


Fig. 7. (a) Secrecy rate for SU 2 versus secrecy rate for SU 1, for different values of maximum transmitted power at the SU, $P_{u_s}^{\max} = P_s^{\max}, \forall\, u_s \in \mathcal{U}_s$, for the proposed scheme. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P_P^{\max} = 30$ dBm, $\bar{R}_{u_p}^{\mathrm{SP}} = 2$ bit/s/Hz, $\forall\, u_p \in \mathcal{U}_p$. (b) Comparison of the total secrecy rate of the SN for different allocation schemes, namely, Optimal Solution, EPA, and GSA, for different values of maximum transmitted power of SUs, $P_{u_s}^{\max} = P_s^{\max}, \forall\, u_s \in \mathcal{U}_s$. System parameters: $N = 128$, $U_p = 10$, $E = 6$, $P_P^{\max} = 30$ dBm, $\bar{R}_{u_p}^{\mathrm{SP}} = 2$ bit/s/Hz, $\forall\, u_p \in \mathcal{U}_p$.

the total transmit power will increase the total secrecy rate. However, the EPA and GSA schemes always have a worse performance than the optimal proposed solution.

VIII. Conclusion

In this paper, we have proposed two cooperative communication schemes (MRC and non-MRC) for secure communication in CRNs where a set of eavesdroppers listen to the information transmission by the PBS and the SUs. In our model, SUs gain access to the network resources as a reward for cooperating to the PN as DF relays to improve the secrecy rate of the PN. We consider a more practical case where the CSI of the eavesdroppers is not available. We formulated our proposed scheme as an optimization problem, solved it using the dual Lagrange approach, and showed that the duality gap tends to zero as the number of subcarriers tends to infinity. We further studied the effect of imperfect CDI on the performance of our proposed scheme using parametric and nonparametric approaches. Using simulations, we studied the efficiency of our proposed scheme in various situations, which showed that the performance of the proposed scheme is better than that of the conventional scheme. As a future work, we will extend our experimental study to multiple-input–multiple-output technology.

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. Li and A. Nosratinia, "Hybrid opportunistic scheduling in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 328–337, Jan. 2012.

[3] Z. Shi, T. Tan, K. C. Teh, and K. H. Li, "Energy efficient cognitive radio network based on multiband sensing and spectrum sharing," *IET Commun.*, vol. 8, no. 9, pp. 1499–1507, Jun. 2014.

[4] O. Simeone *et al.*, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 203–213, Jan. 2008.

[5] W. D. Lu, Y. Gong, S. H. Ting, X. L. Wu, and N. T. Zhang, "Cooperative OFDM relaying for opportunistic spectrum sharing: Protocol design and resource allocation," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2126–2135, Jun. 2012.

[6] A. Zarrebini-Esfahani and M. R. Nakhai, "Secondary spectrum access and cell-edge coverage in cognitive cellular networks," *IET Commun.*, vol. 6, no. 8, pp. 845–851, May 2012.

[7] S. M. M. Toroujeni, S. M.-S. Sadough, and S. A. Ghorashi, "Spectrum leasing for OFDM-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2131–2139, Jun. 2013.

[8] W. Liang, S. X. Ng, and L. Hanzo, "Cooperative communication between cognitive and primary users," *IET Commun.*, vol. 7, no. 17, pp. 1982–1992, Nov. 2013.

[9] J. He, C. Xu, and L. Li, "Power saving for cooperative spectrum sharing-based cognitive radios under primary user short-term rate protection," *IET Commun.*, vol. 6, no. 9, pp. 1097–1103, Jun. 2012.

[10] T. Jing *et al.*, "Cooperative relay selection in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1872–1881, May 2015.

[11] M. Tao and Y. Liu, "Spectrum leasing and cooperative resource allocation in cognitive OFDMA networks," *J. Commun. Netw.*, vol. 15, no. 1, pp. 102–110, Feb. 2013.

[12] W. Lu and J. Wang, "Opportunistic spectrum sharing based on full-duplex cooperative OFDM relaying," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 241–244, Feb. 2014.

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

[14] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[15] B. Han, J. Li, and J. Su, "Optimal relay assignment for secrecy capacity maximization in cooperative ad-hoc networks," in *Proc. IEEE ICC*, Budapest, Hungary, Jun. 2013, pp. 6128–6132.

[16] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Veh. Technol.*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[17] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[18] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative spectrum access toward secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.

[19] H. Jeon, S. W. McLaughlin, I.-M. Kim, and J. Ha, "Secure communications with untrusted secondary nodes in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 1790–1805, Apr. 2014.

[20] K. Lee, O. Simeone, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Nov. 2013.

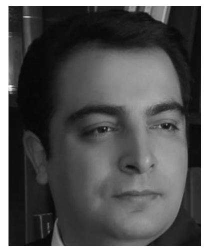
[21] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[22] H. Zhang, H. Xing, X. Chu, A. Nallanathan, and X. W. W. Zheng, "Secure resource allocation for OFDMA two-way relay networks," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, Dec. 2012, pp. 3649–3654.

[23] J. Kim and C. Scott, "Robust kernel density estimation," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, Las Vegas, NV, USA, Apr. 2008, pp. 3381–3384.
[24] N. Mokari, M. R. Abedi, H. Saeedi, and P. Azmi, "Ergodic radio resource allocation based on imperfect channel distribution information," in *Proc. IEEE WCNC*, Istanbul, Turkey, Apr. 2014, pp. 1438–1443.
[25] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X. Wang, and T. Q. S. Quek, "Resource allocation for cognitive small cell networks: A cooperative Bargaining game theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3481–3493, Feb. 2015.
[26] H. Zhang, C. Jiang, X. Mao, and H.-H. Chen, "Interference-limited resource optimization in cognitive femtocells with fairness and imperfect spectrum sensing," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1761–1771, Mar. 2016.
[27] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X. Wen, and M. Tao, "Resource allocation in spectrum-sharing OFDMA femtocells with heterogeneous services," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2366–2377, Jul. 2014.
[28] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[29] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.
[30] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.
[31] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.
[32] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
[33] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[34] N. Mokari and K. Navaie, "Radio resource allocation in OFDM-based cooperative relaying networks for a mixture of elastic and streaming traffic," *IET Commun.*, vol. 5, no. 8, pp. 1083–1089, May 2011.
[35] T. Wang, Y. Fang, and L. Vandendorpe, "Power minimization for OFDM transmission with subcarrier-pair based opportunistic DF relaying," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 471–474, Mar. 2013.
[36] M. S. Alam, J. W. Mark, and X. S. Shen, "Relay selection and resource allocation for multi-user cooperative OFDMA networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2193–2205, May 2013.
[37] X. Zhang *et al.*, "Optimizing network sustainability and efficiency in green cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1129–1139, Feb. 2014.
[38] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[39] A. Meister, *Deconvolution Problems in Nonparametric Statistics*, 1st ed. Berlin, Germany: Springer-Verlag, vol. 112, 2009.
[40] S. J. Sheather, "Density estimation," *Statist. Sci.*, vol. 19, no. 4, pp. 588–597, 2004.
[41] V. C. Raykar, "Probability density function estimation by different methods," in *Proc. ENEE 739Q Spring Course Assignment 1 Rep.*, 2002, pp. 1–8.
[42] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.
[43] T. Wang and L. Vandendorpe, "Sum rate maximized resource allocation in multiple DF relays aided OFDM transmission," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1559–1571, Sep. 2011.
[44] D. W. K. Ng and R. Schober, "Resource allocation and scheduling in multi-cell OFDMA systems with decode-and-forward relaying," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2246–2258, Jul. 2011.
[45] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed. Cambridge, MA, USA: MIT Press, 2009.
[46] S. Boyd, "Convex optimization II," EE364B Course Note, Stanford University, Stanford, CA, USA, 2006. [Online]. Available: http://www.stanford.edu/class/ee364b/
[47] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, "Limited rate feedback scheme for resource allocation in secure relay-assisted OFDMA networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2604–2618, Apr. 2016.

Mohammad Reza Abedi received the M.Sc. degree in electrical engineering from Amirkabir University of Technology, Tehran, Iran.

He is currently a Research Assistant with Tarbiat Modares University, Tehran. His research interests include wireless communications radio resource allocations and cooperative and spectrum sharing.



Nader Mokari received the Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2014.

In October 2015, he joined the Department of Electrical and Computer Engineering, Tarbiat Modares University, as an Assistant Professor. He was also involved in a number of large-scale network design and consulting projects in the telecom industry. His research interests include design, analysis, and optimization of communications networks.

Mohammad Reza Javan (S'10–M'14) received the B.Sc. degree from Shahid Beheshti University, Tehran, Iran, in 2003; the M.Sc. degree from Sharif University of Technology, Tehran, in 2006; and the Ph.D. degree from Tarbiat Modares University, Tehran, in 2013, respectively, all in electrical engineering.

He is currently a Faculty Member with the Department of Electrical Engineering, Shahrood University of Technology, Shahrood, Iran. His research interests include the design and analysis of wireless communication networks, with emphasis on the application of optimization theory.

Halim Yanikomeroglu (S'96–M'98–SM'12) was born in Giresun, Turkey, in 1968. He received the B.Sc. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, in 1990 and the M.A.Sc. degree in electrical engineering (now electrical and computer engineering) and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1992 and 1998, respectively.

During 1993–1994, he was with the Research and Development Group, Marconi Komunikasyon A.S., Ankara. Since 1998, he has been with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where he is currently a Full Professor. He spent the academic year 2011–2012 at TOBB University of Economics and Technology, Ankara, as a Visiting Professor. His research interests include various aspects of wireless technologies, with emphasis on wireless networks. In recent years, his research has been funded by Huawei, Telus, Blackberry, Samsung, Communications Research Centre Canada (CRC), DragonWave, Allen Vanguard, and Nortel. This collaborative research resulted in over 25 patents (granted and applied).

Dr. Yanikomeroglu is a Distinguished Lecturer of the IEEE Communications and the IEEE Vehicular Technology Societies. He has been involved in the organization of the IEEE Wireless Communications and Networking Conference (WCNC) from its inception, including serving as a Steering Committee Member and the Technical Program Chair or Cochair of WCNC 2004 (Atlanta), WCNC 2008 (Las Vegas), and WCNC 2014 (Istanbul). He was the General Cochair of the IEEE Vehicular Technology Conference in Fall 2010 held in Ottawa. He has served on the editorial boards of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and *IEEE Communications Surveys and Tutorials*. He was the Chair of the IEEE's Technical Committee on Personal Communications (now called Wireless Technical Committee). He received the Carleton University Research Achievement Award in 2009, the Carleton University Graduate Students Association Excellence Award in Graduate Teaching in 2010, the Carleton University Faculty Graduate Mentoring Award in 2010, and the IEEE Ottawa Section Outstanding Educator Award in 2014. He is also a registered Professional Engineer in the Province of Ontario, Canada.