sensors

MDPI

Article

Anti-Wiretap Spectrum-Sharing for Cooperative Cognitive Radio Communication Systems

Peiyuan Si [1], Weidang Lu [1,*], Kecai Gu [1], Xin Liu [2,3], Bo Li [4], Hong Peng [1] and Yi Gong [5]

[1] College of Information Engineering, Zhejiang University of Technology, Hangzhou 310014, China; a18158504979@163.com (P.S.); gukecai2015@163.com (K.G.); ph@zjut.edu.cn (H.P.)
[2] School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China; liuxinstar1984@dlut.edu.cn
[3] The 54th Research Institute of CECT, Shijiazhuang 050081, China
[4] School of Information and Electrical Engineering, Harbin Institute of Technology, Weihai 264209, China; libo1983@hit.edu.cn
[5] Shenzhen Engineering Laboratory of Intelligent Information Processing for IoT, Southern University of Science and Technology, Shenzhen 518055, China; gongy@sustech.edu.cn
* Correspondence: luweid@zjut.edu.cn; Tel.: +86-0571-8529-0373

Received: 4 September 2019; Accepted: 23 September 2019; Published: 24 September 2019

Abstract: As wireless communication technology keeps progressing, people's requirements for wireless communication quality are getting higher and higher. Wireless communication brings convenience, but also causes some problems. On the one hand, the traditional static and fixed spectrum allocation strategy leads to high wastefulness of spectrum resources. The direction of improving the utility of spectrum resources by combining the advantages of cooperative communication and cognitive radio has attracted the attention of many scholars. On the other hand, security of communication is becoming an important issue because of the broadcasting nature and openness of wireless communication. Physical-layer security has been brought into focus due to the possibility of improving the security in wireless communication. In this paper, we propose an anti-wiretap spectrum-sharing scheme for cooperative cognitive radio communication systems which can secure the information transmission for the two transmission phases of the cooperative communication. We maximized the secondary system transmission rate by jointly optimizing power and bandwidth while ensuring the primary system achieves its secrecy transmission rate. Useful insights of the proposed anti-wiretap spectrum-sharing scheme are given in the simulation results. Moreover, several system parameters are shown to have a big impact for the simulation results.

Keywords: cognitive radio; cooperative relaying; anti-wiretap; joint resource allocation

1. Introduction

Recently, due to the progress in wireless communication technology, the number of users supported by the wireless communication system has been increasing, and people's requirements for transmission rate are getting higher and higher [1–4]. Wireless communication brings convenience, but also causes some problems such as spectrum scarcity and security problems.

Radio spectrum is a rare and non-renewable precious resource and the demand for radio spectrum resource is expanding rapidly [5,6]. The strategy of radio spectrum allocation is static and fixed, in which relevant the government department divides the spectrum into several frequency bands and reasonably allocates the corresponding frequency bands to the primary users (PU) according to the demand. Even if PU does not use the licensed bandwidth, the other users are still not allowed to use this bandwidth, which results in the waste of wireless spectrum resources.

Cognitive radio is regarded as a prominent solution to solve the problem of spectrum scarcity, which can improve the spectrum use [7–10]. It provides a flexible and low-cost alternative to wireless devices using classical single-protocol and single-frequency bands. Devices can decrease spectrum wastefulness and fill voids in the wireless spectrum with environment-sensing and environment-adapting. Ref. [11] characterizes the radio frequency spectrum opportunities available in a common global system for mobile (GSM) communications channel to support the operation of a cognitive radio network. Dynamic spectrum access technology gives spectrum managers more available spectrum while secondary users (SU) can share the spectrum dynamically [12–15]. Spectrum trading is also used to improve spectrum use in different dimensions, e.g., frequency band and time slot, which allows primary users to share its spectrum resource with SU in exchange for a monetary cost [16–18]. A new primary system spectrum pricing mechanism is proposed in [17], which takes the preferences of heterogeneous secondary users and various quality in leased spectrum due to diverse interference levels and channel characteristics into account. In [18], researchers considered a cognitive dynamic network architecture in which PU get rewarded if they share their connectivity with SU and act as access points.

Due to the broadcasting character and openness of wireless communication, security has become a serious problem. Broadcast features make the transmission of wireless signals less cryptic, which can lead to information leakage. Signals can be received and carried out as long as the eavesdropper has relevant equipment within a certain distance, which results in communication security risks [19–21]. Security attacks include two types: passive attack and active attack [22,23]. Learning or making use of the information of legitimate users are what passive attackers usually do—they do not attack the information itself, i.e., eavesdropping and traffic analysis [24,25]. Active attackers are not only able to involve the process of data modification itself but also interrupt legitimate communication, i.e., DDoS attack [26,27].

There are two main categories of strategy for defending security attacks: new designed networking protocol-based cryptographic encryption approaches, and physical-layer security (PLS) approaches. One of the encryption methods, secured hash function, which can be implemented with several different algorithms, is applied in many fields such as data transfer safety, message authentication, and other user-linked information transfer [28,29]. However, this method is always realized in upper layers, which is challenging to implement in cooperative cognitive radio communication systems. By exploiting the properties of the wireless channel, physical-layer security of relay networks has been remarkable, which is considered to be a quite promising method to improve the security performance of the next-generation wireless communication networks [30–33]. Ref. [34] proposed a multiple relay-based secure transmission scheme in cognitive radio (CR) communication system. Ref. [35] considered physical-layer security under the scenario where a message transmitted from a secondary source to a secondary destination and the eavesdroppers are poisson spatially distributed. Ref. [36] studied physical-layer security performance based on cooperative two-way cognitive relay with a single passive eavesdropper.

In the existing spectrum-sharing protocol for cooperative cognitive radio communication system, the eavesdropper stops eavesdropping information in the second transmission phase, as it finds that the primary users stop transmitting their signal. However, if the eavesdropper is smart enough, it will find that the primary signal is relayed by the cognitive user in the second transmission phase. Then the eavesdropper will also eavesdrop the primary signal in the second transmission phase. Thus, in this paper, we propose an anti-wiretap spectrum-sharing protocol to secure the information transmission for both transmission phases in a cooperative cognitive radio communication system. Specifically, the transmissions are performed through the following two phases. In the first phase, the primary user transmits the redesigned signal combined by the artificial noise and primary information to jam the eavesdropper. In the second phase, secondary and primary user transmit the primary signal with the designed weight coefficients by using a part of the bandwidth to avoid the eavesdropper

eavesdropping the primary information. As a reward, the secondary user can make use of the left bandwidth to transmit its own signal.

The primary contributions of this work are summarized as follows:

- First, we propose an anti-wiretap spectrum-sharing protocol, which can secure the information transmission for both transmission phases in cooperative cognitive radio communication systems.
- Secondly, we formulate a scheme by optimizing power and bandwidth jointly to maximize the secondary system transmission rate while ensuring the required primary system secrecy transmission rate.
- Finally, numerical and simulation results are shown to illustrate the performance of the proposed cooperative spectrum-sharing protocol and reveal the important effects of various system variables.

2. System Model and Problem Formulation

2.1. System Model

As shown in Figure 1, the proposed anti-wiretap spectrum-sharing protocol consists of a primary system, a secondary system, and an eavesdropper (E). The primary system contains a primary user (PU), which includes a primary transmitter (PT) and a primary receiver (PR). The secondary system contains a secondary user (SU), which includes a secondary transmitter (ST) and a secondary receiver (SR). When the primary system is in good channel condition, primary information will be sent directly from PT to PR. On the other hand, if the direct link is in a bad channel condition, the secondary system gains the opportunity to access the primary spectrum through forwarding primary information to help it achieve the secrecy transmission rate. We assume that ST is trustworthy, which will not eavesdrop on the primary information when helping PT forward information to PR. We use h_i, $i = 1, 2, 3, ..., 7$, to represent the corresponding channel coefficients. The noise at all nodes is assumed to be complex additive white Gaussian noise (AWGN) with zero mean and unit variance σ^2. The transmit power of PT and ST is denoted as P_p and P_s, respectively.

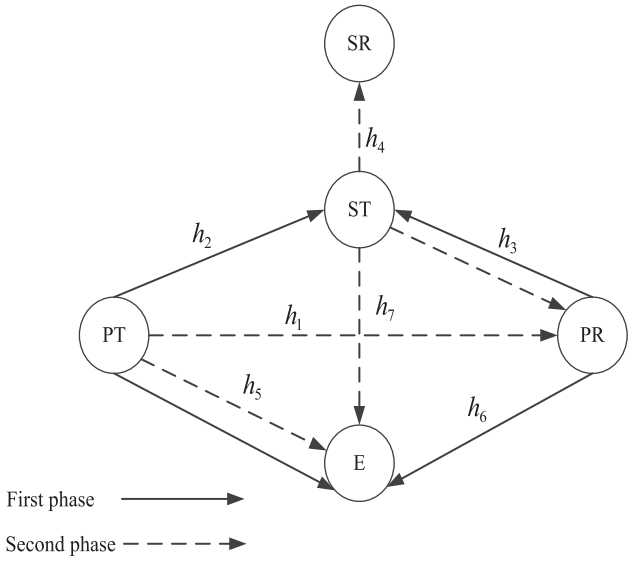

Figure 1. System model.

In the first phase, PT uses all of its bandwidth to transmit the redesigned signal x_{PT}^1, which is a linearly combined signal of primary signal s with power $\beta_1 P_p$ and artificial noise z with power $(1-\beta_1)\,P_p$, where β_1 denotes the power allocation coefficient. Then, $x_{PT}^1 = \sqrt{P_p \beta_1} s + \sqrt{P_p (1-\beta_1)} u_1 z$. To interfere the eavesdropper, PR also transmits signal x_{PR}, which is a signal that contains artificial

noise z with power $(1-\beta_1)P_p$. Then, $x_{PR} = \sqrt{P_p(1-\beta_1)}u_2 z$, where u_1 and u_2 denote the complex weight coefficients. Thus, the received signals at ST and E can be written as

$$r_{ST} = \sqrt{P_p\beta_1}h_2 s + \sqrt{P_p(1-\beta_1)}\,(u_1h_2 + u_2h_3)\,z + n_{ST} \tag{1}$$

$$r_E^1 = \sqrt{P_p\beta_1}h_5 s + \sqrt{P_p(1-\beta_1)}\,(u_1h_5 + u_2h_6)\,z + n_E^1 \tag{2}$$

where n_{ST} and n_E^1 denote the noise received at ST and E in the first phase, respectively.

To guarantee that artificial noise transmitted from PT and PR counteract at ST, u_1 and u_2 should satisfy the following conditions:

$$\begin{cases} u_1h_2 + u_2h_3 = 0 \\ u_1^2 + u_2^2 = 1 \end{cases} \tag{3}$$

Thus, Equation (1) can be rewritten as

$$r_{ST} = \sqrt{P_p\beta_1}h_2 s + n_{ST} \tag{4}$$

Therefore, the information rate at ST and the eavesdropping rate at E can be written as:

$$R_P^1 = \frac{1}{2}w\log_2(1+\beta_1\alpha_2) \tag{5}$$

$$R_E^1 = \frac{1}{2}w\log_2\left(1+\frac{\beta_1\alpha_5}{1+(1-\beta_1)\alpha_m}\right) \tag{6}$$

where $\alpha_2 = \dfrac{P_p|h_2|^2}{\sigma^2}$, $\alpha_5 = \dfrac{P_p|h_5|^2}{\sigma^2}$ and $\alpha_m = \dfrac{P_p|u_1h_5 + u_2h_6|^2}{\sigma^2}$.

In the second phase, ST uses a part of the licensed spectrum bw authorized by the primary system and power $\beta_2 P_s$ to forward the received primary information to PR with decode-and-forward relaying protocol, by transmitting the signal $x_{ST} = \sqrt{P_s\beta_2}v_1 s$. To prevent E eavesdropping on the primary information, PT also transmits the signal $x_{PT}^2 = \sqrt{P_p\beta_2}v_2 s$, where v_1 and v_2 denote the complex weight coefficients.

Thus, the received signal at PR and E can be written as

$$r_{PR} = \sqrt{\beta_2}\left(\sqrt{P_s}v_1h_3 + \sqrt{P_p}v_2h_1\right)s + n_{PR} \tag{7}$$

$$r_E^2 = \sqrt{\beta_2}\left(\sqrt{P_s}v_1h_7 + \sqrt{P_p}v_2h_5\right)s + n_E^2 \tag{8}$$

where n_{PR} and n_E^2 denotes the noise received at PR and E in the second phase, respectively.

To prevent E eavesdropping on the primary information in the second phase, v_1 and v_2 should satisfy the following conditions:

$$\begin{cases} \sqrt{P_s}v_1h_7 + \sqrt{P_p}v_2h_5 = 0 \\ v_1^2 + v_2^2 = 1 \end{cases} \tag{9}$$

Therefore, the eavesdropping rate at E in the second phase is zero and the information rate at PR can be written as:

$$R_P^2 = \frac{1}{2}bw\log_2(1+\beta_2\alpha_n) \tag{10}$$

where $\alpha_n = \dfrac{P_s|v_1h_3|^2 + P_p|v_2h_1|^2}{\sigma^2}$.

Thus, the information rate of primary system and eavesdropping rate at E through two phases transmission can be written as:

$$R_P = \min\{R_P^1, R_P^2\} \tag{11}$$
$$R_E = R_E^1 \tag{12}$$

Then, the secrecy transmission rate of primary system can be written as

$$R_{SEC} = R_P - R_E \tag{13}$$

As a reward for forwarding the primary signal, ST will be permitted to use the remained spectrum and power to transmit its own signal x to SR in the second phase. Then, the received signal at SR can be written as

$$r_{SR} = \sqrt{P_s(1-\beta_2)}h_4 x + n_{SR} \tag{14}$$

Thus, the information rate of secondary system can be written as:

$$R_S = \frac{1}{2}(1-b)w\log_2(1+(1-\beta_2)\alpha_4) \tag{15}$$

2.2. Problem Formulation

With the objective of maximizing the information rate of secondary system with the primary secrecy transmission rate constraint, through joint optimizing the power allocation β_1, β_2 and bandwidth allocation b, the optimization problem can be formulated as

$$\max_{\beta_1,\beta_2,b} R_S \tag{16}$$

subject to

$$\begin{cases} R_{SEC} \geq R_T \\ 0 \leq \beta_1 \leq 1 \\ 0 \leq \beta_2 \leq 1 \\ 0 \leq b \leq 1 \end{cases} \tag{17}$$

where R_T represents the target secrecy transmission rate of the primary system.

3. Optimal Solutions

In this section, we will optimize bandwidth and power allocation jointly under the primary system target secrecy rate constraint.

For convenience of expression, we define

$$\begin{cases} R_2 = w\log_2(1+\alpha_2\beta_1) \\ R_3 = w\log_2(1+\alpha_n\beta_2) \\ R_4 = w\log_2(1+(1-\beta_2)\alpha_4) \end{cases} \tag{18}$$

Thus, the optimization problem in Equation (16) can be written as

$$\max_{\beta_1,\beta_2,b} \frac{1}{2}(1-b)R_4 \tag{19}$$

subject to

$$\begin{cases} \frac{1}{2}R_2 - R_E \geq R_T \\ \frac{1}{2}bR_3 - R_E \geq R_T \\ 0 \leq \beta_1 \leq 1 \\ 0 \leq \beta_2 \leq 1 \\ 0 \leq b \leq 1 \end{cases} \tag{20}$$

Due to the non-convex constraints in Equation (20), it is difficult to obtain the optimal solution directly. We solve the above optimization problem through the following three steps. We will show in the numerical results that the above solution achieves the optimal performance which can be proved through the exhaustive search scheme.

3.1. Finding Optimal Bandwidth Allocation b^* with Fixed Power Allocation β_1 and β_2

To satisfy the second condition of Equation (20), we can obtain

$$b \geq \frac{2(R_T + R_E)}{R_3} \tag{21}$$

From Equation (15), we can find that the target function R_S is a monotonic decreasing function of b with fixed β_1 and β_2. Therefore, we can find the optimal bandwidth allocation b^* as

$$b^* = \frac{2(R_T + R_E)}{R_3} = \frac{2\left(R_T + \frac{1}{2}w\log_2\left(1 + \frac{\beta_1\alpha_5}{1+(1-\beta_1)\alpha_m}\right)\right)}{w\log_2(1+\alpha_n\beta_2)} \tag{22}$$

3.2. Finding Optimal Power Allocation β_1^* with Fixed β_2

Substituting the optimal bandwidth allocation b^* into R_S, we can obtain

$$R_S = \frac{1}{2}\left(1 - \frac{2\left(R_T + \frac{1}{2}w\log_2\left(1 + \frac{\beta_1\alpha_5}{1+(1-\beta_1)\alpha_m}\right)\right)}{w\log_2(1+\alpha_n\beta_2)}\right) w\log_2(1+(1-\beta_2)\alpha_4) \tag{23}$$

To satisfy the first condition of Equation (20), we can obtain

$$\frac{1}{2}w\log_2(1+\beta_1\alpha_2) - \frac{1}{2}w\log_2\left(1 + \frac{\beta_1\alpha_5}{1+(1-\beta_1)\alpha_m}\right) \geq R_T \tag{24}$$

After some manipulation, Equation (24) can be rewritten as

$$f(\beta_1) = A\beta_1^2 + B\beta_1 + C \geq 0 \tag{25}$$

where $A = -\alpha_2\alpha_m$, $B = \alpha_2(1+\alpha_m) - \alpha_m - 2^{\frac{2R_T}{w}}(\alpha_5 - \alpha_m)$ and $C = (1+\alpha_m)\left(1 - 2^{\frac{2R_T}{w}}\right)$.

Assuming $x_1 = \frac{-B + \sqrt{B^2 - 4AC}}{2A}$ and $x_2 = \frac{-B - \sqrt{B^2 - 4AC}}{2A}$ are the two roots of the equation $f(\beta_1) = 0$. It is easy to find that $A < 0$ and $C < 0$. Thus, if $-\frac{B}{2A} < 0$, we can find that two roots x_1 and x_2 are negative. Then, there will be no positive value of β_1 that can satisfy the condition in Equation (25). Thus, we can conclude that $-\frac{B}{2A} \geq 0$. Due to $C < 0$, we can obtain $0 < x_1 < x_2$. From Equation (23), we can find that R_S is a monotonic decreasing function of β_1 with fixed β_2, thus the

optimal value of β_1^* depends on whether x_1 is larger than 1. If x_1 is smaller than 1, $\beta_1^* = x_1$, otherwise there will be no optimal value of β_1^* to satisfy the condition $0 \leq \beta_1 \leq 1$.

3.3. Finding Optimal Power Allocation β_2^*

Substituting the optimal power allocation β_1^* into R_s, we can obtain

$$R_s = \frac{1}{2} w \log_2 (1 + (1 - \beta_2)\alpha_4) - (R_T + R_E) \frac{w \log_2 (1 + (1 - \beta_2)\alpha_4)}{w \log_2 (1 + \beta_2 \alpha_n)} \tag{26}$$

To satisfy the fifth condition of Equation (20), we can obtain $\beta_N \leq \beta_2 \leq 1$, where $\beta_N = \frac{2^{\frac{2(R_T+R_E)}{w}} - 1}{\alpha_n}$.

From Equation (26), it is easy to find that R_S is composed of two decreasing function of β_2. Let $\beta = 1 - \beta_2$, then R_S is composed of two increasing function of β. After some manipulation, we can obtain

$$R_S(\beta) \quad = \quad f(\beta) - g(\beta) \tag{27}$$

where $f(\beta) = \frac{1}{2} w \log_2 (1 + \beta\alpha_4)$ and $g(\beta) = (R_T + R_E) \frac{w \log_2 (1 + \beta\alpha_4)}{w \log_2 (1 + (1 - \beta)\alpha_n)}$.

Introducing a new variable t, $g(\beta) + t = g(\beta)_{max}$, which satisfies $0 \leq t \leq (g(\beta)_{max} - g(\beta)_{min})$, R_S can be rewritten as

$$R_S(\beta, t) = f(\beta) + t - g(\beta)_{max} \tag{28}$$

From Equation (28), we can find that it is a monotonic optimization problem which can be solved by the polyblock outer approximation approach [37,38], which is formed by constructing *Polyblock* covering feasible region **D** step by step. Feasible region **D** is composed of the intersection of a *NormalSet* and a *ReverseNormalSet*. *Polyblock* outer approximation approach is realized as follows: First, choose a block $[l, u]$ as original *Polyblock*. Let z^k denote the vertex which makes the objective function achieve the maximum value among all the vertex in the kth iteration. Let x^k denote the intersection of the line between l and z^k and the feasible region **D** in the kth iteration. The *Polyblock* is gradually specified by splitting $[x^k, z^k]$ from block $[l, z^k]$ in each iteration. Through alternating n components, let one component be equal to the component of x^k, and the other components be equal to the components of z^k, which will result in n new vertices. The iteration stops when the difference between the upper bound (the maximum target value of the vertex) and lower bound (the target value of the current best boundary point) achieves at a given precision.

Thus, our optimization problem can be solved by the polyblock outer approximation approach as shown in Algorithm 1.

Algorithm 1 Polyblock Outer Approximation Algorithm

Step one: Initialization

1. Choose the lower angular point ρ_{min} and the upper angular point ρ_{max} of *Polyblock*. Initializes the current optimal target value $CBV = \infty$, current optimal value $CBS = \emptyset$. Set iteration index $k = 1$ and error tolerance $\epsilon \ll 1$.
2. Initialize the vertex set $\Gamma_1 = \{0\}$, set algorithm terminating mark $f_{stop} = 0$. For convenience of expression, define $R_S(\{\rho_i\}_{i\in\Gamma_1}) = \frac{1}{2} w \log_2(1 + \beta\alpha_4) + t - g(\beta)_{max}$.

Step two: Iteration

3. Traverse vertex set Γ_1, select the vertex that belongs to CBV and update Γ_1.
4. Judge whether Γ_1 is empty. If Γ_1 is empty, set $f_{stop} = 1$, go to 14. Else, go to 5.
5. Chose a vertex z^k that maximize the objective function from set Γ_1, expressed as $z^k \in arg\,max\{V(\{\rho_i\}_{i\in\Gamma})|\{\rho_i\}_{i\in\Gamma} \in \Gamma_k\}$.
6. Judge whether z^k is repeated with the former optimal vertex. If the number of consecutive repetitions is larger than a given value, set $f_{stop} = 1$, go to 14. Else, go to 7.
7. Construct a straight line connecting z^k and ρ_{min}
8. Find the intersection point of the line constructed in 7 and the upper boundary of the feasible region using dichotomy.
9. If $V(x^k) < CBV$, go to 10, else go to 11.
10. Update $CBV = V(x^k)$, set $CBS = x^k$.
11. If $||x^k - z^k|| < \epsilon$, set $f_{stop} = 1$, go to 14. Else, go to 12.
12. Update the current vertex set $\Gamma_{k+1} = \left(\Gamma_k \backslash \{z^k\}\right) \cup \{z^k + \left(x_i^k - z_i^k\right) e_i, \forall i \in \Gamma\}$ and delete the vertexes not belong to $G_{(\rho_0)}$.
13. If Γ_{k+1} is empty, set $f(stop) = 1$, go to 14. Else $k = k + 1$, return to 4.

Step three: Output

14. Output $CBS = \{\rho_{i,(\rho_0)}^{*,sub}\}_{i\in\Gamma_1}$, $R_s(\rho_0) = CBV$.

4. Simulation Results and Discussion

In this section, we investigate the performance of proposed anti-wiretap spectrum-sharing strategy. As shown in Figure 2, PT, PR, ST, SR and E are distributed in a two-dimensional $X - Y$ plane, in which PT is located at (0,0), PR is located at (1,0) and ST moves from point (0,0) to (1,0). The distance of ST to SR is half of the distance of ST to PR. Thus, we can obtain $d_1 = 1, d_2 = 1 - d_3, d_4 = d_3/2$. The distance of E to PT is $d_5 = 0.3$, the distance of E to PR is $d_6 = 1$ and the distance of E to ST is $d_7 = d_4$. Set the path loss coefficient to be $v = -3$ and bandwidth is $w = 1$.

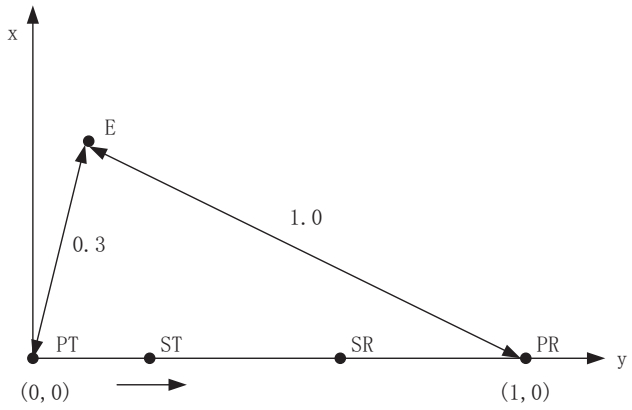

Figure 2. Position of PT, PR, ST, SR and E.

Figure 3 shows the information rate of the secondary system when ST moves from $(0,0)$ to $(1,0)$ under different primary system target secrecy rate. In Figure 3, we can find that the performance of our proposed scheme and exhaustive search scheme are the same, which verifies the effectiveness our proposed scheme. In exhaustive search scheme, the optimal power and bandwidth allocation is obtained with the bisection method. In Figure 3, we can find that the information rate of secondary system becomes smaller when the primary system target secrecy rate becomes larger. It is because that more bandwidth and power will be allocated to forward the primary signal when helping the primary system achieve larger target secrecy rate, which can be illustrated from Figures 4 and 5. Then, less bandwidth and power are left for transmitting the secondary signal, which leads smaller information rate of the secondary system. When $R_T = 1.0$ bps/Hz , the secondary system can access to the primary spectrum only when $0.42 < d_2 < 0.78$. The secondary system cannot access to the primary spectrum when $d_2 \leq 0.42$, which is because that in this case the distance of ST to PR is too far away, leading poor channel condition for the secondary system to help forward the primary signal to PR. Then, the primary system cannot achieve its target secrecy rate. Thus, the secondary system will not be permitted to access to the primary spectrum. When $d_2 \geq 0.78$, the channel condition between PT and ST is too poor for the secondary system to help the primary system achieve the target secrecy rate. Thus, the secondary system cannot access to the primary spectrum. When $R_T = 1.5$ bps/Hz, the similar case happened when ST located in $0.48 < d_2 < 0.64$. In the access range, the information rate of the secondary system becomes larger when d_2 becomes larger. It is because that when d_2 becomes larger, which means that ST gets closer to PR. Then the channel condition between ST and PR becomes better, which will lead to less bandwidth and power to forward the primary signal as illustrated in Figures 4 and 5. Thus, more bandwidth and power can be used to transmit the secondary signal leading larger information rate of the secondary system.

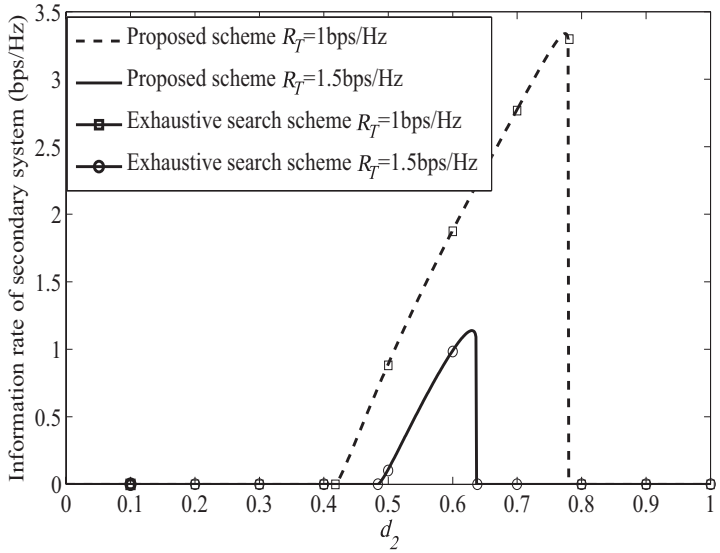

Figure 3. Transmission rate of cognitive user under different target secrecy rate.

Figure 4 shows the optimal bandwidth and power allocation when ST moves from $(0,0)$ to (1,0), when the primary target secrecy rate is $R_T = 1$ bps/Hz. In Figure 4, we can find that in the access range the power and bandwidth allocated to help forward becomes smaller when d_2 becomes larger. It is because that the channel condition between ST and PR becomes better when d_2 becomes larger, which means that the secondary system can reduce bandwidth and power to help the primary system achieve the target secrecy rate. We can also observe form Figure 4 that when d_2 becomes larger, the power used to transmit the artificial noise will becomes smaller. It is because that the information rate of the

secondary system becomes larger when d_2 becomes larger, which leads less power to transmit the artificial noise to interfere the eavesdropper.

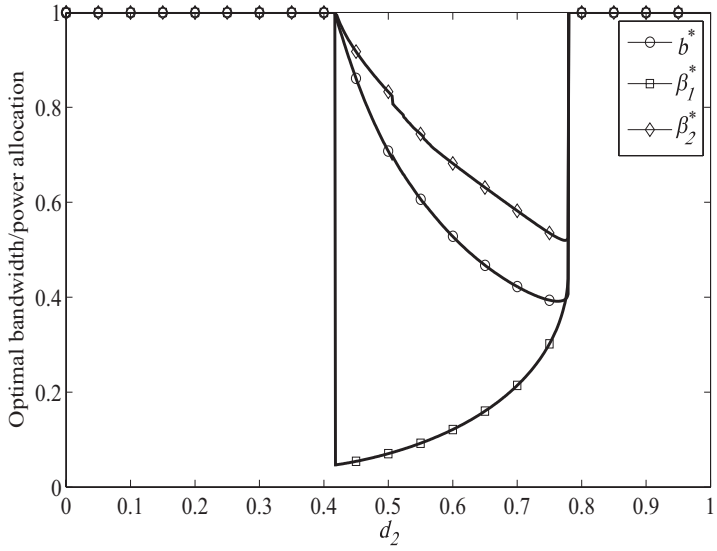

Figure 4. Optimal resource allocation when R_T = 1.0 bps/Hz.

Figure 5 shows the optimal bandwidth and power allocation when ST moves from $(0, 0)$ to $(1, 0)$, when the primary target secrecy rate is $R_T = 1.5$ bps/Hz. Compared to Figure 4, we can find that the access range of the secondary system becomes smaller when the primary system target secrecy rate becomes larger, which is because that better channel is needed to forward the primary signal when helping the primary system achieve larger target secrecy rate. In Figure 5, we can also observe that more bandwidth and power will be allocated to forward the primary signal when helping the primary system achieve larger target secrecy rate with a fixed d_2.

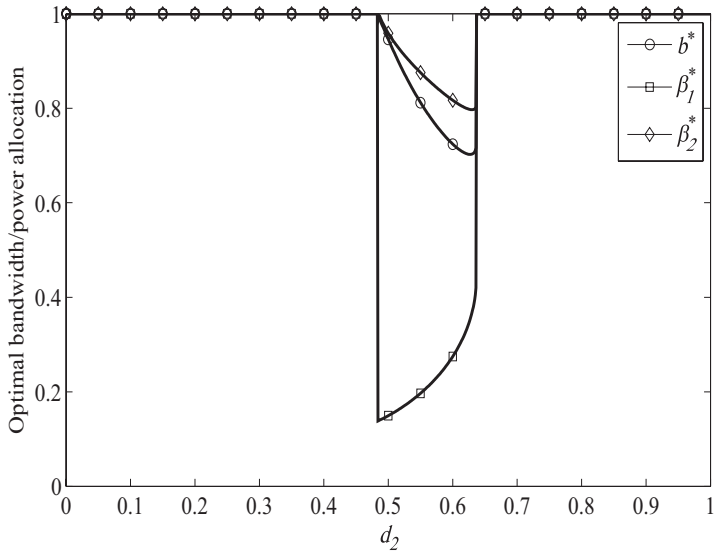

Figure 5. Optimal resource allocation when R_T = 1.5 bps/Hz.

5. Conclusions

In this paper, we proposed an anti-wiretap spectrum-sharing scheme for cooperative cognitive radio communication systems which can secure the information transmission for the two transmission

phases of the cooperative communication. To secure the information transmission in phase 1, PT transmits the redesigned signal which is combined by the artificial noise and primary information to jam the eavesdropper. To secure the information transmission in the phase 2, PT and ST transmit the primary information with the designed weight coefficients by using a part of the bandwidth and power to avoid the eavesdropper eavesdropping the primary information. As a reward, the secondary user can used the remaining bandwidth to transmit its own information. The joint optimization of bandwidth and power allocation is formulated to maximize the secondary system information rate while ensuring the primary system achieve its secrecy transmission rate. In simulation results, we give some useful insights of the proposed anti-wiretap spectrum-sharing scheme and reveal the system parameter impact for the system performance.

Author Contributions: W.L. and P.S. conceived and designed the SWIPT-based CSN model; H.P., K.G. and Y.G. optimized the proposed models; X.L. and B.L. performed the simulations of the model; and W.L. wrote the paper.

Funding: This work was supported by the National Natural Science Foundation of China under Grant 61871348, in part by Shenzhen Science and Technology Program under Grant JCYJ20170817110410346, in part by the Project funded by China Postdoctoral Science Foundation under Grant 2019T120531, and in part by the Fundamental Research Funds for the Provincial Universities of Zhejiang under Grant RF-A2019001.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hu, S.; Yu, B.; Qian, C.; Xiao, Y.; Xiong, Q.; Sun, C.J.; Gao, Y. Non-orthogonal Interleave-Grid Multiple Access Scheme for Industrial Internet-of-things in 5G Network. *IEEE Trans. Ind. Inform.* **2018**, *32*, 5436–5446. [CrossRef]
2. Huang, L.; Bi, S.Z.; Zhang, Y.J. Deep Reinforcement Learning for Online Offloading in Wireless Powered Mobile-Edge Computing Networks. *IEEE Trans. Mob. Comput.* **2018**. [CrossRef]
3. Yang, H.; Li, B.; Liu, G.; Liu, X.; Peng, X. DNF-SC-PNC: A New Physical-Layer Network Coding Scheme for Two-Way Relay Channels with Asymmetric Data Length. *Wirel. Netw.* **2018**. [CrossRef]
4. Lu, W.D.; Gong, Y.; Liu, X.; Wu, J.Y.; Peng, H. Collaborative Energy and Information Transfer in Green Wireless Sensor Networks for Smart Cities. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1585–1593. [CrossRef]
5. Na, Z.; Wang, Y.; Li, X.; Xia, J.; Liu, X.; Xiong, M.; Lu, W. Subcarrier Allocation based Simultaneous Wireless Information and Power Transfer algorithm in 5G cooperative OFDM communication systems. *Phys. Commun.* **2018**, *29*, 164–170. [CrossRef]
6. Li, B.; Yang, J.; Yang, H.; Liu, G.; Ma, R.; Peng, X. Decode-and-Forward Cooperative Transmission in Wireless Sensor Networks based on Physical-Layer Network Coding. *Wirel. Netw.* **2019**. [CrossRef]
7. Bazerque, J.A.; Giannakis, G.B. Distributed Spectrum Sensing for Cognitive Radio Networks by Exploiting Sparsity. *IEEE Trans. Signal Process.* **2010**, *58*, 1847–1862. [CrossRef]
8. Liu X.; Zhang, X.Y.; Jia, M.; Lu, W.D. 5G-based green broadband communication system design with simultaneous wireless information and power transfer. *Phys. Commun.* **2018**, *25*, 539–545. [CrossRef]
9. Zhang, H.; Nie, Y.; Cheng, J.; Leung, V.C.M.; Nallanathan, A. Sensing Time Optimization and Power Control for Energy Efficient Cognitive Small Cell with Imperfect Hybrid Spectrum Sensing. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 730–743. [CrossRef]
10. Lu, W.D.; Wang, J. Opportunistic Spectrum Sharing Based on Full-Duplex Cooperative OFDM Relaying. *IEEE Commun. Lett.* **2014**, *18*, 241–244. [CrossRef]
11. Luís, M.; Oliveira, R.; Dinis, R.; Bernardo, L. RF-Spectrum Opportunities for Cognitive Radio Networks Operating Over GSM Channels. *IEEE Trans. Cognit. Commun. Netw.* **2017**, *3*, 731–739. [CrossRef]
12. Lu, W.D.; Gong, Y.; Ting, S.H.; Wu, X.L.; Zhang, N.T. Cooperative OFDM Relaying for Opportunistic Spectrum Sharing Protocol Design and Resource Allocation. *IEEE Tans. Wirel. Commun.* **2012**, *11*, 2126–2135.
13. Liu X., Jia M.; Zhang X. Y.; Lu W. D. A Novel Multichannel Internet of Things Based on Dynamic Spectrum Sharing in 5G Communication. *IEEE Internet Things J.* **2019**, *6*, 5962–5970. [CrossRef]
14. Fosson, S.; Matamoros, J.; Anton-Haro, C.; Magli, E. Distributed Support Detection of Jointly Sparse Signals. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, 4–9 May 2014; pp. 6434–6438.

15. Lu, W.D.; Zhang, Y.A.; Wang, M.Y.; Liu, X.; Hua, J.Y. Cooperative Spectrum Sharing in OFDM Two-Way Relay Systems With Bidirectional Transmissions. *IEEE Commun. Lett.* **2017**, *21*, 1349–1352. [CrossRef]
16. Bajaj, I.; Lee, Y.H.; Gong, Y. A Spectrum Trading Scheme for Licensed User Incentives. *IEEE Trans. Commun.* **2015**, *63*, 4026–4036. [CrossRef]
17. Li, F.; Lam, K.; Li, X.; Liu, X.; Wang, L.; Leung, V.C.M. Dynamic Spectrum Access Networks with Heterogeneous Users: How to Price the Spectrum. *IEEE Trans. Veh. Technol.* **2018**, *67*, 5203–5216. [CrossRef]
18. Lorenzo, B.; Shafigh, A.S.; liu, J.; González-Castaño, F.J.; Fang, Y. Data and Spectrum Trading Policies in a Trusted Cognitive Dynamic Network Architecture. *IEEE/ACM Trans. Netw.* **2018**, *26*, 1502–1516. [CrossRef]
19. Wang, W.; Kwok, K.C.; Li, H.; Luo, S. On the Impact of Adaptive Eavesdroppers in Multi-Antenna Cellular Networks. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 269–279. [CrossRef]
20. Zhang, H.; Yang, N.; Long, K.; Pan, M.; Karagiannidis, G.K.; Leung, V.C.M. Secure Communications in NOMA System: Subcarrier Assignment and Power Allocation. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1441–1452. [CrossRef]
21. Lai, L.F.; Gamal, H.E. The Relay–Eavesdropper Channel: Cooperation for Secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019. [CrossRef]
22. Fang, D.F.; Qian, Y.; Hu, Q.Y. Security for 5G Mobile Wireless Networks. *IEEE Access* **2018**, *6*, 4850–4874. [CrossRef]
23. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 6th ed.; Pearson: London, UK, 2014.
24. Xu, J.; Duan, L.J.; Zhang, R. Proactive Eavesdropping via Cognitive Jamming in Fading Channels. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2790–2806. [CrossRef]
25. Moon, J.; Lee, H.; Song, C.; Kang, S.; Lee, I. Relay-Assisted Proactive Eavesdropping with Cooperative Jamming and Spoofing. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 6958–6971. [CrossRef]
26. Nagar, S.; Rajput, S.S.; Gupta, A.K.; Trivedi, M.C. Secure routing against DDoS attack in wireless sensor network. In Proceedings of the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India, 9–10 February 2017; pp. 1–6.
27. Wei, W.; Song, H.; Wang, H.; Fan, X. Research and Simulation of Queue Management Algorithms in Ad Hoc Networks under DDoS Attack. *IEEE Access* **2017**, *5*, 27810–27817. [CrossRef]
28. Debnath, S.; Chattopadhyay, A.; Dutta, S. Brief review on journey of secured hash algorithms. In Proceedings of the 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 2–3 November 2017; pp. 1–5.
29. Luo, P.; Athanasiou, K.; Fei, Y.; Wahl, T. Algebraic Fault Analysis of SHA-3 under Relaxed Fault Models. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1752–1761. [CrossRef]
30. Juliato, M.; Gebotys, C. A Quantitative Analysis of a Novel SEU-Resistant SHA-2 and HMAC Architecture for Space Missions Security. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1536–1554. [CrossRef]
31. Bassily, R.; Ekrem, E.; He, X.; Tekin, E.; Xie, J.; Bloch, M.R.; Ulukus, S.; Yener, A. Cooperative security at the physical layer: A summary of recent advances. *IEEE Signal Process. Mag.* **2013**, *30*, 16–28. [CrossRef]
32. Jin, S.; McKay, M.R.; Zhong, C.; Wong, K.-K. Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems. *IEEE Trans. Inf. Theory* **2014**, *56*, 2204–2224. [CrossRef]
33. Zhang, S.; Liew, S.C. Channel coding and decoding in a relay system operated with physical-layer network coding. *IEEE J. Sel. Areas Commun* **2009**, *27*, 788–796. [CrossRef]
34. Li, W.; Xin, M.; Yue, M.; Yinglei, T.; Yong, Z. Security-oriented transmission based on cooperative relays in cognitive radio. *China Commun.* **2013**, *10*, 27–35. [CrossRef]
35. Hu, X.; Zhang, X.; Huang, H.; Li, Y.Y. Secure transmission via jamming in cognitive radio networks with possion spatially distributed eavesdroppers. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016.
36. El-Malek, A.H.; Salhab, A.M.; Zummo, S.A. New Bandwidth Efficient Relaying Schemes in Cooperative Cognitive Two-Way Relay Networks with Physical Layer Security. *IEEE Trans. Veh. Technol.* **2017**, *66*, 5372–5386. [CrossRef]

37. Rubinova, A.; Tuyb, H.; Maysa, H. An Algorithm for Monotonic Global Optimization Problems. *Optimization* **2001**, *49*, 205–221. [CrossRef]
38. Qian, L.; Zhang, S.; Zhang, W.; Zhang, Y. System Utility Maximization with Interference Processing for Cognitive Radio Networks. *IEEE Trans. Commun.* **2015**, *63*, 1567–1579. [CrossRef]