Cooperative Secure Resource Allocation in Cognitive Radio Networks with Guaranteed Secrecy Rate for Primary Users

Nader Mokari, Saeedeh Parsaeefard, Hamid Saeedi, and Paeiz Azmi

***Abstract*—In this paper, we introduce a new cooperative paradigm for secure communication in cognitive radio networks (CRNs) where secondary users (SUs) are allowed to access the spectrum of primary users (PUs) as long as they preserve the secure communication of PUs in the presence of malicious eavesdroppers. To do so, the SU transmission is divided into two hops: at first hop, the SU transmitter sends the information to a relay set and the SU receiver acts as a friendly jammer to disturb the overhearing of eavesdroppers and at the second hop, one of the relays is selected to pass the information to the SU receiver and the SU transmitter acts as a friendly jammer for the PU. In this new setup, the time duration for each hop, the power transmissions of all nodes in CRN, and relay selection at the second hop are allocated in such a way that the secrecy rate of the SU is maximized subject to the minimum required PU's secrecy rate. From primary service perspective, this transforms the possibly disturbing secondary service activities into a beneficial network element. We investigate instantaneous and ergodic resource allocation problems for perfect and imperfect channel state information (CSI). Since these problems are non-convex, we propose a solution based on decomposition of main optimization problem into three subproblems related to the power allocation, time allocation, and relay selection. We show that the power allocation problem can be transformed into a generalized geometric programming (GGP) model via the so-called scaled algorithm and it can be solved very efficiently. Simulation results indicate that in terms of the secondary secrecy rate, the proposed setup outperforms the conventional setup in which the secrecy rate of the PU is not guaranteed.**

***Index Terms*—Cognitive radio networks, ergodic and instantaneous resource allocation, generalized geometric programming (GPP), secure communication.**

I. Introduction

SPECTRUM sharing through cognitive radio networks (CRNs) is a promising approach to increase the spectrum efficiency for next generation of wireless communication networks [1] where the unlicensed/secondary users (SUs) are allowed to access the spectrum of primary users (PUs) subject to maintaining the quality of service (QoS) of PUs. One common model in this context is the underlay approach where the SUs can simultaneously utilize the licensed spectrum of PUs if the resulting interference on the PUs' receivers is kept under a predefined threshold.

Similar to any wireless network, security against overhearing of the third parties, referred to as eavesdroppers, is one of the important issues in CRNs. Recently, physical layer security introduced by [2], is drawing a lot of attentions in which the objective is to maximize the secrecy rate defined as the achievable rate from the transmitter to the legitimate receiver minus the rate overheard by eavesdropper. Obviously, when the channel gain between transmitter and its corresponding receiver is less than the channel gain between transmitter and eavesdropper, the secrecy rate is equal to zero.

For non-cognitive networks, achieving a non-zero secrecy rate is studied from different aspects in non-cooperative [3] as well as cooperative frameworks including cooperative relaying [4], cooperative jamming [5], and jointly cooperative jamming and relaying [6]. Cooperative jamming, also known as friendly jamming, creates interference by legitimate network nodes, transmitting noise [7], [8] or codewords [9], [10], so as to impair the eavesdroppers ability to decode the confidential information, and thus, increase secure communication rates between each legitimate transmitter and receiver. This problem in cognitive case has been considered in [8], [11]–[17]. Information theoretic aspect of secrecy rate are addressed in [11], [12] where the effect of trustworthy SUs to increase the secrecy rate of PU is investigated. Resource allocation (RA) problems to maximize the secondary secrecy rate underlay approach in different MIMO transmission modes are investigated in [13]–[15]. A similar study in a cooperative relaying framework has been proposed in [16]. The effect of friendly jammer in the underlay cognitive radio network was studied in [8]. In [17], the secrecy rate of PU is maximized in MIMO channels subject to the minimum required shannon rate of SU.

In RA problems associated to [13]- [17], the objective is to provide secure transmission for either primary or secondary users subject to the imposed constraints by PUs and in particular, interference threshold constraint in underlay schemes. However, in CRNs, secure communication for both PUs and SUs is of high importance and previously proposed settings do not accommodate secure communications for both primary and secondary users. In this paper, we propose a cooperative paradigm for secure communication in CRNs in which secure communications for both primary and secondary services are simultaneously provided. This goal is achieved by

Manuscript received May 22, 2013; revised September 16, 2013; accepted November 5, 2013. The associate editor coordinating the review of this paper and approving it for publication was R. Zhang.

The authors are with the Department of Electrical and Computer Engineering, Tarbiat Modares University, P. O. Box 14115-194, Tehran, Iran (e-mail: {nader.mokari, parsaeefard, hsaeedi, pazmi}@modares.ac.ir). The corresponding author is H. Saeedi.

This work was supported Iran Telecommunications Research Center (ITRC) under research grant T/500/19232-90/12/28.

Digital Object Identifier 10.1109/TWC.2013.010214.130929

taking advantage of the interference caused by the secondary user activity to reduce the primary service overhearing by the eavesdroppers. From primary service perspective, this transforms the possibly disturbing secondary service activities into a beneficial network element.

The RA problem for the proposed setup is written as an optimization problem with the objective of maximizing the SU's secrecy rate subject to guaranteeing a given PU's secrecy rate. It can be seen that the feasibility set of this problem highly depends on the channel gains, referred to as channel state information (CSI) between network nodes, i.e., the PU, the SU and eavesdroppers, as well as the required primary secrecy rate. Consequently, there is a good chance that the RA problem is not feasible meaning that the secondary secrecy rate is zero.

To make the problem feasible, we propose to expand the feasibility set by deploying relays within the secondary network. Then, at any primary service transmission period, the transmission of SU is done in two hops. In the first hop, the secondary transmitter (ST) sends the information to the set of relays and the secondary receiver (SR) acts as a friendly jammer to interfere the overhearing of eavesdroppers. In the second hop, one of the relays is selected to transmit the information to the SR and the ST acts as a friendly jammer. This setup can be considered as a joint cooperative jamming and relaying scheme where the RA problem includes power allocation of all nodes (i.e., the ST, the SR and relays), relay selection for the second hop, and time allocation for each hop. We show that the expansion of the feasibility set results in higher chance of having a non-zero secondary secrecy rate while maintaining a given primary secrecy rate.

The proposed RA problem is non-convex and we apply the scaled algorithm in [18] to transform it into a convex one with respect to each set of variables. We show that this transformation can be represented as a generalized geometric programing (GGP) problem which can be solved very efficiently using existing approaches such as interior-point algorithms [19]. We consider two cases of RA problems: Instantaneous resource allocation (IRA) and ergodic resource allocation (ERA). In the former case, we assume the availability of perfect CSI between any transmitter and receiver within the network. Consequently, for each new set of CSI values, the IRA problem has to be solved [20]. In the latter case, allocations are made based on the long term channel distribution information (CDI). Apparently, ERA exhibits a less computational complexity compared to that of IRA. However, the drawback of ERA is that we can guarantee a secrecy rate for PUs only in average sense not instantaneously, meaning that there exists the probability that the secrecy rate of PU is below than its predefined threshold called outage probability of primary secrecy rate. To deal with this issue, we introduce a modified ERA problem where the outage probability of primary secrecy rate can be kept below any value of interest.

The last challenge for our setup is the assumption of availability of perfect values of CSI between different nodes of the network is not realistic, mainly due to the existence of malicious eavesdroppers which are not supposed to cooperate with SUs and PUs to provide the CSI values. We approach this challenge by considering imperfect values for CSI and propose the robust counterparts of the RA problems. For the IRA problem, we apply the worst case robust optimization to guarantee the PU's secrecy rate under any condition of error. For The ERA problem, we show that the marginal channel distribution can be used to tackle the uncertainty [21], [22].

An important aspect of the proposed paradigm is that replacing the conventional interference threshold constraint by the primary secrecy rate constraint not only does not decrease the secondary secrecy rate with respect to the conventional case, but can also provide significantly higher secondary secrecy rate.

The rest of this paper is organized as follows. In Section II, the system model is discussed in details. In Section III, the RA problem is introduced and the solution of IRA is presented. Section IV includes two cases of ERA followed by Section V, where the imperfect CSI is considered for both IRA and ERA. Section IV provides simulation results and Section IIV concludes the paper.

II. Network Setup

A. System Model

We consider an interference limited CRN in which there exist a primary network with single transmitter and receiver, a trustworthy secondary network, and a set of eavesdropping malicious nods i.e., $\mathcal{E} = \{1, \cdots, E\}$, which attempt to overhear the primary and secondary messages. The primary transmitter (PT) wants to send confidential data to its corresponding receiver in its own available spectrum B. The primary network allows the ST to access its spectrum as long as the secrecy rate between PT and primary receiver (PR) is higher than a predefined threshold donated by $\mathrm{C}_{\min}^{\mathrm{PT}\rightarrow\mathrm{PR}}$.

In our system model, we assume decode and forward (DF) relaying strategy where the relay nodes are assumed to operate in half-duplex mode, i.e., they do not transmit and receive simultaneously in the same frequency band. Accordingly, the transmission between the secondary transmitter and receiver occurs in two hops: in the *first hop*, the ST transmits data to the selected relay node; and in the *second hop*, the selected relay node sends data to the SR.

The secondary transmitter enjoys this opportunity to transmit messages securely to the secondary receiver, where the secondary network consists of a ST and its corresponding SR, and a set of intermediate nodes i.e., $\mathcal{R} = \{1, \cdots, R\}$.

The intermediate nodes help the ST to transmit the data into the SR as a relay set, as shown in Fig. 1. Accordingly, the transmission between the ST and the SR occurs in two hops:

- **First hop**: Transmission from the ST to relays with duration T_1 where the SR acts as a friendly jammer for the primary service to interfere with eavesdropper's overhearing.
- **Second hop**: Transmission from one selected relay to the SR with duration T_2 where $T = T_1 + T_2$ is the transmission period of the primary service and the ST acts as a friendly jammer for the PT to decrease the eavesdroppers rate.

For both hops, the transmit power of the PT is fixed to P_{PT}. The maximum power of the ST and SR are equal to $\mathrm{P}_{\max}^{\mathrm{ST}}$ and $\mathrm{P}_{\max}^{\mathrm{SR}}$,

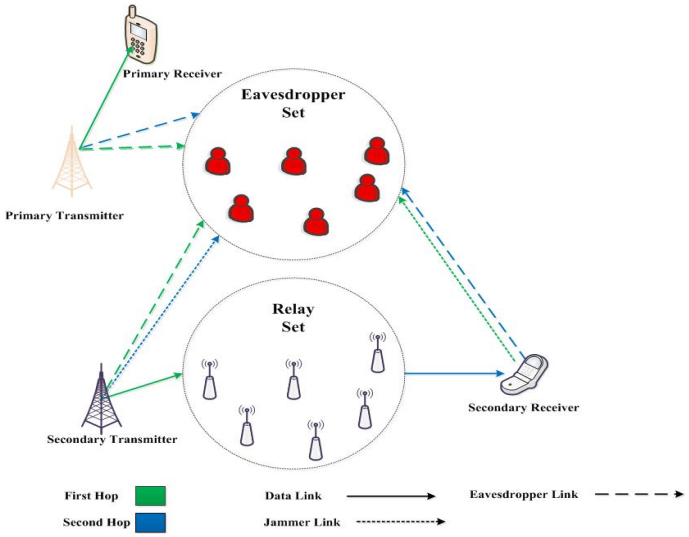

Fig. 1. System model of cooperative CRN with secure transmission.

TABLE I
NOTATIONS OF CSI VALUES BETWEEN EACH TRANSMITTER AND RECEIVER IN OUR SETUP.

Symbol	Description
$h_{\text{PT}\to\text{PR}}$	The CSI between PT and PR
$h_{\text{PT}\to e}$	The CSI between PT and eavesdropper e
$h_{\text{PT}\to r}$	The CSI between PT and relay r
$h_{\text{PT}\to\text{ST}}$	The CSI between PT and ST
$h_{\text{PT}\to\text{SR}}$	The CSI between PT and SR
$h_{\text{ST}\to\text{PR}}$	The CSI between ST and PR
$h_{\text{ST}\to e}$	The CSI between ST and eavesdropper e
$h_{\text{ST}\to r}$	The CSI between ST and relay r
$h_{\text{ST}\to\text{PT}}$	The CSI between ST and PT
$h_{\text{ST}\to\text{SR}}$	The CSI between ST and SR
$h_{\text{SR}\to\text{PR}}$	The CSI between SR and PR
$h_{\text{SR}\to e}$	The CSI between SR and eavesdropper e
$h_{\text{SR}\to r}$	The CSI between SR and relay r
$h_{\text{SR}\to\text{PT}}$	The CSI between SR and PT
$h_{\text{SR}\to\text{ST}}$	The CSI between SR and ST
$h_{r\to\text{PR}}$	The CSI between relay r and PR
$h_{r\to e}$	The CSI between relay r and eavesdropper e
$h_{r\to\text{PT}}$	The CSI between relay r and PT
$h_{r\to\text{SR}}$	The CSI between relay r and SR

respectively and $\mathbf{p}_{\text{max}}^{\text{Relay}} = [\text{p}_{\text{max}}^1, \cdots \text{p}_{\text{max}}^R]$ denotes the vector of maximum transmit power of all relay nodes where p_{max}^r is the maximum transmit power of relay r.

Throughout this paper, the superscripts 1 and 2 are utilized for any parameters in the first and second hops and $m \to n$ is used to denote a correspondence between a transmitter named m and a receiver named n. Accordingly, for transmission from transmitter m to receiver n, $\gamma_{m\to n}^i$ and $c_{m\to n}^i$ denote the corresponding SINR and secrecy rate where superscript $i \in \{1, 2\}$ shows the transmission occurs in hop i. We also assume that N_0B is the white gaussian noise power over bandwidth B which is equal for all users in CRN. Also, $h_{m\to n}$ denotes the CSI between transmitter m and receiver n which is assumed to be fixed during one transmission period. For the case of imperfect CSI, $h_{m\to n}$, $\bar{h}_{m\to n}$ and $\hat{h}_{m\to n}$ show the exact, estimated and error value of the CSI between transmitter m and receiver n. When the CSI is perfect, $h_{m\to n} = \bar{h}_{m\to n}$. The corresponding gain notations are summarized in Table I.

B. First hop

At the first hop, the SINR of the PR is computed as

$$\gamma_{\text{PT}\to\text{PR}}^1(\boldsymbol{p}^1) = \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{PR}}}{N_0B + I_{\text{PR}}^1}, \tag{1}$$

where $\boldsymbol{p}^1 = [p_{\text{ST}}^1, p_{\text{SR}}^1]$ in which p_{ST}^1 is the transmit power of the ST and p_{SR}^1 is the transmit power of the SR at the first hop when it acts as a jammer for eavesdroppers; and I_{PR}^1 is the induced interference in the PR, which is equal to $I_{\text{PR}}^1 = I_{\text{SR}\to\text{PR}}^1 + I_{\text{ST}\to\text{PR}}^1 = p_{\text{SR}}^1 h_{\text{SR}\to\text{PR}} + p_{\text{ST}}^1 h_{\text{ST}\to\text{PR}}$. Similarly, SINR for the first hop at eavesdropper e is equal to

$$\gamma_{\text{PT}\to\text{e}}^1(\boldsymbol{p}^1, e) = \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{e}}}{N_0B + I_{\text{PT}\to\text{e}}^1}, \tag{2}$$

where $I_{\text{PT}\to\text{e}}^1 = I_{\text{SR}\to\text{e}}^1 + I_{\text{ST}\to\text{e}}^1 = p_{\text{SR}}^1 h_{\text{SR}\to\text{e}} + p_{\text{ST}}^1 h_{\text{ST}\to\text{e}}$. In this hop, the secrecy rate of PU is equal to

$$c_{\text{PT}\to\text{PR}}^1(\boldsymbol{p}^1) = \min_e \left\{ c_{\text{PT}\to\text{PR}}^1(\boldsymbol{p}^1, e) \right\}, \tag{3}$$

where

$$c_{\text{PT}\to\text{PR}}^1(\boldsymbol{p}^1, e) = \frac{T_1}{T_1 + T_2} \times \left[\log_2(1 + \gamma_{\text{PT}\to\text{PR}}^1(\boldsymbol{p}^1)) - \log_2(1 + \gamma_{\text{PT}\to\text{e}}^1(\boldsymbol{p}^1, e)) \right]^+.$$

Simultaneously in the secondary network, the ST sends the data to all relay nodes and the SINR of relay r is

$$\gamma_{\text{ST}\to r}^1(\boldsymbol{p}^1, r) = \frac{p_{\text{ST}}^1 h_{\text{ST}\to r}}{N_0B + I_r^1}, \quad \forall r \in \mathcal{R}, \tag{4}$$

where $I_r^1 = I_{\text{SR}\to r}^1 + I_{\text{PT}\to r}^1 = p_{\text{SR}} h_{\text{SR}\to r} + \text{P}_{\text{PT}} h_{\text{PT}\to r}$, and the SINR received at the eavesdropper e is equal to

$$\gamma_{\text{ST}\to e}^1(\boldsymbol{p}^1, e) = \frac{p_{\text{ST}}^1 h_{\text{ST}\to e}}{N_0B + I_{\text{ST}\to e}^1}, \tag{5}$$

where $I_{\text{ST}\to\text{e}}^1 = I_{\text{SR}\to\text{e}}^1 + I_{\text{PT}\to\text{e}}^1 = p_{\text{SR}}^1 h_{\text{SR}\to\text{e}} + \text{P}_{\text{PT}} h_{\text{PT}\to\text{e}}$. Therefore, the secrecy rate of secondary user is

$$c_{\text{ST}\to r}(\boldsymbol{p}^1, r) = \min_{e\in\mathcal{E}} \left\{ c_{\text{ST}\to r}(\boldsymbol{p}^1, e) \right\},$$

where

$$c_{\text{ST}\to r}(\boldsymbol{p}^1, r, e) = \frac{T_1}{T_1 + T_2} \times \left[\log_2(1 + \gamma_{\text{ST}\to r}^1(\boldsymbol{p}^1, r)) - \log_2(1 + \gamma_{\text{ST}\to e}^1(\boldsymbol{p}^1, e)) \right]^+. \tag{6}$$

C. Second hop

In this phase, the SINR of the PR is equal to

$$\gamma_{\text{PT}\to\text{PR}}^2(\boldsymbol{p}^2, r) = \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{PR}}}{N_0B + I_{\text{PR}}^2(r)}, \tag{7}$$

where $\boldsymbol{p}^2 = [p_{\text{ST}}^2, \mathbf{p}_r^2]$ in which p_{ST}^2 is the transmit power of the ST in the second phase and $\mathbf{p}_r^2 = [p_1^2, \cdots, p_R^2]$ is the vector of transmit powers of relay nodes where p_r^2 is the transmit power of relay r at the second hop, and $I_{\text{PR}}^2(r) = I_{\text{ST}\to\text{PR}}^2 + I_{r\to\text{PR}}^2 = p_{\text{ST}}^2 h_{\text{ST}\to\text{PR}} + p_r^2 h_{r\to\text{PR}}$, for all $r \in \mathcal{R}$. The SINR at eavesdropper e is equal to

$$\gamma_{\text{PT}\to\text{e}}^2(\boldsymbol{p}^2, r, e) = \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{e}}}{N_0B + I_{\text{PT}\to\text{e}}^2(r)}, \tag{8}$$

where $I^2_{\text{PT}\to e}(r) = I^2_{\text{ST}\to e} + I^2_{r\to e} = p^2_{\text{ST}} h_{\text{ST}\to e} + p^2_r h_{r\to e}$, for all $r \in \mathcal{R}$. Now, the secrecy rate at the second hop from the PT to the PR is given by

$$c^2_{\text{PT}\to\text{PR}}(\boldsymbol{p}^2, r) = \min_e \left\{ c^2_{\text{PT}\to\text{PR}}(\boldsymbol{p}^2, r, e) \right\}, \tag{9}$$

where

$$c^2_{\text{PT}\to\text{PR}}(\boldsymbol{p}^2, r, e) = \frac{T_2}{T_1+T_2}\times \left[\log_2(1+\gamma^2_{\text{PT}\to\text{PR}}(\boldsymbol{p}^2, r)) - \log_2(1+\gamma^2_{\text{PT}\to\text{e}}(\boldsymbol{p}^2, r, e)) \right]^+.$$

Consequently, the secrecy rate of the PU is obtained as

$$c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) = c^1_{\text{PT}\to\text{PR}}(\boldsymbol{p}^1, r) + c^2_{\text{PT}\to\text{PR}}(\boldsymbol{p}^2, r), \tag{10}$$

where $\boldsymbol{p} = [\boldsymbol{p}^1, \boldsymbol{p}^2]$. At this hop, in the secondary network, the relays send the message from the ST to the SR and the SINR of the SR from relay r is

$$\gamma^2_{r\to\text{SR}}(\boldsymbol{p}^2, r) = \frac{p_r h_{r\to\text{SR}}}{N_0 B + I^2_{\text{SR}}}, \tag{11}$$

where $I^2_{\text{SR}} = I^2_{\text{ST}\to\text{SR}} + I^2_{\text{PT}\to\text{SR}} = p^2_{\text{ST}} h_{\text{ST}\to\text{SR}} + \text{P}_{\text{PT}} h_{\text{PT}\to\text{SR}}$. Also, the eavesdropper SINR from relay r is

$$\gamma^2_{r\to e}(\boldsymbol{p}^2, r, e) = \frac{p_r h_{r\to e}}{N_0 B + I^2_{r\to e}}, \quad \forall r \in \mathcal{R}, \tag{12}$$

in which $I^2_{r\to e} = I^2_{\text{ST}\to e} + I^2_{\text{PT}\to e} = p^2_{\text{ST}} h_{\text{ST}\to e} + \text{P}_{\text{PT}} h_{\text{PT}\to e}$ for all $r \in \mathcal{R}$ and

$$c^2_{r\to\text{SR}}(\boldsymbol{p}^2, r) = \min_{e\in\mathcal{E}} \left\{ c^2_{r\to\text{SR}}(\boldsymbol{p}^2, r, e) \right\},$$

where

$$c^2_{r\to\text{SR}}(\boldsymbol{p}^2, r, e) = \frac{T_2}{T_1+T_2}\times \left[\log_2(1+\gamma^2_{r\to\text{SR}}(\boldsymbol{p}^2, r)) - \log_2(1+\gamma^2_{r\to e}(\boldsymbol{p}^2, r, e)) \right]^+. \tag{13}$$

Finally, the secondary secrecy rate will be

$$c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p}, r) = \min \left\{ c^1_{\text{ST}\to r}(\boldsymbol{p}^1), c^2_{r\to\text{SR}}(\boldsymbol{p}^2) \right\}. \tag{14}$$

Similar to other works in literature, in this paper we assume that the CSI values between different nodes of the network are available to the secondary transmitter to be used in allocating the resources. We then consider the case where such CSI values are imperfect and derive corresponding secrecy rates. We also assume that eavesdroppers use single-user decoding, i.e., while decoding primary user data, secondary user data is considered as noise and vise versa.

III. Instantaneous Resource Allocation Problem and its Solution

A. The RA Problem

From the setup of Section II, the secondary secrecy rate depends on the following parameters which are selected from their corresponding sets:

1) T_1 and T_2 chosen from $\mathcal{T} = \{T_1, T_2 |\ T_1 > 0,\ T_2 > 0,\ T_1 + T_2 = T\}$ which is the set of time intervals for the first and second hops;

2) The transmit power of nodes in two hops i.e., $\mathbf{p}^1$ and $\mathbf{p}^2$, picked up from the set $\mathcal{P} = \{\mathbf{p} |\ \ \mathbf{0} \preceq \mathbf{p} \preceq \mathbf{p}_{\max}\}$ where[1] $\mathbf{p}_{\max} = [\text{P}^{\text{ST}}_{\max}, \text{P}^{\text{SR}}_{\max}, \mathbf{p}^{\text{Relay}}_{\max}]$;

3) The relay r which is deployed in the second hop to transmit the information to the SR for which the corresponding set is denoted by φ where $\varphi = \{\boldsymbol{\rho} |\ \boldsymbol{\rho}.\mathbf{1}^T = 1\}$ in which $\boldsymbol{\rho} = [\rho_1, \cdots, \rho_R]$ and $\rho_r = \{0, 1\}$ for all relay nodes, implying that only one relay is selected for transmission to the SR. Now, the RA problem of the secondary network may be written as

$$\max_{\boldsymbol{\Xi}=\mathcal{T}\cup\varphi\cup\mathcal{P}} \quad \sum_{r=1}^{R} \rho_r c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p}, r), \tag{15}$$
$$\text{s.t. } \text{C}_1 : \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) \geq \text{C}^{\text{PT}\to\text{PR}}_{\min},$$

where $\boldsymbol{\Xi} = \mathcal{T} \cup \varphi \cup \mathcal{P}$ is the vector of optimization variables. In the sequel, prior to solving (15), we provide a discussion on its feasibility to show the effect of defining $\boldsymbol{\Xi}$ on secrecy rate of both PU and SU.

B. Feasibility Condition

As mentioned before, one concern for secrecy rate is that it might be zero depending on the value of $h_{\text{PT}\to\text{PR}}$ and $h_{\text{PT}\to e}$. Now, we want to show how by extending the set of optimization variables, we can increase the chance that (15) is feasible, meaning that the primary secrecy rate is non-zero and greater than $\text{C}^{\text{PT}\to\text{PR}}_{\min}$. In line with existing literature on interference limited networks, the following discussion on feasibility is based on the assumption of high SINR at the PR and the SR [23].

For the case that there is no SU in the network, (15) is feasible, if the following optimization problem has a solution [24]

$$\min_{0\leq\xi} \quad \xi \tag{16}$$
$$\text{s.t.} \qquad \text{C}_1 : \xi \geq \text{C}^{\text{PT}\to\text{PR}}_{\min} - (\log_2 \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{PR}}}{\text{P}_{\text{PT}} h_{\text{PT}\to e}}),\ \forall e \in \mathcal{E},$$

which is a linear programming problem, and it has a solution if $\lambda_{\min}(\mathbf{M}) > 1$ where $\lambda_{\min}$ is the smallest eignevalue of matrix $\mathbf{M}$ which is an $E \times E$ diagonal matrix whose e^{th} element is $\frac{h_{\text{PT}\to\text{PR}}}{2^{\text{C}^{\text{PT}\to\text{PR}}_{\min}} h_{\text{PT}\to e}}$ which only depends on the CSI values and $\text{C}^{\text{PT}\to\text{PR}}_{\min}$.

If SU can access the spectrum via underlay approach i.e., the interference to the PR is less than a given value Γ, the primary secrecy rate is equal to $\log_2(1 + \frac{\text{P}_{\text{PT}} h_{\text{PT}\to\text{PR}}}{N_0 B + \Gamma}) - \log_2(1 + \frac{\text{P}_{\text{PT}} h_{\text{PT}\to e}}{N_0 B + \frac{\Gamma h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}}})$. For high SINR regime, it can be approximated by $\log_2 \frac{h_{\text{PT}\to\text{PR}}}{h_{\text{PT}\to e}} - \log_2 \frac{N_0 B + \frac{\Gamma h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}}}{N_0 B + \Gamma}$. Therefore, (15) is feasible when the following optimization problem has a solution

$$\min_{0\leq\xi} \quad \xi \tag{17}$$
$$\text{s.t. } \xi \geq \text{C}^{\text{PT}\to\text{PR}}_{\min} - (\log_2 \frac{h_{\text{PT}\to\text{PR}}}{h_{\text{PT}\to e}} + \log_2 \frac{N_0 B + \frac{\Gamma h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}}}{N_0 B + \Gamma}).$$

[1]The symbol $\preceq$ represents the element-wise comparison.

As (17) is also a linear programming problem, it has a solution when $\lambda_{\min}(\mathbf{MN}) > 1$ where $\mathbf{N}$ is an $E \times E$ diagonal matrix whose e^{th} element is $\frac{N_0 B + \frac{\Gamma h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}}}{N_0 B + \Gamma}$. For this case, when $h_{\text{ST}\to e}/h_{\text{ST}\to\text{PR}} > 1$, e.g., the CSI between ST and PR is larger than that between ST and eavesdropper, the feasibility set is enlarged compared to the feasibility set of (16). The above discussions can be extended to the case when there is a relay set in the network as shown in the next proposition.

Proposition 1: When relay nodes are used in the network and if the time durations of the two hops are equal and set to $T/2$, the primary secrecy rate is the same as (10) with $T_1 = T_2 = T/2$. In this case, when the noise is negligible and if $\frac{h_{r\to e}}{h_{r\to\text{PR}}} > 1$ and $\frac{h_{\text{SR}\to e}}{h_{\text{SR}\to\text{PR}}} > 1$, (15) is feasible if $\mathcal{F}_1$, defined below, is a non-empty set

$$\mathcal{F}_1 = \left\{ \exists r \in \mathcal{R} | \lambda_{\min}((\mathbf{M}_1)^2 \mathbf{N}_1 \mathbf{N}_2^r) > 2^{2\mathrm{C}_{\min}^{\text{PT}\to\text{PR}}} \right\} \tag{18}$$

where $\mathbf{M}_1$, $\mathbf{N}_1$ and $\mathbf{N}_2^r$ are $E \times E$ diagonal matrices whose e^{th} elements are $\frac{h_{\text{PT}\to\text{PR}}}{h_{\text{PT}\to e}}$, $\frac{h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}}$ and $\frac{h_{r\to e}}{h_{r\to\text{PR}}}$, respectively.

Proof: See Appendix A. ∎

Note that $\frac{h_{r\to e}}{h_{r\to\text{PR}}} > 1$ and $\frac{h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}} > 1$ correspond to the case where the jamming effect of relay nodes and SR is beneficial for the CRN, e.g., the interference of SR and relay r on the set of eavesdropper nodes is greater than that on the PR.

For the case when T_1 and T_2 are not necessarily equal (the setup of this paper), the set defined in (18) is transformed into

$$\mathcal{F}_2 = \left\{ \exists r \in \mathcal{R} | \lambda_{\min}(\mathbf{MN}_1^1 \mathbf{N}_2^{2r}) > 2^{\mathrm{C}_{\min}^{\text{PT}\to\text{PR}}} \right\} \tag{19}$$

where $\mathbf{N}_1^1$ and $\mathbf{N}_2^{2r}$ are $E \times E$ diagonal matrices whose e^{th} elements are $(\frac{h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}})^{\frac{T_1}{T}}$ and $(\frac{h_{\text{PT}\to\text{PR}}}{h_{\text{PT}\to e}})^{\frac{T_2}{T}}$, respectively. Obviously, introducing the relay set in both cases when $\frac{h_{r\to e}}{h_{r\to\text{PR}}} > 1$ and $\frac{h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}} > 1$, leads to the expansion of feasibility set compared to that for the underlay approach. Now, consider the case in which $\frac{h_{r\to e}}{h_{r\to\text{PR}}} > 1$ and $\frac{h_{\text{ST}\to e}}{h_{\text{ST}\to\text{PR}}} \approx 1$, i.e., interference caused by of ST on both PR and eavesdropper are on the same order. As such, (18) and (19) are transformed into

$$\mathcal{F}_1 = \left\{ \exists r \in \mathcal{R} | \lambda_{\min} \left(\mathbf{M}_1 \sqrt{\mathbf{N}_2^r} \right) > 2^{\mathrm{C}_{\min}^{\text{PT}\to\text{PR}}} \right\} \tag{20}$$

and

$$\mathcal{F}_2 = \left\{ \exists r \in \mathcal{R} | \lambda_{\min}(\mathbf{MN}_2^{2r}) > 2^{\mathrm{C}_{\min}^{\text{PT}\to\text{PR}}} \right\}. \tag{21}$$

When $T_2/T > 1/2$, the feasibility region from (21) is larger than that of (20). This comparison shows that by adjusting the time duration of each hop, the feasibility set size of the optimization problem is increased. The non-emptiness of $\mathcal{F}_2$ can be shown by an approach similar to Proposition 1.

The above analysis on the feasibility set of (15) shows that by introducing new optimization variables to the RA problem, new degree of freedom is added to the feasible set and therefore the chance that secrecy rate of $\mathrm{C}_{\min}^{\text{PT}\to\text{PR}}$ can be supported under a given channel condition is increased. In particular, for the setup of this paper, the feasibility set is larger than the setup where there is no relay in the network, e.g., [12]–[15] or there is a relay with fixed time duration for each hop e.g., [16]. Also, the chance of having non-zero secondary secrecy rate is increased.

TABLE II
ALGORITHM I

Step1: Initialize $L_{\max}$, and set $l = 0$,
Step2: Initialize $\boldsymbol{p}^0$ and $\boldsymbol{\rho}^0$ and T_1^0,
Step3: Repeat:
Step4: Find a power allocation with $\boldsymbol{\rho} = \boldsymbol{\rho}^l$ and $T_1 = T_1^l$, using the algorithm proposed in subsection III.C.1,
Step5: Find a relay selection with $\boldsymbol{P} = \boldsymbol{P}^l$ and $T_1 = T_1^l$, using the algorithm proposed in subsection III.C.2,
Step6: Find a time allocation with $\boldsymbol{P} = \boldsymbol{P}^l$ and $\boldsymbol{\rho} = \boldsymbol{\rho}^l$, using the algorithm proposed in subsection III.C.3,
Step7: $l = l + 1$, until $\|\boldsymbol{P}^l - \boldsymbol{P}^{l-1}\| < \varepsilon$ or $l = L_{\max}$.

C. The Iterative Algorithm

It can be seen that (15) is a non-convex optimization problem with respect to $\boldsymbol{\Xi}$. To solve the problem, we utilize the iterative algorithm introduced by [25] where the optimization variables are divided into independent sets of variables. Then, corresponding to each set of variables, the new optimization problem is solved. For example, for our problem, we have three sets of optimization variables: 1) $\mathcal{P}$, 2) $\mathcal{T}$, 3) φ. The optimization problem can be decomposed into three subproblems: 1) Power allocation subproblem, 2) Relay selection subproblem, 3) Time allocation subproblem. The iterative algorithm to solve these subproblems is summarized in Table II. In this algorithm, l is the current iteration number and the superscript l indicates that the associated variable is obtained after the l^{th} iteration. In [25], it has been shown that the iterative algorithms converges to a near optimal solution of (15) if each subproblem can be solved optimally. These subproblems can be either convex or transformed into a convex optimization problem.

1) Power allocation problem: Assuming a fixed value for $\mathcal{T}$ and φ, the power allocation problem is obtained as

$$\begin{aligned} \max_{\mathcal{P}} \quad & \sum_{r=1}^{R} c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p}, r), \\ \text{s.t.} \quad & \sum_{r=1}^{R} c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) \geq \mathrm{C}_{\min}^{\text{PT}\to\text{PR}}. \end{aligned} \tag{22}$$

Although (22) has only one set of optimization variables, it is still a non-convex optimization problem. To transform it into a convex optimization problem, we use the following two steps: 1) Introducing a tight lower bound of secrecy rate based on SCALE algorithm [18] 2) Utilizing exponential auxiliary variables to transform (22) to a standard GP model.

Tight lower bound on secrecy rate:

In order to find the solution, we use the following tight lower bound $\log_2(1+z) \geq \alpha \log_2 z + \beta$ where $\alpha = \frac{\bar{z}}{1+\bar{z}}$, $\beta = \log_2(1+\bar{z}) - \frac{\bar{z}}{1+\bar{z}} \log_2(\bar{z})$ and $\bar{z}$ is the SINR of pervious iteration. Note that this lower bound is tight at $z = \bar{z}$. Hence, we can introduce a lower-bound of the secrecy rate as $c_{\text{ST}\to r}(\boldsymbol{p}^1, r) \geq \overline{c}_{\text{ST}\to r}((\boldsymbol{p}^1, r))$ and $c_{r\to\text{SR}}(\boldsymbol{p}^2, r) \geq$

$\overline{c}_{r\to \mathrm{SR}}(\boldsymbol{p}^2, r)$, where

$$\overline{c}_{\mathrm{ST}\to r}(\boldsymbol{p}^1, r) = \min_{e\in\mathcal{E}} \frac{T_1}{T_1+T_2}\times \left[\alpha_{\mathrm{ST}\to r}\log_2(\gamma^1_{\mathrm{ST}\to r}(\boldsymbol{p}^1, r)) + \beta_{\mathrm{ST}\to r} - \alpha_{\mathrm{ST}\to e}\log_2(\gamma^1_{\mathrm{ST}\to e}(\boldsymbol{p}^1, e)) - \beta_{\mathrm{ST}\to e}\right]^+, \tag{23}$$

and

$$\overline{c}_{r\to \mathrm{SR}}(\boldsymbol{p}^2, r) = \min_{e\in\mathcal{E}} \frac{T_2}{T_1+T_2}\times \left[\alpha_{r\to \mathrm{SR}}\log_2(\gamma^2_{r\to \mathrm{SR}}(\boldsymbol{p}^2, r)) + \beta_{r\to \mathrm{SR}} - \alpha_{r\to e}\log_2(\gamma^2_{\mathrm{ST}\to e}(\boldsymbol{p}^2, r, e) - \beta_{r\to e}\right]^+. \tag{24}$$

Consequently, (14) is transformed into

$$c_{\mathrm{ST}\to r\to \mathrm{SR}}(\boldsymbol{p}, r) \geq \min\left\{\overline{c}_{\mathrm{ST}\to r}(\boldsymbol{p}^1, r), \overline{c}_{r\to \mathrm{SR}}(\boldsymbol{p}^2, r)\right\}.$$

The same procedure can be applied to obtain a convex lower bound for primary secrecy rate as $c_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}, r) \geq \overline{c}_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}, r)$ where

$$\overline{c}_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}, r) = \overline{c}^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1) + \overline{c}^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2, r), \tag{25}$$

in which $\overline{c}^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1) = \min_{e\in\mathcal{E}}\left\{\overline{c}^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1, e)\right\}$, and $\overline{c}^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2), r) = \min_{e\in\mathcal{E}}\left\{\overline{c}^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2, r, e)\right\}$ where

$$\overline{c}^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1, e) = \frac{T_1}{T_1+T_2}\times \left[\alpha^1_{\mathrm{PT}\to \mathrm{PR}}\log_2(\gamma^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1, e)) + \beta^1_{\mathrm{PT}\to \mathrm{PR}} - \alpha^1_{\mathrm{PT}\to e}\log_2(\gamma^1_{\mathrm{PT}\to e}(\boldsymbol{p}^1, e)) - \beta^1_{\mathrm{PT}\to e}\right]^+,$$

and

$$\overline{c}^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2, r, e) = \frac{T_2}{T_1+T_2}\times \left[\alpha_{\mathrm{PT}\to \mathrm{PR}}\log_2(\gamma^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2, r)) + \beta^2_{\mathrm{PT}\to \mathrm{PR}} - \alpha^2_{\mathrm{PT}\to e}\log_2(\gamma^2_{\mathrm{PT}\to e}(\boldsymbol{p}^2, r, e)) - \beta^2_{\mathrm{PT}\to e}\right]^+.$$

Since the introduced lower bound is derived based on the difference of two logarithmic functions, we should demonstrate that this lower bound holds throughout iterations. This is shown in the next proposition.

Proposition 2: In each iteration, the introduced lower bound holds.

Proof: See Appendix II. ∎

In the sequel, we show that the power allocation problem can be transformed into a standard form of GP based on the above introduced lower bound for secrecy rate.

Standard GP model

In a standard form GP, the objective function must be posynomial (and it must be minimized); the equality constraints can only have the form of a monomial equal to one, and the inequality constraints can only have the form of a posynomial less than or equal to one [19]. The main motivation of utilizing GP modelling in our problem is its efficiency and existence of fast algorithms to solve the optimization problems involving a large number of constraints and variables. Moreover, in addition to the efficiency of GP, the corresponding algorithms are not sensitive to initial points and converge to the optimal solution.

To transform our problem into standard form of GP, referred to as GP modelling, we define a set of new variables and express the problem based on them accordingly. For the first hop, let us rewrite the primary SINR as follows:

$$\gamma^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^1) = \frac{1}{z^1_{\mathrm{PT}\to \mathrm{PR}} + a^1_{\mathrm{SR}\to PR}p^1_{\mathrm{SR}} + a^1_{\mathrm{ST}\to PR}p^1_{\mathrm{ST}}}, \tag{26}$$

where $z^1_{\mathrm{PT}\to \mathrm{PR}} = N_0B/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$, $a^1_{\mathrm{ST}\to \mathrm{PR}} = h_{\mathrm{ST}\to \mathrm{PR}}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$, $a^1_{\mathrm{SR}\to \mathrm{PR}} = h_{\mathrm{SR}\to PR}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$ and we consider $y^1_{\mathrm{PT}\to \mathrm{PR}} = \frac{1}{z^1_{\mathrm{PT}\to \mathrm{PR}}+a^1_{\mathrm{SR}\to PR}p^1_{\mathrm{SR}}+a^1_{\mathrm{ST}\to \mathrm{PR}}p^1_{\mathrm{ST}}}$. For $\gamma^1_{\mathrm{PT}\to \mathrm{e}}$, we again have

$$\gamma^1_{\mathrm{PT}\to \mathrm{e}}(\boldsymbol{p}^1, e) = \frac{1}{z^1_{\mathrm{PT}\to e} + a^1_{SR\to e}p^1_{\mathrm{SR}} + a^1_{ST\to e}p^1_{\mathrm{ST}}}, \tag{27}$$

where $z^1_{\mathrm{PT}\to e} = N_0B/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$, $a^1_{\mathrm{ST}\to e} = h_{\mathrm{ST}\to e}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$, $a^1_{\mathrm{SR}\to e} = h_{\mathrm{SR}\to e}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$, $y^1_{\mathrm{PT}\to \mathrm{e}} = z^1_{\mathrm{PT}\to e} + a^1_{\mathrm{SR}\to e}p_{\mathrm{SR}} + a^1_{ST\to e}p^1_{\mathrm{ST}}$. Now, based on new variables, the lower bound of primary secrecy rate is transformed into

$$\overline{c}^1_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{y}^1, e) = \varpi^1_{\mathrm{PT}\to \mathrm{PR}}\log_2(y^1_{\mathrm{PT}\to \mathrm{PR}}) + \varpi^1_{\mathrm{PT}\to \mathrm{e}}\log_2(y^1_{\mathrm{PT}\to \mathrm{e}}) + \log_2(\Gamma^1_{\mathrm{PT}\to \mathrm{PR}}(e)), \tag{28}$$

where $\varpi^1_{\mathrm{PT}\to \mathrm{PR}} = \frac{T_1}{T_1+T_2}\times\alpha^1_{\mathrm{PT}\to \mathrm{PR}}$, $\varpi^1_{\mathrm{PT}\to \mathrm{e}} = \frac{T_1}{T_1+T_2}\times\alpha^1_{\mathrm{PT}\to e}$ and $\Gamma^1_{\mathrm{PT}\to \mathrm{PR}}(e) = \exp\left(\frac{T_1}{T_1+T_2}(\beta^1_{\mathrm{PT}\to \mathrm{PR}} - \beta^1_{\mathrm{PT}\to \mathrm{e}})\right)$.

At the second hop, similar to the first hop, $\gamma^2_{\mathrm{PT}\to \mathrm{PR}}$ can be rewritten as follows:

$$\gamma^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{p}^2, r, e) = \frac{1}{z^2_{\mathrm{PT}\to \mathrm{PR}} + a^2_{r\to \mathrm{PR}}p^2_{\mathrm{r}} + a^2_{\mathrm{ST}\to \mathrm{PR}}p^2_{\mathrm{ST}}}, \tag{29}$$

where $z^2_{\mathrm{PT}\to \mathrm{PR}} = N_0B/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$, $a^2_{\mathrm{ST}\to \mathrm{PR}} = h_{\mathrm{ST}\to \mathrm{PR}}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$, $a^2_{r\to \mathrm{PR}} = h_{r\to \mathrm{PR}}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}})$ and we consider $y^2_{\mathrm{PT}\to \mathrm{PR}} = \frac{1}{z^2_{\mathrm{PT}\to \mathrm{PR}}+a^2_{\mathrm{ST}\to \mathrm{PR}}p^2_{\mathrm{ST}}+a^2_{r\to \mathrm{PR}}p^1_{\mathrm{r}}}$. At second hop, the primary eavesdropper SINR can be written as follows:

$$\gamma^2_{\mathrm{PT}\to \mathrm{e}}(\boldsymbol{p}^2, r, e) = \frac{1}{z^2_{\mathrm{PT}\to e} + a^2_{r\to e}p^1_{\mathrm{r}} + a^2_{\mathrm{ST}\to e}p^2_{\mathrm{ST}}}, \tag{30}$$

where $z^2_{\mathrm{PT}\to e} = N_0B/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$, $a^2_{\mathrm{ST}\to e} = h_{\mathrm{ST}\to e}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$, $a^2_{r\to e} = h_{r\to e}/(\mathrm{P}_{\mathrm{PT}}h_{\mathrm{PT}\to e})$ and we consider $y^2_{\mathrm{PT}\to \mathrm{e}} = z^2_{\mathrm{PT}\to e} + a^2_{r\to e}p^2_{\mathrm{r}} + a^2_{ST\to e}p^2_{\mathrm{ST}}$.

At the second hop, based on the new variables, the lower bound of primary secrecy rate is transformed into

$$\overline{c}^2_{\mathrm{PT}\to \mathrm{PR}}(\boldsymbol{y}^2, e, r) = \varpi^2_{\mathrm{PT}\to \mathrm{PR}}\log_2(y^2_{\mathrm{PT}\to \mathrm{PR}}(r)) + \varpi^2_{\mathrm{PT}\to \mathrm{e}}\log_2(y^2_{\mathrm{PT}\to \mathrm{e}}(r)) + \log_2(\Gamma^2_{\mathrm{PT}\to \mathrm{PR}}(e)), \tag{31}$$

where $\varpi^2_{\text{PT}\to\text{PR}} = \frac{T_2}{T_1+T_2} \times \alpha^2_{\text{PT}\to\text{PR}}$, $\varpi^2_{\text{PT}\to\text{e}} = \frac{T_2}{T_1+T_2} \times \alpha^2_{\text{PT}\to e}$ and $\Gamma^2_{\text{PT}\to\text{PR}}(e) = \exp\left(\frac{T_2}{T_1+T_2}(\beta^2_{\text{PT}\to\text{PR}} - \beta^2_{\text{PT}\to\text{e}})\right)$.

The primary secrecy rate is then obtained as

$$\begin{aligned}\overline{c}_{\text{PT}\to\text{PR}}(\boldsymbol{y}, r, e) = \\ \varpi^1_{\text{PT}\to\text{PR}} \log_2 y^1_{\text{PT}\to\text{PR}} + \varpi^1_{\text{PT}\to\text{e}} \log_2 y^1_{\text{PT}\to\text{e}} + \\ \varpi^2_{\text{PT}\to\text{PR}} \log_2 y^2_{\text{PT}\to\text{PR}}(r) + \varpi^2_{\text{PT}\to\text{e}} \log_2 y^2_{\text{PT}\to\text{e}}(r) \\ + \log_2\left(\Gamma^1_{\text{PT}\to\text{PR}}(e)\Gamma^2_{\text{PT}\to\text{PR}}(e)\right).\end{aligned} \tag{32}$$

Similar to primary secrecy rate, we use the new variables to transform the secondary SINR and secrecy rate. At first hop, the secondary SINR can be defined as

$$\gamma^1_{\text{ST}\to r} = y^1_{\text{ST}} y^1_{\text{ST}\to r} \tag{33}$$

where $y^1_{\text{ST}} = p^1_{\text{ST}}$, $y^1_{\text{ST}\to r} = \frac{1}{z^1_{\text{ST}\to r} + p^1_{\text{SR}} h_{\text{SR}\to r}/h_{\text{ST}\to r}}$, $z^1_{\text{ST}\to r} = (N_0 B + \text{P}_{\text{PT}} h_{\text{PT}\to r})/h_{\text{ST}\to r}$.

The secondary eavesdropper SINR can be defined as

$$\gamma^1_{\text{ST}\to e} = \frac{y^1_{\text{ST}}}{y^1_{\text{ST}\to e}}, \tag{34}$$

where $y^1_{\text{ST}\to e} = z^1_{\text{ST}\to e} + p^1_{\text{SR}} h_{\text{SR}\to e}/h_{\text{ST}\to e}$, $z^1_{\text{ST}\to e} = (N_0 B + \text{P}_{\text{PT}} h_{\text{PT}\to e})/h_{\text{ST}\to e}$.

Based on the new variables, the lower bound of secondary secrecy rate at first hop is

$$\begin{aligned}\overline{c}_{\text{ST}\to r}(\boldsymbol{y}, r, e) = \\ \varpi^1_{\text{ST}\to r} \log_2(y^1_{\text{ST}} y^1_{\text{ST}\to r}) + \varpi^1_{\text{ST}\to e} \log_2(\frac{y^1_{\text{ST}\to e}}{y^1_{\text{ST}}}) \\ + \log_2(\Gamma^1_{\text{ST}\to\text{r}}(e)),\end{aligned} \tag{35}$$

where $\varpi^1_{\text{ST}\to r} = \frac{T_1}{T_1+T_2}\alpha_{\text{ST}\to r}$, $\varpi^1_{\text{ST}\to e} = \frac{T_1}{T_1+T_2}\alpha_{\text{ST}\to e}$ and $\Gamma^1_{\text{ST}\to\text{r}}(e) = \exp\left(\frac{T_1}{T_1+T_2}(\beta^1_{\text{ST}\to\text{r}} - \beta^1_{\text{ST}\to\text{e}})\right)$.

At the second hop,

$$\gamma^2_{\text{r}\to\text{SR}} = y^2_{\text{r}} y^2_{\text{r}\to\text{SR}}, \tag{36}$$

where $y^2_{\text{r}} = p^2_{\text{r}}$, $y^2_{\text{r}\to\text{SR}} = \frac{1}{z^2_{\text{r}\to\text{SR}} + p^2_{\text{ST}} h_{\text{ST}\to r}/h_{\text{SR}\to r}}$, $z^2_{\text{r}\to\text{SR}} = (N_0 B + \text{P}_{\text{PT}} h_{\text{PT}\to r})/h_{\text{r}\to\text{SR}}$.

The secondary eavesdropper SINR is obtained as

$$\gamma^2_{\text{r}\to e} = \frac{y^2_{\text{r}}}{y^2_{\text{r}\to e}}, \tag{37}$$

where $y^2_{\text{r}\to e} = z^2_{\text{r}\to e} + p^2_{\text{ST}} h_{\text{ST}\to e}/h_{\text{r}\to e}$, $z^2_{\text{r}\to e} = (N_0 B + \text{P}_{\text{PT}} h_{\text{PT}\to e})/h_{\text{r}\to e}$.

Finally, the lower bound of secondary secrecy rate at second hop is $\overline{c}_{r\to\text{SR}}(\boldsymbol{y}, r, e) = \varpi^2_{r\to\text{SR}} \log_2(y^2_r y^2_{r\to\text{SR}}) + \varpi^2_{\text{r}\to e} \log_2(\frac{y^2_{r\to e}}{y^2_r}) + \log_2(\Gamma^2_{\text{r}\to\text{SR}}(e))$, where $\varpi^2_{r\to\text{SR}} = \frac{T_2}{T_1+T_2}\alpha^2_{r\to\text{SR}}$, $\varpi^2_{r\to\text{e}} = \frac{T_2}{T_1+T_2}\alpha^2_{r\to\text{e}}$ and $\Gamma^2_{\text{r}\to\text{SR}}(e) = \exp\left(\frac{T_2}{T_1+T_2}(\beta^2_{\text{r}\to\text{SR}} - \beta^2_{\text{r}\to\text{e}})\right)$.

Now we obtain new forms for constraints in the first and second hop based on the new variables. Let us consider $p^1_{\text{ST}} = y^1_{\text{ST}}$ and $p^1_{\text{SR}} = \left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right) h_{\text{ST}\to r}/h_{\text{SR}\to r}$. Now, by some mathematical manipulation $y^1_{\text{ST}\to e}$ can be obtained based on y^1_{ST} and $y^1_{\text{ST}\to r}$ as

$$\text{C}_1 : y^1_{\text{ST}\to e} = \left[z^1_{\text{ST}\to e} + \left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right)\frac{h_{\text{ST}\to r} h_{\text{SR}\to e}}{h_{\text{SR}\to r} h_{\text{ST}\to e}}\right]_{y^1_{\text{ST}\to r} \le \frac{1}{z^1_{\text{ST}\to r}}}$$

where $[x]_a = x$ for any x if statement a holds and otherwise $[x]_a = 0$.

In GP modelling, all the equality constraints should be monomial functions but C1 is still a posynomial function. To take care of this, one can form a relaxation of the considered problem by replacing the equality constraint with an inequality constraint. Consequently, we can replace C1 with $f_1(\boldsymbol{y}, e, r) \le 1$ where

$$f_1(\boldsymbol{y}, e, r) = \begin{cases} \frac{1}{y^1_{\text{ST}\to e}} z^1_{\text{ST}\to e} + \frac{1}{y^1_{\text{ST}\to e}}\left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right) \\ \quad \frac{h_{\text{ST}\to r} h_{\text{SR}\to e}}{h_{\text{SR}\to r} h_{\text{ST}\to e}}, \text{ if } \quad y^1_{\text{ST}\to r} \le \frac{1}{z^1_{\text{ST}\to r}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

The same process can be applied to other constraints and we have

$$\text{C}_2 : y^1_{\text{PT}\to\text{PR}} = \frac{1}{z^1_{\text{PT}\to\text{PR}} + a^1_{SR\to PR}\left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right)\frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^1_{ST\to PR} y^1_{\text{ST}}},$$

$$\text{C}_3 : y^1_{\text{PT}\to\text{e}} = z^1_{\text{PT}\to e} + a^1_{SR\to e}\left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right)\frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^1_{ST\to e} y^1_{\text{ST}}$$

$$f_2(\boldsymbol{y}, e, r) = \begin{cases} y^1_{\text{PT}\to\text{PR}}\Big(z^1_{\text{PT}\to\text{PR}} + a^1_{SR\to PR}\left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right) \\ \quad \frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^1_{ST\to PR} y^1_{\text{ST}}\Big), \text{ if } y^1_{\text{ST}\to r} \le \frac{1}{z^1_{\text{ST}\to r}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

$$f_3(\boldsymbol{y}, r, e) = \begin{cases} \frac{1}{y^1_{\text{PT}\to e}} z^1_{\text{PT}\to e} + \frac{1}{y^1_{\text{PT}\to\text{e}}} a^1_{SR\to e}\left(\frac{1}{y^1_{\text{ST}\to r}} - z^1_{\text{ST}\to r}\right) \\ \quad \frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + \frac{1}{y^1_{\text{PT}\to\text{e}}} a^1_{ST\to e} y^1_{\text{ST}}, \text{ if } y^1_{\text{ST}\to r} \le \frac{1}{z^1_{\text{ST}\to r}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

At the second hop, we define $p^2_{\text{r}} = y^2_2$ and $p^2_{\text{ST}} = \left(\frac{1}{y^2_{\text{r}\to\text{SR}}} - z^2_{\text{r}\to\text{SR}}\right) h_{\text{ST}\to r}/h_{\text{SR}\to r}$ which leads to

$$\text{C}_4 : y^2_{\text{r}\to e} = z^2_{\text{r}\to e} + \left(\frac{1}{y^2_{\text{r}\to SR}} - z^2_{\text{r}\to SR}\right)\frac{h_{\text{ST}\to r} h_{\text{ST}\to e}}{h_{\text{SR}\to r} h_{\text{r}\to e}},$$

$$\text{C}_5 : y^2_{\text{PT}\to\text{PR}} = \frac{1}{z^2_{\text{PT}\to\text{PR}} + a^2_{SR\to PR}\left(\frac{1}{y^2_{\text{r}\to SR}} - z^2_{\text{r}\to SR}\right)\frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^2_{r\to PR} y^2_{\text{r}}}$$

and

$$\text{C}_6 : y^2_{\text{PT}\to\text{e}} = z^2_{\text{PT}\to e} + a^1_{\text{SR}\to e}\left(\frac{1}{y^2_{\text{r}\to\text{SR}}} - z^2_{\text{r}\to\text{SR}}\right)\frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^2_{r\to e} y^2_{\text{r}}.$$

Again in order to use the relaxation method, we define the following functions

$$f_4(\boldsymbol{y}, r, e) = \begin{cases} \frac{1}{y^2_{\text{r}\to e}} z^2_{\text{r}\to e} + \frac{1}{y^2_{\text{r}\to e}}\left(\frac{1}{y^2_{\text{r}\to SR}} - z^2_{\text{r}\to SR}\right) \\ \quad \frac{h_{\text{ST}\to r} h_{\text{ST}\to e}}{h_{\text{SR}\to r} h_{\text{r}\to e}}, \quad \text{if } y^2_{\text{ST}\to r} \le \frac{1}{z^2_{r\to\text{SR}}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

$$f_5(\boldsymbol{y}, r, e) = \begin{cases} y^2_{\text{PT}\to\text{PR}}\Big(z^2_{\text{PT}\to\text{PR}} + a^2_{SR\to PR}\left(\frac{1}{y^2_{\text{r}\to SR}} - z^2_{\text{r}\to SR}\right) \\ \quad \frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + a^2_{r\to PR} y^2_{\text{r}}\Big), \quad \text{if, } y^2_{\text{ST}\to r} \le \frac{1}{z^2_{r\to\text{SR}}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

$$f_6(\boldsymbol{y}, r, e) = \begin{cases} \frac{1}{y^2_{\text{PT}\to e}} z^2_{\text{PT}\to e} + \frac{1}{y^2_{\text{PT}\to\text{e}}} a^1_{\text{SR}\to e}\left(\frac{1}{y^2_{\text{r}\to\text{SR}}} - z^2_{\text{r}\to\text{SR}}\right) \\ \quad \frac{h_{\text{ST}\to r}}{h_{\text{SR}\to r}} + \frac{1}{y^2_{\text{PT}\to\text{e}}} a^2_{r\to e} y^2_{\text{r}}, \quad \text{if} y^2_{\text{ST}\to r} \le \frac{1}{z^2_{r\to\text{SR}}}, \\ 0, \qquad \text{o.w,} \end{cases}$$

Followed by the above new variables and constraints, the power allocation problem is changed to the following optimization problem

$$\begin{aligned} \max_{\boldsymbol{y},\boldsymbol{\pi}} \quad & \sum_{r=1}^{R} \pi_r, \\ \text{s.t.} \quad & \bar{c}_{\text{r}\to\text{SR}}(\boldsymbol{y},r,e) \geq \pi_r, \quad \forall r,e, \\ & \bar{c}_{\text{ST}\to r}(\boldsymbol{y},r,e) \geq \pi_r, \quad \forall r,e, \\ & \sum_{r=1}^{R} \bar{c}_{\text{PT}\to\text{PR}}(\boldsymbol{y},r,e) \geq \text{C}_{\text{min}}^{\text{PT}\to\text{PR}}, \quad \forall e \in \mathcal{E} \\ & f_i(\boldsymbol{y},r,e) \leq 1, \quad \forall r,e,i=1,\ldots,6, \end{aligned} \tag{38}$$

which is a standard GP and can be solved very efficiently via numerical methods as in [26] and [27].

2) Relay Selection: For a fixed value of $\mathcal{P}$ and $\mathcal{T}$, the relay selection problem can be stated as

$$\begin{aligned} \max_{\varphi} \quad & \sum_{r=1}^{R} \rho_r c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p},r), \\ \text{s.t.} \quad & \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p},r) \geq \text{C}_{\text{min}}^{\text{PT}\to\text{PR}}, \end{aligned} \tag{39}$$

which is a binary linear programming with respect to φ and can be solved efficiently via numerical approaches and CVX tool. In addition to our approach, there are different suboptimal approaches for relay selection [16] which can be applied to our problem as follows:

- Maximum Primary Secrecy Rate (MPSR) where the relay which leads to the maximum rate for PUs is selected from the following problem

$$r^* = \arg\max_{r} \{c_{\text{PT}\to\text{PR}}(\boldsymbol{p},r)\} \tag{40}$$

- Minimum Interference on Primary (MIP) where the relay which induces the minimum interference to PUs is selected from the following problem

$$r^* = \arg\min_{r} \{p_r h_{r\to\text{PR}}\} \tag{41}$$

3) Time Allocation: For a fixed value of $\mathcal{P}$ and ϕ, the time allocation problem can be stated as follows

$$\begin{aligned} \max_{\mathcal{T}} \quad & \sum_{r=1}^{R} \rho_r c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p}), \\ \text{s.t.} \quad & \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p},r) \geq \text{C}_{\text{min}}^{\text{PT}\to\text{PR}}, \end{aligned} \tag{42}$$

which is a linear programming problem with respect to $\mathcal{T}$ and can be solved efficiently via numerical approaches and CVX tool. Another approach to reduce the computational complexity is to set $T_1(n) = \Delta T$ for $n = 1, \cdots, N$ where $\Delta T = T/N$. For each value of $T_1(n)$ and $T_2(n) = T - T_1(n)$, the optimal value of power and the selected relay are derived from the proposed iterative algorithms of subsections III.C.1 and II.C.2.

IV. Ergodic Resource Allocation (ERA)

As discussed before, in IRA, the optimization problem is solved for any new channel realization through updating the Lagrangian multipliers. This imposes a high computational complexity. To reduce such overhead, ergodic resource allocation can be deployed in which the objective function is optimized in average sense. In this case, Lagrangian multipliers do not need to be updated for different channel realization. Generally in ERA, the constraints are also satisfied in average sense. In this respect in the next subsection, we formulate the ERA problem corresponding to the IRA problem (15) in which the average secondary secrecy rate is maximized subject to keeping the average primary secrecy rate above a given threshold. The main drawback of this setting is that it only guarantees the primary secrecy rate in long term sense. In other words, the probability that the instantaneous primary secrecy rate is above the threshold is only fifty percent. To take care of this drawback, in Subsection IV-B, we propose a modified ERA problem in which the probability of primary secrecy rate outage is kept above a desired threshold. This ERA problem is referred to as the Probabilistic ERA (P-ERA) while we call the first one the Non-Probabilistic ERA (NP-ERA).

A. Non-probabilistic ERA (NP-ERA)

Assuming that the long term CDI's are available, the NP-ERA is given by

$$\begin{aligned} \max_{\boldsymbol{\Xi}} \quad & \sum_{r=1}^{R} \rho_r \mathbf{E}_{\boldsymbol{h}} \left\{ c_{\text{ST}\to r\to\text{SR}}(\boldsymbol{p}) \right\}, \\ \text{s.t.} \quad & \sum_{r=1}^{R} \rho_r \mathbf{E}_{\boldsymbol{h}} \left\{ c_{\text{PT}\to\text{PR}}(\boldsymbol{p},r) \right\} \geq \text{C}_{\text{min}}^{\text{PT}\to\text{PR}}. \end{aligned} \tag{43}$$

Following the same arguments as Section III, we divide above problem into three subproblems. The corresponding power allocation problem of (43), can be transformed into the standard GP model as

$$\begin{aligned} \max_{\boldsymbol{y},\boldsymbol{\pi}} & \sum_{r=1}^{R} \pi_r, \\ \text{s.t.} \quad & \mathbf{E}_{\boldsymbol{h}} \left\{ \bar{c}_{\text{r}\to\text{SR}}(\boldsymbol{y}(\boldsymbol{h}),r,e) \right\} \geq \pi_r, \quad \forall r,e, \\ & \mathbf{E}_{\boldsymbol{h}} \left\{ \bar{c}_{\text{ST}\to r}(\boldsymbol{y}(\boldsymbol{h}),r,e) \right\} \geq \pi_r, \quad \forall r,e, \\ & \sum_{r=1}^{R} \mathbf{E}_{\boldsymbol{h}} \left\{ \bar{c}_{\text{PT}\to\text{PR}}(\boldsymbol{y}(\boldsymbol{h}),r,e) \right\} \geq \text{C}_{\text{min}}^{\text{PT}\to\text{PR}}, \quad \forall e, \\ & \forall f_i(\boldsymbol{y}(\boldsymbol{h}),r,e) \leq 1, \quad \forall r,e, \forall \boldsymbol{h}, \text{and} i=1,\ldots,6, \end{aligned} \tag{44}$$

The time allocation and relay selection problems for ERA are very similar to the IRA case have thus been omitted.

B. Probabilistic ERA (P-ERA)

By substituting the constraint of Problem (43) with its probabilistic version, we obtain the following ERA problem

$$\max_{\boldsymbol{\Xi}} \quad \sum_{r=1}^{R} \rho_r \mathbf{E}_{\boldsymbol{h}} \left\{ c_{\text{ST}\to r\to \text{SR}}(\boldsymbol{p}) \right\}, \tag{45}$$
$$\text{s.t.} \quad \Pr\left\{ \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) \le \text{C}_{\min}^{\text{PT}\to\text{PR}} \right\} \le \zeta,$$

where $0 < \zeta < 1$ is a predefined threshold of outage probability of primary secrecy rate.Via the probabilistic constraint in (45) for any value of CSI, the instantaneous primary secrecy rate is guaranteed to be above the threshold with a desired probability.

Due to the inclusion of the probabilistic constraint, this problem can not be solved directly by conventional methods. Therefore, we propose to replace the probabilistic constraint with $\mathbf{E}_{\boldsymbol{h}}\left\{ \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) \right\} \ge \hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l)$, where $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l)$ is an auxiliary variable to be explained later. The new problem is then solved using Algorithm I. If the resulting optimization variables satisfy the probabilistic constraint, these variable are treated as the solution of Problem (45). To converge to a feasible solution, we propose a novel approach in which this goal is achieved through an iterative algorithm, referred to as Algorithm II. At the l^{th} iteration of this algorithm, the following problem is solved using Algorithm I:

$$\max_{\boldsymbol{\Xi}} \quad \sum_{r=1}^{R} \rho_r \mathbf{E}_{\boldsymbol{h}} \left\{ c_{\text{ST}\to r\to \text{SR}}(\boldsymbol{p}) \right\}, \tag{46}$$
$$\text{s.t.} \quad \mathbf{E}_{\boldsymbol{h}}\left\{ \sum_{r=1}^{R} \rho_r c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r) \right\} \ge \hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l),$$

where $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l) = \theta(l)\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l-1)$ in which $\theta(l) \in [0,1]$ is a scaling parameter whose value is assigned later. In initialization step i.e., $l = 0$, we set $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l=0) = \omega \text{C}_{\min}^{\text{PT}\to\text{PR}}$ where ω is an arbitrary positive large number. From the obtained parameters, the following outage probability of primary secrecy rate is derived

$$\mathcal{OU}(l) = \Pr\left\{ c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r^*) \le \text{C}_{\min}^{\text{PT}\to\text{PR}} \right\}. \tag{47}$$

Let $\mathcal{D}(l) = |\mathcal{OU}(l) - \zeta|$. If $\mathcal{D}(l) \le \epsilon$, where ϵ is an arbitrary positive small value, the proposed iterative algorithm stops. At each iteration, we set $\theta(l) = (1-\mathcal{D})^{\Theta}$ where Θ is an arbitrary number greater than 1. This iterative algorithm, referred to as Algorithm II is summarized in Table III. The value of $\mathcal{OU}(l)$ can be obtained based on the following proposition.

Proposition 3: For the given solution set of (46), (47) can be obtained from

$$\begin{aligned}\mathcal{OU}(l) &= \Pr\left\{ c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r^*) \le \text{C}_{\min}^{\text{PT}\to\text{PR}} \right\} \\ &= 1 - \prod_{e=1}^{E} \left(1 - \int_0^{+\infty} \frac{x^{\frac{1-T_2}{T_2}}}{T_2} \times \right. \\ &\left[\int_0^{+\infty} F_{\gamma^1_{\text{PT}\to\text{ST}}}\left(\sqrt[T_1]{\frac{2^{\text{C}_{\min}^{\text{PT}\to\text{PR}}}}{x}}(y+1) - 1 \right) f_{\gamma^1_{\text{PT}\to e}}(y) dy \right] \\ &\left. \times \left[\int_0^{+\infty} (y'+1) f_{\gamma^2_{\text{PT}\to\text{ST}}}\left(\sqrt[T_2]{x}(y'+1) - 1 \right) f_{\gamma^2_{\text{PT}\to e}} dy' \right] dx \right)\end{aligned} \tag{48}$$

Proof: See Appendix C. ■

TABLE III
ALGORITHM II

Step1: Initialize the auxiliary variable, $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l=1)$
Step2: Generate the new optimization problem at the l^{th} iteration from (46),
Step2.1: Find the appropriate power, relay and time from section III,
Step3: Compute the outage probability of secrecy rate at the l^{th} iteration, $\mathcal{OU}(l)$ from (47),
Step4: Compute $\mathcal{D}(l) = |\mathcal{OU}(l) - \zeta|$,
Step4.1: If $\mathcal{D}(l) \le \epsilon$, then **go to *Step5***,
Step4.2: Compute $\theta(l) = 1 - \mathcal{D}(l)$ and adjust the auxiliary variables as $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l) = \theta(l)\hat{\text{C}}_{\min}^{\text{PT},\to\text{PR}}(l-1)$, then go to ***Step2***,
Step5: End.

In the sequel, we discuss convergence behavior and speed for Algorithm II. The initial value of $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l)$ is assumed to be very large, making $\mathcal{OU}(l=0)$ pretty close to 1. Hence, $\mathcal{D}(l=0)$ is definitely larger than ϵ. Since $\theta(l) \in [0,1]$ and $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l) = \theta(l)\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l-1)$, $\hat{\text{C}}_{\min}^{\text{PT}\to\text{PR}}(l)$, $\mathcal{OU}(l)$ and $\mathcal{D}(l)$ are decreasing functions with respect to l. Meanwhile $\theta(l)$ is an increasing function with respect to l. Therefore, when $l \to \infty$, $\theta(l)$ tends to 1, implying the convergence of the iterative algorithm.

Note that the speed of convergence can be controlled via Θ. In fact for larger values of Θ, the speed of convergence of algorithm is increased which leads to the reduction of ergodic rate. This is mainly due to the fact that for larger values of Θ, the algorithm jumps over some feasible solutions that may satisfy the probabilistic constraints while they are not global or even strong local optimums. Therefore, a compromise between the complexity of the RA problem and the performance of the secondary network can be obtained via Θ.

V. Imperfect Channel State Information

In this section, we consider a situation where the CSI values between the PU, the SU, relays and eavesdroppers are imperfectly known. We then propose a robust approach to solve the corresponding IRA and ERA problems.

A. Imperfect CSI in IRA

To model the imperfect CSI, the actual value of CSI is considered as the sum of the nominal value of the CSI (the estimated value of the CSI by users) and an additive error [28], e.g.,

$$\mathbf{h}_{\text{PT}\to\text{E}} = \bar{\mathbf{h}}_{\text{PT}\to\text{E}} + \hat{\mathbf{h}}_{\text{PT}\to\text{E}}. \tag{49}$$

where $\mathbf{h}_{\text{PT}\to\text{E}}$, $\bar{\mathbf{h}}_{\text{PT}\to\text{E}}$, and $\hat{\mathbf{h}}_{\text{PT}\to\text{E}}$ are $1\times E$ vectors representing the exact, nominal and additive error of CSI values where their e^{th} elements are denoted by $h_{\text{PT}\to e}$, $\bar{h}_{\text{PT}\to e}$ and $\hat{h}_{\text{PT}\to e}$[2]. For the IRA problem, we apply the worst-case optimization theory as it can preserve the primary secrecy rate under any condition of error where the error is assumed to be bounded in a closed region called uncertainty region [28], [29]. Usually, uncertainly regions for imperfect CSI values are defined by general norm functions such as, e.g., [28]

$$\mathbf{h}_{\text{PT}\to\text{E}} \in \mathcal{R}_{\text{PT}\to\text{E}} = \{\mathbf{h}_{\text{PT}\to\text{E}} \big| \|\mathbf{h}_{\text{PT}\to\text{E}} - \bar{\mathbf{h}}_{\text{PT}\to\text{E}}\| \le \varepsilon_{\text{PT}\to\text{E}}\}, \tag{50}$$

$$\mathbf{h}_{\text{ST}\to\text{E}} \in \mathcal{R}_{\text{ST}\to\text{E}} = \{\mathbf{h}_{\text{ST}\to\text{E}} \big| \|\mathbf{h}_{\text{ST}\to\text{E}} - \bar{\mathbf{h}}_{\text{ST}\to\text{E}}\| \le \varepsilon_{\text{ST}\to\text{E}}\}, \tag{51}$$

$$\mathbf{h}_{r\to\text{E}} \in \mathcal{R}_{r\to\text{E}} = \{\mathbf{h}_{r\to\text{E}} \big| \|\mathbf{h}_{r\to\text{E}} - \bar{\mathbf{h}}_{r\to\text{E}}\| \le \varepsilon_{r\to\text{E}}\},\ \forall r \in \mathcal{R}, \tag{52}$$

$$\mathbf{h}_{\text{SR}\to\text{E}} \in \mathcal{R}_{\text{SR}\to\text{E}} = \{\mathbf{h}_{\text{SR}\to\text{E}} \big| \|\mathbf{h}_{\text{SR}\to\text{E}} - \bar{\mathbf{h}}_{\text{SR}\to\text{E}}\| \le \varepsilon_{\text{SR}\to\text{E}}\}, \tag{53}$$

where $\|\mathbf{x}\|$ is the general norm function. Through the worst case robust optimization theory, the allocated power vector is derived such that in the worst case condition of error in the uncertainty region, the worst case secrecy rate of PU is preserved and the minimum secrecy rate of SU is achieved. Mathematically, the worst case robust counterpart of (15) may be expressed as

$$\max_{\mathcal{Q}} \min_{\mathcal{H}} \sum_{r=1}^{R} \rho_r \bar{c}_{\text{ST}\to r\to\text{SR}}(e^{\boldsymbol{q}^1}, r), \tag{54}$$

$$\text{C}_1 : \sum_{r=1}^{R} \rho_r \bar{c}_{\text{PT}\to\text{PR}}(e^{\boldsymbol{q}}, r) \ge \text{C}_{\min}^{\text{PT}\to\text{PR}}, \quad \forall \mathbf{h} \in \mathcal{H},$$

where $\mathbf{h}$ is the vector of all CSIs in our set up and $\mathcal{H}$ is the set of all the uncertainty regions defined in (50)-(53). Note that (54) is a cumbersome optimization problem and its computational complexity is directly dependent on the definition of norm functions. To simplify the problem and reduce the computational complexity, we utilize the D-norm approach introduced in [30] where each uncertainty region is transformed into the bounded interval, e.g., $h_{\text{PT}\to e} \in [h_{\text{PT}\to e} - \varepsilon_{\text{PT}\to e},\ h_{\text{PT}\to e} + \varepsilon_{\text{PT}\to e}]$ where $\varepsilon_{\text{PT}\to e}$ is the bound of uncertainty region represented by D-norm. Following by the worst case robust optimization, the lower bound of the uncertainty region is considered for each CSI between each transmitter and each eavesdropper. Thus, the robust power allocation problem is transformed into the nominal power allocation problem, e.g., (15), except that all the CSIs between transmitters and eavesdroppers are modified.

B. Imperfect CSI for ERA

In NP-ERA with imperfect CSI, the marginal distribution for each channel is required [21], [22]. Again, the uncertain parameters can be rewritten as (49). The marginal fading distribution for each eavesdropper conditioned on the estimated value is non-zero mean complex Gaussian random variable denoted by $h_{\text{PT}\to\text{E}}|\bar{h}_{\text{PT}\to\text{E}} \sim \mathcal{CN}(\bar{h}_{\text{PT}\to\text{E}}, \sigma^2_{\text{PT}\to\text{E}})$ where $\sigma^2_{\text{PT}\to\text{E}}$ is the prediction of error variance [22]. The same can be applied to (51)-(53). Now, Algorithm I can be applied, except that the Lagrange function is solved based on the conditional means of the CSI values given their estimates, instead of the actual CSI values [22]. The same can also be applied for the P-ERA using Algorithm II, except that at each iteration, conditional means of CSI values given their estimates are used instead of the actual CSI values.

[2]Similar notations are considered for other imperfect CSI values in this section.

VI. Simulation Results

In this section, we provide simulation results to evaluate the performance of the proposed schemes for perfect and imperfect CSI for both IRA and ERA. We assume that all the nodes in the network are placed in the circle with the diameter 5 Km and $h_{m\to n} = \iota/d^{\varsigma}_{m\to n}$ where $d_{m\to n}$ is the distance between transmitter m and receiver n and ι is the fading coefficient and $1 \le \varsigma \le 4$ where ι is taken from a normalized Rayleigh distribution. Maximum power of the ST, SR, PT, and relays are set to 20 Watt and $N_0 B = 1$. We also set $\text{C}_{\min}^{\text{PT}\to\text{PR}} = 2$ Bit/Sec/Hz and R, the number of relay nodes, to 15 unless otherwise stated.

A. Performance Comparison between the Proposed Paradigm and Conventional Underlay Approach

In this paper, our objective is to maximize the secrecy rate of the secondary user subject to guaranteeing a given secrecy rate for primary user as opposed to conventional case where such maximization is subject to the interference threshold constraint. Meanwhile, it is important to see whether using the new constraint causes the secondary secrecy rate to decrease compared to 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. 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. 2, we have reported the values of the resulting primary secrecy rates versus $\frac{h_{\text{ST}\to\text{PR}}}{h_{\text{PT}\to\text{PR}}}$ for different values of interference threshold in IRA case.

Now for different values of primary secrecy rate reported in Fig. 2, we solve the proposed IRA 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 conventional scheme. In Fig. 3, we have plotted η versus $\frac{h_{\text{ST}\to\text{PR}}}{h_{\text{PT}\to\text{PR}}}$. As can be seen in Fig. 3, the value of η is always greater than or equal to 1, implying that the new constraint always provides a superior secondary secrecy rate. This superiority is more pronounced for smaller values of $\frac{h_{\text{ST}\to\text{PR}}}{h_{\text{PT}\to\text{PR}}}$. In other words, we have been able to maintain the secrecy rate of PU, and yet such a benefit has not come at any cost to the secondary secrecy rate. Moreover, as can be seen in Fig. 2, increasing the amount of tolerable interference

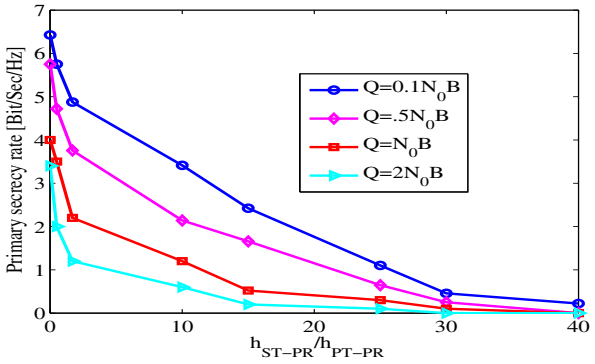

Fig. 2. The primary secrecy rate resulting from the conventional problem versus $\frac{h_{ST\to PR}}{h_{PT\to PR}}$ for different values of Q in IRA.

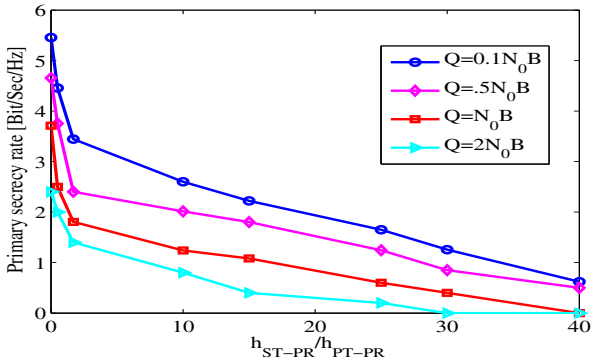

Fig. 4. The primary secrecy rate resulting from the conventional problem versus $\frac{h_{ST\to PR}}{h_{PT\to PR}}$ for different values of Q in ERA.

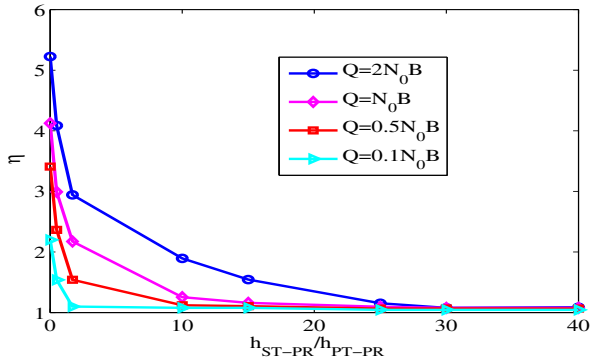

Fig. 3. Comparing the secondary secrecy rate of the proposed paradigm for IRA and the conventional underlay approach versus $\frac{h_{ST\to PR}}{h_{PT\to PR}}$ for different values of Q.

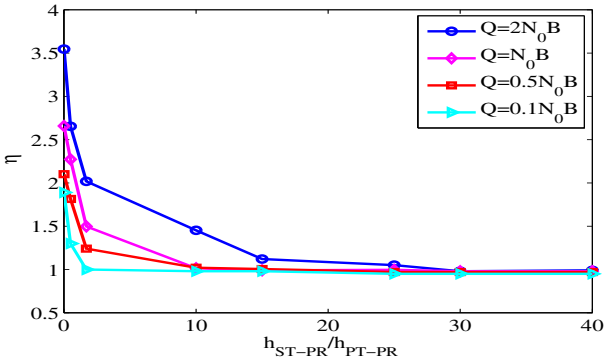

Fig. 5. Comparing the secondary secrecy rate of the proposed paradigm for ERA and the conventional underlay approach versus $\frac{h_{ST\to PR}}{h_{PT\to PR}}$ for different values of Q.

threshold may cause the secrecy rate of PU to considerably decrease and even tend to zero. In such cases, changing the interference threshold constraint to the one proposed by us can guarantee a desired primary secrecy rate while providing a secondary secrecy rate equal or better than the conventional case. Figs. 4 and 5 demonstrate the same trend for secrecy rate of PU and SU for ERA problems.

B. Effect of System Parameters on the SU's Secrecy Rate

In this part, we investigate the effect of system parameters (e.g., perfect and imperfect CSI values, the value of C_{min}^{PT} and the number of relays) on the performance of CRNs for both IRA and ERA.

1) SU's Secrecy Rate in IRA Problem: We demonstrate the effect of increasing the value of C_{min}^{PT} on SU's secrecy rate for IRA in Fig. 6 versus the number of relays. In this figure, $R = 0$ indicates the case where there is no relay node in the network and the SU directly transmits to its corresponding receiver. Clearly, by increasing the number of relays and decreasing the value of C_{min}^{PT}, the secondary secrecy rate is increased. Comparing the secrecy rate of SU for $R = 0$ and $R = 1$ reveals that introducing the set of relay node in CRN considerably increases the secrecy rate of SU while maintains the minimum required secrecy rate of the PU for different values of C_{min}^{PT}. This can be associated to the feasibility set of the IRA problem. As shown in Section II.B, the feasibility set of the IRA problem expands by decreasing the value of C_{min}^{PT} as well as increasing the number of relay. This leads to increasing the secrecy rate of the SU [24].

We also study the effect of expanding the uncertainty region on the secondary secrecy rate of SUs in the IRA in case of imperfect CSI. In this simulation, we assume that the bound of uncertainty regions for (50) - (53) are equal and normalized to the value of estimated CSI values, e.g., $\varepsilon = \varepsilon_{PT\to e}\% = \frac{\|\mathbf{h}_{PT\to e}-\bar{\mathbf{h}}_{PT\to e}\|}{\bar{\mathbf{h}}_{PT\to e}}$. In Fig. 7, the effect of increasing the value of ε on reduction of SU's secrecy rate is demonstrated. Obviously, with increasing the value of ε, the secondary secrecy rate is decreased. This is because based on the worst case robust optimization theory, the SU acts very conservatively against the uncertainty in the CSI between the PU and each eavesdropper and tries to keep the minimum required primary secrecy rate in the maximum extent. Consequently, the SU and relay nodes allocate their transmit power in such a way that the rate of *each eavesdropper* is suppressed and reaching their own maximum secrecy rate is not a priority. This fact is also supported by comparing rate reduction of the SU under different values of C_{min}^{PT}. For larger value of C_{min}^{PT}, the SU's rate reduction is larger compared to smaller values of C_{min}^{PT}.

2) SU's Secrecy Rate in ERA Problem: The effect of increasing the value of C_{min}^{PT} for ERA problem is demonstrated in Fig. 8. In the simulations of this part, we set $\sigma_{PT\to E} = 0.1$ for NP-ERA and P-ERA with imperfect CSI. Fig. 8 shows that by increasing the value of C_{min}^{PT}, the SU's secrecy rate

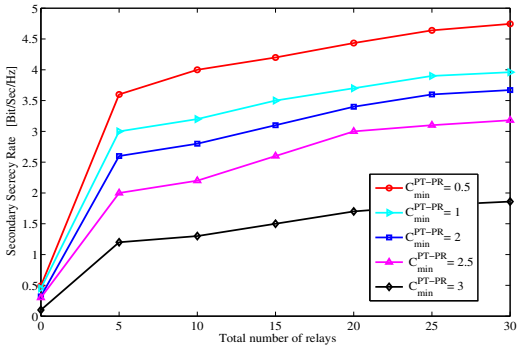

Fig. 6. The effect of increasing the value of C_{min}^{PT} on the SU's secrecy rate for IRA for different number of relays.

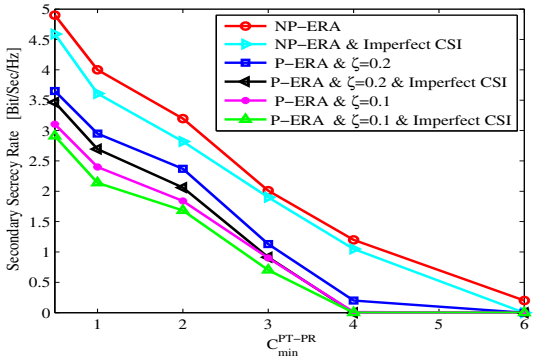

Fig. 8. The effect of increasing the value of C_{min}^{PT} on the SU's secrecy rate for ERA.

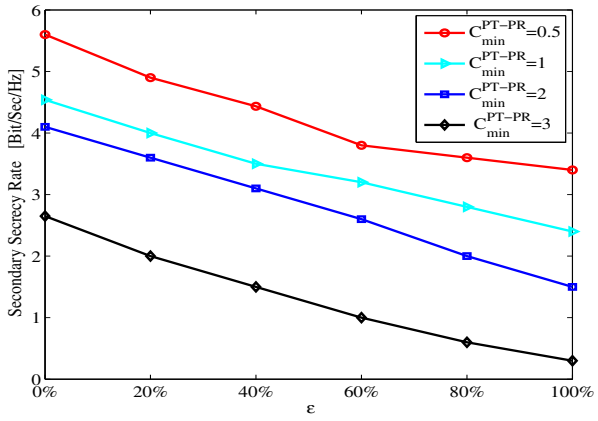

Fig. 7. The secondary secrecy rate versus bound of uncertainty region for different values of C_{min}^{PT}.

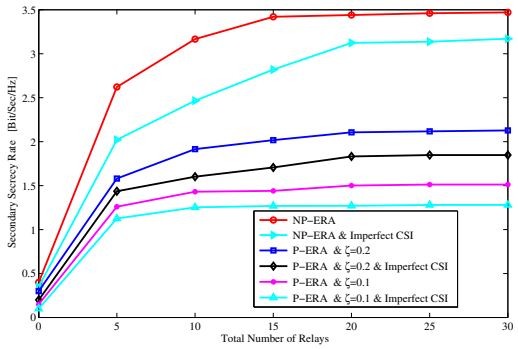

Fig. 9. The effect of increasing the number of relays on the secondary secrecy rate for ERA.

is dramatically decreased. Comparing NP-ERA and P-ERA, we can see that while P-ERA is very desirable from the PU's perspective, it provides a lower rate for the SU. On the other hand in NP-ERA, the SU enjoys a higher rate while the outage probability for primary secrecy rate is increased to fifty percent.

Fig. 9 demonstrates the secondary secrecy rate versus the number of relay nodes in CRNs for NP-ERA and P-ERA. For all schemes of ERA, by increasing the number of relay nodes, the SU's secrecy rate is increased. Clearly, for both NP-ERA and P-ERA, when $R = 0$, the secrecy rate is too small. On the other hand, by introducing one relay node in the network, the secrecy rate of SU is increased considerably which shows the benefit of the proposed introduced cooperative paradigm in CRNs.

C. Effect of Relay Selection Methods on the Secondary Secrecy Rate

We plot the secondary secrecy rate for different relay selection algorithms in Figs. 10 and 11 for both IRA and ERA, respectively. Again, when $R = 0$, the secondary secrecy rate is very small for both IRA and ERA. However, for all methods, by increasing the number of relays, the SU can experience a larger value of secrecy rate as expected. Interestingly, the performance of MPSR is very close to the optimal relay selection. It means that via MPSR with less computational complexity, we attain the near optimal solution which is very desirable from practical implementation perspective. In contrast, the performance of MIP approach is not convincing from the SU's perspective.

D. Effect of Time Allocation on the SU's Secrecy Rate

In Figs. 12 and 13, the SU's secrecy rate versus $\frac{h_{PT\to e}}{h_{PT\to PR}}$ is shown for both IRA and ERA, respectively in two modes: 1) The time intervals of two hops are equal: $T_1 = T_2 = T/2$, referred to as symmetric time allocation, 2) The time intervals of T_1 and T_2 are obtained from Section III. C. 3, referred to as the asymmetric time allocation. From Figs. 12 and 13, it is obvious that the asymmetric time allocation has a better performance in terms of achievable secondary secrecy rate compared to that of the symmetric time allocation for IRA, NP-ERA and P-ERA. When the channel gain between the PU and each eavesdropper increases, the asymmetric time allocation considerably increases the SU's secrecy rate compared to that for the symmetric time allocation. This was already predicted in Section III. B, since by choosing asymmetric time allocation, we are in fact expanding the feasibility set.

E. Iterative Algorithm and its Convergence Behavior

In Figs. 14 and 15, we study the effect of the value of Θ on the performance of iterative algorithm. Fig. 14 demonstrates

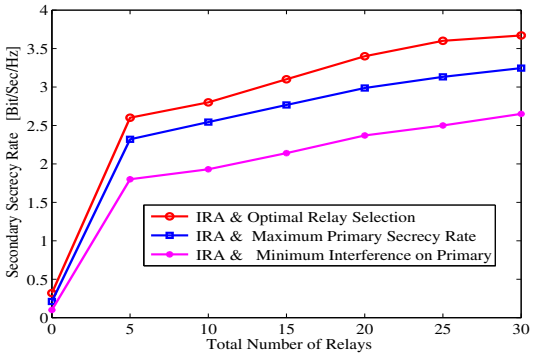

Fig. 10. The effect of relay selection algorithm on the SU's rate for IRA.

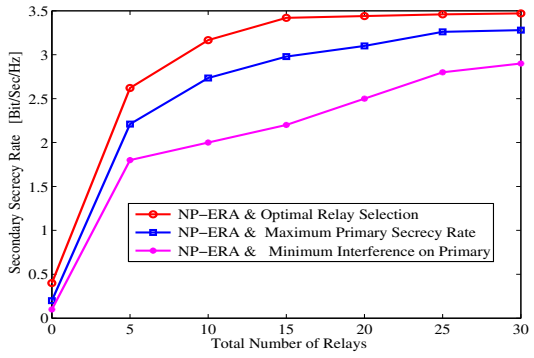

Fig. 11. The effect of relay selection algorithm on the SU's rate for ERA.

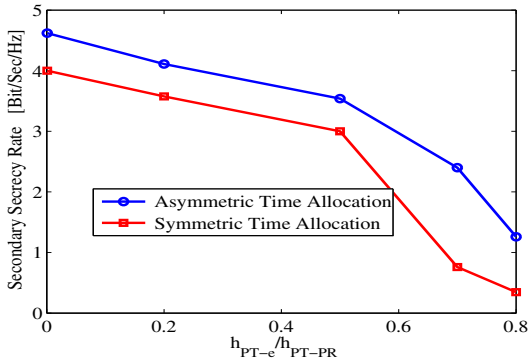

Fig. 12. The SU's secrecy rate versus $\frac{h_{\mathrm{PT}\to e}}{h_{\mathrm{PT}\to \mathrm{PR}}}$ for symmetric and asymmetric time allocation in IRA.

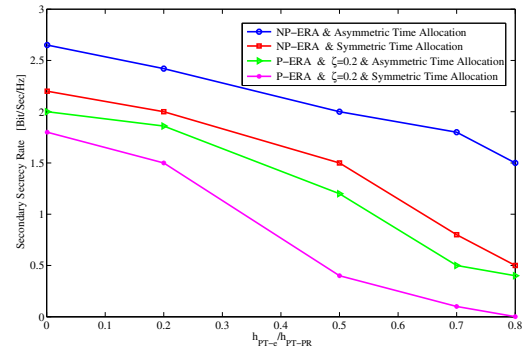

Fig. 13. The SU's secrecy rate versus $\frac{h_{\mathrm{PT}\to e}}{h_{\mathrm{PT}\to \mathrm{PR}}}$ for symmetric and asymmetric time allocation in ERA.

that increasing the value of Θ reduces the SU's secrecy rate in P-ERA for any value of ζ while it reduces the convergence time of iterative algorithm as shown in Fig. 15.

These two figures highlight the effect of Θ on the trade-off between optimality and convergence time for iterative algorithm in CRNs. When a smaller convergence time to reach the solution is required (e.g., in highly dynamic situation such as fast moving users in CRNs), the larger value of Θ is appealing at the cost of reducing SU's secrecy rate. For the case of slow moving users, we can use a smaller value for Θ to reach a larger utility.

VII. Conclusion

In this paper, we proposed a novel cooperative paradigm for secure communication in cognitive radio networks where we simultaneity provide secure communications for both primary and secondary services. The proposed setting is different from previously proposed schemes where maximizing the secondary secrecy rate is only subject to maintaining a certain level quality of service for primary users via the interference threshed constraint. In the proposed IRA and ERA problems, transmit power, relay and time duration of two hops are chosen to maximize the secondary secrecy rate while preserving the primary secrecy rate. By considering imperfect channel state information, we then proposed the robust counterparts of the the proposed IRA and ERA problems and investigated the effect of uncertain parameters on the performance of the system. The proposed idea in fact transforms the possibly disturbing secondary service activities to a beneficial network element.

Appendix A
Proof of Proposition 1

When $T_1 = T_2 = T/2$, C1 in (15) is transformed into $1/2[\log_2(\frac{P_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}}}{N_0B+I^1_{\mathrm{PR}}}) - \log_2(\frac{P_{\mathrm{PT}}h_{\mathrm{PT}\to e}}{N_0B+I^1_{\mathrm{PR}\to e}}) + \log_2(\frac{P_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}}}{N_0B+I^2_{\mathrm{PR}}}) - \log_2(\frac{P_{\mathrm{PT}}h_{\mathrm{PT}\to \mathrm{PR}}}{N_0B+I^2_{\mathrm{PR}\to e}}) \geq C_{\min}$, and for the case of high SINR, i.e., $N_0B << 1$, it is simplified to

$$\frac{h_{\mathrm{PT}\to \mathrm{PR}}}{h_{\mathrm{PT}\to e}}\frac{N_0B+I^1_{\mathrm{PR}\to e}}{N_0B+I^1_{\mathrm{PR}}} \times \frac{h_{\mathrm{PT}\to \mathrm{PR}}}{h_{\mathrm{PT}\to e}}\frac{N_0B+I^2_{\mathrm{PR}\to e}}{N_0B+I^2_{\mathrm{PR}}} \geq 2^{2C_{\min}}, \tag{A.1}$$

which can be rewritten as

$$(\frac{h_{\mathrm{PT}\to \mathrm{PR}}}{h_{\mathrm{PT}\to e}})^2 \times \chi^1 \times \chi^2 \geq 2^{2C_{\min}}, \tag{A.2}$$

where

$$\chi^1 = \frac{I^1_{\mathrm{PR}\to e}}{I^1_{\mathrm{PR}}} = \frac{h_{\mathrm{ST}\to e}}{h_{\mathrm{ST}\to \mathrm{PR}}} \times \frac{1+\frac{p^1_{\mathrm{SR}}h_{\mathrm{SR}\to e}}{p^1_{\mathrm{ST}}h_{\mathrm{ST}\to e}}}{1+\frac{p^1_{\mathrm{SR}}h_{\mathrm{SR}\to \mathrm{PR}}}{p^1_{\mathrm{ST}}h_{\mathrm{ST}\to \mathrm{PR}}}}, \tag{A.3}$$

and

$$\chi^2 = \frac{I^2_{\mathrm{PR}\to e}}{I^2_{\mathrm{PR}}} = \frac{h_{\mathrm{ST}\to e}}{h_{\mathrm{ST}\to \mathrm{PR}}} \times \frac{1+\frac{p^2_r h_{r\to e}}{p^2_{\mathrm{ST}}h_{\mathrm{ST}\to e}}}{1+\frac{p^2_r h_{r\to \mathrm{PR}}}{p^2_{\mathrm{ST}}h_{\mathrm{ST}\to \mathrm{PR}}}}. \tag{A.4}$$

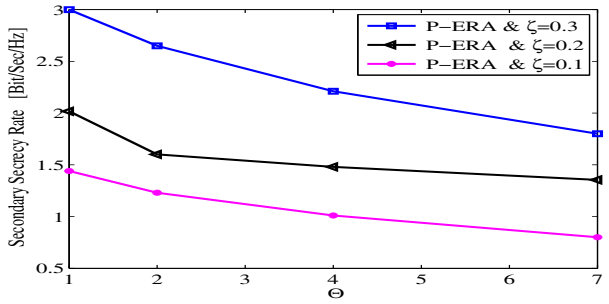

Fig. 14. Effect of the value of Θ on the SU's secrecy rate.

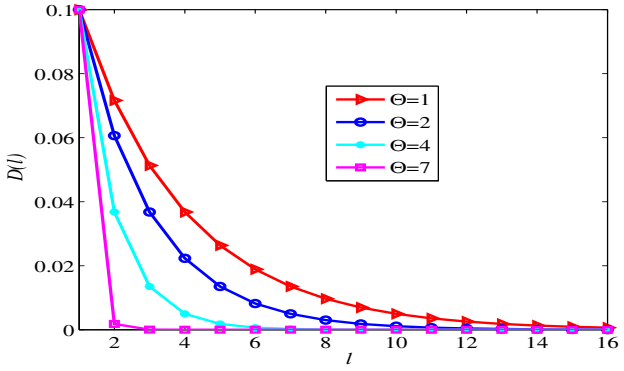

Fig. 15. Effect of the value of Θ on convergence speed of Algorithm II.

To simplify (A.2), let us consider $\chi^1 = \frac{h_{\text{SR}\to e}}{h_{\text{SR}\to \text{PR}}}$ and $\chi^2 = \frac{h_{r\to e}}{h_{r\to \text{PR}}}$. This case corresponds to the condition that the friendly jamming effects of ST, SR and relay r are beneficial for PR, i.e., the imposed interferences of ST, SR and relay r on the eavesdropper e is larger than that of PR. Now, we have

$$(\frac{h_{\text{PT}\to \text{PR}}}{h_{\text{PT}\to e}})^2 \frac{h_{\text{SR}\to e}}{h_{\text{SR}\to \text{PR}}} \frac{h_{r\to e}}{h_{r\to \text{PR}}} \geq 2^{2C_{\min}}. \tag{A.5}$$

(15) is feasible, if there exists one relay node that satisfies (A.5). Consequently, the feasibility region in (18) is derived.

Appendix B
Proof of Proposition 2

To prove the lower bound of secrecy rate, let z_l^1 and z_l^2 be the legitimate and eavesdropper SINR at iteration l, respectively. Accordingly, the secrecy rate can be obtained as follows

$$C_l = \left[\log(1+z_l^1) - \log(1+z_l^2)\right]^+. \tag{B.1}$$

Fact 1: Since C_l is greater than or equal to zero, we have $z_l^1 \geq z_l^2$. Therefore, the secrecy rate can be rewritten as

$$C_l = \log(1+z_l^1) - \log(1+z_l^2). \tag{B.2}$$

The lower bound of secrecy rate based on scale algorithm is defined as

$$\bar{C}_l = \alpha_l^1 \log(z_l^1) + \beta_l^1 - \alpha_l^2 \log(z_l^2) - \beta_l^2, \tag{B.3}$$

where $\alpha_l^1 = \frac{z_{l-1}^1}{1+z_{l-1}^1}$, $\beta_l^1 = \log(1+z_{l-1}^1) - \frac{z_{l-1}^1}{1+z_{l-1}^1}\log(z_{l-1}^1)$, $\alpha_l^2 = \frac{z_{l-1}^2}{1+z_{l-1}^2}$ and $\beta_l^2 = \log(1+z_{l-1}^2) - \frac{z_{l-1}^2}{1+z_{l-1}^2}\log(z_{l-1}^2)$. Now, we want to prove that

$$C_l \geq \bar{C}_l. \tag{B.4}$$

By substituting (B.2) and (B.3) into (B.4), we have

$$\begin{aligned}\log(1+z_l^1) - \log(1+z_l^2) \geq & \\ \frac{z_{l-1}^1}{1+z_{l-1}^1}\log(z_l^1) + \log(1+z_{l-1}^1) - & \\ \frac{z_{l-1}^1}{1+z_{l-1}^1}\log(z_{l-1}^1) - \frac{z_{l-1}^2}{1+z_{l-1}^2}\log(z_l^2) & \\ - \log(1+z_{l-1}^2) + \frac{z_{l-1}^2}{1+z_{l-1}^2}\log(z_{l-1}^2). &\end{aligned} \tag{B.5}$$

With some mathematical manipulation, (B.5) is transformed into

$$\begin{aligned}&\left[\log(\frac{1+z_l^1}{z_l^{1\frac{z_{l-1}^1}{1+z_{l-1}^1}}}) - \log(\frac{1+z_l^2}{z_l^{2\frac{z_{l-1}^2}{1+z_{l-1}^2}}})\right] - \\ &\left[\log(\frac{1+z_{l-1}^1}{z_{l-1}^{1\frac{z_{l-1}^1}{1+z_{l-1}^1}}}) - \log(\frac{1+z_{l-1}^2}{z_{l-1}^{2\frac{z_{l-1}^2}{1+z_{l-1}^2}}})\right] \geq 0.\end{aligned} \tag{B.6}$$

Fact 2: For such an iterative algorithm, based on Theorem 2 of [25], $C_l \geq C_{l-1}$ and, then consequently we have $z_l^1 \geq z_{l-1}^1$ and $z_l^2 \leq z_{l-1}^2$. Based on Fact 1, the first and second term of (B.6) is no-negative. Moreover, Based on Fact 2, the first term is greater than or equal of the second term. Consequently, the lower bound always holds.

Appendix C
Proof of Proposition 3

To prove the equality of (48), let X_1, Y_1 , X_2 and Y_2 be four independent random variables and let $Z_1 = \frac{1+X_1}{1+Y_1}$, $Z_2 = \frac{1+X_2}{1+Y_2}$, and $W = Z_1^{T_1} Z_2^{T_2} = W_1 W_2$. The CDF of Z_1 is given by

$$\begin{aligned}F_{Z_1}(z_1) &= \Pr\{\frac{1+X_1}{1+Y_1} < z_1\} \\ &= \mathbf{E}_Y\left\{\Pr\left\{X_1 < z_1(1+Y_1) - 1 | Y_1\right\}\right\} \\ &= \int_0^{+\infty} F_{X_1}(z_1(y+1)-1) f_{Y_1}(y) dy.\end{aligned} \tag{C.1}$$

Similar to (C.1), the CDF of Z_2 is obtained as

$$F_{Z_2}(z_2) = \int_0^{+\infty} F_{X_2}(z_2(y+1)-1) f_{Y_2}(y) dy. \tag{C.2}$$

From (C.1) and (C.2), the CDF of W_1 and W_2 can be obtained as $F_{W_1}(w) = \Pr\{Z_1^{T_1} < w\} = F_{Z_1}(\sqrt[T_1]{w})\}$ and $F_{W_2}(w) = \Pr\{Z_2^{T_2} < w\} = F_{Z_2}(\sqrt[T_2]{w})\}$. Now, the CDF of W is yielded

as

$$F_W(w) = \Pr\{W_1 W_2 < w\} = \int_0^{+\infty} F_{W_1}(\frac{w}{x}) f_{W_2}(x)dx = \int_0^{+\infty} F_{Z_1}(\sqrt[T_1]{\frac{w}{x}}) \frac{x^{\frac{1-T_2}{T_2}}}{T_2} f_{Z_2}(\sqrt[T_2]{x})dx = \int_0^{+\infty} \frac{x^{\frac{1-T_2}{T_2}}}{T_2} \left[\int_0^{+\infty} F_{X_1}(\sqrt[T_1]{\frac{w}{x}}(y+1) - 1) f_{Y_1}(y)dy \right] \left[\int_0^{+\infty} (y'+1) f_{X_2}(\sqrt[T_2]{x}(y'+1) - 1) f_{Y_2}(y')dy' \right] \quad \text{(C.3)}$$

By rewriting $\mathcal{OU}(l)$ as

$$\mathcal{OU}(l) = \Pr\left\{ \min_e \left\{ c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r^*, e) < \text{C}_{\min}^{\text{PT}\to\text{PR}} \right\} \right\} = 1 - \prod_{e=1}^{E} \Pr\left\{ c_{\text{PT}\to\text{PR}}(\boldsymbol{p}, r^*, e) \geq \text{C}_{\min}^{\text{PT}\to\text{PR}} \right\} \quad \text{(C.4)}$$

$$= 1 - \prod_{e=1}^{E} \left(1 - \Pr\left\{ \left(\frac{1+\gamma_{\text{PT}\to\text{ST}}^1}{1+\gamma_{\text{PT}\to e}^1} \right)^{T_1} \times \left(\frac{1+\gamma_{\text{PT}\to\text{ST}}^2}{1+\gamma_{\text{PT}\to e}^2} \right)^{T_2} \leq 2^{\text{C}_{\min}^{\text{PT}\to\text{PR}}} \right\} \right).$$

and using the above equality the proposition is proved.

REFERENCES

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: an information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

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

[3] F. Renna, N. Laurenti, and H. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

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

[5] A. Mukherjee, A. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[6] J. Chen, R. Zhang, L. Song, and Z. H. B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[7] E. Tekin and A. Yener, "The general gaussian multiple access and twoway wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 4005-4019, June 2008.

[8] 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, 2013.

[9] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[10] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153-3167, May 2011.

[11] Y. Liang, A. Somekh-Baruch, H. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[12] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security,*, vol. 6, no. 3, pp. 831–842, Sept. 2011.

[13] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, June 2010.

[14] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[15] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[16] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, June 2012.

[17] K. Lee, O. Simone, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. 2011 IEEE Int. Conf. Commun.*

[18] J. Papandriopoulos and J. Evans, "Low-complexity distributed algorithms for spectrum balancing in multi-user DSL networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 46, no. 5, pp. 3270–3275, June 2006.

[19] L. V. S. Boyd, S.-J. Kim, and A. Hassibi, "A tutorial on geometric programming," *Optimization Eng.*, vol. 7, no. 5, pp. 67–127, 2007.

[20] N. Mokari, K. Navaie, and M. G. Khoshkholgh, "Downlink radio resource allocation in OFDMA spectrum sharing environment with partial channel state information," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3482–3495, Oct. 2011.

[21] I. C. Wong and B. L. Evans, "Optimal downlink OFDMA resource allocation with linear complexity to maximize ergodic capacity," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 962–971, Mar. 2008.

[22] I. Wong and B. Evans, "Optimal resource allocation in the OFDMA downlink with imperfect channel knowledge," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 232–241, 2009.

[23] M. Chiang, P. Hande, T. Lan, and C. W. Tan, "Power control in wireless cellular networks," *Foundations Trends Netw.*, vol. 2, no. 4, pp. 381–533, July 2008.

[24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[25] T. Wang and L. Vandendorpe, "Iterative resource allocation for maximizing weighted sum min-rate in downlink cellular OFDMA systems," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 223–234, 2011.

[26] Y. Nesterov and A. Nemirovsky, *Interior Point Polynomial Methods in Convex Programming.* SIAM Press, 1994.

[27] J. Lofberg, "Yalmip: yet another LMI parser." Available: http://control.ee.ethz.ch/~joloef/yalmip.php., 2003.

[28] A. B. Gershman and N. D. Sidiropoulos, *Space-Time Processing for MIMO Communications*. John Wiley and Sons, 2005.

[29] A. Ben-Tal and A. Nemirovski, "Selected topics in robust convex optimization," *Mathematical Programming*, vol. 1, no. 1, pp. 125–158, July 2007.

[30] D. Bertsimas and M. Sim, "The price of robustness," *Operations Research*, vol. 52, no. 1, pp. 35–53, Feb. 2004.

Nader Mokari is a Ph.D. student at Tarbiat Modares University, Tehran, Iran. His main research interests include wireless communications, radio resource allocation, secure communication, and spectrum sharing techniques. He is a student member of IEEE.

Saeedeh Parsaeefard (S'09) received the B.Sc. and M.Sc. degrees from Amirkabir University of Tech1nology (Tehran Polytechnic), Tehran, Iran, in 2003 and 2006, respectively, and the Ph.D. degree in electrical and computer engineering from Tarbiat Modares University, Tehran, in 2012. She is currently a Post-Doctoral Research Fellow with the Telecommunication and Signal Processing Laboratory in the Department of Electrical and Computer Engineering at the McGill University, Canada. From November 2010 to October 2011, she was a Visiting Ph.D. Student with the Department of Electrical Engineering, University of California, Los Angeles, CA, USA. Her current research interests include the applications of robust optimization theory and game theory on the resource allocation and management in wireless networks.

Hamid Saeedi (S'01-M'08) received the B.Sc. and M.Sc. degrees from Sharif University of Technology, Tehran, Iran, in 1999 and 2001, respectively, and the Ph.D. degree from Carleton University, Ottawa, ON, Canada, in 2007, all in electrical engineering. In 2008-2009, he was a postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, USA. In 2010, he joined the Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran, where he is now an Assistant Professor. His research interests include coding and information theory, wireless communications, and cognitive radio networks.

Dr. Saeedi is the recipient of some awards including Carleton University Senate Medal for Outstanding Academic Achievement, a Natural Sciences and Engineering Council of Canada (NSERC) Industrial Research and Development Fellowship, and an Ontario Graduate Scholarship.

Paeiz Azmi was born in Tehran, Iran, on April 17, 1974. He received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 1996, 1998, and 2002, respectively. Since September 2002, he has been with the Electrical and Computer Engineering Department of Tarbiat Modares University, Tehran, Iran, where he became an associate professor on January 2006 and he is currently a full professor.

From 1999 to 2001, Prof. Azmi was with the Advanced Communication Science Research Laboratory, Iran Telecommunication Research Center (ITRC), Tehran, Iran. From 2002 to 2005, he was with the Signal Processing Research Group at ITRC. Prof. Azmi is a senior member of IEEE.

His current research interests include modulation and coding techniques, digital signal processing, wireless communications, and estimation and detection theories.