sensors

MDPI

Article

Reciprocally-Benefited Secure Transmission for Spectrum Sensing-Based Cognitive Radio Sensor Networks

Dawei Wang [1,2], Pinyi Ren [1,2,*], Qinghe Du [1,2], Li Sun [1,2] and Yichen Wang [1,2,3]

[1] Department of Information and Communication Engineering, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China; wangdw@stu.xjtu.edu.cn (D.W.); duqinghe@mail.xjtu.edu.cn (Q.D.); lisun@mail.xjtu.edu.cn (L.S.); wangyichen0819@mail.xjtu.edu.cn (Y.W.)

[2] Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China

[3] Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, 865 Changning Road, Shanghai 200050, China

* Correspondence: pyren@mail.xjtu.edu.cn; Tel.: +86-29-8266-4427

Academic Editor: Leonhard M. Reindl
Received: 20 September 2016; Accepted: 18 November 2016; Published: 25 November 2016

Abstract: The rapid proliferation of independently-designed and -deployed wireless sensor networks extremely crowds the wireless spectrum and promotes the emergence of cognitive radio sensor networks (CRSN). In CRSN, the sensor node (SN) can make full use of the unutilized licensed spectrum, and the spectrum efficiency is greatly improved. However, inevitable spectrum sensing errors will adversely interfere with the primary transmission, which may result in primary transmission outage. To compensate the adverse effect of spectrum sensing errors, we propose a reciprocally-benefited secure transmission strategy, in which SN's interference to the eavesdropper is employed to protect the primary confidential messages while the CRSN is also rewarded with a loose spectrum sensing error probability constraint. Specifically, according to the spectrum sensing results and primary users' activities, there are four system states in this strategy. For each state, we analyze the primary secrecy rate and the SN's transmission rate by taking into account the spectrum sensing errors. Then, the SN's transmit power is optimally allocated for each state so that the average transmission rate of CRSN is maximized under the constraint of the primary maximum permitted secrecy outage probability. In addition, the performance tradeoff between the transmission rate of CRSN and the primary secrecy outage probability is investigated. Moreover, we analyze the primary secrecy rate for the asymptotic scenarios and derive the closed-form expression of the SN's transmission outage probability. Simulation results show that: (1) the performance of the SN's average throughput in the proposed strategy outperforms the conventional overlay strategy; (2) both the primary network and CRSN benefit from the proposed strategy.

Keywords: cognitive radio sensor network; secrecy outage probability; spectrum sensing error; power allocation

1. Introduction

Wireless sensor networks have been identified as a promising technology for the ongoing developing intelligent world and are widely deployed for different application fields, such as military, environmental monitoring [1], healthcare [2], smart home [3] and other commercial areas [4]. By taking advantage of the characteristics of the self-organization and flexible expansion [5,6], wireless sensor networks are widely utilized for wireless monitoring and controlling, especially for the smart home system. However, thousands of sophisticated, overlapping and coexisting wireless sensor networks burden the limited licensed spectrum, where sensor nodes (SN) suffer from strong interference.

In addition, the license-exempt industrial, scientific and medical (ISM) bands are crowded with other communication systems, such as WiFi, wireless local area networks (WLANs), Bluetooth, etc. [7]. Therefore, to improve the performance of the wireless sensor networks, making full use of the limited wireless spectrum is a critical issue.

Cognitive radio technology, initially proposed by Mitola [8], greatly relieves the spectrum shortage situation and improves the spectrum efficiency. In cognitive radio networks, the secondary system can share the licensed spectrum through underlay or overlay modes. For the underlay spectrum sharing mode, the secondary network accesses the licensed spectrum concurrently with the transmission of the primary network under the interference temperature constraint. For the overlay spectrum sharing mode, the secondary system detects the unutilized licensed spectrum (known as white space) to access and avoids interference to the primary network. As a promising spectrum sharing approach, the overlay mode, which not only improves the throughput of the secondary network, but also guarantees the quality of service (QoS) requirement of the primary network, will be adopted in this paper. The energy detection technique is mostly utilized in the overlay mode to be aware of the available surrounding spectrum resource [9]. However, since the inevitable spectrum sensing errors will result in the performance degradation of both the primary and secondary networks, the network parameters should be carefully designed to improve the spectrum sensing accuracy [10].

Considering the strong interference from other communication networks in ISM bands and the QoS requirements for applications, wireless sensor networks can integrate the cognitive radio technology and formulate the cognitive radio sensor network (CRSN) to efficiently utilize the spectrum [11,12]. Therefore, the information in the CRSN can be efficiently and reliably transmitted in the unutilized licensed spectrum. Recently, CRSN has attracted much research attention [13–19]. An optimal schedule scheme for a sensor-aided energy-efficient cooperative network was designed in [13]. An energy-efficient channel management scheme was proposed in [14] to save the energy for spectrum sensing and prolong the network lifetime. In [15], the authors designed a spectrum-aware medium access control (MAC) protocol for CRSN. In [16], the authors analyzed the delay performance and designed two channel switch methods for CRSN. The work [17] investigated the modeling methods for information transmission, and [18] analyzed the spectrum efficiency through a graph-theoretic max-flow framework for CRSN. Spectrum and power allocation and routing were jointly considered to maximize the information rate, as well as the lifetime of CRSN [19]. However, in the above works, the effects of the spectrum sensing errors are not considered. Since the inevitable spectrum sensing errors will bring strong interference to the transmission of the primary users (PU), the spectrum sensing accuracy should be improved. Although much more time allocated for the spectrum sensing can improve the spectrum sensing accuracy, there will be less time for SN's transmission, which will decrease the throughput of the sensor network. Therefore, there is a tradeoff between the spectrum sensing accuracy and the QoS provisioning of the CRSN.

Due to the broadcast nature of wireless media, the primary network faces the eavesdropping threat, as all other users in the primary transmission range are potential eavesdroppers. Traditionally, the upper layer encryption and decryption algorithms, assuming limited computational ability at the eavesdropper, are adopted to guarantee the information security. Besides, by employing the characteristics of wireless channels, physical layer security methods, such as cooperative relaying and/or jamming, can also provide perfect information security for the primary confidential messages [20,21]. Through being assisted by one or multiple jammers, cooperative jamming is a simple way to protect the confidential messages against eavesdropping [22–24]. The work in [25] proposed a destination-aided jamming scheme to protect the confidential messages against the untrusted relay. The work in [26] optimally designed the precoding matrix and allocated the transmit power of the source and jammer to maximize the lower-bound secrecy rate in a multi-input multi-output cognitive radio network. In [27], a cooperative node was chosen to act as a cooperative jammer to transmit jamming signals or act as a noise forwarder to transmit dummy codewords. In [28], the secondary destination and transmitter transmitted jamming signals during the primary broadcasting and forwarding phases, respectively, to guarantee the security of the primary information. In [29], the primary system would cooperate with either two secondary users or a cluster of secondary users to improve its secrecy rate. The authors in [30] proposed a cooperative jamming scheme in which the secondary system transmitted the jamming signal to acquire some spectrum opportunities as a reward. In CRSN, we can also utilize the physical layer approach to protect the confidential messages. In addition, we notice that in CRSN, the transmission of the SN also interferes with the eavesdropper, which can be employed to enhance the primary secrecy rate. Therefore, in this paper, we will utilize the interference from the SN to protect the primary confidential messages, and as a reward, the limited spectrum sensing error probability of the CRSN is permitted to satisfy the SN's QoS provisioning. To the best of the authors' knowledge, this is the first work that has investigated the secure transmission of the primary system assisted by CRSN by taking into account the spectrum sensing errors.

In this paper, we propose a reciprocally-benefited secure transmission strategy to protect the primary confidential messages and support the QoS requirement of CRSN. In the proposed strategy, the SN opportunistically shares the unutilized licensed spectrum through spectrum sensing. Due to the inevitable spectrum sensing errors, the primary transmission are interfered by the transmission of the SN. In addition, the primary network faces the security threat from an eavesdropper. Since the interference from the SN also interferes with the eavesdropper, which can be employed to increase the primary secrecy rate, the primary network can permit limited spectrum sensing error probability in exchange for the SN's cooperation. Both CRSN and the primary network can benefit from the cooperation. From the primary service perspective, this transmission strategy transforms the possible disturbed SN's service activities into a reciprocally-benefited mode, and the primary confidential messages are protected. From the SN's service perspective, limited spectrum sensing error probability is permitted, and the SN's QoS is satisfied. Specifically, according to the PUs' activities and spectrum sensing results, there are four system states: (I) the spectrum is idle and detected as idle; (II) the spectrum is occupied and detected as idle; (III) the spectrum is idle and detected as busy; and (IV) the spectrum is occupied and detected as busy. For each state, we analyze the SN's transmission rate and the PUs' secrecy rate. Then, we optimally allocate the SN's transmit power for each state to maximize the average transmission rate of CRSN under the constraints of the SN's average transmission power and the PUs' secrecy outage probability requirements. We give a further discussion for the power allocation scheme and investigate the performance tradeoff between the transmission rate of CRSN and the secrecy outage probability of the primary network. In addition, we analyze the PUs' secrecy rate for the asymptotic scenarios and derive closed-form expression of the SN's transmission outage probability. Extensive simulations are implemented to evaluate the proposed strategy. We investigate the effects of the spectrum sensing time, target detection probability and the PUs' secrecy outage probability on the SN's average throughput. Simulation results show that: (1) the performance of the SN's average throughput in the proposed strategy outperforms the conventional overlay strategy; (2) the primary confidential messages will be protected, and the SN can access the licensed spectrum with permitting limited spectrum sensing error probability.

The rest of this paper is organized as follows. Section 2 describes the system model, as well as the four system states. Section 3 interprets the proposed strategy. The optimal power allocation problem is formulated and solved in this section. In Section 4, we give a further discussion for the power allocation scheme and investigate the performance tradeoff between the transmission rate of CRSN and the secrecy outage probability of the primary network. We conduct extensive simulations in Section 5, and Section 6 concludes the paper.

2. System Model

In this system, a CRSN coexists with a primary network, as shown in Figure 1. The CRSN consists of a SN and a sink node (AN), in which the SN needs to periodically deliver its sensing information to the AN. The primary network consists of a primary transmit (PT) and a primary receiver (PR). In addition, there is an eavesdropper (EV), who eavesdrops on the primary confidential information.

We assume that the eavesdropper is known to the primary network. This assumption is valid when the eavesdropper is a legitimate user that is untrusted by the primary network and can eavesdrop on the confidential messages or transmit and receive its own messages in the different time slots [31–35]. In this system, the CRSN lacks spectrum resources and needs to share the licensed spectrum for its data transmission through spectrum sensing. Due to the inevitable spectrum sensing errors, the SN's transmission will interfere with the EV [36], and we can utilize the interference on the EV to protect the primary confidential messages. Therefore, in the proposed strategy, the confidential messages of the primary network can be protected, and as a reward, the primary network will permit limited spectrum sensing error probability.

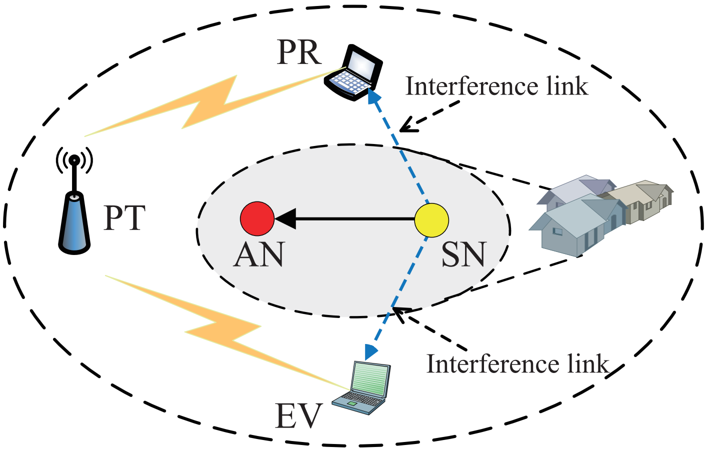


Figure 1. The system model of the proposed strategy.

We assume that the upper layer data packets are divided into equal frames, and the duration of each frame is T. Both the primary network and CRSN experience stationary, ergodic, independent and block Rayleigh fading [37], which indicates that the channel state will be invariant within a frame, but independently vary from one frame to another. The channel power gains of $PT \to PR$, $PT \to EV$, $PT \to SN$, $PT \to AN$, $SN \to PR$, $SN \to EV$ and $SN \to AN$ are denoted as g_{tr}, g_{te}, g_{ts}, g_{ta}, g_{sr}, g_{se} and g_{sa}, respectively, and they are assumed to follow exponential distributions with parameters σ_{tr}^2, σ_{te}^2, σ_{ts}^2, σ_{ta}^2, σ_{sr}^2, σ_{se}^2 and σ_{sa}^2, respectively. We assume that all noise variables in the system are cyclic symmetry complex Gaussian random variables with zero-mean and unit variance. The power budgets of the PT and SN are denoted as P_b and P_s, respectively. To guarantee the security of the primary confidential messages, Wyner's wiretap encoding scheme is adopted in this system, which indicates that the transmission rate and secrecy rate of the confidential messages are set as R_t and R_{sec}, respectively. The difference between R_t and R_{sec}, denoted as $R_e = R_t - R_{sec}$, is the information redundancy available against eavesdropping. A secrecy outage event occurs when the wiretap channel rate exceeds the information redundancy R_{sec}. We assume that the channel state information (CSI) associated with the primary network and CRSN can be perfectly estimated by the SN and PR, and this CSI information is reliably fed back to the AN and PT, respectively. In addition, since the eavesdropper is a known user, we assume that the CSI associated with the EV is available. This assumption is valid when the eavesdropper is an active user [38], a subscribed user [39], a jammer or a classical eavesdropper [40]. Even for the passive eavesdropper, it also can estimate the CSI through local oscillator power inadvertently leaked from the eavesdropper's receiver radio frequency front-end [41].

The transmission activities of the primary network can be modeled as a binary-hypotheses problem [42]; the channel idle probability is denoted as $P(\mathcal{H}_0)$, and the channel busy probability is denoted as $P(\mathcal{H}_1)$, where H_0 denotes that the spectrum is idle and H_1 denotes that the spectrum is occupied. In this system, the SN firstly senses the licensed spectrum with the energy detection method during the first τ part of each frame [43]. The false alarm probability and the detection probability are given by:

$$\begin{cases} p_f = Q\left(\left(\frac{\varepsilon}{\sigma^2} - 1\right)\sqrt{\tau f_s}\right), \\ p_d = Q\left(\left(\frac{\varepsilon}{\sigma^2} - \gamma - 1\right)\sqrt{\frac{\tau f_s}{2\gamma+1}}\right) \end{cases} \tag{1}$$

where $Q(x) = \frac{1}{2\pi}\int_x^{+\infty} e^{-\frac{t^2}{2}} dt$, γ is the received signal-to-noise ratio (SNR), f_s is the sampling frequency, ε is the detection threshold and $\sigma^2 = 1$ is the noise variance.

According to the PT's activities and spectrum sensing results, there are four system states, which are listed as below:

$State0$: the spectrum is idle and detected as idle;
$State1$: the spectrum is occupied and detected as idle;
$State2$: the spectrum is idle and detected as busy;
$State3$: the spectrum is occupied and detected as busy.

In $State0$ and $State2$, the spectrum is idle, and the SN can communicate with the AN freely. In $State1$ and $State3$, the SN should transmit with optimal power to protect the PT's confidential messages. In return, the primary network tolerates limited spectrum sensing error probability. In the next section, we will carefully interpret the proposed strategy.

3. The Reciprocally-Benefited Secure Transmission Strategy

In this section, we firstly analyze the SN's transmission rate and the primary secrecy rate for each state. Then, we optimally allocate the SN's transmit power for each state, so that the average transmission rate of the SN is maximized under the constraint of the maximum permitted primary secrecy outage probability.

3.1. Problem Formulation

In $State0$, the SN can correctly detect the spectrum state as idle with probability:

$$P_0 = P(H_0)\left(1 - p_f\right). \tag{2}$$

Then, the SN accesses the spectrum and transmits with rate $R_s^{(0)}$, which is given by:

$$R_s^{(0)} = \frac{T-\tau}{T}\log_2\left(1 + g_{sa}p_s^{(0)}\right) \tag{3}$$

where $p_s^{(0)}$ is the SN's transmit power in this state. Since the PT stops its transmission, the secrecy rate of this state is zero.

In $State1$, the spectrum is occupied and incorrectly detected as idle with probability:

$$P_1 = P(H_1)(1 - p_d). \tag{4}$$

Under the interference from the PT, the SN transmits with power $p_s^{(1)}$ and achieves rate $R_s^{(1)}$, which is given by:

$$R_s^{(1)} = \frac{T-\tau}{T}\log_2\left(1 + \frac{g_{sa}p_s^{(1)}}{1 + g_{ta}P_b}\right). \tag{5}$$

The SN's transmission will interfere with the EV, and the secrecy rate of the primary network is:

$$\begin{aligned} R_b^{(1)} \;=\; & \left(\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b)-\log_2(1+g_{te}P_b)\right)\right. \\ & \left.+\frac{T-\tau}{T}\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(1)}}\right)-\log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(1)}}\right)\right)\right)^{+} \end{aligned} \tag{6}$$

where the first and second items in Equation (6) are the secrecy rates during the spectrum sensing phase and data transmission phase in *State*1, respectively.

In *State*2, the spectrum is idle and incorrectly detected as busy with probability:

$$P_2 = P\left(H_0\right)p_f. \tag{7}$$

In this state, the SN will transmit with power $p_s^{(2)}$ and achieve rate $R_s^{(2)}$, which is given by:

$$R_s^{(2)} = \frac{T-\tau}{T}\log_2\left(1+g_{sa}p_s^{(2)}\right). \tag{8}$$

Since the PT stops its transmission, the secrecy rate of this state is zero.

In *State*3, the PT occupies the spectrum, and the SN detects the PT's transmission with probability:

$$P_3 = P\left(H_1\right)p_d. \tag{9}$$

To protect the PT's transmission, the SN transmits with power $p_s^{(3)}$ and achieves rate $R_s^{(3)}$, which is given by:

$$R_s^{(3)} = \frac{T-\tau}{T}\log_2\left(1+\frac{g_{sa}p_s^{(3)}}{1+g_{ta}P_b}\right). \tag{10}$$

Then, under the interference from the SN, the secrecy rate of the primary network is:

$$\begin{aligned} R_b^{(3)} \;=\; & \left(\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b)-\log_2(1+g_{te}P_b)\right)\right. \\ & \left.+\frac{T-\tau}{T}\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(3)}}\right)-\log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(3)}}\right)\right)\right)^{+}. \end{aligned} \tag{11}$$

where the first and second items are the secrecy rates during the spectrum sensing phase and data transmission phase in *State*3, respectively.

Therefore, the average transmission rate of the SN is given by:

$$\begin{aligned} R_s =& \mathbb{E}\left(R_s^{(0)}P_0+R_s^{(1)}P_1+R_s^{(2)}P_2+R_s^{(3)}P_3\right) \\ =& \mathbb{E}\left(R_s^{(0)}\right)P_0+\mathbb{E}\left(R_s^{(1)}\right)P_1+\mathbb{E}\left(R_s^{(2)}\right)P_2+\mathbb{E}\left(R_s^{(3)}\right)P_3 \end{aligned} \tag{12}$$

where $\mathbb{E}\left(\cdot\right)$ is the expectation operation. Under the SN's interference, the secrecy outage probability of the primary network is:

$$P_{sec}^{out} = \Pr\left(R_b^{(1)} \le R_{sec}\right)P_1 + \Pr\left(R_b^{(3)} \le R_{sec}\right)P_3. \tag{13}$$

To maximize the SN's average transmission rate under the constraint of the primary maximum permitted secrecy outage probability, the optimal power allocation problem is formulated as:

$$\mathbf{P1}: \max_{p_s^{(i)}, i=0,1,2,3} \quad R_s \\ s.t. \quad \begin{cases} P_{sec}^{out} \leq P_{th}, \\ P_{sn}^{ave} \leq P_{av}, \\ 0 \leq p_s^{(i)} \leq P_s, i=0,1,2,3 \end{cases} \tag{14}$$

where P_{th} is the maximum permitted primary secrecy outage probability, P_{av} is the SN's average power budget and P_{sn}^{ave} is the SN's average power consumption, which is given by:

$$P_{sn}^{ave} = \frac{T-\tau}{T}\left(\mathbb{E}\left(p_s^{(0)}\right)P_0 + \mathbb{E}\left(p_s^{(1)}\right)P_1 + \mathbb{E}\left(p_s^{(2)}\right)P_2 + \mathbb{E}\left(p_s^{(3)}\right)P_3\right). \tag{15}$$

3.2. Optimal Power Allocation

In this section, we will solve the optimization problem given in Equation (14) to acquire the optimal power allocation for each system state. Since the secrecy outage probability constraint in Equation (14) is not convex over $\left\{p_s^{(i)}, i=0,1,2,3\right\}$, **P1** cannot be solved through the traditional convex optimization algorithms. To solve this problem, indicator functions $\varphi\left(p_s^{(1)}\right)$ and $\varphi\left(p_s^{(3)}\right)$ are introduced, which are given by:

$$\varphi\left(p_s^{(1)}\right) = \begin{cases} 0, R_b^{(1)} \geq R_c, \\ 1, R_b^{(1)} < R_c \end{cases} \tag{16}$$

and:

$$\varphi\left(p_s^{(3)}\right) = \begin{cases} 0, R_b^{(3)} \geq R_{sec}, \\ 1, R_b^{(3)} < R_{sec} \end{cases} \tag{17}$$

respectively. Since the spectrum sensing time is very short compared with the duration of a frame, we ignore the first items of the right side of $R_b^{(1)}$ and $R_b^{(3)}$ [44,45]. Then, $\check{R}_b^{(1)} \approx R_b^{(1)}$ and $\check{R}_b^{(3)} \approx R_b^{(3)}$ where $\check{R}_b^{(1)}$ and $\check{R}_b^{(3)}$ are given by:

$$\begin{cases} \check{R}_b^{(1)} = \frac{T-\tau}{T}\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(1)}}\right) - \log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(1)}}\right)\right)^+, \\ \check{R}_b^{(3)} = \frac{T-\tau}{T}\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(3)}}\right) - \log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(3)}}\right)\right)^+ \end{cases} \tag{18}$$

respectively. Therefore, the optimal problem **P1** can be rewritten as:

$$\mathbf{P2}: \max_{\substack{p_s^{(i)}, \\ i=0,1,2,3}} R_s \\ s.t. \begin{cases} \mathbb{E}\left(\varphi\left(p_s^{(1)}\right)\right)P_1 + \mathbb{E}\left(\varphi\left(p_s^{(3)}\right)\right)P_3 \leq P_{th}, \\ P_{sn}^{ave} \leq P_{av}, \\ 0 \leq p_s^{(i)} \leq P_s, i=0,1,2,3. \end{cases} \tag{19}$$

The optimal problem **P2** can be solved through the Lagrange dual method [46]. The Lagrange function of **P2** can be derived as:

$$\mathcal{L}\left(p_s^{(1)}, p_s^{(1)}, p_s^{(2)}, p_s^{(3)}\right) = R_s + \mu\left(P_{th} - \left(\varphi\left(p_s^{(1)}\right)\right)P_1 - \left(\varphi\left(p_s^{(3)}\right)\right)P_3\right) + \lambda\left(P_{av} - P_{sn}^{ave}\right). \tag{20}$$

Then, the Lagrange dual function of the maximum problem, denoted by $\mathcal{G}(\lambda,\mu)$, can be formulated as:

$$\begin{aligned} \mathbf{P3}: \quad & \max_{\substack{p_s^{(i)},\\ i=0,1,2,3}} \mathcal{L}\left(\mathbf{p_s^{(0)}}, \mathbf{p_s^{(1)}}, \mathbf{p_s^{(2)}}, \mathbf{p_s^{(3)}}\right) \\ & s.t. \quad 0 \le p_s^{(i)} \le P_s, i = 0,1,2,3. \end{aligned} \tag{21}$$

The dual problem is:

$$\mathbf{P4}: \min_{\lambda,\mu} \mathcal{G}(\lambda,\mu) \qquad s.t.\, \lambda,\mu > 0. \tag{22}$$

Since the optimal variables of $p_s^{(0)}$, $p_s^{(1)}$, $p_s^{(2)}$, $p_s^{(3)}$ corresponding to the four system states are independent of each other, the Lagrange function can be written as:

$$\begin{aligned} \mathcal{L}\left(p_s^{(1)}, p_s^{(1)}, p_s^{(2)}, p_s^{(3)}\right) = & \,\mathbb{E}\left(R_s^{(0)}\right)P_0 + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(0)}\right)P_0\right) \\ & + \mathbb{E}\left(R_s^{(1)}\right)P_1 + \mu\left(P_{th} - \varphi\left(p_s^{(1)}\right)P_1\right) + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(1)}\right)P_1\right) \\ & + \mathbb{E}\left(R_s^{(2)}\right)P_2 + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(2)}\right)P_2\right) \\ & + \mathbb{E}\left(R_s^{(3)}\right)P_3 + \mu\left(P_{th} - \varphi\left(p_s^{(3)}\right)\right)P_3 + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(3)}\right)P_3\right) \\ & - \mu P_{th} - 3\lambda P_{av} \end{aligned} \tag{23}$$

Then, the problem **P3** can be decomposed as:

$$\begin{aligned} \mathbf{P3a}: \quad & \max_{p_s^{(0)}} \mathbb{E}\left(R_s^{(0)}\right)P_0 + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(0)}\right)P_0\right) \\ & s.t. \;\; 0 \le p_s^{(0)} \le P_s, \end{aligned} \tag{24}$$

$$\begin{aligned} \mathbf{P3b}: \quad & \max_{p_s^{(1)}} \mathbb{E}\left(R_s^{(1)}\right)P_1 + \mu\left(P_{th} - \varphi\left(p_s^{(1)}\right)P_1\right) + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(1)}\right)P_1\right) \\ & s.t. \;\; 0 \le p_s^{(1)} \le P_s, \end{aligned} \tag{25}$$

$$\begin{aligned} \mathbf{P3c}: \quad & \max_{p_s^{(2)}} \mathbb{E}\left(R_s^{(2)}\right)P_2 + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(2)}\right)P_2\right) \\ & s.t. \;\; 0 \le p_s^{(2)} \le P_s \end{aligned} \tag{26}$$

and:

$$\mathbf{P3d}: \quad \max_{p_s^{(3)}} \mathbb{E}\left(R_s^{(3)}\right) P_3 + \mu\left(P_{th} - \varphi\left(p_s^{(3)}\right) P_3\right) + \lambda\left(P_{av} - \frac{T-\tau}{T}\mathbb{E}\left(p_s^{(3)}\right) P_3\right)$$
$$s.t.\ \ 0 \le p_s^{(3)} \le P_s. \tag{27}$$

Therefore, the problem can be decomposed into four optimal problems, corresponding to the transmit power $p_s^{(0)}$, $p_s^{(1)}$, $p_s^{(2)}$, $p_s^{(3)}$, respectively.

For $State0$ and $State2$, we firstly derive the partial derivatives of $p_s^{(0)}$ and $p_s^{(2)}$ as:

$$\begin{cases} \dfrac{\partial \mathcal{L}}{\partial p_s^{(0)}} = \dfrac{(T-\tau)\, g_{sa}}{T\left(1+g_{sa}p_s^{(0)}\right)} P_0 - \lambda P_0 \frac{T-\tau}{T}, \\ \dfrac{\partial \mathcal{L}}{\partial p_s^{(2)}} = \dfrac{(T-\tau)\, g_{sa}}{T\left(1+g_{sa}p_s^{(2)}\right)} P_2 - \lambda P_2 \frac{T-\tau}{T}. \end{cases} \tag{28}$$

Applying the Karush–Kuhn–Tucker conditions and setting the partial derivatives equal to zero, we can acquire the SN's transmit power in $State0$ and $State2$ as:

$$\begin{cases} p_s^{(0)} = \left(\frac{1}{\lambda} - \frac{1}{g_{sa}}\right)^+, \\ p_s^{(2)} = \left(\frac{1}{\lambda} - \frac{1}{g_{sa}}\right)^+. \end{cases} \tag{29}$$

For $p_s^{(1)}$ in $State1$, the decomposed optimal problem is:

$$\mathbf{P5}: \max_{p_s^{(1)}} R_s^{(1)} P_1 + \lambda\left(P_{av} - \frac{T-\tau}{T} P_1 p_s^{(1)}\right) + \mu\left(P_{th} - P_1 \varphi\left(p_s^{(1)}\right)\right). \tag{30}$$

Since the value $\varphi\left(p_s^{(1)}\right)$ is determined by $\check{R}_b^{(1)}$ and R_{sec}, the optimal $p_s^{(1)}$ is derived according to the relationship between $\check{R}_b^{(1)}$ and R_{sec}. When $\check{R}_b^{(1)} = R_{sec}$, we can acquire the following equation as:

$$A\left(p_s^{(1)}\right)^2 + Bp_s^{(1)} + C = 0. \tag{31}$$

where $\nu = 2^{\frac{R_{sec}(T-\tau)}{T}}$ and:

$$\begin{cases} A = (\nu - 1)\, g_{sr} g_{se}, \\ B = (\nu - 1)\left(g_{sr} + g_{se}\right) + \left(\nu g_{sr} g_{te} - g_{se} g_{tr}\right) P_b, \\ C = \nu\left(1 + g_{te}P_b\right) - \left(1 + g_{tr}P_b\right). \end{cases} \tag{32}$$

Remark 1. *In the derivation of Equation (18), we assume that* $\check{R}_b^{(1)} \approx R_b^{(1)}$ *and* $\check{R}_b^{(3)} \approx R_b^{(3)}$. *Compared with* $R_b^{(1)}$ *and* $R_b^{(3)}$, *the term* $\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b) - \log_2(1+g_{te}P_b)\right)$ *in* $R_b^{(1)}$ *and* $R_b^{(3)}$ *is ignored. Next, we will evaluate the effect of this assumption and take State*1 *for example. When the information can be securely and reliably transmitted to the primary destination, the effect of this assumption can be evaluated by:*

$$\begin{aligned}\theta^{(1)} &= \frac{\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b)-\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(1)}}\right)\right)}{R_b^{(1)}}\\ &= \frac{1}{1+\frac{T-\tau}{\tau}\times\frac{\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(1)}}\right)-\log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(1)}}\right)\right)}{\left(\log_2(1+g_{tr}P_b)-\log_2(1+g_{te}P_b)\right)}}\\ &\overset{(\mathrm{a})}{\leq} \frac{1}{1+\frac{T-\tau}{\tau}\times\frac{R_{sec}}{\log_2(1+g_{tr}P_b)}}\end{aligned} \tag{33}$$

where in (a)*, we utilize the approximations of:*

$$\begin{cases}\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(1)}}\right)-\log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(1)}}\right)\geq R_{sec},\\ \log_2\left(1+g_{tr}P_b\right)-\log_2\left(1+g_{te}P_b\right)\leq\log_2\left(1+g_{tr}P_b\right).\end{cases} \tag{34}$$

Since the information can be securely and reliably transmitted to the primary destination, $\log_2(1+g_{tr}P_b)\geq R_t > R_{sec}$*. Therefore,*

$$\theta^{(1)} < \frac{\tau}{T}. \tag{35}$$

In addition, as the spectrum sensing time is too short compared with the data transmission time and can be ignored [44,45], therefore $\theta^{(1)}$ *is very small, and we can ignore the term* $\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b)-\log_2(1+g_{te}P_b)\right)$ *in* $R_b^{(1)}$*. Similarly, the term* $\frac{\tau}{T}\left(\log_2(1+g_{tr}P_b)-\log_2(1+g_{te}P_b)\right)$ *in* $R_b^{(3)}$ *can be ignored.*

3.2.1. Equation (31) Has No Root: $B^2-4AC<0$

For this scenario, $\check{R}_b^{(1)}$ is always less than R_{sec}, which means that the primary network will experience secrecy outage even under the assistance of CRSN. Then, the optimal problem can be rewritten as:

$$\mathbf{P6}: \max_{p_s^{(1)}} R_s^{(1)}P_1+\lambda\left(P_{av}-\frac{T-\tau}{T}P_1p_s^{(1)}\right)+\mu\left(P_{th}-P_1\right). \tag{36}$$

Set $l\left(p_s^{(1)}\right) = R_s^{(1)}P_1+\lambda\left(P_{av}-\frac{T-\tau}{T}P_1p_s^{(1)}\right)+\mu\left(P_{th}-P_1\right)$. According to the Karush–Kuhn–Tucker conditions, we can derive:

$$\begin{cases}\frac{dl}{dp_s^{(1)}}<0,\ \text{if}\ p_s^{(1)}=0,\\ \frac{dl}{dp_s^{(1)}}=0,\ \text{if}\ 0\leq p_s^{(1)}\leq P_s,\\ \frac{dl}{dp_s^{(1)}}>0,\ \text{if}\ p_s^{(1)}=P_s.\end{cases} \tag{37}$$

Therefore, the optimal $p_s^{(1)}$ can be acquired as:

$$p_s^{(1)}=\begin{cases}0, & \frac{1}{\lambda}<\frac{1+g_{ta}P_p}{g_{sa}},\\ \frac{1}{\lambda}-\frac{1+g_{ta}P_b}{g_{sa}}, & \frac{1+g_{ta}P_b}{g_{sa}}\leq\frac{1}{\lambda}\leq P_s+\frac{1+g_{ta}P_b}{g_{sa}},\\ P_s, & \frac{1}{\lambda}>P_s+\frac{1+g_{ta}P_b}{g_{sa}}.\end{cases} \tag{38}$$

3.2.2. Equation (31) Has Two Roots: $B^2 - 4AC \geq 0$

For this scenario, Equation (31) has two roots denoted as $p_s^{(1)-}$ and $p_s^{(1)+}$. Let the first-order derivative of the optimal problem **P6** equal zero; the optimal $p_s^{(1)*}$ can be derived as:

$$p_s^{(1)*} = \frac{1}{\lambda} - \frac{1 + g_{ta} P_b}{g_{sa}}. \tag{39}$$

For this scenario, the optimal transmit power of $p_s^{(1)}$ is derived as:

- $p_s^{(1)} = 0$, when $p_s^{(1)-} \leq p_s^{(1)*} \leq 0 \leq p_s^{(1)+} < P_s$, $p_s^{(1)-} < p_s^{(1)*} \leq 0 \leq P_s \leq p_s^{(1)+}$, $p_s^{(1)-} < p_s^{(1)+} \leq p_s^{(1)*} \leq 0 < P_s$ and $p_s^{(1)-} \leq p_s^{(1)*} < p_s^{(1)+} \leq 0 < P_s$.
- $p_s^{(1)} = p_s^{(1)-}$, when $0 < p_s^{(1)*} \leq p_s^{(1)-} \leq P_{pk} < p_s^{(1)+} andf \left(p_s^{(1)*}\right) \leq f\left(p_s^{(1)-}\right)$ and $0 < p_s^{(1)*} \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s andf \left(p_s^{(1)-}\right) \leq f\left(p_s^{(1)*}\right)$.
- $p_s^{(1)} = p_s^{(1)*}$, when $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < p_s^{(1)*} \leq P_s andf \left(p_s^{(1)+}\right) \leq f\left(p_s^{(1)*}\right)$, $p_s^{(1)-} \leq 0 < p_s^{(1)*} \leq p_s^{(1)+} < P_s$, $p_s^{(1)-} \leq 0 < p_s^{(1)*} \leq P_s \leq p_s^{(1)+}$, $0 \leq p_s^{(1)-} < p_s^{(1)*} \leq P_s < p_s^{(1)+}$, $0 < p_s^{(1)*} \leq p_s^{(1)-} \leq P_s < p_s^{(1)+} andf \left(p_s^{(1)*}\right) > f\left(p_s^{(1)-}\right)$, $0 \leq p_s^{(1)-} < p_s^{(1)+} < p_s^{(1)*} \leq P_s andf \left(p_s^{(1)+}\right) \leq f\left(p_s^{(1)*}\right)$, $0 \leq p_s^{(1)-} < p_s^{(1)*} \leq p_s^{(1)+} \leq P_s$, $0 < p_s^{(1)*} \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s andf \left(p_s^{(1)-}\right) > f\left(p_s^{(1)*}\right)$ and $p_s^{(1)-} < p_s^{(1)+} \leq 0 < p_s^{(1)*} \leq P_s$.
- $p_s^{(1)} = p_s^{(1)+}$, when $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*} andf \left(p_s^{(1)+}\right) > f(P_s)$, $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < p_s^{(1)*} \leq P_s andf \left(p_s^{(1)+}\right) > f\left(p_s^{(1)*}\right)$, $0 \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s < p_s^{(1)*} andf \left(p_s^{(1)+}\right) > f(P_s)$ and $0 \leq p_s^{(1)-} < p_s^{(1)+} < p_s^{(1)*} \leq P_s andf \left(p_s^{(1)+}\right) > f\left(p_s^{(1)*}\right)$.
- $p_s^{(1)} = P_s$, when $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*} andf \left(p_s^{(1)+}\right) \leq f(P_s)$,$p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*} andf \left(p_s^{(1)+}\right) \leq f(P_s)$, $p_s^{(1)-} \leq 0 \leq P_s < p_s^{(1)*} \leq p_s^{(1)+}$, $p_s^{(1)-} \leq 0 \leq P_s < p_s^{(1)*} \leq p_s^{(1)+}$, $0 \leq p_s^{(1)-} \leq P_s < p_s^{(1)+} < p_s^{(1)*}$, $0 \leq p_s^{(1)-} \leq P_s < p_s^{(1)*} \leq p_s^{(1)+}$, $0 \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s < p_s^{(1)*} andf \left(p_s^{(1)+}\right) \leq f(P_s)$, $p_s^{(1)-} < p_s^{(1)+} \leq 0 < P_s < p_s^{(1)*}$, $0 < P_s \leq p_s^{(1)-} < p_s^{(1)+} < p_s^{(1)*}$, $0 < P_s \leq p_s^{(1)-} < p_s^{(1)*} \leq p_s^{(1)+}$, $0 < P_s < p_s^{(1)*} \leq p_s^{(1)-} < p_s^{(1)+}$ and $0 \leq p_s^{(1)*} \leq P_s \leq p_s^{(1)-} < p_s^{(1)+}$.

Proof. The derivation process of $p_s^{(1)}$ is shown in Appendix A. □

Similarly, $p_s^{(3)}$ is derived with the same method as $p_s^{(1)}$, which is omitted due to the space limitation. Then, the optimal transmit power for four system states is derived by taking into account the SN's average power constraint, spectrum sensing errors, as well as the primary secure requirement. Next, we will briefly analyze the performance of the proposed strategy.

4. Performance Analysis

In this section, we will give a further discussion for the power allocation strategy. In addition, the performance tradeoff between the transmission rate of CRSN and the secrecy outage probability of the primary network is investigated. Then, we investigate the primary secrecy rate for the asymptotic scenarios and derive the closed-form expression of the SN's transmission outage probability.

4.1. Further Discussion of the SN's Transmit Power

In Section 3.2, we have derived the optimal transmit power for four system states. Now, some further discussions about the power allocation strategy will be given in this section.

- In *State*0 and *State*2, the channel is idle, and the SN will access the licensed spectrum with power $p_s^{(0)}$ and $p_s^{(2)}$, respectively. Under the average transmit power constraint, $p_s^{(0)}$ and $p_s^{(2)}$ are derived through the optimal water-filling method.

- In $State1$ and $State3$, the SN's transmission will affect the secrecy outage probability of the primary network. Since the derivation of $p_s^{(1)}$ is similar with $p_s^{(3)}$, we take $p_s^{(1)}$ for example.

  (1) If $B^2 - 4AC < 0$, the channel quality between the PT and the PR is always worse than the channel quality between the PT and the EV. Under this condition, the primary information security cannot be guaranteed even though the SN optimally allocates its transmit power to interfere with the EV. Therefore, for this case, the SN will access the licensed spectrum with its maximum transmission power as shown in Equation (38).

  (2) If $B^2 - 4AC \geq 0$, there are six cases, which are shown in Appendix A, and we take $p_s^{(1)-} \leq 0 < p_s^{(1)+} \leq P_s$ and $p_s^{(1)-} \leq 0 < p_s^{(1)+} \leq P_s$ for example.

  Case 1: If $p_s^{(1)-} \leq 0 < P_s \leq p_s^{(1)+}$, it indicates that the direct transmission channel quality of the primary network is sufficiently good, and the eavesdropper cannot acquire the primary confidential messages even without the assistance of the SN. In this case, the SN will transmit with its maximum power as shown in Equation (38).

  Case 2: If $p_s^{(1)-} \leq 0 < p_s^{(1)+} \leq P_s$, it indicates that the channel quality between the PT and the PR is neither sufficiently better nor worse than the channel quality between the PT and the EV. In this scenario, the tradeoff between the CRSN's performance and the primary secrecy outage probability constraint needs to be studied. Set $h\left(p_s^{(1)}\right) = R_s^{(1)}P_1 + \lambda\left(P_{av} - \frac{T-\tau}{T}P_1 p_s^{(1)}\right) + \mu P_{th}$ and $f\left(p_s^{(1)}\right) = h\left(p_s^{(1)}\right) - \mu\varphi\left(p_s^{(1)}\right)$. Suppose $\ell = \min\left\{p_s^{(1)*}, P_s\right\}$. Obviously, if the CRSN refuses the cooperation request from the PT, the CRSN can acquire the maximum transmission rate. We can denote μ as the cost that the CRSN has to pay if the secrecy outage probability of the primary network is caused. If $f(\ell) + \mu < f\left(p_s^{(1)*}\right)$, the CRSN will transmit with a large power ℓ to maximize its own performance and, thus, causes a primary secrecy outage because the CRSN only needs to pay a relatively small cost. However, if $f(\ell) + \mu \geq f\left(p_s^{(1)*}\right)$, the CRSN will use a low power $p_s^{(1)*}$ to guarantee the secure transmission of the primary network since the cost due to the secrecy outage is large. Therefore, the performance tradeoff between the transmission rate of the CRSN and the secrecy outage probability of primary network can be acquired.

4.2. Asymptotic Secrecy Rate Analysis

In this section, we will give the asymptotic analysis for the primary secrecy rate under the condition that $P_b \to 0$ and $P_s \to \infty$. In $State1$ and $State3$, the secure capacities of the primary network are:

$$\begin{aligned} R_b^{(i)} &\approx \frac{T-\tau}{T}\left(\log_2\left(1+\frac{g_{tr}P_b}{1+g_{sr}p_s^{(i)}}\right) - \log_2\left(1+\frac{g_{te}P_b}{1+g_{se}p_s^{(1)}}\right)\right)^+ \\ &= \frac{T-\tau}{T}\left(\log_2\left(\frac{1+g_{se}p_s^{(i)}}{1+g_{sr}p_s^{(i)}} \times \frac{1+g_{sr}p_s^{(i)}+g_{bm}P_b}{1+g_{se}p_s^{(i)}+g_{te}P_b}\right)\right)^+, \end{aligned} \tag{40}$$

where $i = 1$ and 3 stand for $State1$ and $State3$, respectively.

4.2.1. $P_b \to 0$

When $P_b \to 0$, the secrecy rate of the primary network can be approximately quantified by its first-order derivative with respect to P_b at $P_b = 0$. Then, the secrecy rate can be acquired as:

$$R_{sec}^{(i)}(P_b) = \dot{R}_{sec}^{(i)}(0)P_b + o(P_b), i = 1, 3, \tag{41}$$

where $\dot{R}_{sec}^{(i)}(0)$ is the first-order derivative at $P_b = 0$ and $o(P_b)$ denotes the high-order item. According to $R_{sec}^{(i)}$ in Section 3.1, the secrecy rate of the primary network can be rewritten as:

$$R_{sec}^{(i)} = \frac{T-\tau}{T}\left(\frac{g_{bm}\left(1+g_{se}p_s^{(i)}\right)-g_{te}\left(1+g_{sr}p_s^{(i)}\right)}{\left(1+g_{sr}p_s^{(i)}\right)\left(1+g_{se}p_s^{(i)}\right)}P_b+o\left(P_b\right)\right)^+, \tag{42}$$

where the first item of Equation (42) is the first derivative of $R_{sec}^{(i)}$. Under this condition, the secrecy rate of the primary network is almost zero. The channel quality between the EV and the primary network and between the EV and the CRSN and the power allocation strategy have almost no effect on the secrecy rate.

4.2.2. $P_s \to \infty$

When $P_s \to \infty$, the average transmit power constraint in **P1** can be removed. Then, the optimal problem can be rewritten as:

$$\mathbf{P6}: \max_{\substack{p_s^{(i)},\\ i=0,1,2,3}} R_s \qquad s.t.\, P_{sec}^{out} \le P_{th}. \tag{43}$$

Adopting the same method in Section 3.2, in *State*0 and *State*1, we can acquire:

$$p_s^{(0)} = p_s^{(2)} = P_s. \tag{44}$$

In *State*1 and *State*3, the optimal power is:

- $B^2 - 4AC < 0$, $p_s^{(1)} = p_s^{(3)} = P_s$.
- $B^2 - 4AC \ge 0$, there are two roots, which are denoted as $p_s^{(1)-}$ and $p_s^{(1)+}$. Set $i = 1,3$. Since $R_s^{(i)}$ is a monotonically-increasing function with respect to $p_s^{(i)}$ and $P_s > p_s^{(1)+}$, $R_s^{(i)}(P_s) > \max\left\{R_s^{(i)}\left(p_s^{(1)-}\right), R_s^{(i)}\left(p_s^{(1)+}\right)\right\}$. Then, if $\max\left\{p_s^{(1)-}, p_s^{(1)+}\right\} > 0$, the optimal power is one value of zero, $p_s^{(i)-}$, $p_s^{(i)+}$ and P_s that can maximize the function $\left(R_s^{(i)} - \mu\varphi\left(p_s^{(i)}\right)\right)$. Otherwise, the optimal power is $p_s^{(i)} = P_s$.

Then, substituting $p_s^{(1)}$ and $p_s^{(3)}$ into Equation (40), we can derive the secrecy rate of the primary network.

4.3. The Outage Probability Analysis of the CRSN

To guarantee the secure transmission of the primary network, the CRSN should dynamically adjust its transmission power. Set the target transmission rate of the SN as R_s. In *State*0 and *State*2, the SN will transmit without the interference from primary network and acquire the transmission rate as $R_s^{(0)}$ and $R_s^{(0)}$, respectively. Set the target transmission rate of the CRSN as R_s. Then, the outage probabilities for *State*0 and *State*2 are:

$$\begin{cases} P_{out}^{(0)} = \Pr\left(R_s^{(0)} < R_s\right) = 1 - \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}}-1}{\sigma_{sh}^2 p_s^{(0)}}\right), \\ P_{out}^{(2)} = \Pr\left(R_s^{(2)} < R_s\right) = 1 - \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}}-1}{\sigma_{sh}^2 p_s^{(2)}}\right), \end{cases} \tag{45}$$

respectively. In *State*1 and *State*3, the SN's transmission will be interfered by the primary network. Then, the outage probabilities corresponding to *State*1 and *State*3 are derived as:

$$\begin{cases} P_{out}^{(1)} = \Pr\left(R_s^{(1)} < R_s\right) = 1 - \frac{\sigma_{bh}^2 \sigma_{sh}^2 p_s^{(1)}}{\left(2^{\frac{TR_s}{T-\tau}} - 1\right)\sigma_{bh}^2 + \sigma_{sh}^2 p_s^{(1)}} \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(1)}}\right), \\ P_{out}^{(3)} = \Pr\left(R_s^{(1)} < R_s\right) = 1 - \frac{\sigma_{bh}^2 \sigma_{sh}^2 p_s^{(3)}}{\left(2^{\frac{TR_s}{T-\tau}} - 1\right)\sigma_{bh}^2 + \sigma_{sh}^2 p_s^{(3)}} \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(3)}}\right). \end{cases} \tag{46}$$

In *State*0, the spectrum is idle and correctly detected with probability as $P_1 = P(H_0)\left(1 - p_f\right)$, and the SN transmits with power $p_s^{(0)}$. In *State*1, the spectrum is occupied and incorrectly detected as idle with probability as $P_1 = P(H_1)(1 - p_d)$, and the SN transmits with power $p_s^{(1)}$. In *State*2, the spectrum is idle and incorrectly detected as busy with probability $P_2 = P(H_0)\, p_f$, and the SN transmits with power $p_s^{(2)}$. In *State*3, the spectrum is occupied and correctly detected with probability $P_3 = P(H_1)\, p_d$, and the SN transmits with power $p_s^{(3)}$. Therefore, the average outage probability of the sensor network is:

$$\begin{aligned} P_{out}^{s} &= P_{out}^{(0)} P_0 + P_{out}^{(1)} P_1 + P_{out}^{(2)} P_2 + P_{out}^{(3)} P_3 \\ &= \left(1 - \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(0)}}\right)\right) P(H_0)\left(1 - p_f\right) \\ &\quad + \left(1 - \frac{\sigma_{bh}^2 \sigma_{sh}^2 p_s^{(1)}}{\left(2^{\frac{TR_s}{T-\tau}} - 1\right)\sigma_{bh}^2 + \sigma_{sh}^2 p_s^{(1)}} \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(1)}}\right)\right) P(H_0)\, p_f \\ &\quad + \left(1 - \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(2)}}\right)\right) P(H_1)(1 - p_d) \\ &\quad + \left(1 - \frac{\sigma_{bh}^2 \sigma_{sh}^2 p_s^{(3)}}{\left(2^{\frac{TR_s}{T-\tau}} - 1\right)\sigma_{bh}^2 + \sigma_{sh}^2 p_s^{(3)}} \exp\left(-\frac{2^{\frac{TR_s}{T-\tau}} - 1}{\sigma_{sh}^2 p_s^{(3)}}\right)\right) P(H_1)\, p_d. \end{aligned} \tag{47}$$

5. Simulation Results

In this section, we will evaluate the performance of the primary network and CRSN. In the simulation, the frame duration T is set to be 50 ms. The path loss of the channel is set to be three. The SN's average power and peak power are set to be 10 dB and 15 dB, respectively. The peak power of the PT is set to be 15 dB. In the simulation, we choose the simulation parameters according to the previous works on wireless sensor networks [47], cognitive radio networks [48] and CRSN [49–51]. In addition, these values are application-specific parameters and will vary according to the demands of the applications and constraints. The simulation assumptions, as well as other previous simulations will contribute to the development of the realistic CRSN architecture. In addition, changing some assumptions, such as the spectrum sensing method, will slightly affect the conclusions in this paper, and therefore, the obtained results in this paper reveal the general effects of the parameters on the performance in CRSN. For the proposed scheme, the critical parameters, such as channel idle probability, the spectrum sensing time, the power budget of the PT and the secrecy outage threshold, which will affect the performance of the proposed strategy, will be investigated in this section.

In Figure 2, we plot the SN's average throughput versus the spectrum idle probability $P(H_0)$. In this figure, we can observe that the SN's average throughput is a monotonically increasing function with respect to $P(H_0)$. The reason is that the large spectrum idle probability indicates that there will be more interference-free spectrum access opportunities for the SN's transmission, and the throughput of the CRSN will increase. In addition, more time allocated for spectrum sensing will result in less time for the SN's transmission. Therefore, the average throughput of the SN will decrease. The throughput of the CRSN will decrease when a long time is allocated for spectrum sensing even through the detection probability will increase. Moreover, we also plot the traditional overlay scheme for contrast. Since the overlay scheme does not consider the cooperation between the primary network and the CRSN, the CRSN may be interfered by the PT when the occupied spectrum is detected as idle or miss the idle spectrum opportunity when the idle spectrum is detected as busy. Therefore, the throughput of the overlay scheme is lower than our proposed strategy.

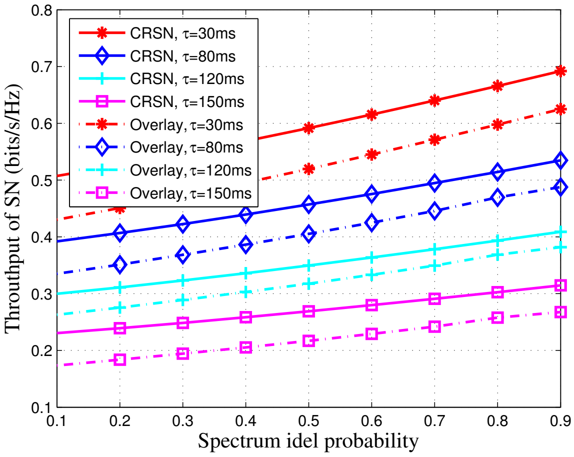


Figure 2. SN's average throughput of the proposed strategy as a function of the spectrum idle probability. The transmit power of the primary transmit (PT) is set to $P_b = 15$ dB, and the target secrecy outage probability is set to $P_{th} = 0.1$.

In Figure 3, we show the SN's average throughput of the proposed scheme versus the spectrum sensing time and the target detection probability. In this figure, we can observe that SN's rate will decrease when more time is consumed for spectrum sensing. The reason is that when more time is allocated for spectrum sensing, there will be less time for the SN's data transmission. Since $p_s^{(0)} = p_s^{(2)}$ and $p_s^{(1)} = p_s^{(3)}$, the average rate is $R_s = 2P\left(H_0\right)\mathbb{E}\left(R_s^{(0)}\right) + 2P\left(H_1\right)\mathbb{E}\left(R_s^{(1)}\right)$, which is not a function of the target detection probability. Therefore, the SN's average rate will keep the same when the target detection probability changes.

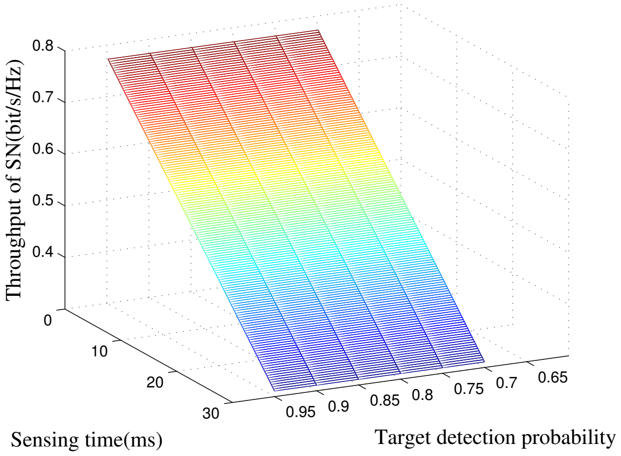


Figure 3. SN's average throughput of the proposed strategy as a function of the spectrum sensing time and target detection probability. The spectrum idle probability is set to $P\left(H_0\right)$, the transmit power of the PT is set to $P_b = 15$ dB, and the target secure outage probability is set to $P_{th} = 0.1$.

In Figure 4, we show the SN's average rate versus the spectrum sensing time τ and the spectrum idle probability $P(H_0)$. In this figure, we can observe that the SN's average rate is a monotonically-increasing function with respect to $P(H_0)$. The reason is that a large value of the spectrum idle probability indicates that there will be more interference-free spectrum access opportunities for the SN's transmission regardless of the security requirement of the primary network. In addition, the long spectrum sensing time indicates that the SN occupies a short time for information transmission, and the throughput will decrease.

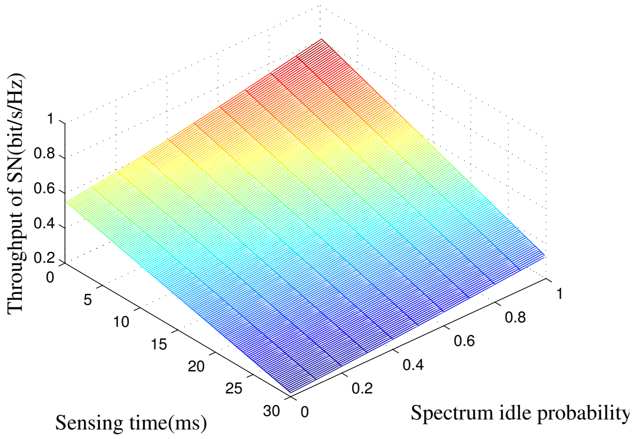


Figure 4. SN's average throughput of the proposed strategy as a function of the spectrum sensing time and spectrum idle probability. The transmit power of the BS is set to $P_p = 15$ dB, and the target secure outage probability is set to $P_{th} = 0.1$.

In Figure 5, we show the SN's average throughput versus the spectrum idle probability $P(H_0)$ and the target secrecy outage probability P_{th}. A small value of P_{th} indicates that the secrecy outage probability constraint is stringent. Then, the SN has to spend more power to interfere with the eavesdropper and guarantee the secure transmission of the primary network. Therefore, the throughput of the SN will decrease. In addition, more power allocated for the SN's data transmission will result in the increasing of the SN's throughput. A large value of $P(H_0)$ indicates that there are more interference-free spectrum access opportunities regardless of the security requirement of the primary network. Under this condition, the SN can transmit with large power and achieve high transmission throughput.

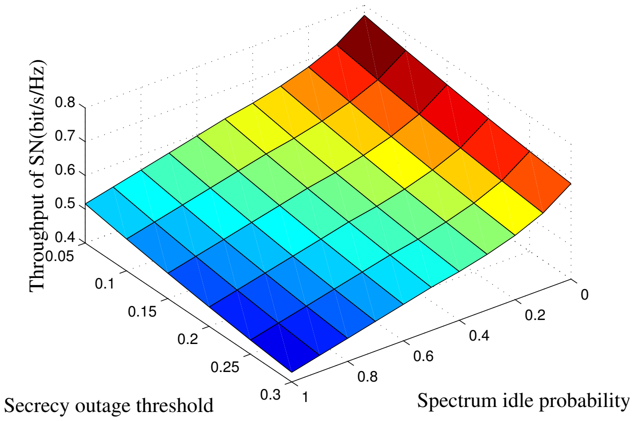


Figure 5. SN's average throughput of the proposed strategy as a function of the target secrecy outage probability and spectrum idle probability. The transmit power of the PT is set to $P_b = 15$ dB, and the spectrum sensing time is set to $\tau = 1$ ms.

In Figure 6, we show the SN's average rate versus the PT's transmit power P_b and the spectrum idle probability $P(H_0)$. A large value P_b indicates that there will be more power consumed for the primary network to guarantee its secure transmission. Then, the SN will consume less power to cooperate with the primary network, which contributes to increasing the SN's throughput. In addition, when P_b is large, the detection probability will improve, and the CRSN can fully utilize the spectrum and optimally control its transmit power to maximize its throughput.

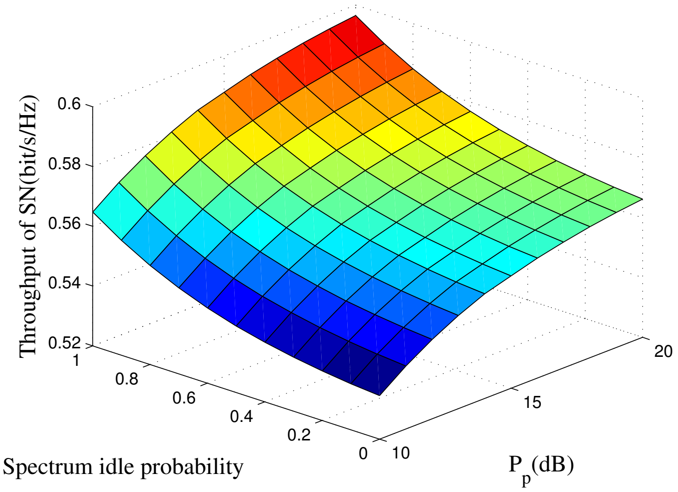


Figure 6. SN's average throughput of the proposed strategy as a function of the PT's transmit power P_b and spectrum sensing time τ. The idle probability is set to $P(H_0) = 0.8$, and the target secrecy outage probability is set to $P_{th} = 0.1$.

6. Conclusions

In this paper, we proposed a cooperative secure transmission strategy, which would benefit both the primary network and the CRSN. In this strategy, the SN's transmission would protect primary information security, and as a reward, limited spectrum sensing error probability was permitted. Based on the primary activities and spectrum sensing results, there were four system states in the system. In each state, we analyzed the SN's transmission rate and the primary secrecy rate and, then, optimally allocated the SN's transmit power to maximize the SN's average rate under the constraint of the maximum permitted primary secrecy outage probability. In addition, we gave further discussion for the power allocation strategy and the performance tradeoff between the transmission rate of the CRSN, and the secrecy outage probability of the primary network was investigated. Moreover, we investigated the primary secrecy rate for the asymptotic scenarios and derived closed-form expression of the SN's transmission outage probability. Simulation results showed that: (1) the performance of the SN's average throughput in the proposed strategy outperformed the conventional overlay strategy; (2) the primary confidential messages were protected, and the QoS requirement of the CRSN is satisfied.

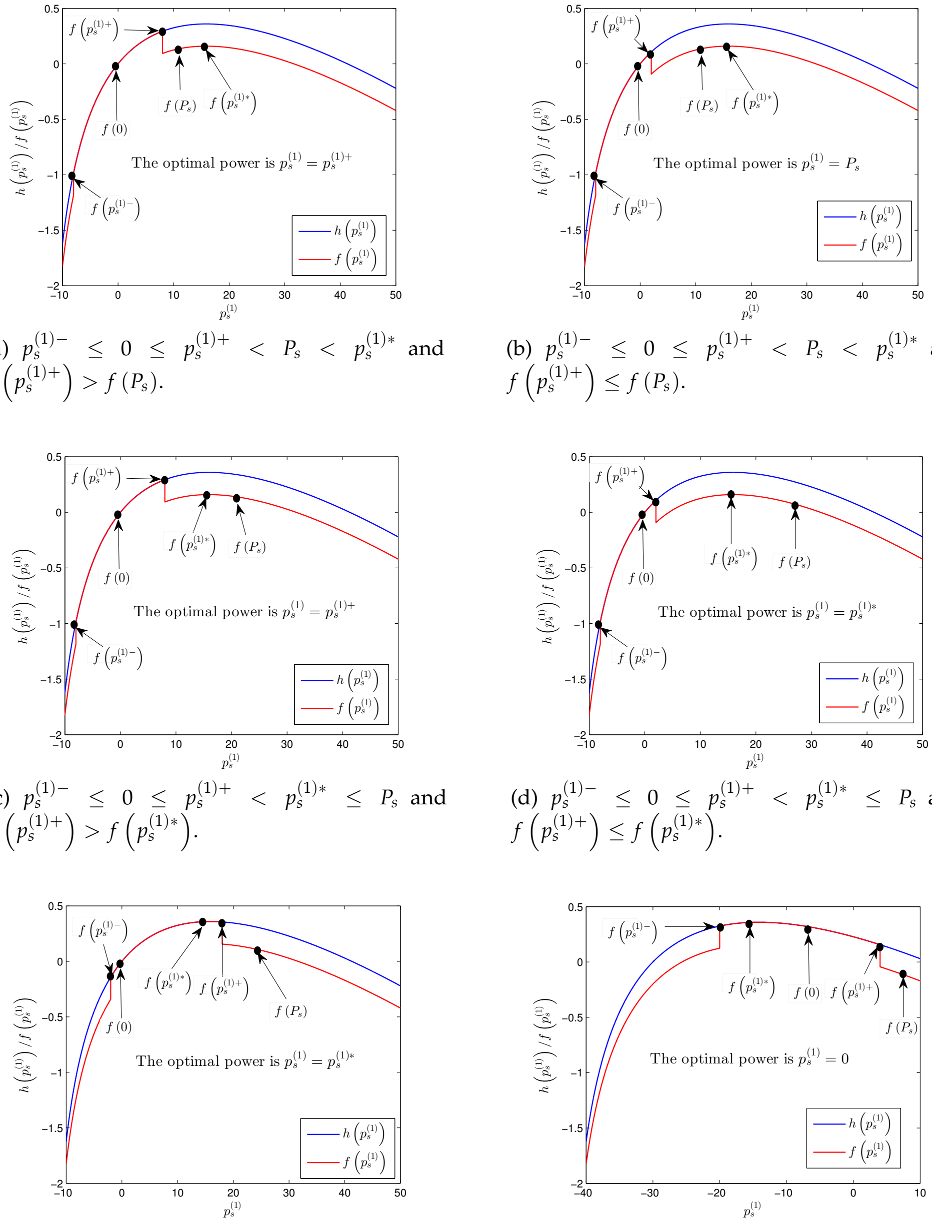
Acknowledgments: The research work reported in this paper is supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61431011, the National Hi-Tech Research and Development Program of China (863) under Grant No. 2014AA01A707, the Key laboratory of wireless sensor network and communication, Chinese Academy of Sciences (No. 2015003) and the Fundamental Research Funds for the Central Universities.

Author Contributions: D.W. conceived of the study, proposed the idea, designed the specific scheme and drafted the manuscript. P.R. participated in the coordination of the research and searched for funding to support the work. Q.D. coordinated the research and corrected the manuscript. Y.W. and L.S. proofread the manuscript. All authors read and approved the final manuscript.

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

Appendix A. The Derivation Process of $p_s^{(1)}$

Set $h\left(p_s^{(1)}\right) = R_s^{(1)} P_1 + \lambda\left(P_{av} - \frac{T-\tau}{T} P_1 p_s^{(1)}\right) + \mu P_{th}$ and $f\left(p_s^{(1)}\right) = h\left(p_s^{(1)}\right) - \mu\varphi\left(p_s^{(1)}\right)$. Then, there are six cases in the derivation of the optimal transmit power. In Figure A1, we only show the first case, and the other five cases are similar to this case.



(a) $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*}$ and $f\left(p_s^{(1)+}\right) > f\left(P_s\right)$.

(b) $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*}$ and $f\left(p_s^{(1)+}\right) \leq f\left(P_s\right)$.

(c) $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < p_s^{(1)*} \leq P_s$ and $f\left(p_s^{(1)+}\right) > f\left(p_s^{(1)*}\right)$.

(d) $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < p_s^{(1)*} \leq P_s$ and $f\left(p_s^{(1)+}\right) \leq f\left(p_s^{(1)*}\right)$.

(e) $p_s^{(1)-} \leq 0 < p_s^{(1)*} \leq p_s^{(1)+} < P_s$.

(f) $p_s^{(1)-} \leq p_s^{(1)*} \leq 0 \leq p_s^{(1)+} < P_s$.

Figure A1. Illustration of $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s$.

- $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s$: If $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < P_s < p_s^{(1)*}$ and $f\left(p_s^{(1)+}\right) > f\left(P_s\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)+}$, which is shown in Figure A1a. Otherwise, if $f\left(p_s^{(1)+}\right) \leq f\left(P_s\right)$, the optimal transmit power is $p_s^{(1)} = P_s$, which is shown in Figure A1b. If $p_s^{(1)-} \leq 0 \leq p_s^{(1)+} < p_s^{(1)*} \leq P_s$ and $f\left(p_s^{(1)+}\right) > f\left(p_s^{(1)*}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)+}$, which is shown in Figure A1c. Otherwise, if $f\left(p_s^{(1)+}\right) \leq f\left(p_s^{(1)*}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$, which is shown in Figure A1d. If $p_s^{(1)-} \leq 0 < p_s^{(1)*} \leq p_s^{(1)+} < P_s$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$, which is shown in Figure A1e. If $p_s^{(1)-} \leq p_s^{(1)*} \leq 0 \leq p_s^{(1)+} < P_s$, the optimal transmit power is $p_s^{(1)} = 0$, which is shown in Figure A1f.

- $p_s^{(1)-} \leq 0 \leq P_s \leq p_s^{(1)+}$: If $p_s^{(1)-} \leq 0 \leq P_s \leq p_s^{(1)+} < p_s^{(1)*}$ or $p_s^{(1)-} \leq 0 \leq P_s < p_s^{(1)*} \leq p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = P_s$. If $p_s^{(1)-} \leq 0 < p_s^{(1)*} \leq P_b \leq p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. If $p_s^{(1)-} < p_s^{(1)*} \leq 0 \leq P_s \leq p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = 0$.
- $0 \leq p_s^{(1)-} \leq P_s < p_s^{(1)+}$: If $0 \leq p_s^{(1)-} \leq P_s < p_s^{(1)+} < p_s^{(1)*}$ or $0 \leq p_s^{(1)-} \leq P_s < p_s^{(1)*} \leq p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = P_s$. If $0 \leq p_s^{(1)-} < p_s^{(1)*} \leq P_s < p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = (1)*$. If $0 < p_s^{(1)*} \leq p_s^{(1)-} \leq P_s < p_s^{(1)+}$ and $f\left(p_s^{(1)*}\right) > f\left(p_s^{(1)-}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. Otherwise, if $f\left(p_s^{(1)*}\right) \leq f\left(p_s^{(1)-}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)-}$.
- $0 \leq p_s^{(1)-} < p_s^{(1)+} \leq P_b$: If $0 \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s < p_s^{(1)*}$ and $f\left(p_s^{(1)+}\right) > f\left(P_s\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)+}$. Otherwise, if $f\left(p_s^{(1)+}\right) \leq f\left(P_s\right)$, the optimal transmit power is $p_s^{(1)} = P_s$. If $0 \leq p_s^{(1)-} < p_s^{(1)+} < p_s^{(1)*} \leq P_s$ and $f\left(p_s^{(1)+}\right) > f\left((1)*\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)+}$. Otherwise, if $f\left(p_s^{(1)+}\right) \leq f\left(p_s^{(1)*}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. If $0 \leq p_s^{(1)-} < p_s^{(1)*} \leq p_s^{(1)+} \leq P_s$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. If $0 < p_s^{(1)*} \leq p_s^{(1)-} < p_s^{(1)+} \leq P_s$ and $f\left(p_s^{(1)-}\right) > f\left(p_s^{(1)*}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. Otherwise, if $f\left(p_s^{(1)*}\right) \leq f\left(p_s^{(1)-}\right)$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)-}$.
- $p_s^{(1)-} < p_s^{(1)+} \leq 0 < P_s$: If $p_s^{(1)-} < p_s^{(1)+} \leq 0 < P_s < p_s^{(1)*}$, the optimal transmit power is $p_s^{(1)} = P_s$. If $p_s^{(1)-} < p_s^{(1)+} \leq 0 < p_s^{(1)*} \leq P_s$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$. If $p_s^{(1)-} < p_s^{(1)+} \leq p_s^{(1)*} \leq 0 < P_s$ or $p_s^{(1)-} \leq p_s^{(1)*} < p_s^{(1)+} \leq 0 < P_s$, the optimal transmit power is $p_s^{(1)} = 0$.
- $0 < P_b \leq p_s^{(1)-} < p_s^{(1)+}$: If $0 < P_s \leq p_s^{(1)-} < p_s^{(1)+} < p_s^{(1)*}$, $0 < P_s \leq p_s^{(1)-} < p_s^{(1)*} \leq p_s^{(1)+}$ or $0 < P_s < p_s^{(1)*} \leq p_s^{(1)-} < p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = P_s$. If $0 \leq p_s^{(1)*} \leq P_b \leq p_s^{(1)-} < p_s^{(1)+}$, the optimal transmit power is $p_s^{(1)} = p_s^{(1)*}$.

Therefore, the $p_s^{(1)}$ for this scenario is derived.

References

1. Oliveira, L.M.L.; Rodrigues, J.J.P.C. Wireless sensor networks: A survey on environmental monitoring. *J. Commun.* **2011**, *6*, 143–151.
2. Shen, H.; Li, Z.; Qin, C. Efficient data collection for large-scal mobile monitoring applications. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 1424–1436.
3. Langhammer, N.; Kays, R. Performance evaluation of wireless home automation networks in indoor scenarios. *IEEE Trans. Smart Grid* **2012**, *3*, 2252–2261.
4. Suryadevara, N.K.; Mukhopadhyay, S.C.; Kelly, S.D.T.; Gill, S.P.S. WSN-based smart sensors and actuator for power management in intelligent buildings. *IEEE/ASME Trans. Mechatron.* **2015**, *20*, 564–571.
5. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *IEEE Commun. Mag.* **2002**, *40*, 101–114.
6. Chiara, B.; Andrea, C.; Davide, D.; Roberto, V. An overview on wireless sensor networks technology and evolution. *Sensors* **2009**, *9*, 6869–6896.
7. Baker, S.D.; King, S.W.; Welch, J.P. Performance measures of ISM-band and conventional telemetry. *IEEE Eng. Med. Biol. Mag.* **2004**, *23*, 27–36.
8. Mitola, J.; Maguire, G.Q. Cognitive radio: Making software radios more personal. *IEEE Pers. Commun.* **1999**, *6*, 13–18.

9. Zhang, W.; Mallik, R.K.; Letaief, K. Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 5761–5766.
10. Liang, Y.C.; Zeng, Y.; Peh, E.C.Y.; Hoang, A.T. Sensing-throughput tradeoff for cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1326–1337.
11. Akan, O.B.; Karli, O.B.; Ergul, O. Cognitive radio sensor networks. *IEEE Netw.* **2009**, *23*, 3369–3380.
12. Asokan, A.; Ayyappadas, R. Survey on cognitive radio and cognitive radio sensor networks. In Proceedings of the 21st IEEE International Conference on Electronics Circuits and Systems (ICECS-2014), Marseille, France, 7–10 December 2014; pp. 1–7.
13. Deng, R.; Chen, J.; Yen, C.; Cheng, P.; Sun, Y. Energy-efficient cooperative spectrum sensing by optimal scheduling in sensor-aided cognitive radio networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 716–725.
14. Han, J.A.; Jeon, W.S.; Jeong, D.G. Energy-efficient channel management scheme for cognitive radio sensor networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 1905–1920.
15. Jamal, A.; Than, C.K.; Wong, W.C. CR-WSN MAC: An energy efficient and spectrum aware MAC protocol for cognitive radio sensor network. In Proceedings of the 9th International Conference on Cognitive Radio Oriented Wireless Networks, Oulu, Finland, 2–4 June 2014; pp. 67–72.
16. Liang, Z.; Feng, S.; Zhao, D.; Shen, X. Delay performance analysis for supporting real-time traffic in a cognitive radio sensor network. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 325–335.
17. Chen, Y.; Woo, W.L.; Wang, C.X. Channel modeling of information transmission over cognitive interrogator-sensor networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 2–15.
18. Lin, S.C.; Chen, K.C. Improving spectrum efficiency via in-network computations in cognitive radio sensor networks. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1222–1234.
19. Gulbahar, B.; Akan, O.B. Information theoretical optimization gains in energy adaptive data gathering and relaying in cognitive radio sensor networks. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1788–1797.
20. Wyner, A.D. The wirThe wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
21. Zou, Y.; Zhu, J.; Yang, L.; Liang, Y.C.; Yao, Y.D. Securing physical-layer communications for cognitive radio networks. *IEEE Commun. Mag.* **2015**, *53*, 1788–1797.
22. Yang, J.; Kim, I.M.; Kim, D.I. Power-constrained optimal cooperative jamming for multiuser broadcast channel. *IEEE Wirel. Commun. Lett.* **2013**, *2*, 411–414.
23. Sun, L.; Ren, P.; Du, Q.; Wang, Y.; Gao, Z. Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Commun. Lett.* **2015**, *19*, 463–466.
24. Xu, Q.; Ren, P.; Du, Q.; Sun, L. Secure Secondary Communications with Curious Primary Users in Cognitive Underlay Networks. In Proceedings of the IEEE Vehicular Technology Conference (VTC-Spring), Nanjing, China, 15–18 May 2016; pp. 1–5.
25. Park, K.H.; Wang, T.; Alouini, M.S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1741–1751.
26. Liau, Q.Y.; Leow, C.Y.; Ding, Z. Physical layer security rsing two-path successive relaying. *Sensors* **2016**, *16*, 846.
27. Bassily, R.; Ulukus, S. Deaf cooperative and relay selection strategies for secure communication in multiple relay networks. *IEEE Trans. Signal Process.* **2013**, *61*, 1544–1554.
28. Mokari, N.; Parsaeefard, S.; Saeedi, H.; Azmi, P. Cooperative seure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1085–1073.
29. Zhang, N.; Lu, N.; Cheng, N.; Mark, J.W.; Shen, X. Cooperative sepctrum access towards secure information transfer for CRN. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2453–2464.
30. Stanojev, I.; Yener, A. Improving secrecy rate via spectrum leasing for friendly jamming. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 134–145.
31. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888.
32. Li, J.; Petropulu, A.P.; Weber, S. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process.* **2011**, *59*, 4985–4996.
33. Yang, Y.; Li, Q.; Ma, W.; Ge, J.; Ching, P.C. Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. *IEEE Signal Process. Lett.* **2013**, *20*, 35–38.
34. Wang, H.-M.; Luo, M.; Yin, Q.; Xia, X.-G. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 2007–2020.

35. Fakoorian, S.A.A.; Swindlehurst, A.L. Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer. *IEEE Trans. Signal Process.* **2011**, *59*, 5013–5022.
36. Zhang, R.; Song, L.; Han, Z.; Jiao, B. Physical layer security for two-way untrusted relaying with friendly jammers. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3693–3704.
37. Sun, L.; Zhang, T.; Li, Y.; Niu, H. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3801–3807.
38. Gopala, P.K.; Lai, L.; Gamal, H.E. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4686–4698.
39. Chorti, A.; Perlaza, S.M.; Han, Z.; Poor, H.V. On the resilience of wireless multiuser networks to passive and active eavesdroppers. *IEEE J. Sel. Areas Commun.* **2012**, *31*, 1850–1863.
40. Zhou, X.; Maham, B.; Hjorunges, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907.
41. Mukherjee, A.; Swindlehurst, A.L. Detecting passive eavesdroppers in the MIMO wiretap channel. In Proceedings of the 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2012), Kyoto, Japan, 25–30 March 2012; pp. 2809–2812.
42. Wang, Y.; Ren, P.; Gao, F.; Su, Z. A hybrid underlay/overlay transmission mode for cognitive radio netwroks with statistical quality-of-service provisioning. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1482–1498.
43. Wang, Y.; Ren, P.; Du, Q.; Zhang, C. Optimal resource allocation for spectrum sensing based cognitive radio networks with statistical QoS guarantees. *Mobile Netw. Appl.* **2012**, *17*, 711–720.
44. Fanous, A.; Ephremides, A. Ephremides, Access schemes for mitigating the effects of sensing errors in cognitive wireless netowrks. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 3343–3352.
45. Shafie, A.E. Cognitive access protocol for alleviating sensing errors in cognitive multiple-access systems. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 297–300.
46. Boyd, S.; Vandenberghe, L. *Vandenberghe, Convex Optimization*; Cambridge University Press: London, UK, 2004.
47. Wang, X.; Berger, T. Spatial channel reuse in wireless sensor networks. *Wirel. Netw.* **2008**, *14*, 133–146.
48. Lee, W.-Y.; Akyildiz, I.F. Optimal spectrum sensing framework for cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 3845–3857.
49. Oto, M.C.; Akan, B. Energy-efficient packet size optimization for cognitive radio sensor networks. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1544–1553.
50. Shah, G.A.; Alagoz, F.; Fadel, E.A.; Akan, O.B. A spectrum-aware clustering for efficient multimedia routing in cognitive radio sensor networks. *IEEE Trans. Veh. Technol.* **2014**, *63*, 3369–3380.
51. Ozger, M.; Fadel, E.; Akan, O.B. Event-to-sink spectrum-aware clustering in mobile cognitive radio sensor networks. *IEEE Trans. Mob. Comput.* **2016**, *15*, 2221–2233.