Lu et al. EURASIP Journal on Wireless Communications and Networking
(2017) 2017:193
DOI 10.1186/s13638-017-0981-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Joint resource optimization for secure transmission in cooperative CR networks

Weidang Lu[1*], Kecai Gu[1], Min Jia[2], Zhanghui Lu[3] and Hong Peng[1]

Abstract

In this paper, we investigate the joint resource allocation to provide secure information transmission in a five-node cooperative cognitive radio network, which contains a primary transmitter (PT), a primary receiver (PR), a secondary transmitter (ST), a secondary receiver (SR), and an eavesdropper (E). To ensure the information is securely transmitted, PT and PR use a part of the power to transmit artificial noise (i.e., jamming signal) to confuse the eavesdropper. Specifically, in the first phase, PT transmits its signal, which contains secrecy information and artificial noise, by using all of its power and bandwidth. In the second phase, ST accesses to the PT's licensed bandwidth as a trusted relay by allocating a fraction of the bandwidth and power to forward PT's information with decode-and-forward (DF) relaying protocol. As a reward, ST can utilize the remaining bandwidth and power to transmit its own information simultaneously. We study the joint optimization of the time, bandwidth, and power allocation to maximize ST's transmission rate while satisfying PT's secrecy transmission rate requirements. Numerical results demonstrate that our strategy can achieve a win-win result.

Keywords: Cooperative cognitive radio, Physical layer security, Artificial noise, Secrecy rate

1 Introduction

Communication security is always a critical issue due to the openness and broadcast nature of the wireless transmission. Physical layer security (PHY) has received significant attention due to its potential to improve the security of information transmission in wireless communication [1–3]. Wyner [2] firstly introduces the concept of wiretap channel in his early pioneering works, and it was expanded to broadcast channels by Csiszar and Korner [3] who prove no information leakage to eavesdropper by channel coding technology later. Secrecy rate, which is defined as the difference between the achievable rate of primary channel and wiretap channel, is usually taken to evaluate the effectiveness of the secrecy system model. In the traditional wireless networks, a positive secrecy rate can be obtained if the primary channel is more "advantageous" than the wiretap channel. In other words, communication security can be achieved by encoding and decoding technology. However, the phenomenon that wiretap channel is better than primary channel is very common in wireless environment due to the non-controllability of channel.

In such a situation, the problem can be solved reasonably with the help of cooperative nodes. In the sight of information-theoretic, the essence of PHY security is to extend the superiority of the primary channel to wiretap channel. Cooperative relaying and cooperative jamming [4–8] have been deeply and widely studied. In a cooperative relaying system, cooperative nodes act as relays and help forward the source node information to the destination node by using decode-and-forward (DF) or amplify-and-forward (AF) relaying protocol to gain channel diversity gain and greatly improve the primary system's performance. Different with the cooperative relaying system, in cooperative jamming system, cooperative nodes act as jammers aiming to interfere eavesdroppers around by sending jamming signals to decrease the wiretap link's performance while impairing the primary link performance. Deng et al. [4] and Deng et al. [5] investigate that whether the cooperative nodes should operate as relay or jammer in two proposed schemes, namely, direct transmission scheme (DTS) and relay transmission, respectively (RTS). A relative, detailed, and thorough of cooperation technology in PHY security are presented in [6].

* Correspondence: luweid@zjut.edu.cn
[1]College of Information Engineering, Zhejiang University of Technology, Zhejiang, Hangzhou 310014, China
Full list of author information is available at the end of the article

Another issue is the poor bandwidth utilization due to the rarity of available bandwidth resources and the fixed bandwidth assignment stratagem in the conventional wireless networks. Once the bandwidth resources are assigned to the specific users, the others will not be allowed to access, even if it is not used by the authorized users. To improve the bandwidth utilization, various different dynamic bandwidth access and sharing technologies [9–11] have been proposed and attract considerable attention. An anti-interference cooperative bandwidth sharing strategy in [9] is proposed to maximize the secondary user's rate while guaranteeing primary user's service with joint optimization of time and bandwidth. There are mainly two typical bandwidth access strategies. (1) Underlay: cognitive user access to the licensed bandwidth, coexistent and shared bandwidth that is authorized as long as the designed threshold is satisfied. (2) Overlay: secondary users keep sensing bandwidth and utilize the unused licensed bandwidth, which requires the secondary user to empty out the bandwidth immediately once the authorized user needs to use the bandwidth, thus designing an effective bandwidth sensing algorithm is very important.

In this paper, we take the achievable secrecy rate as the primary system performance metric. In order to ensure the primary information is securely transmitted, we introduce artificial noise [12–16] and redesign the secrecy information transmission. Furthermore, an anti-interference spectrum sharing strategy is proposed to improve the bandwidth utilization, in which the secondary user serves as a trusted relay for the PU in DF relaying protocol to improve the performance of the primary link. As a reward, the secondary user can obtain opportunity to access the primary bandwidth and then transmit its own information at the same time.

The main contributions of this paper are as follows: Firstly, we propose an anti-interference spectrum sharing strategy based on trusted relay for secure transmission in cooperative CR networks. Secondly, the joint optimization of time, bandwidth, and power is obtained to maximize secondary transmission rate while guaranteeing the primary secrecy performance. Finally, simulation results demonstrate that our proposed scheme can benefit for both primary and secondary systems.

The rest of this paper is organized as follows. Section 2 presents the system model, and Section 3 formulates the optimization problem. The joint optimization of time, bandwidth, and power is derived in Section 4. In Section 5, simulation results are presented to evaluate our proposed scheme. Finally, Section 6 concludes the paper.

2 System model

As shown in Fig. 1, the system consists of five nodes including a primary transmitter (PT), a primary receiver (PR), a secondary transmitter (ST), a secondary receiver (SR), and a passive eavesdropper (E) which is only interested in PT's information. We assume ST is trusted and adopting DF relaying protocol to forward PT's information. PR works in a full-duplex mode. The channel is considered to be a quasi-static Rayleigh channel and keeps static in several time slots. For simplicity, the noise at all nodes are assumed to be complex additive white Gaussian (AWGN) with zero mean and unit variance σ_n^2. h_i denotes the channel coefficient. The power of PT and ST are constrained to P and P_s, respectively.

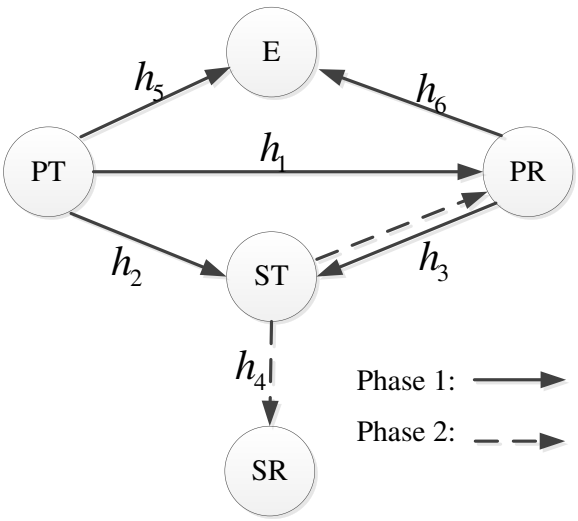

Fig. 1 System model

In order to keep PT's information transmission security, the transmission process is divided into two phases. In the first phase, PT broadcasts the designed signal, which contains the secrecy information and artificial noise, to PR and ST with all the licensed bandwidth. Meanwhile, PR utilizes this period to transmit the corresponding designed artificial noise. In the second phase, PT stops transmitting signal and authorizes the bandwidth resource to ST. As soon as ST accesses to the PT's licensed bandwidth, it allocates a part of the power and bandwidth to relay PT's signal with DF relaying protocol. As ST helps the primary system achieve the target secrecy rate, as a reward, the left bandwidth will be granted to ST to transmit ST's signal to SR at the same time. Our target is to maximize the secondary system rate while keeping primary system achieves the target secrecy rate.

3 Problem formulation

PT tries to seek help from the neighboring nodes as it is not safe to directly transmit its information to PR. ST can obtain the cooperation opportunity and access to the licensed bandwidth if and only if it can help PT achieve the target secrecy rate through the following two phases.

In phase 1: This phase occupies a fraction of t during one time slot. To keep information safe, the source transmits a designed signal $x_{\mathrm{PT}} = \sqrt{P\alpha}s + \sqrt{P(1-\alpha)}u_1 z$ by using all the bandwidth w while PR transmits the artificial noise $x_{\mathrm{PR}} = \sqrt{P(1-\alpha)}u_2 z$ simultaneously, where s and z denotes the secrecy information and artificial noise, respectively, P denotes PT's total power, and α denotes the allocation factor between the secrecy information and artificial noise.

The received information at ST and E can be expressed respectively as

$$r_{\mathrm{ST}} = \sqrt{P\alpha}h_2 s + \sqrt{P(1-\alpha)}z(u_1 h_2 + u_2 h_3) + n_{\mathrm{ST}} \quad (1)$$

$$r_{\mathrm{E}} = \sqrt{P\alpha}h_5 s + \sqrt{P(1-\alpha)}z(u_1 h_5 + u_2 h_6) + n_{\mathrm{E}} \quad (2)$$

where $n_{\mathrm{ST}} \sim CN(0, \sigma^2)$ and $n_{\mathrm{E}} \sim CN((0, \sigma^2)$ is the noise at ST and E, respectively, and u_1 and u_2 are the complex weight coefficients, selected from null space. To avoid the interference to the secondary user, the artificial noise is designed to be canceled at ST. Then

$$\begin{cases} u_1 h_2 + u_2 h_3 = 0 \\ u_1^2 + u_2^2 = 1 \end{cases} \quad (3)$$

Thus, (1) can be rewritten as

$$r_{\mathrm{ST}} = \sqrt{P\alpha}h_2 s + n_{ST} \quad (4)$$

For notational convenience, we define

$$\begin{cases} \rho_1 = P|h_1|^2/\sigma^2 \\ \rho_2 = P|h_2|^2/\sigma^2 \\ \rho_3 = P_s|h_3|^2/2\sigma^2 \\ \rho_4 = P_s|h_4|^2/2\sigma^2 \\ \rho_5 = P|h_5|^2/\sigma^2 \\ \rho_E = P|u_1 h_5 + u_2 h_6|^2/\sigma^2 \end{cases}$$

Then, the transmission information rate at ST can be calculated as

$$R_p^1 = tw\log_2(1 + \alpha\rho_2) \quad (5)$$

Similarly, the information rate that eavesdropper wiretap from PT can be calculated as

$$R_E^1 = tw\log_2\left(1 + \frac{\alpha\rho_5}{1 + (1-\alpha)\rho_E}\right) \quad (6)$$

As PR has a priori knowledge of artificial noise, it can remove the jamming signal directly. The received signal at PR can be expressed as

$$r_{\mathrm{PR}} = \sqrt{P\alpha}s + n_{\mathrm{PR}} \quad (7)$$

where $n_{\mathrm{PR}} \sim CN(0, \sigma^2)$ is the noise at PR. We can obtain the information rate at PRas

$$R_d^1 = tw\log_2(1 + \alpha\rho_1) \quad (8)$$

In phase 2, this phase occupies a fraction of $1 - t$ during one time slot. PT authorizes ST to access to the licensed bandwidth. ST utilizes DF, relaying protocol to forward the received signal by using its half power and bw bandwidth. Meanwhile, it uses the rest bandwidth and power to transmit its own information to SR. Then, the information rate at PR and SR can be calculated respectively as

$$R_d^2 = (1-t)bw\log_2(1 + \rho_3) \quad (9)$$

$$R_S = (1-t)(1-b)w\log_2(1 + \rho_4) \quad (10)$$

Using maximum ratio combination (MRC), the information rate at PR can be given as

$$R_p^2 = \begin{cases} tw\log_2(1 + \alpha\rho_1 + \rho_3) + [b(1-t)-t]w\log_2(1 + \rho_3) & b(1-t) \geq t \\ (1-t)bw\log_2(1 + \alpha\rho_1 + \rho_3) + [t-b(1-t)]w\log_2(1 + \alpha\rho_1) & b(1-t) < t \end{cases} \quad (11)$$

After two phases of transmission, the information rate between $PT \rightarrow PR$ links can be represented as

$$R_p = \min\left\{R_p^1, R_p^2\right\} \quad (12)$$

The achievable secrecy rate is defined as the difference between the achievable rate of main channel and the achievable rate of eavesdropper channel. Obviously, the achievable secrecy rate is the lower bound of the secrecy capacity.

$$R_{\mathrm{SEC}} = (R_{\mathrm{PR}} - R_{\mathrm{ERV}})^+ \quad (13)$$

where R_{PR} and R_{ERV} denotes the instance achievable secrecy rate of primary receiver and eavesdropper, respectively.

With this definition, the instance secrecy rate of primary system can be expressed as

$$R_{\mathrm{Q}} = (R_{\mathrm{P}} - R_{\mathrm{E}})^+ \quad (14)$$

Note that the eavesdropper is only interesting in wiretapping the primary information, and it has no knowledge that the primary information is forwarded by ST. Thus, it keeps silence in the second phase. Then, we have $R_{\mathrm{E}} = R_{\mathrm{E}}^1$.

With the objective of maximizing secondary system rate by joint time, power, and bandwidth allocation with the primary secrecy rate constraint, the following joint optimization problem is formulated.

$$\max_{a,t,b} R_S \quad (15)$$

subject to

$$\begin{cases} 0\le\alpha\le 1 \\ 0\le b\le 1 \\ 0\le t\le 1 \\ R_{\mathrm{Q}}\le R_{\mathrm{T}} \end{cases} \tag{16}$$

where R_{T} is the target secrecy rate of primary system.

4 Optimal solutions

In this section, we study the joint optimization of time, power, and bandwidth with the primary system target secrecy rate constraint.

Obviously, the last condition of (16) can be equivalent to the following two conditions

$$R_p^1 - R_{\mathrm{E}}^1 \ge R_{\mathrm{T}} \tag{17}$$

$$R_p^2 - R_{\mathrm{E}}^1 \ge R_{\mathrm{T}} \tag{18}$$

Problem (15) is difficult to solve directly, mainly due to the non-convex constraints of (17) and (18). The above problem can be solved with the following three steps: (I) find the optimal bandwidth allocation b^* with fixed time and power allocation, (II) find the optimal time allocation t^* with fixed power allocation, and (III) find the optimal power allocation α^*. We will show in the numerical results that there is no performance gap between the above solutions with the exhaustive search method.

For simplicity, we define

$$\begin{cases} R_2 = w\log_2(1+\alpha\rho_2) \\ R_3 = w\log_2(1+\rho_3) \\ R_4 = w\log_2(1+\rho_4) \\ R_5 = w\log_2(1+\rho_3+\alpha\rho_1) \\ R_d = w\log_2(1+\alpha\rho_1) \\ R_E = w\log_2\left(1+\dfrac{\alpha\rho_5}{1+(1-\alpha)\rho_E}\right) \end{cases}$$

With the above definitions, R_p^1, R_p^2 and R_S in (5), (11) and (10) can be rewritten as follows

$$R_p^1 = tR_2 \tag{19}$$

$$R_p^2 = \begin{cases} tR_5 + [b(1-t)-t]R_3 & b(1-t)\ge t \\ b(1-t)R_5 + [t-b(1-t)]R_d & b(1-t) < t \end{cases} \tag{20}$$

$$R_S = (1-t)(1-b)R_4 \tag{21}$$

In (20), we can find that R_p^2 has two different values. Then, the optimal time, power, and bandwidth is obtained by analyzing the different value of R_p^2.

Condition 1: when $b(1-t)\ge t$, then $R_p^2 = tR_5 + [b(1-t)-t]R_3$. We can obtain $b\ge\frac{t}{1-t}$.

(I) To satisfy the condition (18), we can obtain

$$b\ge b_1 = \frac{R_{\mathrm{T}} - t(R_5 - R_3 - R_{\mathrm{E}})}{R_3(1-t)} \tag{22}$$

Thus, we can obtain

$$\max\left\{\frac{t}{1-t}, b_1\right\}\le b\le 1 \tag{23}$$

From (21), it is easy to find that R_S monotonically decreases with b. Thus, the optimal bandwidth allocation can be given as

$$b^* = \max\left(\frac{t}{1-t}, b_1\right) \tag{24}$$

(II) To satisfy the condition $0 \le b^* \le 1$, we can obtain

$$t\le \min\left\{\frac{1}{2}, \frac{R_3 - R_{\mathrm{T}}}{2R_3 + R_{\mathrm{E}} - R_5}, \frac{R_{\mathrm{T}}}{R_5 - R_3 - R_{\mathrm{E}}}\right\} \tag{25}$$

In (24), we can find that b^* may have two different values. Thus, the optimal time allocation is based on the different values of b^*.

Case 1: when $b^* = \frac{t}{1-t}$, which means $\frac{t}{1-t}\ge b_1$. We can obtain

$$t\ge \frac{R_{\mathrm{T}}}{R_5 - R_{\mathrm{E}}} \tag{26}$$

To satisfy the condition (17), we can obtain

$$t\ge \frac{R_{\mathrm{T}}}{R_2 - R_{\mathrm{E}}} \tag{27}$$

Thus, we can obtain

$$\max\left\{\frac{R_{\mathrm{T}}}{R_2 - R_{\mathrm{E}}}, \frac{R_{\mathrm{T}}}{R_5 - R_{\mathrm{E}}}\right\}\le t\le \min \left\{\frac{1}{2}, \frac{R_3 - R_{\mathrm{T}}}{2R_3 + R_{\mathrm{E}} - R_5}, \frac{R_{\mathrm{T}}}{R_5 - R_3 - R_{\mathrm{E}}}\right\} \tag{28}$$

From (21), it is easy to find that R_S monotonically decreases with t. Thus, the optimal time allocation can be given as

$$t^* = \max\left(\frac{R_{\mathrm{T}}}{R_2 - R_{\mathrm{E}}}, \frac{R_{\mathrm{T}}}{R_5 - R_{\mathrm{E}}}\right) \tag{29}$$

Case 2: when $b^* = b_1$, which means $\frac{t}{1-t}\le b_1$. We can obtain

$$t\le \frac{R_{\mathrm{T}}}{R_5 - R_{\mathrm{E}}} \tag{30}$$

Thus, we can obtain

$$\frac{R_T}{R_2-R_E} \le t \le \min\left\{\frac{1}{2}, \frac{R_3-R_T}{2R_3+R_E-R_5}, \frac{R_T}{R_5-R_3-R_E}, \frac{R_T}{R_5-R_E}\right\} \tag{31}$$

Substituting $b^* = b_1$ into (21), R_s can be rewritten as

$$R_S = \frac{R_4(R_3-R_T-t(2R_3+R_E-R_5))}{R_3} \tag{32}$$

From (32), we can find that when $2R_3 + R_E - R_5 \ge 0$, R_S monotonically decreases with t. Thus, the optimal time allocation can be given as

$$t^* = \frac{R_T}{R_2-R_E} \tag{33}$$

When $2R_3 + R_E - R_5 < 0$, R_S monotonically increases with t. Thus, the optimal time allocation can be given as

$$t^* = \min\left\{\frac{1}{2}, \frac{R_3-R_T}{2R_3+R_E-R_5}, \frac{R_T}{R_5-R_3-R_E}, \frac{R_T}{R_5-R_E}\right\} \tag{34}$$

(III) With the optimal bandwidth and time allocation, the optimal power allocation can be obtained by equivalently solving the following problem

$$\alpha^* = \arg\max_{0\le\alpha\le1} R_S(\alpha, b^*(\alpha), t^*(\alpha)) \tag{35}$$

Remarkably, problem (35) is still difficult to solve directly due to the non-convex property of the target function. We apply one-dimensional search to obtain the optimal power allocation.

Condition 2: when $b(1-t) < t$, then $R_p^2 = b(1-t)R_5 + [t-b(1-t)]R_d$. We can obtain $b < \frac{t}{1-t}$.

(I) To satisfy the condition (18), we can obtain

$$b \ge b_2 = \frac{R_T - t(R_d-R_E)}{(1-t)(R_5-R_d)} \tag{36}$$

Thus, we can obtain

$$b_2 \le b < \frac{t}{1-t} \tag{37}$$

From (21), it is easy to find that R_S monotonically decreases with t. Thus, the optimal time allocation can be given as

$$b^* = b_2 \tag{38}$$

(II) Substituting $b^* = b_2$ into (21), R_s can be rewritten as

$$R_S = \frac{R_4}{R_5-R_d}[R_5-R_d-R_T-t(R_5+R_E-2R_d)] \tag{39}$$

From (39), we can find that when $R_5 + R_E - 2R_d \ge 0$, R_S monotonically decreases with t.

To satisfy the condition $0 \le b^* \le 1$, we can obtain

$$\frac{R_T-R_5+R_d}{2R_d-R_E-R_5} \le t \le \frac{R_T}{R_d-R_E} \tag{40}$$

Thus, we can obtain

$$\max\left(\frac{R_T}{R_2-R_E}, \frac{R_T-R_5+R_d}{2R_d-R_E-R_5}\right) \le t \le \frac{R_T}{R_d-R_E} \tag{41}$$

And the optimal time allocation can be given as

$$t^* = \max\left(\frac{R_T}{R_2-R_E}, \frac{R_T-R_5+R_d}{2R_d-R_E-R_5}\right) \tag{42}$$

When $R_5 + R_E - 2R_d < 0$, R_S monotonically increases with t. To satisfy the condition $0 \le b^* \le 1$, we can obtain

$$t \le \min\left(\frac{R_T-R_5+R_d}{2R_d-R_E-R_5}, \frac{R_T}{R_d-R_E}\right) \tag{43}$$

Thus, we can obtain

$$\frac{R_T}{R_2-R_E} \le t \le \min\left(\frac{R_T-R_5+R_d}{2R_d-R_E-R_5}, \frac{R_T}{R_d-R_E}\right) \tag{44}$$

And the optimal time allocation can be given as

$$t^* = \min\left(\frac{R_T-R_5+R_d}{2R_d-R_E-R_5}, \frac{R_T}{R_d-R_E}\right) \tag{45}$$

(III) With the similar method used in condition 1, the optimal power allocation can be given as

$$\alpha^* = \arg\max_{0\le\alpha\le1} R_S(\alpha, b^*(\alpha), t^*(\alpha)) \tag{46}$$

5 Simulation results

The performance of our proposed strategy for a five-node model is investigated with MATLAB in this section. We assume the five nodes are located in a two-dimensional X-Y plane. PT, PR are fixed at points (0, 0) and (1, 0), respectively. Let ST move from PT to PR on the positive X-axis. The distance between ST and SR is set to be half of the distance between ST and PR. Thus, $d_1 = 1$, $d_2 = 1 - d_3$, $d_4 = d_3/2$. The eavesdropper is fixed at the point where $d_5 = 0.3$, $d_6 = 1$. The path loss exponent is set to be 3. The power of PT and PR are both 10 dB. Unless otherwise stated, other parameters such as bandwidth and noise are set to 1 in our simulation.

Figure 2 describes the secondary system transmission rate versus the location of ST under different target secrecy rate. It can be observed from Fig. 2 that there is no performance gap between our proposed algorithm and exhaustive search method. In Fig. 2, we can find that when $R_T = 2$ bps/Hz, at the very start, $0 \le d_2 \le 0.062$, ST is close to PT, which means the PT → ST link is good; with the help of ST, PT can achieve the target secrecy

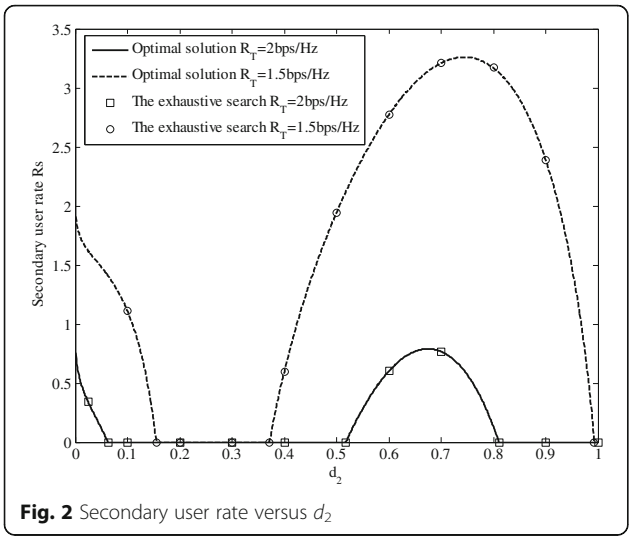

Fig. 2 Secondary user rate versus d_2

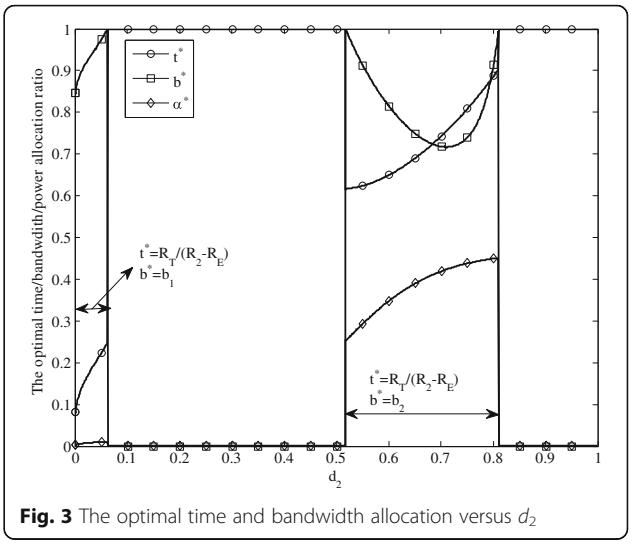

Fig. 3 The optimal time and bandwidth allocation versus d_2

rate and ST can access to the licensed spectrum. As ST moves to PR, $0.062 \le d_2 \le 0.52$, the PT → ST link is getting worse; meanwhile, wiretap channel is becoming better and the eavesdropper wiretap more information. The target secrecy rate cannot be satisfied; R_s returns to zero and ST cannot access to the licensed spectrum. With ST moving further to PR, when $0.52 \le d_2 \le 0.81$, the wiretap channel is not very good and the ST → PR link is good enough for ST to help primary system achieve its target secrecy rate. Therefore, ST can access to the licensed bandwidth and the secondary user rate is positive. When $d_2 > 0.81$, ST is far away from PT and the PT → ST link becomes terrible; ST cannot access to the licensed bandwidth and R_s return to zero. We can also observe from Fig. 2 that the secondary user can obtain larger access range when the target secrecy rate becomes smaller.

Figure 3 shows the optimal time, power, and bandwidth allocation ratio versus the different location of ST when $R_T = 2$ bps/Hz. When $0 \le d_2 \le 0.062$, PT is very close to ST and the PT → ST link is very good; PT only needs to allocate a small amount of time to achieve secrecy rate. Only a small part of the power is allocated for PT's information transmission, and the left power is used to transmit the artificial noise for secure transmission. With ST moves far away from PT, PT needs to allocate more time and bandwidth resources to achieve the target secrecy rate. When $0.062 \le d_2 \le 0.52$, ST cannot help PT achieve the target secrecy rate and ST cannot access to the licensed bandwidth. Thus, $t^* = 1, b^* = 0$. As ST moves further away from PT, when $0.52 \le d_2 \le 0.81$, the PT → ST link is becoming worse and PT needs to allocate more time and power to guarantee the primary system achieve the target secrecy rate in phase 1. When $d_2 \ge 0.81$, the PT → ST link is becoming terrible and ST cannot access to the licensed spectrum and $t^* = 1, b^* = 0$.

Figure 4 shows the optimal time, power, and bandwidth allocation ratio versus the different location of ST when $R_T = 1.5$ bps/Hz. In Fig. 4, we can find that the secondary user can obtain larger access range with smaller target secrecy rate. We can also observe from Fig. 4 that with the same location of ST, more time, power, and bandwidth will be left for the secondary user transmission when the target secrecy rate becomes smaller, which will lead larger secondary user rate, which can be also illustrated in Fig. 2.

Figure 5 shows the secondary user rate comparison between our proposed scheme and the scheme proposed in [16], in which ST forwards the primary signal and transmits its own signal simultaneously by using the same bandwidth in the second phase. Thus, the primary and secondary system will interfere with each other, which will affect the performance of both primary and secondary systems. In Fig. 5, we can observe that the

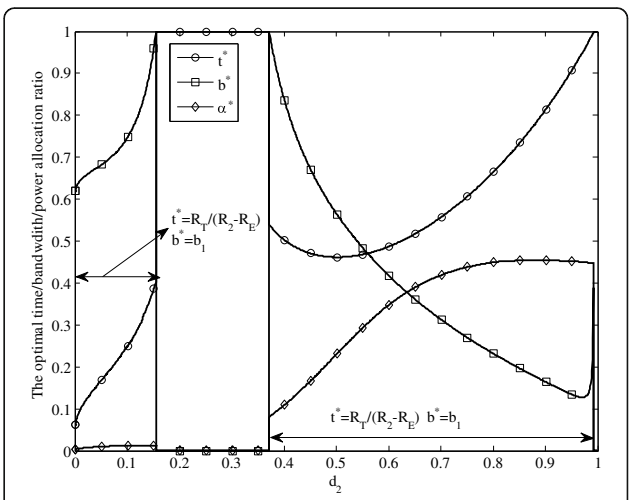

Fig. 4 The optimal power allocation ratio versus d_2

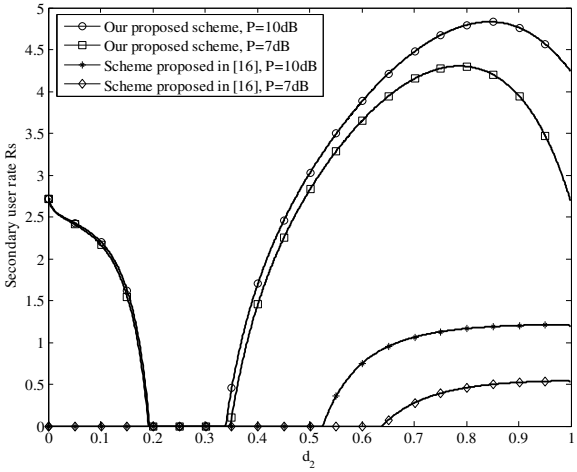

Fig. 5 Secondary user rate comparison versus d_2

secondary system transmission rate of the scheme in [16] is worse than our proposed scheme, and the spectrum access region of the scheme proposed in [16] is also smaller with different transmit power, which is due to the interference caused at PR and SR.

Figure 6 shows the transmission rate of secondary system and eavesdropper wiretapped versus the different location of ST with different location of eavesdropper when $R_T = 1.5$ bps/Hz. In Fig. 6, we can find that the access region becomes larger when the eavesdropper is farther away from PT. It is because that when the distance between the eavesdropper and PT becomes larger, the channel between them will be worse. Then, the eavesdropper wiretapped transmission rate becomes smaller, which means that the primary system can use less power to transmit the artificial noise. More power can be used to transmit the primary information in the first phase.

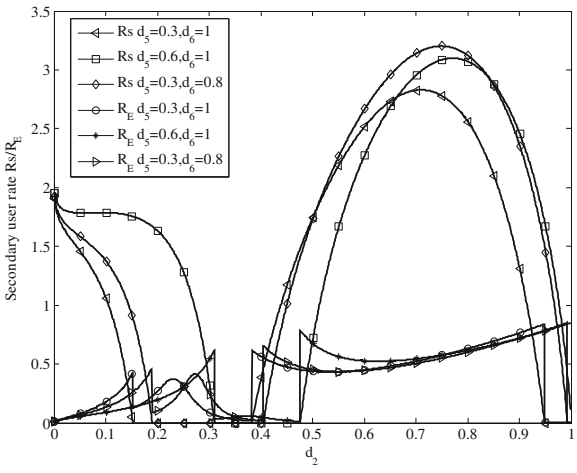

Fig. 6 Transmission rate of secondary system and eavesdropper wiretapped versus d_2 with different location of eavesdropper

Thus, in the second phase, ST can use less power to forward the primary information, and more power will be left for transmitting its own information, which leads to larger access region.

6 Conclusions

In this paper, we proposed a joint resource optimization based on spectrum sharing strategy for a secure transmission. Specifically, the secondary user serves as a trusted DF relay for the primary user, in which it uses a part of the bandwidth and power to forward PT's information. And in reward, it uses the remained resources to transmit its own information. We study the joint optimization of time, bandwidth, and power to maximize the secondary user's rate while guaranteeing the primary user achieves the target secrecy rate. Moreover, the closed-form expression of optimal time and bandwidth allocation are derived. Numerical result demonstrates that the proposed strategy can achieve a win-win result.

Acknowledgements

The authors would like to thank Xin Liu of Dalian University of Technology for the helpful discussions related to Section 4 of this paper.

Authors' contributions

WL and KG conceived and designed the corresponding system model; HP and ZL optimized the proposed models; MJ performed the simulations of the model; WL and KG wrote the paper. All authors read and approved the final manuscript.

Funding

This work was supported by China National Science Foundation under Grant No. 61402416 and 61601221, a project funded by China Postdoctoral Science Foundation under Grant No. 2017M612027.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]College of Information Engineering, Zhejiang University of Technology, Zhejiang, Hangzhou 310014, China. [2]School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China. [3]Haitian Plastics Machinery Group Co., Ltd, Ningbo, Zhejiang, China.

Received: 10 August 2017 Accepted: 6 November 2017
Published online: 17 November 2017

References

1. Y Zou, J Zhu, L Yang, CL Ying, YD Yao, Securing physical-layer communications for cognitive radio networks. IEEE Commun. Mag. **53**, 48–54 (2015)
2. AD Wyner, The wire-tap channel. Bell Labs Tech. J. **54**, 1355–1387 (1975)
3. I Csiszar, J Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**, 339–348 (1978)
4. H Deng, HM Wang, W Guo, W Wang, Secrecy transmission with a helper: to relay or to jam. IEEE Trans. Inf. Forensics Secur. **10**, 293–307 (2015)
5. H Deng, HM Wang, W Wang, Q J Yin, in *IEEE International Conference on Communications Workshops (ICC)*. Secrecy transmission with a helper: to relay or not to relay (IEEE Press, Sydney, 2014), pp. 825–830
6. HM Wang, XG Xia, Enhancing wireless secrecy via cooperation: signal design and optimization. IEEE Commun. Mag. **53**, 47–53 (2015)

7. L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**, 1875–1888 (2010)
8. NQ Bao, N Linh-Trung, M Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wirel. Commun. **12**, 6076–6085 (2013)
9. W Lu, J Wang, W Ge, F Li, J Hua, L Meng, An anti-interference cooperative bandwidth sharing strategy with joint optimization of time and bandwidth. J. Commun. Networks **16**, 141–145 (2014)
10. S Hu, Z Liu, YL Guan, W Xiong, G Bi, S Li, Sequence design for cognitive CDMA communications under arbitrary spectrum hole constraint. IEEE J. Sel. Areas Commun. **32**(11), 1974–1986 (2014)
11. S Hu, G Bi, YL Guan, S Li, TDCS-based cognitive radio networks with multiuser interference avoidance. IEEE Trans. Commun. **61**(12), 4828–4835 (2013)
12. S Goel, R Negi, Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**, 2180–2189 (2008)
13. HM Wang, CD Wang, WK Ng, Artificial noise assisted secure transmission under training and feedback. IEEE Trans. Signal Process. **63**, 6285–6298 (2015)
14. L Zhang, H Zhang, D Wu, D Yuan, *Improving physical layer security for MISO systems via using artificial noise. IEEE Global Communications Conference* (2015), pp. 1–6
15. XY Zhou, MR McKay, *Physical layer security with artificial noise: Secrecy capacity and optimal power allocation, 3rd International Conference on Signal Processing and Communication Systems* (2009), pp. 1–5
16. N Zhang, N Lu, N Cheng, JW Mark, XS Shen, Cooperative spectrum access towards secure information transfer for CRNs. IEEE J. Sel. Areas Commun. **31**(11), 2453–2464 (2013)