Enhancing Secrecy Rate in Cognitive Radio Networks via Stackelberg Game

Ali Al-Talabani, *Member, IEEE*, Yansha Deng, *Member, IEEE*,
Arumugam Nallanathan, *Senior Member, IEEE*, and Huan X. Nguyen, *Senior Member, IEEE*

***Abstract*— In this paper, a game theory-based cooperation scheme is investigated to enhance the physical layer security in both primary and secondary transmissions of a cognitive radio network (CRN). In CRNs, the primary network may decide to lease its own spectrum for a fraction of time to the secondary nodes in exchange of appropriate remuneration. We consider the secondary transmitter node as a trusted relay for primary transmission to forward primary messages in a decode-and-forward fashion and, at the same time, allows part of its available power to be used to transmit artificial noise (i.e., jamming signal) to enhance primary and secondary secrecy rates. In order to allocate power between message and jamming signals, we formulate and solve the optimization problem for maximizing the secrecy rates under malicious attempts from eavesdroppers. We then analyze the cooperation between the primary and secondary nodes from a game-theoretic perspective where we model their interaction as a Stackelberg game with a theoretically proved and computed Stackelberg equilibrium. We show that the spectrum leasing based on trading secondary access for cooperation by means of relay and jammer is a promising framework for enhancing security in CRNs.**

***Index Terms*— Cognitive radio, game theory, information security**

I. Introduction

RECENTLY, physical layer (PHY) security has drawn significant attention as an alternative for cryptographic algorithms at the upper layers of protocol stack in secure communication systems [2]–[4]. Security threats may be induced by the passive eavesdropping node(s) which try to intercept the communication between authenticated nodes. Traditionally, there have been several significant challenges for cryptographic approaches of upper layers in protocol stacks, e.g., private key management complexity, key distribution obstacles, and key transmission security issues.

Manuscript received December 31, 2015; revised May 8, 2016 and July 1, 2016; accepted July 1, 2016. Date of publication July 11, 2016; date of current version November 15, 2016. This paper was presented at the IEEE Global Telecommunications Conference, San Diego, CA, USA, Dec. 2015 [1]. The associate editor coordinating the review of this paper and approving it for publication was W. Saad.

A. Al-Talabani, Y. Deng, and A. Nallanathan are with the Department of Informatics, King's College London, London WC2R 2LS, U.K. (e-mail: ali.al-talabani@kcl.ac.uk; yansha.deng@kcl.ac.uk; arumugam.nallanathan@gmail.com).

H. X. Nguyen is with the School of Science and Technology, Middlesex University, London NW4 4BT, U.K. (e-mail: h.nguyen@mdx.ac.uk).

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

Digital Object Identifier 10.1109/TCOMM.2016.2589931

Recent years, a promising approach towards achieving secure communications has been developed by Wyner in [5]: information theoretic secrecy. The idea of information theoretic secrecy lies in exploiting the randomness of the communication channels to ensure the secrecy of the transmitted messages. In PHY security, the figure of merit is secrecy rate defined as which is the difference between the transmission rate of the source-destination link and that of the source-eavesdropper link. However, the secrecy rate would be equal to zero when the source-destination channel is worse than the source-eavesdropper channel. For a Gaussian channel, the achievable secrecy rate equals to the difference between the mutual information accumulated at the destination and that accumulated at the eavesdropper (ED), which is not less than zero [6].

In addition, many recent studies have focused on particular interest of the cooperative jamming paradigm. Since the open nature of the wireless medium makes it susceptible to malicious eavesdropping. In [7], the authors proposed cooperative jamming to counter this vulnerability which is caused by eavesdroppers. In cooperative jamming, includes interference is created by the network nodes to transmit noise or codewords to impair the eavesdroppers' ability in decoding the confidential information [8]. The authors in [9] considered the power allocation optimization problem to maximize the secrecy rate in a two hop wireless relay network. The work in [10] maximized the secrecy rate of the primary network while satisfying a required rate for the secondary network by using the optimal beamformer design at the secondary transmitter with multiple antennas.

The work in [11] considered the secrecy rate maximization problem based on game theory, where the jammer introduces pricing charges for its jamming service based on the amount of the interference caused to the eavesdropper. This secrecy rate maximization problem is formulated into a Stackelberg game where the jammer and the legitimate transmitter play the roles of leader and follower of the game. In [12], the authors demonstrated that cooperative jamming leads to substantial secrecy rate improvement. This study involved multiple potential jammers, their competition between which are modeled for bandwidth access via distributed resource allocation mechanisms such as auctioning and the power control game. With the goal of maximizing their data transmission rate priced by the jammer's power, the transmit power of cooperative jammers is generally proportional to the amount of leased

bandwidth. In [8], the authors considered a scenario where an external eavesdropper attempts to decode the primary users message. The primary user allows the secondary user to share the primary user's spectrum to improve its own secrecy rate through cooperative jamming from the secondary user. A different setup is investigated in [3], the secondary user wants to keep its message confidential from the primary network, which means that the primary receiver is viewed as an eavesdropper from the secondary network perspective. In [14], the inner and outer bounds on the capacity equivocation region are derived.

Recently, there has been a growing interest in modeling and analyzing communication systems using game-theoretic approaches. The authors in [15] considered a four-node cognitive scenario where the secondary receiver (SR) is treated as a potential eavesdropper with respect to the primary transmission. The secondary transmitter can help the primary transmission, while guarantee that the primary message is not leaked to the secondary user(s). They investigated three different optimization problems: the maximization of the primary secrecy rate, the maximization of the secondary rate and the minimization of the secondary transmit power. Furthermore, they analyzed the cooperation between the primary transmitter (PT) and secondary transmitter (ST) from a game-theoretic perspective, in which their interaction is modeled as a Stackelberg game. It is known that the primary and secondary users have their own interests and thus do not cooperate unconditionally, non-cooperative game theory tools are a common approach to model their interaction in cognitive radio networks (CRNs) with secrecy constraints [16] or without secrecy constraints [17], [18]. An appropriate model for such scenarios is the Stackelberg game model [19] with the game leader selling some fraction of its spectrum and the follower awarded a share of the spectrum for its cooperation, as in [20].

Cooperative game theory was studied in [22] to demonstrate the improvement in secrecy capacity of an ad-hoc network, when users form coalitions to nullify the signals overheard by eavesdroppers via collaborative beamforming. For a hierarchical multi-hop system with different potential paths to the base station, a distributed tree formation game was proposed in [23]. Han *et al.* [24] demonstrated Stackelberg game where a legal transmitter pays a number of external helpers to jam an eavesdropper, and computed the corresponding equilibrium prices and convergence properties. They also examined a similar scenario in [25], where an auction game was used alternatively to model the transactions between transmitters and helping jammers. Anand and Chandramouli studied an M-user non-cooperative power control game with secrecy considerations in [26], and applied pricing functions to improve the energy efficiency and sum secrecy capacity of the network. Fakoorian *et al.* discussed in [27] and [28] how Kalai-Smorodinsky bargaining solutions and zero-sum games are adopted to allow the transmitters to find an operating point that balances network performance and fairness. In [29], game theory is used by multiple eavesdroppers to decide whether to collude or not in a MISO wiretap channel. The authors in [30] modeled the interaction between primary users and secondary users as a Stackelberg game in which transmission power levels are the key to maximize data rates. Also, the study in [3] considers cognitive transmitter should ensure that the primary message is not leaked to the secondary user by using cooperative jamming. The authors of this study investigate the optimal power allocation and power splitting at the secondary transmitter for cognitive model to maximize the secondary energy efficiency (EE) under secrecy constraints.

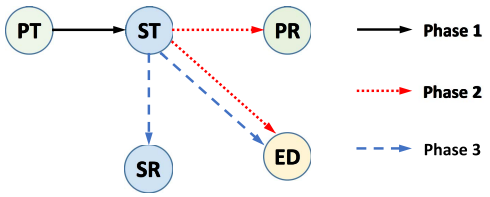

Fig. 1. Illustration of cognitive radio (CR) system model in Scenario 1.

From the above mentioned studies, it can be shown that the ST can be utilized as either a relay to forward the primary information or a jammer to send jamming signal. The target is to enhance primary secrecy rate and improve secondary transmission rate. Inspired by [9], we propose a novel scenario where ED can intercept the primary and secondary transmissions, ST is acted as a trusted relay and jammer by allocating part of its transmitted power to emit an artificial noise to create interference to EDs to protect the primary and secondary transmissions. The main benefit of this novel scenario is to protect the primary and secondary transmissions against eavesdroppers whereas previous studies highlighted only protection of primary transmissions against eavesdroppers. We assume that primary receiver (PR) and SR have knowledge of artificial noise to overcome the artificial noise at a legal receiver.

We study two scenarios where Stackelberg game theory based cooperative scheme is used to improve the achievable primary secrecy rate (PSR) and secondary secrecy rate (SSR). In scenario 1, a single ED is considered as shown in Fig.1, where the PT broadcasts its encoded signal to ST in Phase 1 with an assumption that the ED is out of range of PT; then the ST forwards the primary message with artificial noise to the PR in Phase 2; and the ST sends its own signal with artificial noise to SR in Phase 3. In this scenario, we applied Stackelberg game to analyze the primary secrecy rate in Phase 2, and the secondary secrecy rate in Phase 3. Different from the transmission scheme in scenario 1, in scenario 2 as indicated in Fig. 2, the SR is applied as multi-antenna jammer in Phase 1 to reduce leakage rate at eavesdroppers. Furthermore, in scenario 2, we consider the following two types of multiple eavesdroppers as follows:

- *Colluding eavesdroppers*: All eavesdroppers can be seen as a single eavesdropper due to their joint processing action, and the optimal receiver strategy is based on maximum ratio combining which combines the effects of all eavesdroppers in deriving closed forms of PSR and SSR [21].
- *Non-colluding eavesdroppers*: The secrecy rate is determined by that of the most malicious eavesdropper,

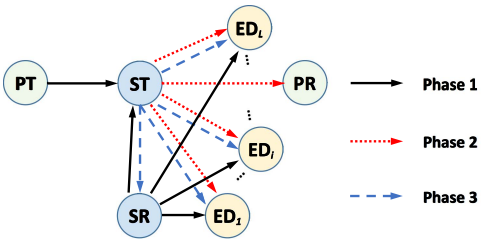

Fig. 2. Illustration of CR system model in Scenario 2.

considering that each eavesdropper overhears the primary or secondary communication individually.

In such networks, a primary node may lease portions of a licensed spectrum to a secondary node in exchange for some form of compensation. Moreover, retribution from secondary to primary nodes is in the form of cooperative relaying and jamming to enhance primary secret transmission. This scenario avoids the regulatory issues or money transactions that commonly hinder the implementation of the property-rights spectrum leasing concept [38].

In the context of the aforementioned schemes, we propose novel system designs, the power allocation and the time allocation designs for primary and secondary transmissions that maximize the achievable PSR and SSR subject to a total transmit power constraint. We should note that codeword design for meeting the achievable secrecy rates is not considered in this work. The main contributions of this work are summarized as follow:

- In Scenario 1, with a single eavesdropper, we provide an efficient optimization maximize both PSR and SSR under the flat fading channel model. In particular, we analyze and solve the primary and secondary power allocation problems at the ST using time slot allocation of spectrum lease.
- In Scenario 1, it is shown that our secrecy rates achieved with our proposed 3-phase system is higher than of other studies ([12], [13]) which are based on external jammer under the same geometric environment.
- In Scenario 2, we study design and analysis for the proposed CRNs under the malicious attempt of multiple eavesdroppers (colluding eavesdroppers and non-colluding eavesdroppers) around ST to highlight the impact of multiple eavesdroppers on the PSR and SSR. We analyze and solve the power allocation problem and time allocation problem.
- In Scenario 2, it is shown that the secrecy rate achieved for CRNs under the colluding eavesdropper is significantly lower than that under non-colluding eavesdroppers.

The remaining of this paper is organized as follows. In Section II, we define our system model and achievable secrecy rates in cognitive Scenario 1. Section III presents the possible optimization problems for the given scenarios and their game-theoretic approach in Scenario 2. We then compare those scenarios through numerical simulations in Section IV. Finally, Section V concludes this paper.

II. Enhancing Secrecy Rates Using Stackelberg Game: A Single Eavesdropper (Scenario 1)

In this section, we considered a cooperative CRNs where the ST is allowed to access the primary spectrum, as long as it acted as the jammer for the ED and the relay for the primary transmission as illustrated in Fig. 1, consisting of the following single antenna nodes: a PT, a PR, a cognitive ST, an SR and a single ED (i.e., Scenario 1). We assume that the legal primary and secondary destinations have *a priori* knowledge of the jamming signal sent by the ST (relay). This is achieved by communicating the legal source and destination in a two-step process. In the first step, the phase response of the channel is probed, and in the second step the information bearing signal is modified to precompensate for the phase effects of the channel. Since the channels between the legal source and destination are completely different from the channels between the legal source and eavesdroppers, this process is secure ([33], [34]). We assume the following: i) each node carries a single omnidirectional antenna; ii) the relaying strategy of decode-and-forward (DF) is employed; and iii) global channel state information (CSI) is available by a standard channel estimation (CE) technique, e.g., the training based CE (TBCE). In TBCE technique, the pilot symbols are used for acquiring an estimated CSI prior to actual data transmission, then the channel is estimated using the combined knowledge of the transmitted and received signals [36], [37]. To enhance the achievable secrecy rate, the ST allocates part of its transmit power to emit jamming signal, and the rest of its transmit power to emit information signal.

For the transmit single message W, which is uniformly distributed over $\{1, \ldots, 2^{nR}\}$ with R as the rate of communication, and the n is the block length of communication. The sender maps W to $X^n = X_1, \ldots, X_n$, the intended receiver receives $Y^n = Y_1, \ldots, Y_n$ and decodes $\hat{W}$, and eavesdropper overhears the output $Z^n = Z_1, \ldots, Z_n$. The perfect secrecy rate R_{sec} is considered as achievable if for any $\epsilon > 0$, there exists a sequence of codes $(2^{nR}, n)$ such that for any $n > n(\epsilon)$, we have [39]

$$P_e^n = P\left(W \neq \hat{W}\right) \leq \epsilon, \; R_e = \frac{1}{n} H\left(W | Z^n\right) \geq R_{sec} - \varepsilon, \quad (1)$$

where R_e is the equivocation rate.

The secrecy capacity C_{sec} is defined as the maximum achievable perfect secrecy rate, which is given as

$$C_{sec} \triangleq \sup_{P_e^n \leq \varepsilon} R_{\text{sec}} = \max_{f_W} [I(X, Y) - I(X, Z)]^+. \quad (2)$$

The achievable secrecy rate can be defined as

$$\begin{aligned} R_{sec} &= [\max_{f_W}(I(X, Y)) - \max_{f_W}(I(X, Z))]^+ \\ &= (R_D - R_E)^+, \end{aligned} \quad (3)$$

where R_D is the maximum information rate from the transmitter to the intended receiver, and R_E is the maximum leakage rate from the transmitter to the eavesdropper. For convenience, we remove the $(\cdot)^+$ sign from here on.

A. Proposed Cooperative CRNs

Our system has three phases as follows:

1) Phase 1: The PT decides to allocate only a fraction $(1-\alpha)$ of the whole time slot for transmission from the PT to the ST (where $0 < \alpha < 1$.). The remaining fraction will be used in Phases 2 and 3. We assume that transmission from the PT is invisible at the ED. The PT encodes a confidential message into a $N-$length block codeword (s), where PT has power constraint as follows [30]:

$$P_p = \frac{1}{N}\sum_{k=1}^{N} |s_k|^2 \leq P_{MAX}, \tag{4}$$

where P_{MAX} is the maximum primary power of PT. In phase I, the ST is used as a relay and the received signal at ST is

$$X_{ST} = \sqrt{P_p} h_{ps} s + n_{ST}, \tag{5}$$

where s is the primary message signal, P_p is the primary power level, $n_{ST} \sim \mathcal{CN}(0, \sigma^2)$ is the noise at ST, and $h_{ps} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between PT and ST. For notational convenience, let us define

$$\rho_{ps} = \frac{P_p \left|h_{ps}\right|^2}{\sigma^2}.$$

Then, the information rate at the ST, R_{PS}, is obtained as

$$R_{PS} = (1-\alpha)\log_2(1+\rho_{ps}). \tag{6}$$

2) Phase 2: The ST then forwards secure primary message to the PR within the fraction $\alpha\beta$ (where $0 < \beta < 1$) of the considered time slot.[1] In this phase, for security reason, the ST also sends the artificial noise (denoted by z)[2] using a faction $(1-\epsilon)$ of the available power level P_s (where $0 < \epsilon < 1$). Furthermore, the ST encodes a confidential message into same a $n-$length block codeword of phase 1, where ST has power constrained as follows

$$P_s = \frac{1}{n}\sum_{k=1}^{n} \left|\hat{s}_k\right|^2 \leq P_{s,MAX}, \tag{7}$$

where $P_{s,MAX}$ is the maximum secondary power of ST. The received signal at the PR after removing the artificial noise (which is assumed to be known at the PR) is

$$X_{PR} = \sqrt{\epsilon P_s} h_{sp} \hat{s} + n_{PR}, \tag{8}$$

and the received signal at the ED in Phase 2 is

$$X_{ED}^{(2)} = \sqrt{\epsilon P_s} h_{se} \hat{s} + \sqrt{(1-\epsilon)P_s} h_{se} z + n_{ED}, \tag{9}$$

where $\hat{s}$ is the re-encoded primary message signal, the artificial noise $z \sim \mathcal{CN}(0,1)$, $h_{sp} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and the PR, and $h_{se} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and the ED. After removing the artificial noise, the information rate at PR is obtained as

$$R_{SP} = \alpha\beta \log_2(1+\epsilon\rho_{sp}), \tag{10}$$

where

$$\rho_{sp} = \frac{P_s \left|h_{sp}\right|^2}{\sigma^2}.$$

Then the information leakage at the ED in Phase 2 is

$$R_{SE}^{(2)} = \alpha\beta \log_2\left(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}\right), \tag{11}$$

where

$$\rho_{se} = \frac{P_s \left|h_{se}\right|^2}{\sigma^2}.$$

According to [9], the achievable PSR, denoted by R_{PSEC}, can be written as

$$\begin{aligned} R_{PSEC} &= R_{SP} - R_{SE}^{(2)} \\ &= \alpha\beta\left(\log_2(1+\epsilon\rho_{sp}) - \log_2\left(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}\right)\right). \end{aligned} \tag{12}$$

3) Phase 3: The ST then send its own secure secondary message to the SR within the remaining faction $\alpha(1-\beta)$ of the considered time slot. Again, we assume that the same codeword for artificial noise and the same power allocation strategy (i.e., same ϵ) are used for this secondary transmission to simplify our analysis. The received signal at the SR (after removing the artificial noise) is

$$X_{SR} = \sqrt{\epsilon P_s} h_{ss} s_1 + n_{SR}, \tag{13}$$

while the received signal at the ED in phase 3 is

$$X_{ED}^{(3)} = \sqrt{\epsilon P_s} h_{se} s_1 + \sqrt{(1-\epsilon)P_s} h_{se} z + n_{ED}, \tag{14}$$

where s_1 is the secondary message signal and $h_{ss} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and SR. After removing the artificial noise at SR, the information rate at the SR is represented as

$$R_{SS} = \alpha(1-\beta)\log_2(1+\epsilon\rho_{ss}), \tag{15}$$

where

$$\rho_{ss} = \frac{P_s \left|h_{ss}\right|^2}{\sigma^2}.$$

Also, the leakage rate at the ED in this phase can be written as

$$R_{SE}^{(3)} = \alpha(1-\beta)\log_2\left(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}\right). \tag{16}$$

Similarly, we can obtain SSR, denoted by R_{SSEC} as

$$\begin{aligned} R_{SSEC} &= R_{SS} - R_{SE}^{(3)} \\ &= \alpha(1-\beta)\left(\log_2(1+\epsilon\rho_{ss}) - \log_2\left(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}\right)\right). \end{aligned} \tag{17}$$

[1] We consider a single ST only in this work. However, for the case of multiple STs, the relay selection process can be applied before the most competitive ST can be chosen to deliver the message to the PR

[2] Note that the PR could also do the same thing in Phase 1 by sending the artificial noise to interfere with the reception of eavesdropper in Phase 1. This will certainly improve secure rate, however, at the expense of more power consumption.

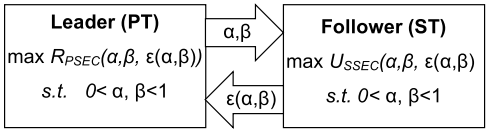

Fig. 3. Stackelberg game model.

B. Maximization of Achievable Secrecy Rates Using Stackelberg Game

We can formulate the maximization problem of available secrecy rates as a Stackelberg game where the PT is considered as the leader and the ST is the follower. The leader will try to maximize its primary secrecy rate R_{psec} while the follower will try to maximize its utility. The PT's optimal transmission parameters (α^*, β^*) and the corresponding power choice of the ST, ϵ^*, are jointly referred as the Stackelberg equilibrium. We can consider interaction between the primary and secondary transmissions as shown in Fig. 3. The ST is aware of parameters (α, β) and optimizes its power level towards the goal of maximizing its utility:

$$U_{SSEC}(\alpha, \beta, \epsilon(\alpha, \beta)) = R_{SSEC} - k\epsilon, \tag{18}$$

where k is the pricing constant. We present the following lemma.

Lemma 1: The utility of secondary transmission in (18) *is concave in terms of* ϵ.

Proof: In order to prove the concavity of the secondary transmission's utility, we derive the second derivative of (18) with respect to ϵ as

$$\frac{\partial^2 U_{SSEC}}{\partial^2 \epsilon} = q\left(-\frac{\rho_{ss}^2}{(1+\epsilon\rho_{ss})^2} - \frac{\rho_{se}^2}{(1+(1-\epsilon)\rho_{se})^2}\right), \tag{19}$$

where $q = \alpha(1-\beta)/(\ln 2)$. Obviously, the second derivative in (19) is negative. Thus, the utility of the secondary transmission is concave in terms of ϵ. ∎

The optimal solution of secondary transmission problem can be obtained as follows

$$\epsilon^* = \arg \max_{0<\alpha,\beta,\epsilon<1} U_{SSEC}(\alpha, \beta, \epsilon(\alpha, \beta)). \tag{20}$$

To find optimum ϵ^*, we can differentiate U_{ssec} with respect to ϵ and equate it to zero, as follows:

$$\frac{\partial U_{SSEC}}{\partial \epsilon} = q\left(\frac{\rho_{ss}}{(1+\epsilon\rho_{ss})} - \frac{\rho_{se}}{(1+(1-\epsilon)\rho_{se})}\right) - k = 0$$
$$\Rightarrow k/q = \frac{\rho_{ss}}{(1+\epsilon\rho_{ss})} - \frac{\rho_{se}}{(1+(1-\epsilon)\rho_{se})} \tag{21}$$

After simplification, we can obtain ϵ as

$$a\epsilon^2 + b\epsilon + c = 0, \tag{22}$$

where

$$a = \rho_{ss}\rho_{se}, \tag{23}$$
$$b = \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \frac{2\rho_{ss}\rho_{se}q}{k}, \tag{24}$$
$$c = \frac{q}{c_1}(\rho_{ss} - \rho_{se} + \rho_{ss}\rho_{se}) - \rho_{se} - 1. \tag{25}$$

Therefore, the optimal ϵ^* is

$$\epsilon^* = \begin{cases} 0, & \epsilon_2 \le 0 \\ 1, & \epsilon_1 \le 1 \\ \max_{\epsilon\in\{\epsilon_1,\epsilon_2\}} U_{ssec}(\epsilon), & 0 \le \epsilon_1 \le \epsilon_2 \le 1 \\ \max_{\epsilon\in\{0,1,\epsilon_i\}} U_{ssec}(\epsilon), & \text{only } \epsilon_i \in [0,1], i = 1 \text{ or } 2 \end{cases} \tag{26}$$

where

$$\epsilon_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}, \quad \epsilon_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

The PT, acting as the game leader, determines the fraction α and the ratio β towards the goal of maximizing its secrecy rate, knowing that its decision will affect the strategy selected by the ST (the follower). The solution is given as

$$\alpha^*, \beta^* = \arg \max_{0<\alpha,\beta,\epsilon<1} R_{PSEC}(\alpha, \beta, \epsilon^*(\alpha, \beta)) \tag{27}$$

Theorem 1: The allocated power level ϵ^* *and time slot* α^* *are the Nash equilibrium of the proposed game.*

Proof: According to DF scheme, we would assume that $R_{sp} \le R_{ps}$ in order to find the relationship between α and β to facilitate the solution of the above optimization problem. We can obtain the following relationship according to the assumption of DF scheme.

$$R_{SP} = R_{PS}$$
$$\Rightarrow \beta = \frac{(1-\alpha)}{\alpha}\frac{\log_2(1+\rho_{ps})}{\log_2(1+\epsilon\rho_{sp})}. \tag{28}$$

According to lemma 1, U_{SSEC} is strictly concave in terms of ϵ for a given values of α and β. Furthermore, R_{PSEC} is an increasing function of α then the primary transmission (leader) will select the best response $\epsilon^*(\alpha)$ of secondary transmission (follower) as

$$\alpha^* = \arg\max R_{PSEC}(\alpha, \epsilon^*(\alpha)). \tag{29}$$

Therefore, α^* and $\epsilon^*(\alpha^*)$ form the Nash equilibrium of the proposed Stackelberg game. ∎

III. Extension to Multiple Eavesdroppers (Scenario 2)

We consider Scenario 2 (see Fig. 2), by having multiple eavesdroppers which are located in the range of the ST, to highlight the effect of multiple eavesdroppers on the secrecy rates. In this case , we cannot consider same assumption as in Scenario 1 that all eavesdroppers are located out of range of the PT, to enhance the secure transmission, we consider SR as jammer with multiple transmit antennas and transmit jamming signal at phase I. The three phases for both cases of colluding and non colluding eavesdroppers are considered. Furthermore, we derive closed form expressions for both PSR and SSR in each case.

A. Case I: Colluding Eavesdroppers

In this case, all eavesdroppers are cooperated through a central processing so they can be considered as a single eavesdropper with multiple antennas. Also, we assume that the eavesdroppers are homogeneous, i.e., each eavesdropper experiences the same received signal power on average, and that all eavesdroppers are uniformly located around legitimate transmitter ST [21].

1) Phase 1: We consider the PT cooperates with ST by allocated only a fraction $(1-\alpha)$ of the whole time slot whereas the SR, with multiple transmit antennas, sends the jamming signal using power vector $\mathbf{w}_J$ to both of the ST and ED within the fraction $(1-\alpha)$. In this phase, the received signal X_{ST} at the ST is

$$X_{ST} = \sqrt{P_p} h_{ps} s + \sqrt{P_J} \mathbf{h}_{rs} \mathbf{w}_J z_J + n_{ST}, \tag{30}$$

where $\mathbf{h}_{(rs)} \sim \mathcal{N}(\mathbf{0}_K, d^{-\delta}\mathbf{I}_K)$ is the channel vector (of length K due to K multiple transmit antennas at SR) between SR and ST, $z_J \sim \mathcal{CN}(0,1)$, δ is the path loss exponent, d is the distance between SR and ST and $n_{ST} \sim \mathcal{CN}(0, \sigma^2)$. The received signal at the ED_i (where $i = 1, 2, \ldots L$) in Phase 1 is

$$X_{PE,i} = \sqrt{P_p} h_{pe} s + \sqrt{P_J} \mathbf{h}_{re} \mathbf{w}_J z_J + n_{ED,i}, \tag{31}$$

where $\mathbf{h}_{(re)} \sim \mathcal{N}(\mathbf{0}_K, d^{-\delta}\mathbf{I}_K)$ is the channel vector (of length K due to K multiple transmit antennas at SR) between SR and ST, $n_{ED,i} \sim \mathcal{CN}(0, \sigma^2)$. Using projection matrix theory to remove an interference of SR (jammer) in legal receiver (ST) , we can achieve $|\mathbf{w}_J|$ as follows

$$|\mathbf{w}_J| = \frac{(\mathbf{I} - \mathbf{h}_{rs}(\mathbf{h}_{rs}\mathbf{h}_{rs}{}^{\dagger})^{-1}\mathbf{h}_{rs}^{\dagger})\mathbf{h}_{re}}{\left|((\mathbf{I} - \mathbf{h}_{rs}(\mathbf{h}_{rs}\mathbf{h}_{rs}{}^{\dagger})^{-1}\mathbf{h}_{rs}^{\dagger})\mathbf{h}_{re}\right|}, \tag{32}$$

where $|\mathbf{w}_J \mathbf{w}_J{}^{\dagger}| = 1$

Therefore, the information rate at ST is is given by (6) whereas the leakage rate at ED_i can be written as follows:

$$R_{PE,i} = (1-\alpha)\log_2\left(1 + \frac{P_p h_{pe}}{\sigma^2 + P_J \left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right|}\right), \tag{33}$$

where $\mathbf{W}_J = \mathbf{w}_J\mathbf{w}_J{}^{\dagger}$.

2) Phase 2: The ST has DF relay function and forwards secure primary message $\hat{s}$ to PR in $\alpha\beta$ in presence of L eavesdroppers according to a parameter $0 < \beta < 1$. The received signal X_{PR} and rate R_{SP} are given by (8) and (10) respectively due to canceling of artificial noise in PR. Then the leakage rate R_{SEi} at i^{th} ED can be written as

$$R_{SE,i} = \alpha\beta\log_2\left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J \left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}\right), \tag{34}$$

where $h_{se} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between ST and the i^{th} ED. According to [21] and [35], the authors take the sum of the signal to interference and noise ratio $(SINR)$s of the colluding eavesdroppers due to their cooperation. In our paper, we assume that a central processing unit will handle the sequential Markov chain observations among eavesdroppers and according to [32], we can approximate $(\sum_{i=1}^{L} log_2(1+SINR_i)) \cong \sum_{i=1}^{L} SINR_i$ considering the approximation $(log_2(1+SINR_i)) \cong SINR_i$ for long distance transmissions or energy-limited scenarios. Furthermore, this assumption represents worst case of eavesdroppers $(i.e.(\sum_{i=1}^{L} log_2(1+SINR_i) > log_2(1+\sum_{i=1}^{L} SINR_i)))$. Therefore, we rewrite R_{SE} as

$$\begin{aligned} R_{SE} &= \sum_{i=1}^{L} R_{SE,i}{}^{(2)} \\ &= \sum_{i=1}^{L} \alpha\beta\left(\log_2\left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}\right)\right). \end{aligned} \tag{35}$$

Also, the information rate R_P at PR is given as

$$\begin{aligned} R_P &= \min(R_{PS}, R_{SP}) \\ &= \min\left(\log_2(1+\rho_{ps}), \log_2(1+\epsilon\rho_{sp})\right). \end{aligned} \tag{36}$$

The achievable primary secrecy rate R_{PSEC} can then be written as

$$\begin{aligned} &R_{PSEC} \\ &= \alpha\beta\left(R_p - \sum_{i=1}^{L}\log_2\left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}\right)\right). \end{aligned} \tag{37}$$

2) Phase 3: The ST transmits secondary message to SR in time slot $\alpha(1-\beta)$ in the presence of L eavesdroppers. The secondary receiver SR extracts only information signal, then the information rate at the SR is given by (15), while the rate at multiple eavesdroppers is represented as

$$\begin{aligned} &R_{SE}{}^{(3)} = \sum_{i=1}^{L} \\ &\times\left(\alpha(1-\beta)(\log_2\left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}\right)\right). \end{aligned} \tag{38}$$

We can obtain secondary secrecy rate R_{SSEC} by substituting R_{ss} and R_{se} as

$$\begin{aligned} U_{SSEC} &= R_{SSEC} - k\epsilon = R_{SS} - R_{SE}^{(3)} - k\epsilon \\ &= \alpha(1-\beta)(\log_2(1+\epsilon\rho_{ss}) \\ &\quad - \sum_{i=1}^{L}(\alpha(1-\beta) \\ &\quad \times\left(\log_2\left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}\right)\right) \\ &\quad - k\epsilon. \end{aligned} \tag{39}$$

Lemma 2: The utility of secondary transmission in colluding eavesdroppers that has the identical channel gains of

colluding eavesdroppers around legal transmitter are concave in terms of ϵ.

Proof: Since all eavesdroppers have identical channel gains around ST and SR, we can consider that

$$|h_{se,1}| = |h_{se,2}| = \ldots = |h_{se,L}|$$

which leads to

$$\rho_{se,1} = \rho_{se,2} = \ldots = \rho_{se,L} = \rho_{se}.$$

Also, we assume

$$|h_{re,1}| = |h_{re,2}| = \ldots = |h_{re,L}|$$

Therefore, the achievable U_{SSEC} is written as

$$\begin{aligned} U_{SSEC} &= R_{ssec} - k\epsilon = R_{ss} - R_{se} - k\epsilon \\ &= \alpha(1-\beta) \\ &\quad \times \left(\log_2(1+\epsilon\rho_{ss}) - \log_2 \right. \\ &\quad \left. \times \left(1 + \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J \left| \mathbf{h}_{re}^{\dagger} \mathbf{W}_J \mathbf{h}_{re} \right| + (1-\epsilon) P_s h_{se}} \right) \right) \\ &\quad - k\epsilon. \end{aligned} \tag{40}$$

In order to prove the concavity of the secondary transmission's utility, we derive the second derivative of (40) with respect to ϵ as

$$\begin{aligned} \frac{\partial^2 U_{SSEC}}{\partial^2 \epsilon} = q \left(\frac{-\rho_{ss}^2}{(1+\epsilon\rho_{ss})^2} \right. \\ \left. + \frac{-L\rho_{se}^2}{1 + \frac{P_J \left| \mathbf{h}_{re}^{\dagger} \mathbf{W}_J \mathbf{h}_{re} \right|}{\sigma^2} + (1-\epsilon)\rho_{se}} \right) \end{aligned} \tag{41}$$

where $q = \alpha(1-\beta)/2\ln 2$. Obviously, the second derivative in (41) is negative and therefore the utility of secondary transmission in colluding eavesdroppers is concave in terms of ϵ. ■

We consider the same interaction between the primary and secondary transmissions as shown in Fig. 3. This case reflects the impact of L eavesdroppers on the PSR and SSR. To find optimum ϵ^*, we can differentiate U_{SSEC} with respect to ϵ. We assume $\rho_{re} = \frac{P_J \left| \mathbf{h}_{re}^{\dagger} \mathbf{W}_J \mathbf{h}_{re} \right|}{\sigma^2}$ for simplicity, then the optimal ϵ^* is one of the positive real roots of $a\epsilon^2 + b\epsilon + c = 0$, where a,b and c are given as

$$a = \rho_{ss}\rho_{se}, \tag{42}$$

$$\begin{aligned} b = \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \rho_{ss}\rho_{re} \\ - \frac{(1+L)\rho_{ss}\rho_{se}q}{k}, \end{aligned} \tag{43}$$

$$\begin{aligned} c = \frac{q}{c_1}(\rho_{ss} - L\rho_{se} + \rho_{ss}\rho_{se} + \rho_{ss}\rho_{re}) \\ - \rho_{se} - 1 - \rho_{re}. \end{aligned} \tag{44}$$

Then we can apply theorem 1 to find optimum values of (α, β).

B. Case 2: Non-Colluding Eavesdroppers

We consider all eavesdroppers having non-homogeneous distribution around the ST (i.e., eavesdroppers are distributed randomly with different distances around the ST). In this case, each eavesdropper will have their own information rate, denoted now by $R_{se,i}, i = 1, 2, \cdots, L$. Thus, we formulate the two following problems:

1) Problem 1: Maximizing PSR in Phase 2 for its worst case scenario:

$$\max_{0<\alpha,\beta,\epsilon<1} \min_i R_{psec,i} \tag{45}$$

where $i = 1, 2, \ldots, L,$, $R_{psec,i} = R_{ps} - R_{se,i}$, and $R_{se,i}^{(2)}$ is the leakage rate of the ith ED in Phase 2. Note that

$$\min_i R_{psec,i} = R_{ps} - \max_i R_{se,i}^{(2)}.$$

2) Problem 2: Maximizing SSR in Phase 3 for its worst case scenario:

$$\max_{0<\alpha,\beta,\epsilon<1} \min_i R_{ssec,i} \tag{46}$$

where $R_{ssec,i} = R_{ss} - R_{se,i}^{(3)}$ and $R_{se,i}^{(3)}$ is the leakage rate of the ith ED in Phase 3. Similarly, we have

$$\min_i R_{ssec,i} = R_{ss} - \max_i R_{se,i}^{(3)}.$$

To solve the aforementioned two problems, we can consider standard max min problem. The min problem is solved and then we can apply the proposed Stackelberg game based algorithm in Scenario 1 to find the suboptimal values of α, β, and ϵ, which corresponds to the worst case of eavesdropping.

IV. Results and Discussion

In this section, we present the numerical results and related discussion. We consider the two optimization problems from the previous sections according to the Stackelberg game. We studied the secrecy performance under two scenarios: Scenario 1 and Scenario 2.

A. Scenario 1: Comparison With Previous Work

In this section, we compare our proposed system with jammer that caused an interference in legal receiver as in [13]. We consider the same setting used in this previous study in [13]: $P_s = 2$mw, noise variance $\sigma^2 = 1$mw, pricing factor $k = 0.01$, $|h_{ps}|^2 = 0.6$, $|h_{se}|^2 = 0.3$ and $|h_{ss}|^2 = 0.8$. In [13], the authors considered two secondary users (one the relay and another for jammer) in order to enhance the secrecy rates in primary transmission of CR. In this previous study, there are two schemes which represented by relay and non friendly jammer (R-J) and equal-duration relay non-friendly jammer (EDRJ). Note that the only difference between EDRJ and R-J schemes is that in EDRJ scheme the time durations for the first two phases are equal and the secrecy rate is maximized without considering time allocation. We now compare our proposed scheme with these two schemes. Fig. 4 indicates that the proposed system outperforms the R-J and EDRJ schemes significantly due to removal an interference of jamming signal in legal destinations.

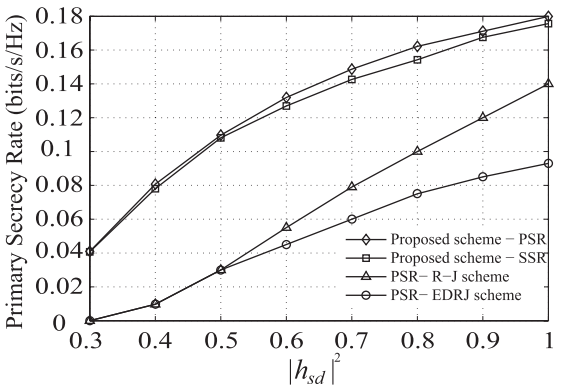

Fig. 4. Secrecy rate: comparison with jammer caused interference at legal receiver approach.

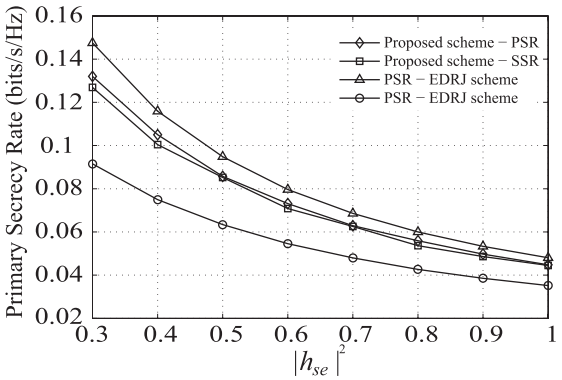

Fig. 5. Secrecy rate: comparison with friendly jammer without interference at legal receiver approach.

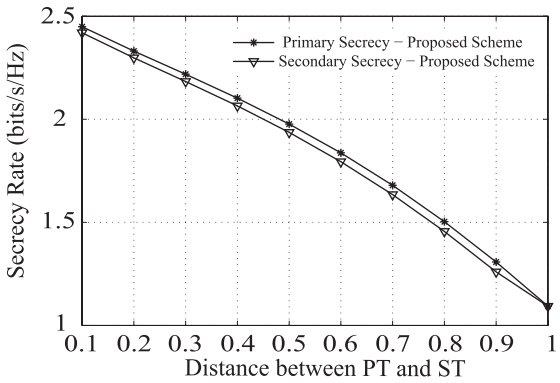

Fig. 6. Secrecy rate versus distance of PT and ST.

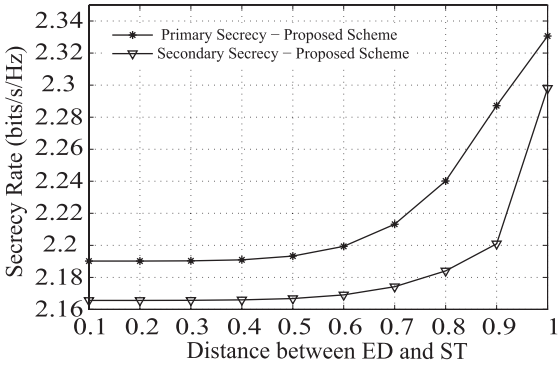

Fig. 7. Secrecy rate versus distance between ED and ST.

Furthermore, Fig.5 indicates the comparison between proposed system and equal-duration relay jammer transmissions(EDJ) with respect to h_{se}. EDJ scheme included the SR is treated as a potential eavesdropper with respect to the primary transmission. Since the primary users are the legacy owners of the spectrum, the confidentiality of the primary message should be considered. In this context, the primary transmitter PT may be assisted by the trustworthy secondary transmitter ST if the cooperation could improve the secrecy performance, while the ST benefits as it is awarded a share of the spectrum for its data transmission. Therefore, ST is acted as friendly jammer and the time duration of primary and jammer transmissions are same. This scheme is similar to jammer's operation in [12] except that EDJ doesn't cause an interference in legal transmitter. This comparison is performed to highlight the effect of an interaction between the time and power allocation by Stackelberg game on performing balance process between maximum values for both primary and secondary secrecy rates. We note that primary secrecy rate of proposed system is slightly less than of friendly jammer especially in high channel coefficient between legitimate transmitter and eavesdropper, whereas secondary secrecy rate of proposed system is significantly higher than that of friendly jammer. Also, the proposed system has the gap between the primary and secondary secrecy rates that less significantly than of EDJ scheme. This feature which proves that the PSR and SSR of Stackelberg game is fairer than that of EDJ due to the tradeoff between allocated power ϵ and time durations α and β to obtain maximum values for both primary and secondary secrecy rates.

B. Fixed Locations of the PR, ST and SR

We fix the PR, ST and SR locations at the coordinates (0, 0.6), (0, 0) and (0, 0.4), respectively, to find the effect of PT and ED distances on the PSR and SSR. These coordinates are normalized to square area with 1km^2. We assume path loss model $h_{ij} = d^{-\delta}$ is used with path loss exponent $\delta = 3$. We also consider the primary and secondary signal to noise ratios (SNRs) are 5 dB and the pricing coefficient is $k = 0.25$.

Figure 6 indicates the optimum primary and secondary secrecy rates with respect to distance between PT and ST when the coordinates of the ED is fixed at (1, 0). It is noted that optimum secrecy rates of both primary and secondary transmissions decrease when the PT is farther away from the ST, this is because of the decreasing ρ_{ps} would reduce R_{ps} according to (6). Therefore, the information rate of relay (ST) decreases according to the condition $R_{sp} \leq R_{ps}$.

Fig. 7 shows the optimum PSR and SSR with respect to distance of the ED when the location of the PT is fixed at (0.2, 0). It is noted that optimum secrecy rates of both primary and secondary transmissions increase when the ED is further away from the ST because the information rate of the ED decreases with degradation of h_{se} according to (12) and (17).

Figure 8 shows the optimum ϵ (power level fraction of the ST to carry the message signal) with respect to the distance

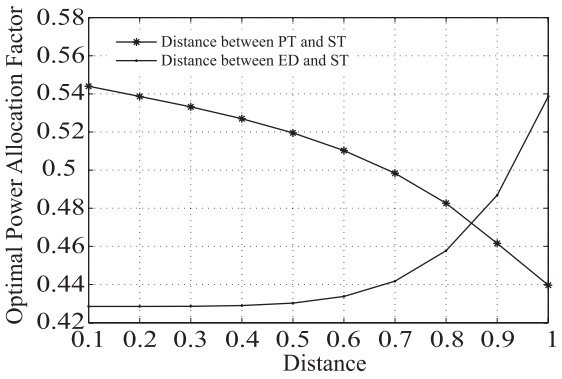

Fig. 8. ϵ^* versus distance.

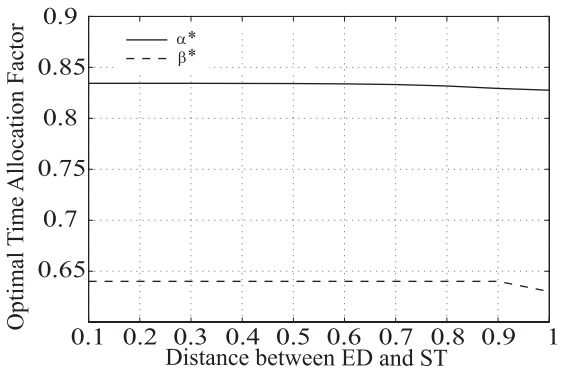

Fig. 10. α^* and β^* versus distance between ED and ST.

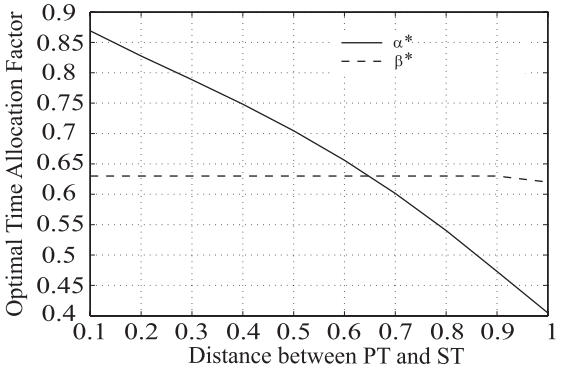

Fig. 9. α^* and β^* versus between PT and ST.

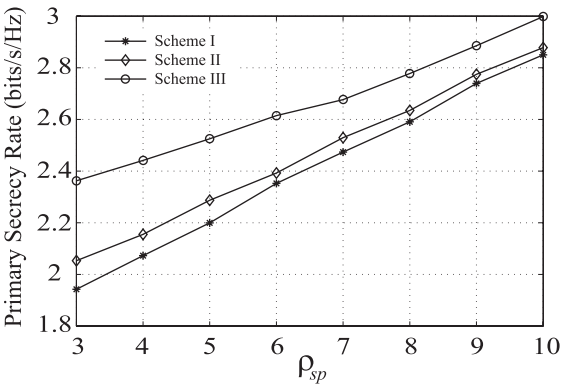

Fig. 11. Primary secrecy rate versus ρ_{sp}.

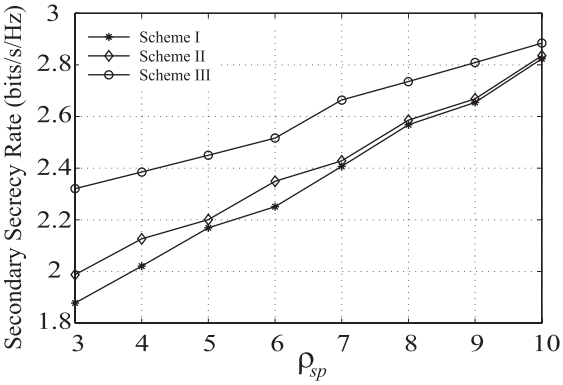

Fig. 12. Secondary secrecy rate versus ρ_{sp}.

between the PT and ST when the coordinates of the ED is fixed at (1.0, 0). We find that optimum ϵ reduces when the PT is far away from the ST, this is because the received power at the ST decreases with increasing the distance between ED and ST. On the other hand, this figure shows the optimum ϵ versus the distance between ED and ST when the coordinates of the PT is fixed at (0,0.2). It is noted that optimum ϵ increases when ED is farther from the ST, this is because $(1-\epsilon^*)$ decreases due to decreasing of the information rate of the ED.

Fig.9 shows the optimum α and β versus the distance between the PT and ST when the coordinates of the ED is fixed at (1.0,0). We can find that β^* slightly changes with the distance, whereas α^* is significantly decreased with the distance for two reasons: firstly the activation time of transmission between the PT and the relay is independent of β^* according to (6); secondly, the activation time of transmission between relay ST and PR decreases with increasing $(1-\alpha^*)$ (time slot of transmission between the PT and relay) due to the degradation of h_{ps} and R_{ps} according to (6).

Figure 10 indicates that optimum α and β versus the distance between the ED and ST when the coordinates of PT is (0,0.2). It is noted that β^* is reduced significantly because h_{se} has main effect on relay and secondary transmissions in Phase 2 ($\beta^*\alpha^*$) and Phase 3 $\alpha^*(1-\beta^*)$ according to (12) and (17), respectively. In another observation, α^* decreases less significantly because h_{se} has no effect on Phase 1 $(1-\alpha^*)$ of the primary transmission due to our assumption that primary transmission is invisible at the ED.

C. Fixed Locations of the PT, PR, ST and SR

The locations of the PT, PR, ST and SR are fixed at the coordinates (0,0.2),(0.6, 0), (0, 0) and (0, 0.4), respectively, in order to find the effect of ρ_{sp} on the secrecy rates in two later phases. We consider three schemes depending on locations of ED as follow: Scheme I (1.0,0), Scheme II (0.9,0) and Scheme III (0.6,0). Figures 11 and 12 indicate the optimum primary and secondary secrecy rates with respect to ρ_{sp} in these three schemes. It is noted that the optimum secrecy rates of the three schemes increase significantly with ρ_{sp} according to (12) and (17), respectively.

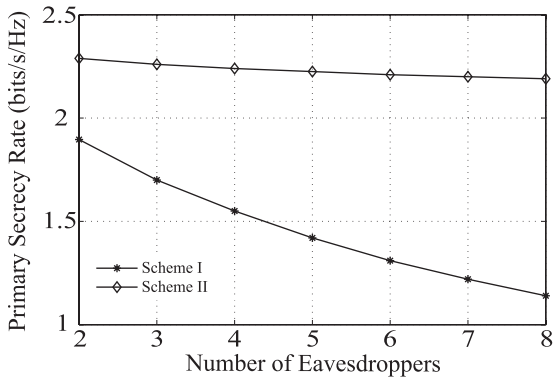

Fig. 13. Primary secrecy rate versus number of eavesdropper.

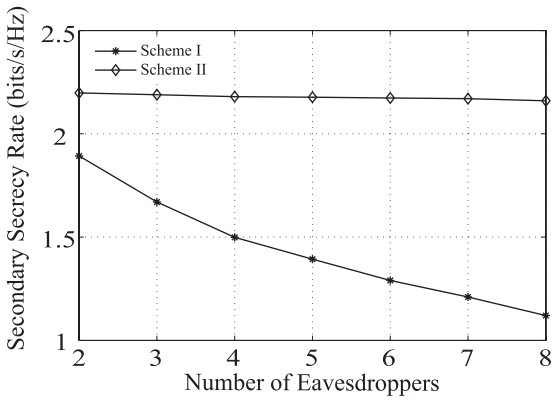

Fig. 14. Secondary secrecy rate versus number of eavesdropper.

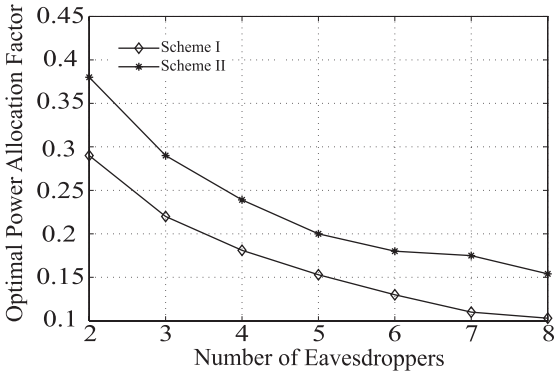

Fig. 15. ϵ^* versus number of eavesdropper.

D. Scenario 2

We consider same locations and parameters as in the preceding subsection with K=2. Figures 13 and 14 indicate that primary and secondary secrecy rates decrease significantly in both cases with increasing number of eavesdroppers according to (37) and (40). We can also note that scheme II (non-colluding eavesdroppers) has secrecy rate higher than scheme I (colluding eavesdroppers) because scheme I combines the effects of all eavesdroppers whereas scheme II picks the worst response (minimum secrecy rate) from one of the eavesdroppers.

Figure 15 shows that ϵ^* reduces significantly with increasing number of eavesdroppers, due to the fact that more power should be allocated to the artificial noise with increasing the number of eavesdroppers. Also, ϵ^* has higher level when the distance between ST and ED increases, due to the fact that less power should be allocated to the artificial noise with reducing of R_{es1}.

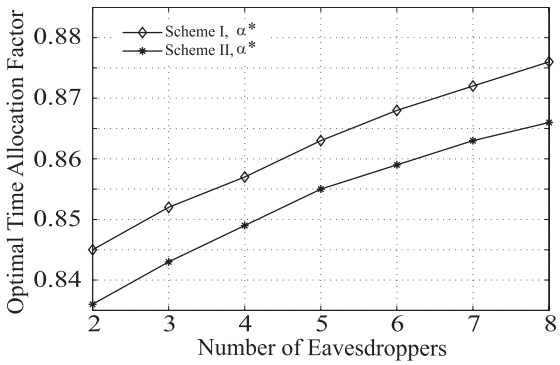

Fig. 16. α^* versus number of eavesdropper.

Figure 16 shows that α^* increases significantly with increasing number of eavesdroppers because we need to increase activation time of phases II and III to keep reasonable values of secrecy rates with increasing the number of eavesdroppers. Furthermore, α^* is needed to increase with further distance between ST and ED.

V. Conclusion

In this paper, we proposed a game theory based cooperation method to optimize the primary secrecy rate and secondary secrecy rate in CRNs. This mechanism is built upon the spectrum leasing paradigm, wherein a secondary transmitter is permitted to use some of its own power level to transmit an artificial noise to destination(s) while the legitimate destination has prior knowledge of the artificial noise. Interaction between the cooperative nodes is based on the Stackelberg game concept. We considered two scenarios, single eavesdropper and multiple eavesdroppers, where we formulated and solved optimization problems in each scheme aiming at maximizing the achievable secrecy rates on the primary and secondary transmissions subject to allocated power and lease time slot constraints. Numerical results confirmed that our proposed cooperative scheme significantly improves the secrecy rates of the CRNs. Furthermore, we remark numerically that achievable PSR and SSR of Stackelberg game is fairer than that of other existing algorithms due to the tradeoff between the allocated power and the time slot durations by Stackelberg game.

References

[1] A. Al-Talabani, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio via game theory," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[2] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

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

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[6] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[8] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[9] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *Proc. IEEE ICC*, Jun. 2011, pp. 1–5.
[10] K. Lee, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Nov. 2013.
[11] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.
[12] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. K. Rasmussen, and M. Skoglund, "On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 451–463, Mar. 2014.
[13] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.
[14] H. G. Bafghi, S. Salimi, B. Seyfe, and M. R. Aref, "Cognitive interference channel with two confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2010, pp. 952–956.
[15] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.
[16] E. Toher, O. O. Koyluoglu, and H. El Gamal, "Secrecy games over the cognitive channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2010, pp. 2637–2641.
[17] Z. Han and K. J. R. Liu, "Noncooperative power-control game and throughput game over wireless networks," *IEEE Trans. Commun.*, vol. 53, no. 10, pp. 1625–1629, Oct. 2005.
[18] Z. Han and K. J. R. Liu, *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[19] M. Simaan and J. B. Cruz, Jr., "On the Stackelberg strategy in nonzero-sum games," *J. Optim. Theory Appl.*, vol. 11, no. 5, pp. 533–555, May 1973.
[20] I. Stanojev and A. Yener, "Cooperative jamming via spectrum leasing," in *Proc. IEEE Int. Symp. Modeling Optim. Mobile, Ad Hoc Wireless Netw. (WiOpt)*, May 2011, pp. 265–272.
[21] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.
[22] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Başar, "Physical layer security: Coalitional games for distributed cooperation," in *Proc. 7th Int. Symp. WiOPT*, 2009, pp. 1–8.
[23] W. Saad, X. Zhou, B. Maham, T. Başar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.
[24] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *Eurasip J. Wireless Commun. Netw.*, vol. 2009, p. 452907, Jan. 2010.
[25] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Improved wireless secrecy rate using distributed auction theory," in *Proc. 5th ICMAS*, Fujian, China, Dec. 2009, pp. 442–447.
[26] S. Anand and R. Chandramouli. *Secrecy capacity of multi-terminal networks with pricing*, accessed on Sep. 14, 2016. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.143.5267
[27] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Game theoretic beamforming designs," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Nov. 2010, pp. 2099–2103.
[28] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the MISO interference channel," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 170–181, Jan. 2013.
[29] J. P. Cho, Y.-W. P. Hong, and C.-C. J. Kuo, "A game theoretic approach to eavesdropper cooperation in MISO wireless networks," in *Proc. IEEE ICASSP*, May 2011, pp. 3428–3431.
[30] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.
[31] F. Gabry, A. Zappone, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 437–440, Aug. 2015.
[32] G. Kim, "Scheduling in wireless ad hoc networks: Algorithms with performance guarantees," Ph.D. dissertation, ProQuest, Ann Arbor, MI, USA, 2008.
[33] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.
[34] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.
[35] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.
[36] Q. Ma and C. Tepedelenlioglu, "Antenna selection for space-time coded systems with imperfect channel estimation," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 710–719, Feb. 2007.
[37] W. M. Gifford, M. Z. Win, and M. Chiani, "Diversity with practical channel estimation," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1935–1947, Jul. 2005.
[38] J. O. Neel, "Analysis and design of cognitive radio networks and distributed radio resource management algorithms," Dept. Elect. Compu. Eng., Ph.D. dissertation, Virginia Polytech. Inst., Blacksburg, VA, USA, Sep. 2006.
[39] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

Ali Al-Talabani (M'09) received the B.Sc. degree in electrical engineering and the M.Sc. degree in electrical engineering/electronic and communications from the Department of Electrical Engineering, College of Engineering, University of Baghdad, in 1997 and 2000, respectively. He joined Kings College London in 2011, where he is pursuing the Ph.D. degree with the Centre for Telecommunications Research. He is also currently a Research Associate with Loughborough University. He was with the General Organization Company/Ministry of Industries and Minerals as a Research Assistant, Baghdad, Iraq, from 2000 to 2001. His research involved design and implementation of HF receiver with high sensitivity. In 2002, he joined the Academia, Information and Communications Engineering Department, University of Baghdad, Iraq, from 2002 to 2009, as a Lecturer, and the Information Technology Department, College of Applied Sciences, Sur, Oman, from 2009 to 2011, where he has been involved in many research projects.

Yansha Deng (S'13–M'16) received the Ph.D. degree in electrical engineering from the Queen Mary University of London, U.K., in 2015. She is currently a Post-Doctoral Research Fellow with the Department of Informatics, King's College London, U.K. Her research interests include massive MIMO, HetNets, molecular communication, cognitive radio, cooperative networks, and physical layer security. She received the Best Paper Award in ICC 2016. She has served as a TPC member for many IEEE conferences, such as the IEEE GLOBECOM and ICC.

Arumugam Nallanathan (S'97–M'00–SM'05) is currently a Professor of wireless communications with the Department of Informatics, King's College London. He served as the Head of Graduate Studies with the School of Natural and Mathematical Sciences, King's College London, from 2011 to 2012. He was an Assistant Professor with the Department of Electrical and Computer Engineering, National University of Singapore, from 2000 to 2007. He has authored over 300 technical papers in scientific journals and international conferences. His research interests include 5G wireless networks, molecular communications, energy harvesting and cognitive radio networks. He is a co-recipient of the Best Paper Award presented at the IEEE International Conference on Communications in 2016 and the IEEE International Conference on Ultra-Wideband in 2007. He is an IEEE Distinguished Lecturer.

He is also an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2006 to 2011, the IEEE WIRELESS COMMUNICATIONS LETTERS, and the IEEE SIGNAL PROCESSING LETTERS. He served as the Chair of the Signal Processing and Communication Electronics Technical Committee of the IEEE Communications Society, the Technical Program Co-Chair (MAC track) for the IEEE WCNC 2014, the Co-Chair of the IEEE GLOBECOM 2013 (Communications Theory Symposium), the Co-Chair of the IEEE ICC 2012 (Signal Processing for Communications Symposium), the Co-Chair of the IEEE GLOBECOM 2011 (Signal Processing for Communications Symposium), the Technical Program Co-Chair of the IEEE International Conference on UWB 2011 (IEEE ICUWB 2011), the Co-Chair of the IEEE ICC 2009 (Wireless Communications Symposium), the Co-Chair of the IEEE GLOBECOM 2008 (Signal Processing for Communications Symposium), and the General Track Chair for IEEE VTC 2008. He received the IEEE Communications Society SPCE Outstanding Service Award 2012 and the IEEE Communications Society RCC Outstanding Service Award 2014.

Huan X. Nguyen (M'06–SM'15) received the B.Sc. degree with the Hanoi University of Science and Technology, Vietnam, in 2000, and the Ph.D. degree from the University of New South Wales, Australia, from 2003 to 2006. He has been with several universities in the U.K. He is currently a Senior Lecturer with the School of Science and Technology, Middlesex University, London, U.K. His research interests include PHY security, energy harvesting, MIMO techniques, network coding, relay communication, cognitive radio, and multi-carrier systems. He is currently serving as the Editor of the *KSII Transactions on Internet and Information Systems*.