Cooperative Spectrum Access Towards Secure Information Transfer for CRNs

Ning Zhang, *Student Member, IEEE,* Ning Lu, *Student Member, IEEE,* Nan Cheng, *Student Member, IEEE,* Jon W. Mark, *Life Fellow, IEEE,* Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In cognitive radio networks (CRNs), secure information transfer is of paramount importance for primary users (PUs), while secondary users (SUs) mainly desire to ease the starvation for transmission opportunities. To meet such different requirements, cooperation between PUs and SUs can be leveraged and therefore create a win-win situation. In this paper, we investigate cooperative spectrum access for CRNs, which targets to improve the secure transmission of PUs via cooperating SUs that would be incented by certain transmission opportunities. Two types of cooperation schemes are proposed, whereby the PU either cooperates with two individual SUs or a cluster of SUs, which are referred to as relay-jammer (R-J) scheme and cluster-beamforming (C-B) scheme, respectively. In R-J scheme, two individual SUs act as a relay and a friendly jammer to improve the PU's secrecy; In return, the PU allocates a fraction of access time for the SUs' transmission. To achieve the maximum secrecy rate, joint time and power allocation is considered. Particularly, the cooperating relay and jammer determine the optimal transmission power, while the PU decides the optimal time allocation strategy. In C-B scheme, the PU cooperates with a cluster of SUs to enhance the secrecy of the primary link via collaborative beamforming, where three different approaches are proposed for the scenarios with one eavesdropper, with multiple eavesdroppers, and without eavesdroppers' information, respectively. To maximize the secrecy rate, the weight selection and time allocation are also studied. Simulation results are given to validate the proposed schemes and demonstrate that the PU can significantly enhance the secrecy through cooperation.**

***Index Terms*—Cooperative spectrum access, security, cognitive radio networks, beamforming, CCRN.**

I. Introduction

COGNITIVE radio network (CRN) is envisaged to improve spectrum utilization by allowing unlicensed users to opportunistically exploit the unused spectrum bands which are owned by licensed users [1]–[3]. Before accessing the spectrum bands, unlicensed users need to conduct spectrum sensing [4]. However, spectrum sensing may be inaccurate due to the presence of multipath fading and shadowing. Moreover, the energy consumption of spectrum sensing for identifying the unused spectrum bands is significant as well. As an alternative, unlicensed users can cooperate with licensed users to improve the latter's transmission performance, and in return to gain transmission opportunities as a reward. This form of CRN is known as cooperative cognitive radio network (CCRN).

Recently, there has been a flurry of research activities in CCRN [5]–[9]. In [5], a three-phase cooperation scheme is proposed, whereby the PU cooperates with a set of SUs in the first two phases to increase PU's transmission rate, and the cooperating SUs start their transmissions in the last phase. In [6], the cooperation between PUs and SUs is also performed in a three-phase fashion, whereby SUs cooperates with the PU to improve the PU's utility and then share the rewarding resource via a payment mechanism. Different from [5], the PU maximizes its utility based on the transmission rate and the revenue obtained from SUs. In [7], a two-phase cooperation scheme is proposed, whereby the PU transmits its signal to the SU in the first phase, and then the SU decodes the received signal and superimposes it with its own signal to broadcast in the second phase, using different power levels. In summary, the above cooperation schemes aim to improve the performance of PUs in terms of transmission rate, reliability, or revenue, while SUs gain transmission opportunities as a reward.

Since security is a critical issue in wireless environments due to the broadcast nature of wireless communications [10], PUs also have the need for secure communications. Traditionally, the security is dealt with by encryption at upper layers; yet, it becomes very challenging for a network without infrastructure [11]. Moreover, the encryption algorithms could be compromised and an alternative way for enhancing the security is to protect the transmitted signal from being received or decoded by the eavesdroppers [12]. Recently, physical (PHY) layer security, or information-theoretic security, has attracted a lot of attentions in the research community [13]–[15], which exploits the properties of the wireless channel to secure communications. In [13], it is shown that the perfectly secure information can be transmitted at a nonzero rate from the source to the destination, while the eavesdropper cannot learn anything regarding it. This rate is referred to the *secrecy rate*, which is defined as 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.

To address the above issue, user cooperation has been introduced to enhance the secrecy of communications [16]–[20]. In [16], three types of schemes using decode-and-forward

Manuscript received November 17, 2012; revised April 11, 2013. This work was presented in part at IEEE Wireless Communications and Networking Conference (WCNC), April 2013. This work has been supported by The Natural Sciences and Engineering Research Council (NSERC) of Canada under Grant No. RGPIN7779.

N. Zhang, N. Lu, N. Cheng, J.W. Mark, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1 (e-mail:{n35zhang, n7lu, n5cheng, jwmark, sshen}@uwaterloo.ca).

Digital Object Identifier 10.1109/JSAC.2013.131130.

(DF), amplify-and-forward (AF), and cooperative jamming, are proposed to improve the secrecy via cooperation. In [17], distributed beamforming is leveraged at relays to enhance the source's secrecy. Nevertheless, these schemes cannot be applied directly to CRNs because the special features of CRNs have not been taken into consideration: i) PUs have higher priorities for spectrum usage in CRNs; ii) it might not be reasonable to assume that PUs and SUs cooperate unconditionally with each other, since they have their own interests. Considering the features of CRNs, a cooperation based spectrum access is studied in [21], which improves the security of the primary link and provides transmission opportunities to SUs. However, the cooperation objective is achieved at the expense of employing multiple antennas and only the scenario with a single eavesdropper is considered. In reality, the assumption of multiple antennas might not be feasible. Moreover, more practical scenarios, where there exist multiple eavesdroppers or the information regarding eavesdropper(s) is not available, need to be investigated.

In this paper, we investigate cooperative spectrum access for secure information transfer in CRNs. Considering the features of CRNs, the cooperation is performed on a mutual benefit basis. Since the PU has higher priority on spectrum usage, the objective of cooperation is to maximize the secrecy rate of the PU, given that SUs have the requirement on the transmission rate. Specifically, two types of cooperation schemes are proposed, whereby the PU cooperates with SUs to deliver information securely and in return grants spectrum access opportunities to the SUs. The PU can either cooperate with two individual SUs (as a relay and a jammer), or a cluster of SUs, which are referred to as relay-jammer (R-J) scheme and cluster-beamforming (C-B) scheme, respectively. In R-J scheme[1], the relay SU employs DF mode to transmit the PU's information, and in the meanwhile the jammer SU creates artificial noise to confound the eavesdropper. In C-B scheme, the SUs in the cluster enhance the secrecy of the PU's communication via collaborative beamforming and the cooperation is studied for three different scenarios: in the presence of an eavesdropper, in the presence of multiple eavesdroppers, and without the channel state information (CSI) of eavesdroppers, respectively. Especially, zero-forcing beamforming is employed for the last two scenarios. To maximize the secrecy rate, different from the existing works on PHY layer security, joint time and transmission power allocation is considered in R-J scheme, while the selection of the beamforming weight and time allocation strategy are jointly studied in C-B scheme.

In a nutshell, the contribution in this paper is mainly four-fold. First, in the presence of an eavesdropper, a cooperative spectrum access scheme for two individual SUs is proposed to enhance the PU's security and gain transmission opportunities; Second, for a cluster SUs, different cooperation approaches are proposed for the following scenarios: with a single eavesdropper, with multiple eavesdroppers, and without any information about eavesdroppers; Third, to the best of our knowledge, this is the first work to maximize the secrecy rate by jointly allocating time and transmission power; Finally, closed-form solutions in the low SNR regime[2] are derived and numerical results show that with the proposed cooperation schemes, the secrecy of the primary link can be enhanced via cooperation with SUs.

[1]R-J scheme is only considered for the scenario with one eavesdropper.

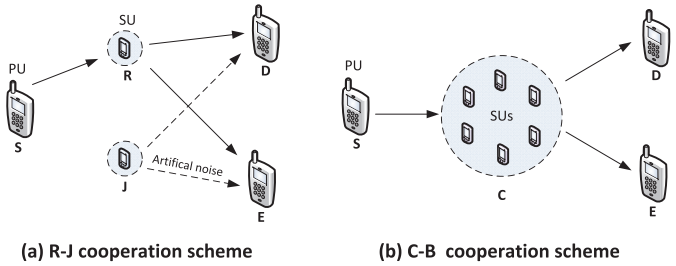


Fig. 1. System model.

The remainder of the paper is organized as follows. The detailed description of the system model is given in Section II. In Section III, R-J scheme is proposed, along with the computation in terms of the transmission power and time allocation. In Section IV, two C-B schemes are presented for the scenario when the eavesdroppers' CSI is known, which can be further divided into two cases: with one eavesdropper and with multiple eavesdroppers. Section V discusses the cooperation under the case when the eavesdroppers' CSI is unavailable. Simulation results are provided in Section VI, followed by the conclusion and future work in Section VII.

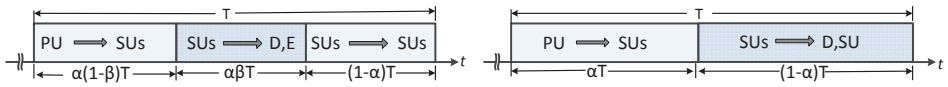
II. System Model

We present the system model in this section. As depicted in Fig. 1, the system consists of a primary source (S), a primary destination (D), multiple SUs, and an eavesdropper (E) or multiple eavesdroppers who aim to decode the PU's information [22]. In the primary network, S holds a time slot of duration T to communicate with D over a bandwidth of W Hz. Different from [22] [23], which assume that there is no direct link between S and either D or E, and only focus on the secure information transfer from the relays to D, we consider a more general case where there exist direct links. It is known that when the channel between S and D is worse than that between S and E, the secrecy rate is zero. To transfer information securely, S either chooses two cooperating SUs, i.e., a relay SU (R) and a jammer SU (J), or a cluster (C) of SUs for cooperation, which are all considered friendly[3]. This common assumption can be found in [17]–[24]. The cooperation between the PU and untrusted SUs has been studied in one of our previous work [25], where trust values of SUs are taken into consideration.

Cooperation can be performed in a three-phase fashion or a two-phase fashion. The time structure for the three-phase cooperation is shown in Fig. 1(a). A fraction α of the duration T is used for the transmission from S to D, which is further divided into two parts according to β, where $0 < \alpha, \beta < 1$.

[2]The low SNR regime is considered just for simplicity of derivation and it will not restrict the application of the proposed cooperative schemes to the more general scenarios.

[3]For SUs, the first and foremost need is to acquire access opportunities for transmissions. In this regard, SUs don't have much motivation to compromise PUs' secrecy. Otherwise, PUs may not be interested in cooperation with SUs. As a consequence, SUs will lose transmission opportunities.



(a) Three-phase coopeartion **(b) Two-phase coopeartion**

Fig. 2. Time frame structure for cooperation

Particularly, in the first phase of $\alpha(1-\beta)T$, S transmits data to cooperating SUs, which is also overheard by D and E. In the second phase, a subsequent duration of $\alpha\beta T$ is leveraged for the transmission from cooperating SUs to D. For R-J scheme, shown in Fig. 1(a), R employs DF protocol to relay the PU's message to D, and simultaneously J transmits an artificial jamming signal to confound E. For C-B scheme, shown in Fig. 1(b), the SUs in C first decode the PU's message and then each of them forwards a weighted version of that message to D via collaborative beamforming. In the last phase, the remaining $(1-\alpha)T$ is granted to cooperating SUs for transmitting their own data as a reward, in which the relay SU and jammer SU access the channel in a TDMA fashion, while the SUs in C transmit the data to a common secondary receiver via collaborative beamforming [26]. To ease presentation, the period for the first two phases, i.e., (αT), is termed as cooperation period, while the last phase of $(1-\alpha)T$ is termed as rewarding period. When there exist multiple eavesdroppers, C-B scheme is carried out in a two-phase fashion, as shown in Fig. 1(b). The operation in the first phase is the same as that of the previous cases. In the second phase, the cluster simultaneously transmits the PU's message and its own data.

Since SUs will not cooperate with the PU unconditionally, SUs have a requirement on the *expected* overall transmission rate $\bar{R}_{EX}$, which SUs desire through cooperation. However, for the three-phase cooperation, the *actual* average transmission rate of SUs depends on the time period granted by the PU. From the PU's perspective, it tends to grant less time to SUs, and hence transmission rate of SUs obtained via cooperation will be much less than $\bar{R}_{EX}$. In order to enforce the PU to grant an acceptable rewarding time, SUs' strategy is to determine the effort that they are willing to make during cooperation, i.e., the maximum power P_{max}^{C} for cooperation, according to the transmission rate obtained. As a result of the SUs' strategy[4], if the PU chooses a lager α, although the cooperation period is prolonged, the cooperating SUs will choose a lower transmission power, which will lead to a decrease in the performance during the cooperation period. Then, the overall secrecy rate may be reduced. If the PU chooses a smaller α to acquire more effort from SUs during the cooperation period, although the performance in the cooperation period is increased, the time for that period is reduced, which may cause a drop in the overall secrecy rate.

A slow, flat, block Rayleigh fading environment is considered, where the channel remains static in one time slot and changes independently over different time slots. The channel coefficient from S to D is denoted by h_{SD}. Similarly, we have h_{SR}, h_{SE}, h_{RD}, h_{RE}, h_{JD}, and h_{JE}. The global CSI is available for the system, including D-related CSI (D-CSI) and E-related CSI (E-CSI), which is a common assumption in PHY layer security literature. The cooperation when E-CSI is unavailable will be discussed in Section V. In addition, additive white Gaussian noise is assumed with zero mean and the one-side power spread density is N_0. Moreover, each node is equipped with a single antenna and communicates with each other in a half-duplex mode.

In the following, matrices and vectors are denoted by bold uppercase letters and bold lowercase letters, respectively. $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^\dagger$ denote the conjugate, transpose, and conjugate transpose, respectively. $\mathbf{I}$ denotes the identity matrix. $[x]^+$ denotes the maximum value between x and 0, while $x^\star$ denotes the optimal value of x. $|\cdot|$ denotes the magnitude of a channel or the absolute value of a complex number, while $\|\cdot\|$ is the Euclidean norm of a vector or a matrix.

III. R-J Cooperation Scheme

A. Problem Formulation

1) Secrecy Rate of PU: We use secrecy rate as a measure for the secure communication. To obtain the secrecy rate, the transmission rates at different nodes are calculated as follows.

In the first phase, S transmits data to R and the transmission rate at R is given by

$$R_R = W\log_2(1+\gamma), \tag{1}$$

where $\gamma = \frac{P|h_{SR}|^2}{WN_0}$ and P is the transmission power of the PU.

In the second phase, R relays the PU's message to D using DF protocol, and simultaneously J broadcasts an artificial jamming signal. Since D receives signals in both the first and second phases, the transmission rate R_D at D using maximal ratio combining (MRC) is given by

$$R_D = W\log_2(1+\xi+\frac{P_R|h_{RD}|^2}{WN_0+P_J|h_{JD}|^2}), \tag{2}$$

where $\xi = P|h_{SD}|^2/(WN_0)$ is the SNR from the first phase, and P_R and P_J are the transmission power of R and J during cooperation, respectively.

Likewise, E also receives signals during the first two phases. Therefore, the transmission rate at E can be expressed as follows:

$$R_E = W\log_2(1+\delta+\frac{P_R|h_{RE}|^2}{WN_0+P_J|h_{JE}|^2}), \tag{3}$$

where $\delta = P|h_{SE}|^2/(WN_0)$ is the SNR from the first phase.

When the DF cooperative communication is applied, the overall transmission rate of D and E equal to the minimum rate of the first two phases, respectively [27], i.e.,

$$\begin{aligned}\bar{R}_D &= \min\{\alpha(1-\beta)R_R, \alpha\beta R_D\}\\ \bar{R}_E &= \min\{\alpha(1-\beta)R_R, \alpha\beta R_E\}\end{aligned} \tag{4}$$

[4]The strategy of SUs for the two-phase cooperation is explicitly explained in Section IV-B and Section V, respectively.

By definition, the *secrecy rate* R_{SEC} is given by:

$$R_{SEC} = [R_D - R_E]^+, \tag{5}$$

Substituting (4) into (5), the overall secrecy rate is then given by

$$\bar{R}_{SEC} = [\min\{\alpha(1-\beta)R_R, \alpha\beta R_D\} - \alpha\beta R_E]^+ \tag{6}$$

2) Overall Transmission Rate of SUs: Let $P_{S,i}$ be the transmission power of SU_i for its own communication, where $i = \mathsf{R}$ or J. SUs are considered to have the same power constraint P_{max}. R and J transmit in a TDMA mode and the overall transmission rate of SU_i is given by

$$\bar{R}_{S,i} = \frac{1-\alpha}{2} W \log_2(1 + \frac{P_{S,i}|h_{S,i}|^2}{WN_0}), \tag{7}$$

where $h_{S,i}$ is the channel coefficient from i to its corresponding receiver.

As mentioned in the system model, SUs have an requirement on the *expected* overall transmission rate $\bar{R}_{EX}$ via cooperation. From (7), $\bar{R}_{S,i}$ is related to the time period granted by the PU. To measure SUs' degree of satisfaction on $\bar{R}_{S,i}$, $U_{S,i}$ is defined as $U_{S,i} = \min\{\frac{\bar{R}_{S,i}}{\bar{R}_{EX}}, 1\}$, which implies how satisfactory SU_i is with $\bar{R}_{S,i}$. For instance, if $\bar{R}_{S,i} = \bar{R}_{EX}$, $U_{S,i}$ is equal to 1. In order to enforce the PU to grant an acceptable rewarding time, SUs' strategy is to determine the effort that they are willing to make during cooperation, i.e., the maximum power P^C_{max} for cooperation, according to the degree of satisfaction. For simplicity, $P^C_{max} = U_{S,i} \cdot P_{max}$. In other words, the degree of effort that the SU is willing to make depends on the degree of the satisfaction obtained. For example, if $U_{S,i} = 1$, the SU is willing to devote full power P_{max} for cooperation, i.e., $P^C_{max} = P_{max}$.

3) Secrecy Rate Maximization: Since the SU typically does not have much transmission opportunities, it aims at maximizing the throughput by adopting P_{max} for its own transmission. Thus, given a certain α, $\bar{R}_{S,i} = \frac{1-\alpha}{2} W \log_2(1 + \frac{P_{max}|h_{S,i}|^2}{WN_0})$. Based on the degree of the satisfaction, P^C_{max} can be determined, which is a function of α. As shown in (6), $\bar{R}_{SEC}$ is related to α, β, and the transmission power P_R and P_J, which are constrained by P^C_{max}. From PU's perspective, the objective of cooperation is to maximize the overall secrecy rate $\bar{R}_{SEC}$. Therefore, the PU chooses the time allocation coefficients α and β, while the SUs determine the optimal transmission power for cooperation, which can be formulated as the following optimization problem:

$$\begin{aligned} &\max_{\alpha,\beta,P_R,P_J} \bar{R}_{SEC} \\ &\text{s.t. } 0 < \alpha,\ \beta < 1,\ 0 \le P_R \le P^C_{max},\ 0 \le P_J \le P^C_{max}. \end{aligned} \tag{8}$$

B. Cooperation Parameters Determination

The time allocation coefficients and transmission power can be optimized by solving the above optimization problem. To do this, the procedure can be divided into two steps: i) given α, R and J select the optimal transmission power; and ii) S selects the optimal $\alpha^\star$, $\beta^\star$ to maximize the secrecy rate, aware of the results of the first step.

From (6), for a given α, the overall secrecy rate $\bar{R}_{SEC}$ not only depends on $R_D - R_E$, but also on β. In fact, $\bar{R}_{SEC}$ can be further expressed as follows:

$$\begin{aligned} \bar{R}_{SEC} &= [\alpha\beta(R_D - R_E)]^+ = \alpha[\frac{R_R(R_D - R_E)}{R_R + R_D}]^+ \\ &= \alpha[R_R - \frac{R_R(R_R + R_E)}{R_R + R_D}]^+, \end{aligned} \tag{9}$$

where R_R, R_D and R_E are given by (1), (2), and (3), respectively. The derivation is given in the Appendix. Note that given α, the optimal $\beta^\star = \frac{R_R}{R_R + R_D}$.

In the literature, most of the existing works assume the time duration for the transmission from S to R and from R to D are equal, and try to maximize $R_D - R_E$ based on this assumption. However, R_R and R_D are typically not the same. Furthermore, the overall transmission rate is the minimum one between $\bar{R}_R$ and $\bar{R}_D$ for DF strategy. Thus, it is not optimal to assign equal duration for these two phases. From (9), it can be seen that the secrecy rate cannot achieve the optimum value by only maximizing $R_D - R_E$. This is because when R_D increases, $R_D - R_E$ increases, but β decreases. Note that the objective function in (9) has encapsulated the above factors and in this paper we study the nontrivial case where the secrecy rate is positive.

1) Power Allocation: Since the relay is leveraged to increase the transmission rate at destination compared with that at the eavesdropper, it requires that $|h_{RD}| > |h_{RE}|$. The job of the jammer is to create more interference at the eavesdropper than at the destination and it is necessary that $|h_{JE}| > |h_{JD}|$. In what follows, to achieve the maximum secrecy rate, the optimal transmission power of relay SU and jammer SU are analyzed, respectively, when α is given.

a) Relay SU: Since R_R is fixed, maximizing $\bar{R}_{SEC} = R_R - R_R(R_R + R_E))/(R_R + R_D)$ is equivalent to minimizing $f(P_R, P_J) \triangleq (R_R + R_E)/(R_R + R_D)$. Similar to [28], we study the case in the low SNR regime, which corresponds to the cases of long-distance transmissions or energy-limited scenarios. We approximate $\log_2(1 + snr) \approx snr$ [29]. Based on (1), (2), (3), and the approximation, we have

$$f(P_R, P_J) = \frac{\Psi_E + P_R|h_{RE}|^2/(WN_0 + P_J|h_{JE}|^2)}{\Psi_D + P_R|h_{RD}|^2/(WN_0 + P_J|h_{JD}|^2)}, \tag{10}$$

where $\Psi_D = \gamma + \xi$ and $\Psi_E = \gamma + \delta$. Take the first order derivative of f with respect to P_R and it is always negative because $|h_{RD}| > |h_{RE}|$. Therefore, $f(P_R, P_J)$ is a monotonically decreasing function of P_R and the optimal transmission power $P^\star_R$ is P^C_{max} for maximizing the secrecy rate. Note that P^C_{max} is a function of α.

b) Jammer SU: The optimal transmission power $P^\star_J$ is selected such that the objective function in (10) can be maximized. The derivative of (10) with respect to P_J is proportional to a quadratic function in the following form:

$$\frac{\partial f}{\partial P_J} \propto \psi_1 \cdot P_J^2 + \psi_2 \cdot P_J + \psi_3, \tag{11}$$

where

$$\begin{aligned} \psi_1 =& |h_{JD}||h_{JE}|P_R(|h_{RD}|\Psi_E|h_{JE}| - |h_{RE}|\Psi_D|h_{JD}|) \\ \psi_2 =& 2|h_{JD}||h_{JE}|N_0P_R(|h_{RD}|\Psi_E - |h_{RE}|\Psi_D) \\ \psi_3 =& |h_{RD}||h_{RE}|P_R^2N_0(|h_{JD}| - |h_{JE}|) + \\ & N_0^2(|h_{RD}|\Psi_E|h_{JE}| - |h_{RE}|\Psi_D|h_{JE}|). \end{aligned}$$

Since $|h_{RD}| > |h_{RE}|$ and $|h_{JE}| > |h_{JD}|$, we have $\psi_1 > 0$, $\psi_2 > 0$, and $P_R = P^C_{max}$. If $\psi_3 > 0$, there is no positive root for the quadratic function in (11) and $\frac{\partial f}{\partial P_J} > 0$ for the range from 0 to P^C_{max}. Thus, $P^\star_J$ equals to 0 to maximize the secrecy rate, indicating a non-jamming scenario. If $\psi_3 < 0$, there is one positive root $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1}$. When $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1} > P^C_{max}$, $\frac{\partial f}{\partial P_J} < 0$ for the range from 0 to P^C_{max} and hence $P^\star_J$ should be selected as P^C_{max}. Otherwise, $P^\star_J$ should be equal to $\frac{-\psi_2+\sqrt{\psi_2^2-4\psi_1\psi_3}}{2\psi_1}$.

2) Time Allocation: From (9), the objective function has taken the factor of β into consideration. Given α, the optimal transmission power of SUs has been obtained in the previous section. Therefore, the optimal $\beta^\star$ can be easily determined by

$$\beta^\star = \frac{R_R}{R_R + R_D}, \tag{12}$$

where R_D is the transmission rate at D when R and J choose the optimal transmission power.

The optimal $\alpha^\star$ can be determined by solving the following equation:

$$\alpha^\star = \arg\max \alpha\beta(R_D - R_E) \tag{13}$$

Note that β, R_D, and R_E are all functions of α ($0 < \alpha < 1$).

IV. C-B Cooperation Scheme with E-CSI

In this section, we discuss the cooperation between the PU and a cluster of SUs when E-CSI is available. We propose a three-phase cooperation scheme and a two-phase cooperation scheme for the scenarios in the presence of an eavesdropper and multiple eavesdroppers, respectively. To maximize the secrecy rate, time allocation and weights selection are jointly considered.

A. C-B Scheme for Single Eavesdropper (CBSE)

1) Problem Formulation:

a) Secrecy Rate of PU: In the presence of one eavesdropper, the cooperation is performed in a three-phase fashion, as shown in Fig. 2(a). In the first phase, the PU broadcasts to the cluster the signal $\sqrt{P}s$, where s is the information symbol with $E\{|s|^2\} = 1$, which is overheard by D and E. In order for all the cluster members to successfully decode the signal, the transmission rate R_R from S to C is determined by the worst channel between S and the cluster members.

$$R_R = W\log_2(1 + \min_i \frac{P|h_{SR,i}|^2}{N_0 W}), \tag{14}$$

where $h_{SR,i}$ is the channel from S to ith SU in the cluster. Denote by $y_{D,1}$ and $y_{E,1}$ the signal received at D and E in the first phase, respectively, which can be given by

$$\begin{aligned} y_{D,1} &= \sqrt{P}h_{SD}s + n_{SD} \\ y_{E,1} &= \sqrt{P}h_{SE}s + n_{SE} \end{aligned} \tag{15}$$

where n_{SD} and n_{SE} are the noise at D and E, respectively.

In the second phase, each SU in the cluster decodes the received symbol and forwards a weighted version of the re-encoded symbol $\tilde{s}$ to D. Let $\mathbf{w}$ be the column vector of the weights of all SUs in the cluster and N be the number of SUs in the cluster. Then, the received signals $y_{D,2}$ and $y_{E,2}$ at D and E in the second phase can be written respectively as:

$$\begin{aligned} y_{D,2} &= \mathbf{h}^\dagger_{RD}\mathbf{w}\tilde{s} + n_{RD} \\ y_{E,2} &= \mathbf{h}^\dagger_{RE}\mathbf{w}\tilde{s} + n_{RE} \end{aligned} \tag{16}$$

where $\mathbf{h}_{RD} = [h^*_{D,1}, h^*_{D,2}, ..., h^*_{D,N}]^T$ and $\mathbf{h}_{RE} = [h^*_{E,1}, h^*_{E,2}, ..., h^*_{E,N}]^T$. Note that $h_{D,i}$ and $h_{E,i}$ are the complex channel coefficients from the ith SU in the cluster to D and E, respectively, where $i \in \{1, 2, ..., N\}$. n_{RD} and n_{RE} are the noise at D and E, respectively.

Assume that the cooperating SUs use the same codewords as S. The transmission rate at D and E are given as follows:

$$\begin{aligned} R_D &= W\log_2(1 + \xi + \frac{\mathbf{w}^\dagger\mathbf{h}_{RD}\mathbf{h}^\dagger_{RD}\mathbf{w}}{N_0 W}) \\ R_E &= W\log_2(1 + \delta + \frac{\mathbf{w}^\dagger\mathbf{h}_{RE}\mathbf{h}^\dagger_{RE}\mathbf{w}}{N_0 W}), \end{aligned} \tag{17}$$

where ξ and δ are the same as that in (2) and (3), respectively. Substituting (14) and (17) into (6), we can obtain the overall secrecy rate.

b) Overall Transmission Rate of SUs: In the third phase, the SUs in the cluster transmit the data to the secondary receiver via collaborative beamforming. The overall rate $\bar{R}_S$ at the secondary receiver can be given by

$$\bar{R}_S = (1-\alpha)W\log_2(1 + \frac{\mathbf{v}^\dagger\mathbf{h}_{RS}\mathbf{h}^\dagger_{RS}\mathbf{v}}{N_0 W}), \tag{18}$$

where $\mathbf{v}$ is the column vector of the weights of all cooperating SUs for the secondary transmission and $\mathbf{h}_{RS} = [h^*_{S,1}, h^*_{S,2}, ..., h^*_{S,N}]^T$. Note that $h_{S,i}$ is the complex channel coefficient from the ith SU in the cluster to the secondary receiver. To maximize the transmission rate, the SUs select the optimal $\mathbf{v}^\star$, under the total power constraint, which can be formulated as follows:

$$\begin{aligned} \max_{\mathbf{v}} \quad & \mathbf{v}^\dagger\mathbf{h}_{RS}\mathbf{h}^\dagger_{RS}\mathbf{v} \\ s.t. \quad & \mathbf{v}^\dagger\mathbf{v} \le P_{max} \end{aligned} \tag{19}$$

To achieve the maximum transmission rate, $\mathbf{v}$ should lie in the space spanned by $\mathbf{h}_{RS}$. Thus, $\mathbf{v}^\star$ can be given by $\mathbf{v}^\star = \sqrt{P_{max}}\frac{\mathbf{h}_{RS}}{\|\mathbf{h}_{RS}\|}$, where $\| \mathbf{h}_{RS} \|$ is the Euclidean norm of $\mathbf{h}_{RS}$. Therefore, given a certain α, the overall transmission rate $\bar{R}_S$ is given by

$$\bar{R}_S = (1-\alpha)W\log_2(1 + \frac{P_{max} \| \mathbf{h}_{RS} \|^2}{N_0 W}). \tag{20}$$

c) Secrecy Rate Maximization: Similar to Section III-A2 and III-A3, the cluster of SUs, as a whole, determines the maximum power P^C_{max} for cooperation based on the satisfaction obtained. Substituting (14) and (17) into (9), we can obtain $\bar{R}_{SEC}$. To maximize $\bar{R}_{SEC}$, the PU selects the optimal time allocation coefficients and the SUs determine the best beamforming weights under a total power constraint.

2) Cooperation Parameters Determination:

a) Optimal Weight Selection: The SUs select the optimal weight $\mathbf{w}^\star$ to maximize the secrecy rate $\bar{R}_{SEC}$. From (9), given α, maximizing $\bar{R}_{SEC}$ is equivalent to maximizing $(R_R + R_D)/(R_R + R_E)$. Substituting (17) into it, the optimal

weight can be determined by solving the following problem.

$$\max_{\mathbf{w}} \frac{\Psi_D + \mathbf{w}^\dagger \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger \mathbf{w}}{\Psi_E + \mathbf{w}^\dagger \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger \mathbf{w}} \quad s.t. \quad \mathbf{w}^\dagger\mathbf{w} \le P_{max}^C$$

where $\Psi_D = (\gamma+\xi)N_0W$ and $\Psi_E = (\gamma+\delta)N_0W$. Let us rewrite $\mathbf{w} = \sqrt{P_{max}^C}\hat{\mathbf{w}}$, where $\hat{\mathbf{w}}^\dagger\hat{\mathbf{w}}$=1. The above problem is then transformed into the following form:

$$\max_{\mathbf{w}} \frac{\Psi_D + p\hat{\mathbf{w}}^\dagger \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger \hat{\mathbf{w}}}{\Psi_E + p\hat{\mathbf{w}}^\dagger \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger \hat{\mathbf{w}}} \quad s.t. \quad \hat{\mathbf{w}}^\dagger\hat{\mathbf{w}} = 1, p \le P_{max}^C \tag{21}$$

To guarantee $\bar{R}_{SEC}$ to be positive, it is necessary that the numerator is greater than the denominator. Due to this necessary condition, the derivative of the objective function in (21) with respect to p is positive and $\bar{R}_{SEC}$ is maximized when $p = P_{max}^C$. Thus, the above optimization problem can be further rewritten as

$$\max_{\hat{\mathbf{w}}} \frac{\hat{\mathbf{w}}^\dagger \mathbf{Q}_{RD}\hat{\mathbf{w}}}{\hat{\mathbf{w}}^\dagger \mathbf{Q}_{RE}\hat{\mathbf{w}}} \quad s.t. \quad \hat{\mathbf{w}}^\dagger\hat{\mathbf{w}} = 1 \tag{22}$$

where

$$\mathbf{Q}_{RD} = \frac{\Psi_D}{P_{max}^C}\mathbf{I} + \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger \text{ and } \mathbf{Q}_{RE} = \frac{\Psi_E}{P_{max}^C}\mathbf{I} + \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger.$$

The problem in (22) is a generalized eigenvector problem and the optimal $\hat{\mathbf{w}}^\star$ is selected as the uniform eigenvector of $\mathbf{Q}_{RD}\mathbf{Q}_{RE}^{-1}$ corresponding to its largest eigenvalue. Therefore, given α, the optimal $\mathbf{w}^\star = \sqrt{P_{max}^C}\hat{\mathbf{w}}^\star$.

b) Time Allocation: Similar to III-B2, $\beta^\star$ can be determined by substituting (17) into (12), when optimal $\mathbf{w}$ is selected. The optimal $\alpha^\star$ can be determined by solving the following problem, when the optimal weights and β are selected.

$$\alpha^\star = \arg\max \alpha\beta(R_D - R_E) \tag{23}$$

Note that β, R_D, and R_E are all functions of α ($0 < \alpha < 1$).

B. C-B Scheme for Multiple Eavesdroppers (CBME)

1) Problem Formulation: For the case of multiple eavesdroppers, the cooperation can be performed in a two-phase way, as shown in Fig. 2(b). The operation in the first phase is the same as that in the previous cases and the transmission rate R_R is given in (14).

In the second phase, instead of relaying the PU's data and transmitting its own data in different phases, the cluster transmits $\mathbf{x}$ which is the sum of the weighted version of the PU's information symbol $\tilde{s}$ and its information symbol z with $E\{|z|^2\} = 1$. Therefore, $\mathbf{x}$ can be represented by $\mathbf{x} = \mathbf{w}\tilde{s} + \mathbf{v}z$, where $\mathbf{w}$ and $\mathbf{v}$ are the column vectors of the weights of all SUs for transmitting the PU's symbol and SUs' symbol, respectively. Then, the received signals $y_{D,2}$ and $\mathbf{y}_{E,2}$ at D and eavesdroppers in the second phase can be written respectively as:

$$\begin{aligned} y_{D,2} &= \mathbf{h}_{RD}^\dagger \mathbf{w}\tilde{s} + \mathbf{h}_{RD}^\dagger \mathbf{v}z + n_{RD} \\ \mathbf{y}_{E,2} &= \mathbf{H}_{RE}^\dagger \mathbf{w}\tilde{s} + \mathbf{H}_{RE}^\dagger \mathbf{v}z + \mathbf{n}_{RE} \end{aligned} \tag{24}$$

where $\mathbf{H}_{RE}$ is the matrix of channel coefficients between the SUs and eavesdroppers, and $\mathbf{n}_{RE}$ is the noise vector at eavesdroppers. To transmit the PU's data and its own data simultaneously, the cluster utilizes the approach based on zero-forcing beamforming, which is similar to the work in [30]. By doing so, the SUs' transmission will not interfere with the concurrent transmission of the PU, and vice versa. To this end, $\mathbf{v}$ should be in the null space of $\mathbf{h}_{RD}^\dagger$ such that $\mathbf{h}_{RD}^\dagger\mathbf{v} = 0$ and $\mathbf{w}$ should be in the null space of $\mathbf{h}_{RS}^\dagger$ such that $\mathbf{h}_{RS}^\dagger\mathbf{w} = 0$. Therefore, the overall transmission rate $\bar{R}_S$ at the secondary receiver is

$$\bar{R}_S = (1-\alpha)W\log_2(1 + \frac{|\ \mathbf{h}_{RS}^\dagger\mathbf{v}\ |^2}{N_0W}). \tag{25}$$

Different from the pervious case, it is not necessary to enforce the PU to grant a reasonable period of time to SUs due to the following reasons: i) relaying PU's data and transmitting SUs' data occupy the same period, and hence, the PU itself will not just allocate a quite short duration for the second phase, which affects the PU's performance as well; and ii) the cluster can achieve the expected transmission rate $\bar{R}_{EX}$ on its own, i.e., $\bar{R}_S = \bar{R}_{EX}$, by choosing $\mathbf{w}$ and $\mathbf{v}$. Denote by P_1 and P_2 the transmission power for relaying the PU's data $\tilde{s}$ and transmitting its own data z, respectively, where $P_1 = \mathbf{w}^\dagger\mathbf{w}$ and $P_2 = \mathbf{v}^\dagger\mathbf{v}$. Since the cluster has a total power budget P_{max}, it holds that $P_1 + P_2 \le P_{max}$. To maximize the secrecy rate of the PU and guarantee the expected transmission rate $\bar{R}_{EX}$ of the SUs, the cluster chooses the suitable $\mathbf{w}$ and $\mathbf{v}$ under the total power constraint, while the PU determines α.

2) Cooperation Parameters Determination: For convenience, let $\mathbf{w} = \sqrt{P_1}\hat{\mathbf{w}}$ and $\mathbf{v} = \sqrt{P_2}\hat{\mathbf{v}}$, respectively, where $\hat{\mathbf{w}}^\dagger\hat{\mathbf{w}} = 1$ and $\hat{\mathbf{v}}^\dagger\hat{\mathbf{v}} = 1$. To select the optimal $\mathbf{w}^\star$ and $\mathbf{v}^\star$, we perform the following two steps: i) determine the optimal $\hat{\mathbf{w}}^\star$ and $\hat{\mathbf{v}}^\star$ given P_1 and P_2; and ii) select P_1 and P_2, based on the results of the previous step.

a) Step 1: We first determine the optimal $\hat{\mathbf{w}}^\star$ and $\hat{\mathbf{v}}^\star$. For $\hat{\mathbf{v}}$, the objective is to maximize the transmission rate at the secondary receiver, under the constraint of no interference at D. Therefore, the optimal $\hat{\mathbf{v}}^\star$ can be determined by solving the following optimization problem.

$$\max_{\hat{\mathbf{v}}} |\ \mathbf{h}_{RS}^\dagger\hat{\mathbf{v}}\ |^2 \quad s.t.\ \mathbf{h}_{RD}^\dagger\hat{\mathbf{v}} = 0 \text{ and } \hat{\mathbf{v}}^\dagger\hat{\mathbf{v}} = 1 \tag{26}$$

From (26), it can be seen that $\hat{\mathbf{v}}$ is orthogonal to $\mathbf{h}_{RD}$, which means $\hat{\mathbf{v}}$ belongs to the subspace of $\mathbf{h}_{RD}^\perp$, i.e., the null space of $\mathbf{h}_{RD}$. To maximize the objective function in (26), the optimal $\hat{\mathbf{v}}^\star$ should be selected in the direction of the orthogonal projection of $\mathbf{h}_{RS}$ onto $\mathbf{h}_{RD}^\perp$. Thus, $\hat{\mathbf{v}}^\star$ can be determined as follows:

$$\hat{\mathbf{v}}^\star = \frac{(\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger)\mathbf{h}_{RS}}{\|\ (\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger)\mathbf{h}_{RS}\ \|}, \tag{27}$$

where $\mathbf{I} - \hat{\mathbf{h}}_{RD}\hat{\mathbf{h}}_{RD}^\dagger$ is the orthogonal projector onto $\mathbf{h}_{RD}^\perp$ and $\hat{\mathbf{h}}_{RD}$ is the normalized vector of $\mathbf{h}_{RD}$.

For $\hat{\mathbf{w}}$, the objective is to maximize the secrecy rate of the PU. Due to the presence of multiple eavesdroppers, it is typically difficult to obtain the optimal $\hat{\mathbf{w}}^\star$. Instead, a suboptimal solution is devised as follows. The cluster selects

$\hat{\mathbf{w}}$ to null out the PU's information at all eavesdroppers[5], i.e., $\mathbf{H}_{RE}^{\dagger}\hat{\mathbf{w}} = 0$. By doing so, the transmission rate at all eavesdroppers are zero. Thus, maximizing the secrecy rate is equivalent to maximizing R_D, which can be given by

$$R_D = W\log_2(1+\xi+P_2\frac{\mid \mathbf{h}_{RD}^{\dagger}\hat{\mathbf{w}} \mid^2}{N_0W}), \tag{28}$$

where ξ is the same as that in (2).

As mentioned before, $\mathbf{w}$ should also be in the null space of $\mathbf{h}_{RS}^{\dagger}$. Thus, the optimal $\hat{\mathbf{w}}^{\star}$ can be selected such that $\mid \mathbf{h}_{RD}^{\dagger}\hat{\mathbf{w}} \mid$ is maximized under the constraint that $\mathbf{H}_{RE}^{\dagger}\hat{\mathbf{w}} = 0$ and $\mathbf{h}_{RS}^{\dagger}\mathbf{w} = 0$. Define a matrix $\mathbf{H}_R$, which contains $\mathbf{h}_{RS}$ and $\mathbf{H}_{RE}$, i.e., $\mathbf{H}_R = [\mathbf{h}_{RS}\ \mathbf{H}_{RE}]$. Then, the constraint becomes $\mathbf{H}_R^{\dagger}\mathbf{w} = 0$. To satisfy it, $\hat{\mathbf{w}}$ should belong to the subspace of $\mathbf{H}_R^{\perp}$, i.e., the null space of $\mathbf{H}_R$. To maximize $\mid \mathbf{h}_{RD}^{\dagger}\hat{\mathbf{w}} \mid$, the optimal $\hat{\mathbf{w}}^{\star}$ should be closest to $\mathbf{h}_{RD}^{\dagger}$ and meanwhile belongs to $\mathbf{H}_R^{\perp}$. Thus, $\hat{\mathbf{w}}^{\star}$ should be the orthogonal projection of $\mathbf{h}_{RD}$ onto the subspace $\mathbf{H}_R^{\perp}$. Then, $\hat{\mathbf{w}}^{\star}$ can be given by

$$\hat{\mathbf{w}}^{\star} = \frac{(\mathbf{I}-\mathbf{H}_R(\mathbf{H}_R^{\dagger}\mathbf{H}_R)^{-1}\mathbf{H}_R^{\dagger})\mathbf{h}_{RD}}{\parallel (\mathbf{I}-\mathbf{H}_R(\mathbf{H}_R^{\dagger}\mathbf{H}_R)^{-1}\mathbf{H}_R^{\dagger})\mathbf{h}_{RD} \parallel}, \tag{29}$$

where $\mathbf{I}-\mathbf{H}_R(\mathbf{H}_R^{\dagger}\mathbf{H}_R)^{-1}\mathbf{H}_R^{\dagger}$ is the orthogonal projector on $\mathbf{H}_R^{\perp}$.

b) Step 2: Determination of P_1, P_2 and α. Substituting (27) and (29) into (25) and (28), respectively, it can be seen that $\bar{R}_S$ is a function of P_1 and α, while R_D is a function of P_2. Given a certain α, the cluster needs to select P_1 to meet the expected transmission rate $\bar{R}_{EX}$ and the rest of power, i.e., P_2, contributes to R_D. Similar to the Appendix, when the secrecy rate is maximized, we have $\alpha = \frac{R_D}{R_R+R_D}$. Therefore, we have the following equations:

$$\begin{aligned}(1-\alpha)W\log_2(1+\frac{P_1 \mid \mathbf{h}_{RS}^{\dagger}\hat{\mathbf{v}}^{\star} \mid^2}{N_0W}) &= \bar{R}_{EX}\\ \alpha = \frac{R_D}{R_R+R_D} \quad P1+P2 &= P_{max}.\end{aligned} \tag{30}$$

Solving the above equations, we have

$$\begin{aligned}P_1 &= \frac{(R_RN_0+W\xi N_0+\mid \mathbf{h}_{RD}^{\dagger}\hat{\mathbf{w}}^{\star} \mid^2)\bar{R}_{EX}}{R_R \mid \mathbf{h}_{RS}^{\dagger}\hat{\mathbf{v}}^{\star} \mid^2 + \mid \mathbf{h}_{RD}^{\dagger}\hat{\mathbf{w}}^{\star} \mid^2 \bar{R}_{EX}}\\ \alpha &= 1-\frac{N_0\bar{R}_{EX}}{P_1 \mid \mathbf{h}_{RS}^{\dagger}\hat{\mathbf{v}}^{\star} \mid^2}\end{aligned} \tag{31}$$

V. C-B Cooperation Scheme without E-CSI (CBNE)

When E-CSI is unknown, it is impossible for the PU to determine the optimal length for the rewarding time, i.e., $(1-\alpha)T$. Therefore, from the perspective of the PU, it desires that the SUs will make their best efforts to help for secure communication. To this end, the PU grants a period time to SUs such that the need of SUs can be met, i.e., $\bar{R}_{EX}$ of the SUs can be obtained. In return, the SUs will make the best efforts to help the PU, i.e., to devote the maximum power P_{max} for cooperation.

[5]Note that the number of SUs needs to be greater than that of eavesdroppers for this purpose.

A. Problem Formulation

The cooperation is carried out in a three-phase fashion, as shown in Fig. 2(a). In the first phase, the transmission rate from S to the cluster and D are the same as in Section IV-A, which are given by (14) and (17), respectively.

In the second phase, all the cluster members transmit a combination of a weighted version of the re-encoded symbol $\tilde{s}$ and an artificial noise. Similar to [31], the artificial noise is leveraged to mask the concurrent transmission from S to D. As such, the cluster transmits $\mathbf{x}$, which is given by $\mathbf{x} = \mathbf{w}\tilde{s}+\mathbf{n}_a$, where $\mathbf{w}$ is the column vector of the weights of all SUs in the cluster and $\mathbf{n}_a$ is the artificial noise. Then, the received signals $y_{D,2}$ and $\mathbf{y}_{E,2}$ at D and eavesdroppers in the second phase can be written as:

$$\begin{aligned}y_{D,2} &= \mathbf{h}_{RD}^{\dagger}\mathbf{w}\tilde{s}+\mathbf{h}_{RD}^{\dagger}\mathbf{n}_a+n_{RD}\\ \mathbf{y}_{E,2} &= \mathbf{h}_{RE}^{\dagger}\mathbf{w}\tilde{s}+\mathbf{h}_{RE}^{\dagger}\mathbf{n}_a+\mathbf{n}_{RE}\end{aligned} \tag{32}$$

As mentioned before, the total power constraint of the cluster for cooperation is P_{max}. Denote the power spent for transmitting the information symbol $\tilde{s}$ and the artificial noise $\mathbf{n}_a$ by P_I and P_N, respectively. It holds that $P_I+P_N \le P_{max}$. To enhance the security of the PU, the cluster has to allocate the power properly.

Due to the unknown CSI related to the eavesdroppers, the cluster performs in the following way. In order to avoid interfering with D, the artificial noise should be transmitted in the null space of $\mathbf{h}_{RD}$ such that $\mathbf{h}_{RD}^{\dagger}\mathbf{n}_a = 0$. Moreover, instead of transmitting in certain dimension, the power of artificial noise should be spread uniformly in the dimensions of the null space of $\mathbf{h}_{RD}$ [27]. Since the artificial noise does not interfere with D but the eavesdroppers, more power allocated to the artificial noise is more beneficial to increase the secrecy rate. However, allocating all the power to the artificial noise will cause that the transmission rate at D becomes extremely low, which is not desired. To avoid this, the power allocated to information symbol transmission, i.e., $\mathbf{w}^{\dagger}\mathbf{w}$, should guarantee that the transmission rate at D is above a predefined required transmission rate, which is similar to the work in [17]. Denote this predefined rate by $\bar{R}_Q$ and $\bar{R}_D$ should be greater than $\bar{R}_Q$ in order to meet this requirement. Therefore, the cluster allocates the minimum power for the information symbol transmission to achieve $\bar{R}_Q$ so that more power can be left to be utilized to confound the eavesdroppers.

The last phase is the same as that in Section IV-A and the overall transmission rate $\bar{R}_S$ can be expressed as (20), for a given α.

B. Cooperation Parameters Determination

1) Optimal Weight Selection: To achieve the above goal, we first determine the minimum power for $\bar{R}_Q$, which can be obtained by solving the following problem:

$$\begin{aligned}&\min_{\mathbf{w}} \quad \mathbf{w}^{\dagger}\mathbf{w}\\ &s.t. \quad \alpha W\log_2(1+\xi+\frac{\mathbf{w}^{\dagger}\mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}\mathbf{w}}{N_0W}) \ge \bar{R}_Q,\end{aligned} \tag{33}$$

where ξ is the same as in (2). The left hand side of the constraint is the overall transmission rate, which equals to α

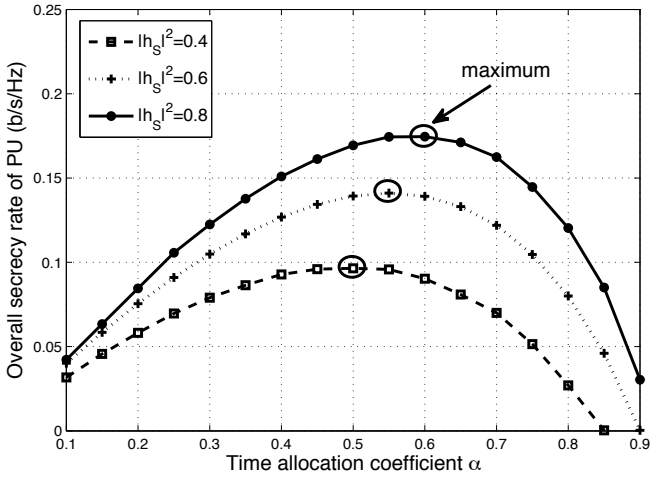


Fig. 3. Overall secrecy rate of PU versus α for R-J scheme for $|h_S^2|$ =0.4, 0.6, 0.8, respectively ($|h_{RD}|^2 = 0.8$, $|h_{RE}|^2 = 0.5$, $|h_{JD}|^2 = 0.4$, $|h_{JE}|^2 = 0.8$, and R_{EX}=0.4 bit/s/Hz).

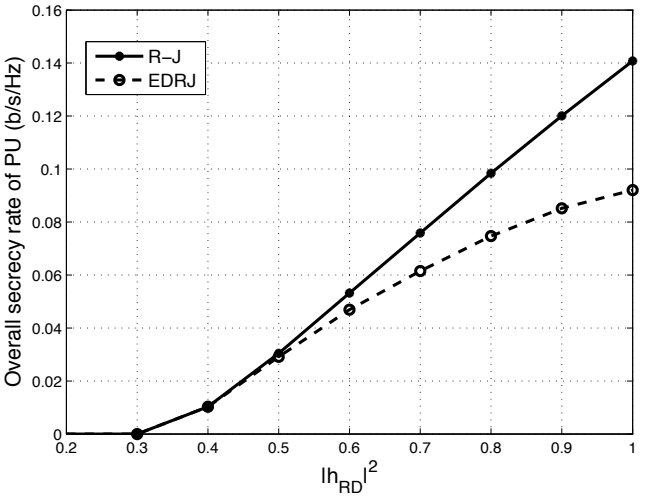


Fig. 4. Comparison between R-J scheme and EDRJ scheme ($|h_{SD}|^2 = 0.3$, $|h_{SE}|^2 = 0.4$, $|h_{SR}|^2 = 0.6$, $|h_{RE}|^2 = 0.3$, $|h_{JD}|^2 = 0.3$, and $|h_{JE}|^2 = 0.5$)

multiplied by R_D in (17). The inequality constraint yields the same result as the equality constraint. Thus, for the low SNR regime, the constraint can be further represented by

$$\mathbf{w}^\dagger \mathbf{h}_{RD} \mathbf{h}_{RD}^\dagger \mathbf{w} = \vartheta, \tag{34}$$

where $\vartheta = N_0 W(\frac{R_Q}{\alpha W} - \xi)$. Defining $\widetilde{\mathbf{H}} = \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger$ and applying the method of Lagrange multipliers, the Lagrange multiplier function is given by

$$L(\mathbf{w}, \lambda) = \mathbf{w}^\dagger \mathbf{w} - \lambda(\mathbf{w}^\dagger \widetilde{\mathbf{H}} \mathbf{w} - \vartheta), \tag{35}$$

where λ is the Lagrange multiplier. Take the derivative of $L(\mathbf{w}, \lambda)$ with respect to $\mathbf{w}^\dagger$, and let it be equal to zero. Then, we have $\widetilde{\mathbf{H}}\mathbf{w} = \frac{\mathbf{w}}{\lambda}$. It can be seen that $1/\lambda$ is the eigenvalue of $\widetilde{\mathbf{H}}$, while $\mathbf{w}$ is the corresponding eigenvector. Multiplying both sides of this equation by $\mathbf{w}^\dagger \lambda$, we can obtain

$$\mathbf{w}^\dagger \mathbf{w} = \lambda \mathbf{w}^\dagger \widetilde{\mathbf{H}} \mathbf{w} = \lambda \vartheta, \tag{36}$$

where the last equality holds due to the constraint in (34). It can be seen that minimizing the transmission power, i.e., $\mathbf{w}^\dagger \mathbf{w}$, is equivalent to minimizing λ or to maximizing $1/\lambda$, since ϑ is a constant. Therefore, the optimal $\mathbf{w}^\star$ should be selected as the eigenvector of $\widetilde{\mathbf{H}}$ corresponding to its largest eigenvalue. In other words, $\mathbf{w}^\star$ can be given by $\mathbf{w} = \varsigma \mathbf{n}$, where $\mathbf{n}$ is the normalized principal eigenvector of $\widetilde{\mathbf{H}}$ and the scalar ς is given by $\varsigma = \sqrt{\frac{\vartheta}{\mathbf{n}^\dagger \widetilde{\mathbf{H}} \mathbf{n}}}$. With $\mathbf{w}^\star$, the cluster spends the minimum power to meet the QoS requirement, and then, more power can be utilized to spread the artificial noise to confound the eavesdroppers.

2) Time Allocation: $\beta^\star$ can be determined by substituting (17) into (12), when the optimal $\mathbf{w}^\star$ is selected. The PU selects α such that the SUs can achieve the expected transmission rate and in return the SUs make their best efforts to help the PU. The overall transmission rate $\bar{R}_S$ at the secondary receiver is given in (20). To achieve $\bar{R}_{EX}$, α can be determined as

$$\alpha = 1 - \frac{\bar{R}_{EX}}{P_{max} \parallel \mathbf{h}_{RS} \parallel^2} \tag{37}$$

VI. Simulation Results

In this section, we present simulation results to provide insight of the proposed cooperation schemes. In the simulation, the bandwidth W and T are set to be one unit, while P_{max} and noise power are set to 2 mw and 1 mw, respectively. For R-J scheme, Fig. 3 shows the trends of the overall secrecy rate $\bar{R}_{SEC}$ of the PU with respect to the time allocation coefficient α, for different channel h_S between the SU and its corresponding receiver. It can be seen that $\bar{R}_{SEC}$ first increases and then decreases with α increasing due to the fact that SUs determine their effort according to the time that the PU grants to them. In addition, the maximum $\bar{R}_{SEC}$ is circled for the three lines and the corresponding optimal $\alpha^\star$ is 0.5, 0.55, and 0.6, respectively. Moreover, both $\bar{R}_{SEC}$ and the optimal $\alpha^\star$ increase when the channel gain $|h_S|$ increases. This is because a better channel condition between the SU and its corresponding receiver results in a better transmission rate, and hence, the PU can allocate a shorter period of time to SUs to achieve the same level of SUs' effort, or the SUs are willing to devote more transmission power for cooperation when given the same rewarding time.

Fig. 4 shows $\bar{R}_{SEC}$ of the PU obtained by using R-J scheme and equal-duration relay jammer (EDRJ) scheme. The only difference between EDRJ scheme and R-J scheme is that the time durations for the first two phases in EDRJ are equal and the secrecy rate is maximized without considering time allocation. It can be seen that R-J scheme outperforms EDRJ because R-J scheme jointly optimizes the time and transmission power to maximize $\bar{R}_{SEC}$. In other words, the scheme without considering time allocation is not optimal, which is consistent to the analysis in Section III-B.

Fig. 5 shows the access time of SUs (i.e., $1 - \alpha^*$) when cooperating with the PU using R-J scheme. It can be seen that the access time decreases when the channel gain of h_{RS} increases. This is because with a better channel, the PU can grant a shorter time to SUs to obtain the same level of efforts from SUs to maximize the PU's secrecy rate. It also shows that

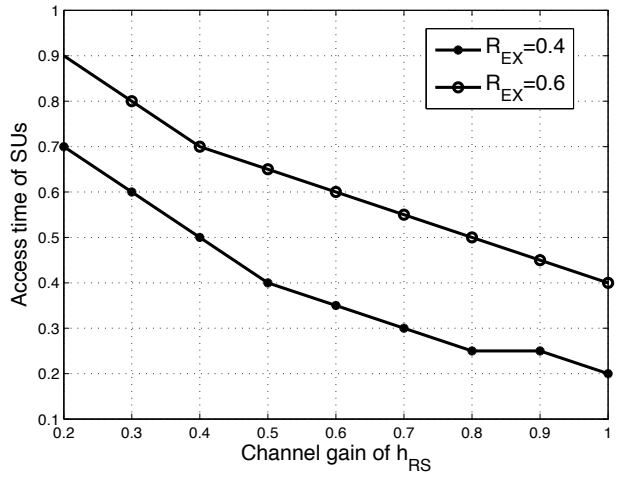


Fig. 5. Access time of SUs versus channel condition h_{RS} for R-J scheme.

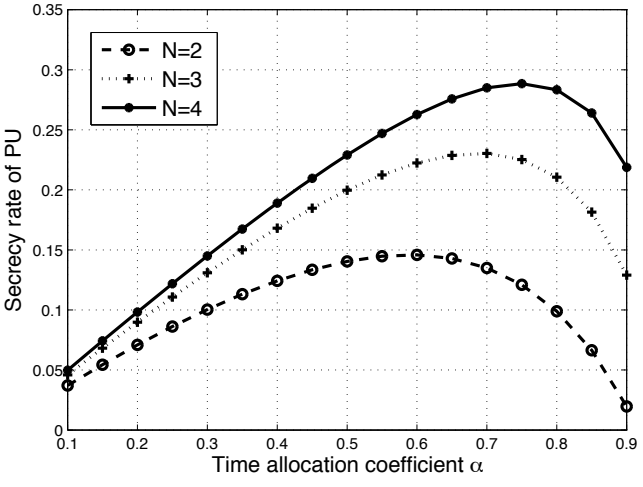


Fig. 6. Overall secrecy rate of the PU versus α for CBSE scheme ($|h_{SD}|^2 = 0.3$, $|h_{SE}|^2 = 0.4$, the worst channel $|h_{SR,i}|^2$ is set to 0.4).

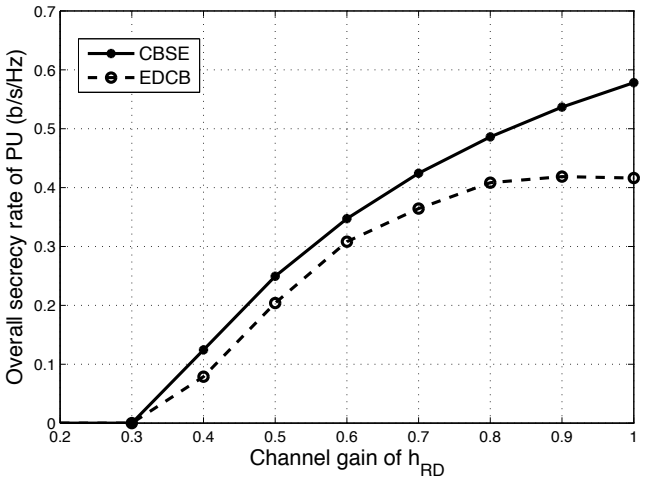


Fig. 7. Comparison between CBSE scheme and EDCB scheme ($|h_{RE}| = 0.3$, $|h_{SD}| = 0.3$, $|h_{SE}| = 0.4$, $N = 3$, and the worst channel $|h_{SR,i}|^2 = 0.4$).

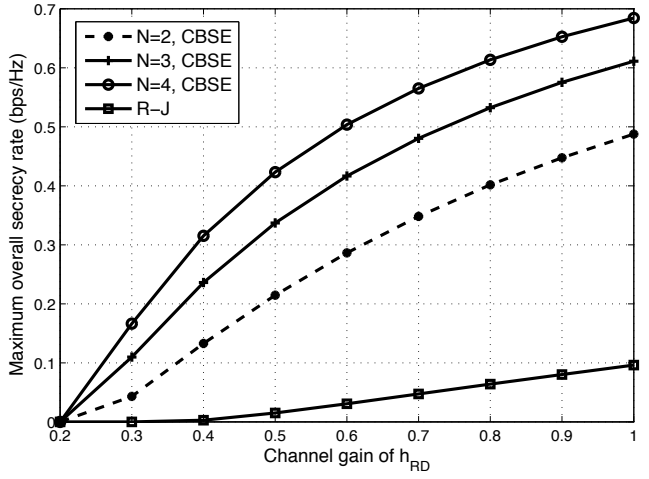


Fig. 8. Comparison between R-J scheme and CBSE scheme.

with a smaller expected transmission rate, the PU can grant a shorter time to SUs to achieve the same level of SUs' effort, or the SUs are willing to devote more transmission power for cooperation when given the same rewarding time.

Fig. 6 shows $\bar{R}_{SEC}$ of the PU when cooperating with a cluster of SUs. For simplicity, the complex channels between all the SUs and D are approximately the same and equal to $e^{j\frac{\pi}{4}}$; similarly the complex channels between SUs and E are set to $0.8e^{j\frac{\pi}{4}}$. It can be seen that there exists an optimal $\alpha^\star$ such that $\bar{R}_{SEC}$ can achieve the maximum value. This is because of the result of the strategy of SUs, which is presented in the system model. Moreover, $\bar{R}_{SEC}$ increases when the total number of SUs (N) in the cluster increases. This is because more SUs can provide larger array gain to increase the secrecy rate.

In the following simulations, the complex channel coefficient h is given by $|h| \cdot e^{j\theta}$, where $|h|$ is the channel gain and θ is uniformly distributed in $[0, 2\pi)$. We obtain the average results using Monte Carlo simulation which consists of 1000 trials. Fig. 7 shows $\bar{R}_{SEC}$ of the PU obtained by using CBSE and equal-duration cluster beamforming scheme (EDCB) in the presence of an eavesdropper. The only difference between EDCB and CBSE is that the time durations for the first two phases are equal in EDCB and the secrecy rate is maximized without considering time allocation. It can be seen that CBSE outperforms EDCB. That is because CBSE jointly optimizes the time and beamforming weights to maximize $\bar{R}_{SEC}$.

Fig. 8 shows $\bar{R}_{SEC}$ of the PU obtained by using CBSE scheme and R-J scheme. When the size of the cluster is equal to 2, which is the same to the number of SUs in R-J scheme, the secrecy rate obtained using CBSE is higher than that of R-J scheme. Moreover, the secrecy rate increases with the number of SUs in the cluster. This is because more SUs can provide larger array gain to increase the secrecy rate.

Fig. 9 shows the access time of SUs using CBSE scheme when cooperating with the PU. It reveals that the access time reduces when the channel gain increases. The reason is that the PU can grant a shorter time to SUs to get the same efforts from SUs. Moreover, a smaller expected rate results in a shorter access time, since SUs needs less time for a smaller

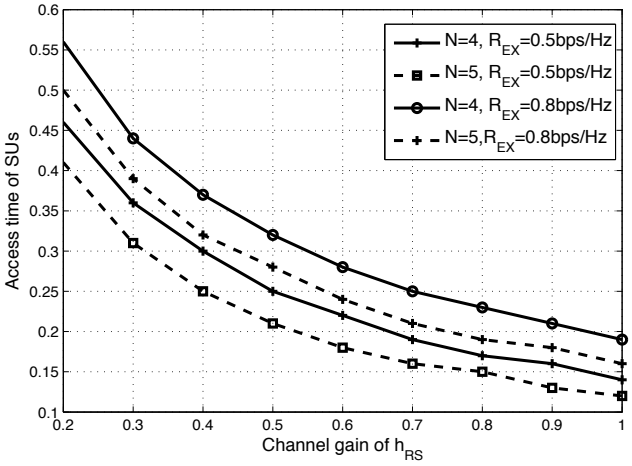


Fig. 9. Access time versus channel condition h_{RS}.

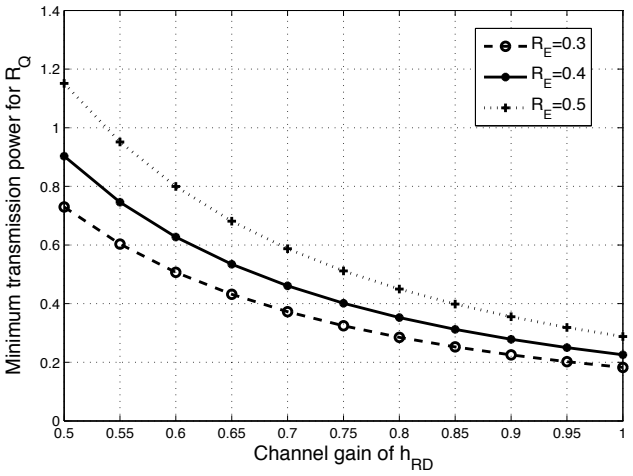


Fig. 11. Minimum transmission power versus $|h_{RD}|$ for CBNE scheme ($|h_{RE}| = 0.4$, $|h_{RD}| = 0.5, 0.1$, $\bar{R}_Q = 0.5$ b/s/Hz and $N = 3$).

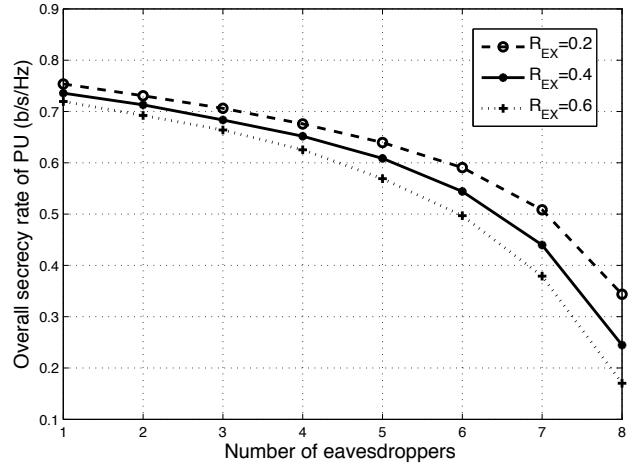


Fig. 10. $\bar{R}_{SEC}$ of PU versus the number of eavesdroppers for CBME scheme ($|h_{RE}| = 0.4$, $|h_{RD}| = 0.5$, $|h_{RS}| = 0.6$, and $N = 10$).

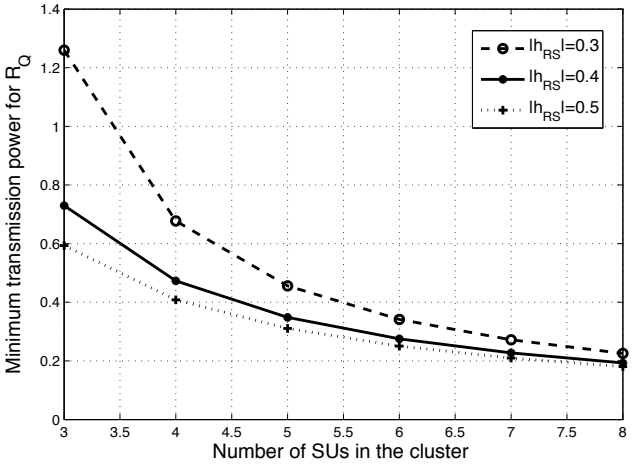


Fig. 12. Minimum transmission power versus the number of SUs for CBNE scheme ($|h_{RD}| = 0.5$, $\bar{R}_{EX} = 0.3$ b/s/Hz).

expected rate. With more SUs in the cluster, the access time will be reduced because more SUs provide larger array gain to increase the transmission rate.

Fig. 10 shows the overall secrecy rate of the PU with respect to the number of eavesdroppers (M) for different expected transmission rate of SUs. It can be seen that $\bar{R}_{SEC}$ drops as M increases. Moreover, it can also be seen that a lower $\bar{R}_{EX}$ results in a larger overall secrecy rate. This is because the SUs can spend less transmission power to achieve a lower $\bar{R}_{EX}$, and hence more power can be used to increase the secrecy rate of the PU.

Fig. 11 shows the minimum transmission power of SUs with respect to $|h_{RD}|$ for different expected transmission rate of SUs. It can be seen that the minimum transmission power drops as $|h_{RD}|$ increases. This is because SUs can spend less transmission power to achieve the same QoS requirement, with a better channel condition. It can also be seen that a smaller $\bar{R}_{EX}$ results in a lower transmission power. The reason is that only a shorter time is needed for SUs to achieve a smaller $\bar{R}_{EX}$, which causes a larger α; and then, the SUs can spend less transmission power to achieve the same $\bar{R}_Q$.

Fig. 12 shows the trends of the minimum transmission power of SUs versus the number of SUs in the cluster. It can be seen that the minimum transmission power drops as the number of SUs increases. Moreover, a smaller $|h_{RS}|$ results in a larger transmission power. This is because a longer duration for rewarding time is needed for SUs to achieve $\bar{R}_{EX}$ when $|h_{RS}|$ is smaller, which causes a smaller α; and hence, the SUs need to spend more transmission power to help the PU to satisfy the QoS requirement.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed two types of cooperative spectrum access to enhance the security of the PU and provide channel access opportunities to SUs. In order to enhance the security, the PU can either cooperate with two individual SUs (R-J scheme) or a cluster of SUs (C-B scheme). For R-J

scheme, the two SUs act as one relay and one friendly jammer to increase the secrecy rate of the PU in the presence of one eavesdropper. For C-B scheme, a cluster of SUs enhance the secrecy of the PU's communication via collaborative beamforming. Especially, for C-B scheme, three cooperation approaches have been proposed for the scenarios with one eavesdropper, with multiple eavesdroppers, and without any information about eavesdroppers. To maximize the secrecy rate, joint time and transmission power allocation is considered in R-J scheme, while time allocation and weight selection are jointly optimized in C-B schemes. We have shown through simulation results that with the proposed schemes, the secrecy of PU's communications can be significantly enhanced and the SUs can acquire certain access time.

In our future work, for R-J scheme, we plan to introduce the degrees of freedom provided by quadrature signaling to share the rewarding time among relay and jammer SUs, similar to the work in [9] [32]. Moreover, the partner selection will also be considered. For C-B scheme, the cooperation for a more general case where SUs have individual power constraints will be studied. In addition, we will also consider how to cooperate in the presence of imperfect CSI.

APPENDIX

When $\alpha(1-\beta)R_R \geq \alpha\beta R_D$, we have $\beta \leq \frac{R_R}{R_R+R_D}$. Then, the secrecy rate in (6) can be given by $[\alpha\beta R_D - \alpha\beta R_E]^+ = \alpha\beta[(R_D - R_E)]^+$, which is a monotonically increasing function with respect to β. To maximize the secrecy rate, β should take the maximum value $\frac{R_R}{R_R+R_D}$. Substituting $\beta = \frac{R_R}{R_R+R_D}$ into (6), the secrecy rate can be rewritten as follows: $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+$. When $\alpha(1-\beta)R_R \leq \alpha\beta R_D$, we have $\beta \geq \frac{R_R}{R_R+R_D}$. Then, the secrecy rate in (6) can be given by $[\alpha(1-\beta)R_R - \alpha\beta R_E]^+$. which is a monotonically decreasing function of β. To maximize the secrecy rate, β should take the minimum value $\frac{R_R}{R_R+R_D}$. Substituting $\beta = \frac{R_R}{R_R+R_D}$ into (6), the secrecy rate can be rewritten as follows: $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+$. As shown above, for the two cases, to maximize the $\bar{R}_{SEC}$, β always equals to $\frac{R_R}{R_R+R_D}$. Moreover, when β takes the optimal value, it holds that $\alpha(1-\beta)R_R = \alpha\beta R_D$. Thus, $\bar{R}_{SEC} = \alpha[\frac{R_R(R_D-R_E)}{R_R+R_D}]^+ = \alpha[R_R - \frac{R_R(R_R+R_E}{R_R+R_D})]^+$.

REFERENCES

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[2] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[3] Y. Liu, L. Cai, and X. Shen, "Spectrum-aware opportunistic routing in multi-hop cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1958–1968, 2012.

[4] H. Cheng and W. Zhuang, "Simple channel sensing order in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 676–688, 2011.

[5] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 203–213, 2008.

[6] J. Zhang and Q. Zhang, "Stackelberg game for utility-based cooperative cognitiveradio networks," in *Proc. ACM MobiHoc'09*, 2009.

[7] Y. Han, A. Pandharipande, and S. Ting, "Cooperative decode-and-forward relaying for secondary spectrum access," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 4945–4950, 2009.

[8] A. Alshamrani, X. Shen, and L. Xie, "Qos provisioning for heterogeneous services in cooperative cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 819–830, 2011.

[9] B. Cao, L. Cai, H. Liang, J. Mark, Q. Zhang, H. Poor, and W. Zhuang, "Cooperative cognitive radio networking using quadrature signaling," in *Proc. IEEE INFOCOM'12*, 2012.

[10] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "Grs: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, pp. 28–35, 2011.

[11] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 2, pp. 40–47, 2012.

[12] N. Anand, S. Lee, and E. Knightly, "Strobe: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE INFOCOM'12*, 2012.

[13] L. Ozarow and A. Wyner, "Wire-tap channel ii," in *Advances in Cryptology*. Springer, pp. 33–50, 1985.

[14] J. Huang and A. Swindlehurst, "Robust secure transmission in miso channels based on worst-case optimization," *IEEE Trans. Signal Proces.*, vol. 60, no. 4, pp. 1696–1707, 2012.

[15] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, 2011.

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

[17] H. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Proces.*, vol. 60, pp. 3532–3545, 2012.

[18] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[19] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Proces.*, vol. 59, no. 3, pp. 1317–1322, 2011.

[20] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Proces.*, no. 99, pp. 1–1, 2011.

[21] K. Lee, O. Simeone, C. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. IEEE ICC'11*, 2011.

[22] Z. Gao, Y. Yang, and K. Liu, "Anti-eavesdropping space-time network coding for cooperative communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898–3908, 2011.

[23] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in *Annual Allerton Conference on Communication, Control, and Computing*, 2008.

[24] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative networking towards secure communications for crns," in *Proc. IEEE WCNC'13*, 2013.

[25] N. Zhang, N. Lu, R. Lu, J. W. Mark *et al.*, "Energy-efficient and trust-aware cooperation in cognitive radio networks," in *Proc. IEEE ICC'12*, 2012.

[26] H. Ochiai, P. Mitran, H. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4110–4124, 2005.

[27] L. Tang, X. Gong, J. Wu, and J. Zhang, "Secure wireless communications via cooperative relaying and jamming," in *Proc. IEEE GLOBECOM'11*, 2011.

[28] M. Gursoy, "Secure communication in the low-snr regime: A characterization of the energy-secrecy tradeoff," in *Proc. IEEE ISIT'09*, 2009.

[29] G. Kim, *Scheduling in wireless ad hoc networks: algorithms with performance guarantees*. ProQuest, 2008.

[30] A. Wiesel, Y. C. Eldar, and S. Shamai, "Zero-forcing precoding and generalized inverses," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4409–4418, 2008.

[31] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[32] V. Mahinthan, J. W. Mark, and X. Shen, "A cooperative diversity scheme based on quadrature signaling," *IEEE Trans. Wireless Commun.*, vol. 6, no. 1, pp. 41–45, 2007.

Ning Zhang (S'12) received the B.Sc. degree from Beijing Jiaotong University and the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2010, respectively. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His current research interests include cooperative networking, cognitive radio networks, physical layer security, and vehicular networks.

Ning Lu (S'12) received the B.Sc. and M.Sc. degrees from Tongji University, Shanghai, China, in 2007 and 2010, respectively. He is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His current research interests include capacity and delay analysis, media access control, and routing protocol design for vehicular networks. Mr. Lu served as a Technical Program Committee Member for IEEE 2012 International Symposium on Personal, Indoor, and Mobile Radio Communications.

Nan Cheng (S'13) is currently a Ph.D. candidate in the department of Electrical and Computer Engineering, the University of Waterloo, Waterloo, ON, Canada. He received his B.S. degree and M.S. degree from Tongji University, China, in 2009 and 2012, respectively. Since 2012, he has been a research assistant in the Broadband Communication Research group in ECE Department, the University of Waterloo. His research interests include vehicular communication networks, cognitive radio networks, and resource allocation in smart grid.

Jon W. Mark (M'62-SM'80-F'88-LF'03) received the Ph.D. degree in electrical engineering from McMaster University in 1970. In September 1970 he joined the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, where he is currently a Distinguished Professor Emeritus. He served as the Department Chairman during the period July 1984-June 1990. In 1996 he established the Center for Wireless Communications (CWC) at the University of Waterloo and is currently serving as its founding Director. Dr. Mark had been on sabbatical leave at the following places: IBM Thomas J. Watson Research Center, Yorktown Heights, NY, as a Visiting Research Scientist (1976-77); AT&T Bell Laboratories, Murray Hill, NJ, as a Resident Consultant (1982-83): Laboratoire MASI, UniversitPierre et Marie Curie, Paris France, as an Invited Professor (1990-91); and Department of Electrical Engineering, National University of Singapore, as a Visiting Professor (1994-95). He has previously worked in the areas of adaptive equalization, image and video coding, spread spectrum communications, computer communication networks, ATM switch design and traffic management. His current research interests are in broadband wireless communications, resource and mobility management, and cross domain interworking.

Dr. Mark is a Life Fellow of IEEE and a Fellow of the Canadian Academy of Engineering. He is the recipient of the 2000 Canadian Award for Telecommunications Research and the 2000 Award of Merit of the Education Foundation of the Federation of Chinese Canadian Professionals. He was an editor of IEEE TRANSACTIONS ON COMMUNICATIONS (1983-1990), a member of the Inter-Society Steering Committee of the IEEE/ACMTRANSACTIONS ON NETWORKING (1992-2003), a member of the IEEE Communications Society Awards Committee (1995-1998), an editor of Wireless Networks (1993-2004), and an associate editor of Telecommunication Systems (1994-2004).

Xuemin (Sherman) Shen (IEEE M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering.

He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published many papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair for IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications.

Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, a Fellow of the Canadian Academy of Engineering, a Fellow of Engineering Institute of Canada, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.