sensors

Article

Cooperative Jammer Selection for Secrecy Improvement in Cognitive Internet of Things

Ping Xie [1], Ling Xing [1], Honghai Wu [1], Jung Taek Seo [2] and Ilsun You [2,*]

[1] Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China; xieping_1984@bupt.edu.cn (P.X.); xingling_my@163.com (L.X.); whh1010@gmail.com (H.W.)
[2] Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, Korea; seojt@sch.ac.kr
* Correspondence: ilsunu@gmail.com

Received: 29 October 2018; Accepted: 28 November 2018; Published: 4 December 2018

Abstract: Smart homes can improve the quality of life and be implemented by Internet of Things (IoT) technologies. However, security is a very important issue in smart homes. For this reason, we propose a secrecy transmission protocol for primary user (PU) by selecting friendly jammer in cognitive IoT model. In particular, a secondary transmitter (ST) is selected to transmit secondary signals by the PU's frequency spectrum, while another ST is chosen to transmit artificial noise to protect the transmission confidentiality of the PU against eavesdropping. Moreover, two selection schemes are presented to confirm the former and the latter ST, and the goal is to optimize the secondary transmission performance and the primary security performance, respectively. For the non-security model and the proposed protocol, we derive the closed-form expressions of the intercept probability and the outage probability for the PU. We also obtain the closed-form expression of outage probability for the secondary user. The numerical results show that the security performance of the PU is significantly enhanced in our protocol compared to the non-security model. In addition, the outage performance of the secondary users is also improved in high secondary transmit SNR region.

Keywords: aided opportunistic jamming; artificial noise; cognitive Internet of things; intercept probability; physical layer security

1. Introduction

The Internet of Things (IoT) is an emerging wireless application [1] and has many applications [2,3]. Many techniques for IoT have arisen in recent years such as adaptive monitoring techniques [4–6]. Moreover, IoT technologies can implement smart homes, which can improve the quality of life. However, the security and privacy problems are very important in smart homes [7] and have received significant interest [8–12]. Furthermore, combining cognitive radio technique and IoT, Cognitive Internet of Things (CIoT) is proposed, which is an enhanced IoT paradigm. However, the available bandwidth for IoT is very limited. Thus, the spectrum efficiency is a key issue for IoT design [13,14]. To improve the utilization efficiency of radio spectrum, Cognitive Radio (CR) [15] is a promising technology [16]. In Cognitive Radio Networks (CRN), unlicensed users opportunistically access to the licensed spectrum band [17]. Furthermore, unlicensed users cannot harm the performance of primary users. However, since the spectrum access is dynamic and the communication mode is broadcast communication in wireless communication, any unlicensed users and eavesdroppers can have access to the shared spectrum. Therefore, the eavesdroppers readily overhear any active transmissions over wireless networks. However, cognitive radio technology also introduces some new security threats, e.g., using the shared spectrum by selfish behavior, reporting false sensing information, etc. Therefore, ensuring security is a key issue in CIoT.

To ensure security, physical-layer security technology is an effective confidentially protection mechanism [18–22]. In Ref. [23], when the wiretap channel condition between a source node and an eavesdropper node is worse than the channel condition between the source node and the destination node, the source node can successfully communicate with the destination node in perfect secrecy. Ref. [22] emphasized that both the primary users (PUs) and secondary users (SUs) must be defended from eavesdropping in cognitive networks. Specifically, it is legitimate that the SUs are allowed to access the primary spectrum by cooperating with the PUs, where the SUs act as a relay or a friendly jammer to elevate the PU's secrecy [24]. Some studies [25,26] reveal that resource allocation is an efficient approach to ensure the PU's security requirement while achieving good transmission performance for the SUs who cooperate with the PUs. In addition, both the secure communications for PUs and SUs are considered in Ref. [25]. In contrast, Refs. [27–29] studied some transmission schemes to maximize secrecy rate or to minimize secrecy outage probability for the SUs in the underlay cognitive models, respectively. In addition, the user selection in cooperative transmission is also an efficient method to enhance the security performance for communication systems due to the multiuser gain. The security enhanced technologies of the SUs is investigated with the user selection in Refs. [21,30,31]. However, transmission protocols for improving the secrecy performance of the PUs are barely known. How to design the transmission protocol for protecting the PU's security requirement remains a crucial issue in cognitive Internet of things model, where home terminal-to-terminal communication coexists with uplink or downlink of the femtocell station.

To improve the primary secrecy performance and secondary outage performance, we employ cooperative jammer and multi-user diversity technology in this paper. Namely, artificial noise is transmitted by selecting a secondary transmitter (ST), which can improve the outage performance of the primary system. Moreover, an ST has access to the primary spectrum if it can improve the outage performance of the secondary performance and satisfy the interference threshold. To encourage the secondary transmitter to act as a friendly jammer, the interference threshold for secondary system is relaxed by primary system in this paper. The main contributions are summarized as follows:

- We propose a ST cooperative transmission protocol by selecting jammer, which transmits an artificial noise to disturb the eavesdropper.
- We propose a selection scheme to determine the friendly jammer and secondary signal transmitter. The ST, which can provide the smallest intercept probability, is chosen as the friendly jammer to transmit artificial noise.
- We derive the closed-form expressions of the intercept probability and the outage probability for the primary system over Rayleigh fading channels, respectively. We also derive the outage probability of the secondary user over Rayleigh channels.

The remainder of the paper is organized as follows. The system model of cooperative jammer selection for primary systems is provided in Section 2. Section 3 analyzes the performances of transmission and security for our proposed protocol. Section 4 provides numerical simulations for the proposed protocol. Section 5 concludes this paper.

Notations: The channels coefficients over links PS → PD, PS → SR, PS → E, $\mathrm{ST}_i \to \mathrm{PD}$, $\mathrm{ST}_i \to \mathrm{SR}$, $\mathrm{ST}_o \to \mathrm{E}$, and $\mathrm{ST}_i \to \mathrm{E}$ are denoted by h_{P}, h_{PS}, h_{PE}, $h_{\mathrm{S}_i\mathrm{P}}$, h_{S_i}, $h_{\mathrm{S}_o\mathrm{E}}$, and $h_{\mathrm{S}_i\mathrm{E}}$, respectively. R_{P} denotes the minimum rate of transmission for primary systems. We also use R_{S} to denote the minimum rate of transmission for secondary systems. The transmit power of ST and PT are denoted by P_{P} and P_{S}, respectively. The expectation of a variable X is denoted by $E[X]$. The probability of a variable X is denoted by $\Pr\{X\}$.

2. The System Models and the Selection Schemes for STs

In this section, we propose a ST cooperative transmission protocol and a selection scheme to determine the friendly jammer and secondary transmitter. Figure 1b shows The system configuration of our protocols. The system model comprises a primary pair (PS-PD), an eavesdropper (E), a secondary receiver (SR) and K secondary transmitters ST_i, where $i \in I$, $I = \{1, \ldots, K\}$. In this transmission models, one secondary user is selected as a friendly jammer to interfere with eavesdropping at first, which is denoted by ST_o, $o \in I$. The other one has access to the licensed spectrum if the secondary transmission cannot cause an outage over link (PS→PD), which is denoted by ST_i, $i \in I$ and $i \neq o$. However, the transmitted information of primary users can be overheard by the eavesdropper. To prevent eavesdropping, ST_o transmits the artificial noise to interfere the eavesdropper. In the proposed model, PD and SR know the information of the artificial noise and the eavesdropper does not know the information. Therefore, PD and SR will not be affected by the artificial noise, which may disturb the eavesdropper. In the proposed protocol, on the one hand, ST_o, which provides the most optimal security performance, is selected as a cooperative jammer. On the other hand, if the best outage performance of the secondary system is achieved by selecting a secondary user ST_i, and the interference threshold of the primary system is satisfied for the secondary user ST_i, then ST_i has access to the licensed spectrum. Furthermore, we study two criterions, which are used to select the cooperative jammer and secondary information transmitter, respectively. In addition, we assume that $h_v \sim \mathcal{CN}(0, \sigma_v^2)$, where $v \in \{\mathrm{P}, \mathrm{PS}_i, \mathrm{PE}, \mathrm{S}_i\mathrm{P}, \mathrm{S}_i, \mathrm{S}_o\mathrm{E}, \mathrm{S}_i\mathrm{E}\}$. We also assume that noises are Additive White Gaussian Noise (AWGN) with zero mean and variance N_0.

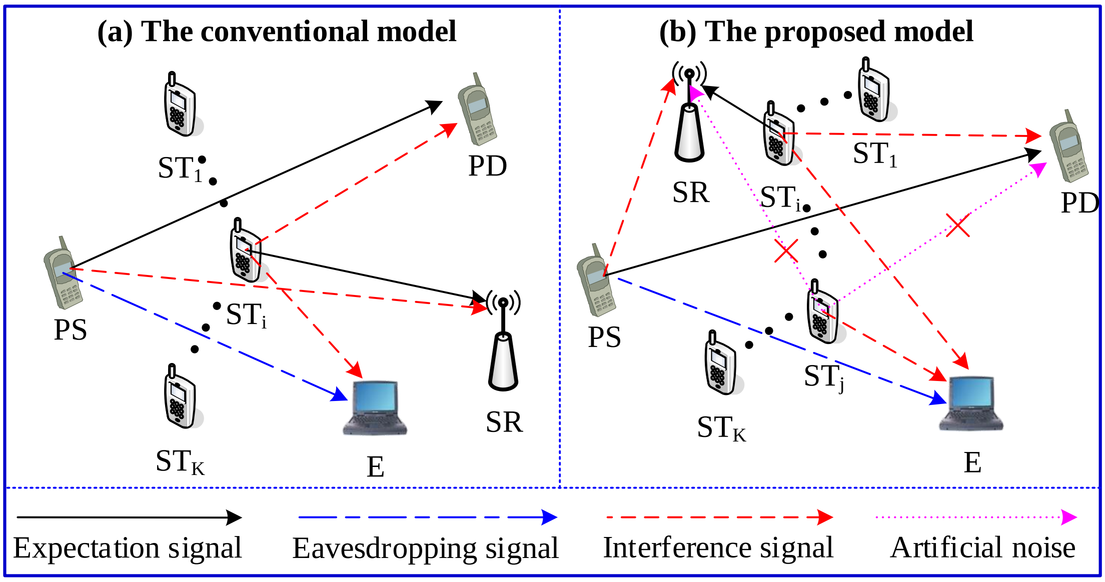

Figure 1. The system models.

2.1. *The System Model Based on the Security Enhancement Approach by Friendly Jammer Selection*

To ensure the Quality of Service (QoS) of the primary system, the interference to primary users caused by secondary users must be less than a given threshold (i.e., the interference threshold is satisfied by secondary users). The secondary users have access to the licensed spectrum if they satisfy the above condition. A collection of the secondary transmitters is expressed as S, in which all STs can meet the interference threshold. The transmission process of the proposed protocol is illustrated as follows.

When $S = \emptyset$, the primary signals are transmitted by PS, the artificial noise is transmitted by ST_o, but the secondary transmission is interrupted and SR does not work. PD can eliminate perfectly the artificial noise, which leads to a serious threat to the correct reception of the primary signals at E. Thus, the received signals at PD and E in this case are given by

$$y_{\mathrm{P}}^{S=\emptyset}(t) = \sqrt{P_{\mathrm{P}}} h_{\mathrm{P}} x_{\mathrm{P}}(t) + n_{\mathrm{P}}(t), \tag{1}$$

and

$$y_{\mathrm{E}}^{S=\varnothing}\left(t\right)=\sqrt{P_{\mathrm{P}}}h_{\mathrm{PE}}x_{\mathrm{P}}\left(t\right)+\sqrt{P_{\mathrm{S}}}h_{\mathrm{S}_o\mathrm{E}}x_{\mathrm{n}}\left(t\right)+n_{\mathrm{E}}\left(t\right), \tag{2}$$

where $x_{\mathrm{P}}\left(t\right)$ and $x_{\mathrm{n}}\left(t\right)$ represent the primary signal and the artificial noise, respectively. Furthermore, normalizing, $E[|x_{\mathrm{P}}\left(t\right)|^2]=1$ and $E[|x_{\mathrm{n}}\left(t\right)|^2]=1$. $n_{\mathrm{P}}\left(t\right)$ and $n_{\mathrm{E}}\left(t\right)$ denote the noises at PS and E, respectively. Hence, the instantaneous capacities of the channel PS → PD and the channel PS → E are given by

$$C_{\mathrm{P}}^{S=\varnothing}=\log_2\left(1+P_{\mathrm{P}}|h_{\mathrm{P}}|^2/N_0\right) \tag{3}$$

and

$$C_{\mathrm{E}}^{S=\varnothing}=\log_2\left(1+\frac{P_{\mathrm{P}}|h_{\mathrm{PE}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_o\mathrm{E}}|^2+N_0}\right). \tag{4}$$

When $S\neq\varnothing$, denoting $S=S_l$ and having $S\in\{\varnothing\}\cup S_l$, the primary signals, secondary signals and artificial noise are transmitted by PS, ST_i and ST_o, respectively, in the same spectrum band, where $\mathrm{ST}_i\in S_l$, $\mathrm{ST}_o\in S_l$ and $l=1,2,\ldots,2^{K-1}-1$. In this case, mutual interferences are aroused between the primary and secondary users. The artificial noise is eliminated perfectly at PD and SR, but leads a serious threat to the correct reception of the primary signals at E. Thus, the received signals at PD, SR and E are given by

$$y_{\mathrm{P}}^{S=S_l}\left(t\right)=\sqrt{P_{\mathrm{P}}}h_{\mathrm{P}}x_{\mathrm{P}}\left(t\right)+\sqrt{P_{\mathrm{S}}}h_{\mathrm{S}_i\mathrm{P}}x_{\mathrm{S}}\left(t\right)+n_{\mathrm{P}}\left(t\right), \tag{5}$$

$$y_{\mathrm{S}}^{S=S_l}\left(t\right)=\sqrt{P_{\mathrm{S}}}h_{\mathrm{S}_i}x_{\mathrm{S}}\left(t\right)+\sqrt{P_{\mathrm{P}}}h_{\mathrm{PS}}x_{\mathrm{P}}\left(t\right)+n_{\mathrm{S}}\left(t\right), \tag{6}$$

and

$$y_{\mathrm{E}}^{S=S_l}\left(t\right)=\sqrt{P_{\mathrm{P}}}h_{\mathrm{PE}}x_{\mathrm{P}}\left(t\right)+\sqrt{P_{\mathrm{S}}}h_{\mathrm{S}_o\mathrm{E}}x_{\mathrm{n}}\left(t\right)+\sqrt{P_{\mathrm{S}}}h_{\mathrm{S}_i\mathrm{E}}x_{\mathrm{S}}\left(t\right)+n_{\mathrm{E}}\left(t\right), \tag{7}$$

where $x_{\mathrm{S}}\left(t\right)$ is the secondary signal and $n_{\mathrm{S}}\left(t\right)$ denotes the noise at SR. Moreover, we assume that $E[|x_{\mathrm{S}}\left(t\right)|^2]=1$. Hence, the capacities of the channels PS → PD, ST_i → SR, and PS → E are given by

$$C_{\mathrm{P}}^{S=S_l}=\log_2\left(1+\frac{P_{\mathrm{P}}|h_{\mathrm{P}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{P}}|^2+N_0}\right), \tag{8}$$

$$C_{\mathrm{S}}^{S=S_l}\log_2\left(1+\frac{P_{\mathrm{S}}|h_{\mathrm{S}_i}|^2}{P_{\mathrm{P}}|h_{\mathrm{PS}}|^2+N_0}\right), \tag{9}$$

and

$$C_{\mathrm{E}}^{S=S_l}=\log_2\left(1+\frac{P_{\mathrm{P}}|h_{\mathrm{PE}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_o\mathrm{E}}|^2+P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{E}}|^2+N_0}\right), \tag{10}$$

where $o,i\in I$ and $i\neq o$. The number of elements in set S_l is denoted by $L-1$. It is easy to know $S_l=\{i|C_{\mathrm{P}}\geq R_{\mathrm{P}},i\in I,i\neq o\}$, $\bar{S}_l=\{i|C_{\mathrm{P}}<R_{\mathrm{P}},i\in I,i\neq o\}$ and $S_l\cup\bar{S}_l=\{\mathrm{ST}_i|i\in I,i\neq o\}$. Hence, if $C_{\mathrm{P}}>C_{\mathrm{E}}$, then the physical-layer secrecy is obtained. If $C_{\mathrm{P}}<C_{\mathrm{E}}$, the secrecy intercept event happens. Its definition refers to [32]. Hence, in wireless systems, the physical-layer security is measured by its probability. Two selection criteria of ST_o and ST_i are described in detail in the next subsection.

2.2. The Selection Schemes for ST_o and ST_i

In the multi-users underlay cognitive model, the primary security performance, and the primary and secondary transmission performances are the three most important indicators in system performance analysis. Moreover, the security performance of primary users can be improved effectively since a secondary user acts as a friendly jammer to interfere eavesdropping. By choosing a suitable user as the friendly jammer will further enhance the primary security performance. To optimize the primary physical-layer security performance, a secondary transmitter is selected to serve as a cooperative jammer, we use ST_o to denote the secondary transmitter, which can provide the most optimal security for the primary. Thus, the selection criteria of ST_o can be written as

$$J = \arg \min_{j \in \{1,\ldots,K\}} \Pr\left\{C_{\mathrm{P}}^{S=\varnothing} < C_{\mathrm{E}}^{S=\varnothing}\right\} = \arg \max_{j \in \{1,\ldots,K\}} |h_{\mathrm{S}_j\mathrm{E}}|^2, \tag{11}$$

where $C_{\mathrm{P}}^{S=\varnothing}$ and $C_{\mathrm{E}}^{S=\varnothing}$ are calculated by Equations (3) and (4), respectively. In addition, the secondary transmission performance is significantly improved by cooperative rewards that some primary spectrum is released or the value of interference threshold is relaxed for secondary transmission. However, different secondary transmitters have different transmission efficiencies. To maximize the secondary transmission performance, a secondary transmitter is denoted by ST_i that satisfies the interference threshold. Moreover, ST_i has access to the licensed spectrum if the optimal outage performance of the secondary system is obtained by ST_i. The selection criteria for ST_i can be written as

$$\mathrm{ST}_i = \arg \min_{\mathrm{ST}_i \in S_l} \Pr\left\{C_{\mathrm{S}}^{S=S_l} < R_{\mathrm{S}}\right\} = \arg \max_{\mathrm{ST}_i \in S_l} C_{\mathrm{S}}^{S=S_l}, \tag{12}$$

where $C_{\mathrm{S}}^{S=S_l}$ is calculated by Equation (9). Therefore, we focus on the selection of the secondary, which can have access to the primary spectrum and can be the cooperative jammer.

2.3. The Conventional Non-Security Model

As shown in Figure 1a, the system model of the conventional non-security management protocol comprise of a primary pair (PS-PD), an eavesdropper (E), a secondary receiver (SR) and K secondary transmitters ST_i $(1, \ldots, K)$. This conventional model is a typical cognitive underlay system, where STs can have access to the primary spectrum and need to satisfy the interference threshold settled by primary system. Compared with the conventional model, we can see that the received signals at PD and SR and the corresponding instantaneous capacities are identical. In contrast, the received signals at E and the corresponding instantaneous capacities are different. Thus, if $S^C = \varnothing$, the received signals at E and the corresponding instantaneous capacities are given by

$$y_{\mathrm{E}}^{C}(t) = \sqrt{P_{\mathrm{P}}} h_{\mathrm{PE}} x_{\mathrm{P}}(t) + n_{\mathrm{E}}(t) \tag{13}$$

and

$$C_{\mathrm{E}}^{C}(t) = \log_2\left(1 + P_{\mathrm{P}}|h_{\mathrm{PE}}|^2/N_0\right). \tag{14}$$

If the secondary signal is transmitted over primary spectrum (namely, $S^C = \varnothing$), the received signals at E and the corresponding instantaneous capacities are given by

$$y_{\mathrm{E}}^{C}(t) = \sqrt{P_{\mathrm{P}}} h_{\mathrm{PE}} x_{\mathrm{P}}(t) + \sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_i\mathrm{E}} x_{\mathrm{S}}(t) + n_{\mathrm{E}}(t) \tag{15}$$

and

$$C_{\mathrm{E}}^{C} = \log_2\left(1 + \frac{P_{\mathrm{P}}|h_{\mathrm{PE}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{E}}|^2 + N_0}\right). \tag{16}$$

3. Performance Analysis

3.1. The Primary Outage Probability for the Proposed Protocols

We use Ω_{P} to denote an event, which represents an occurrence of outage of the channel PS → PD. Hence, if $C_{\mathrm{P}}^{S=\varnothing} < R_{\mathrm{P}}$ or $C_{\mathrm{P}}^{S\neq\varnothing} < R_{\mathrm{P}}$, the event Ω_{P} occurs. Obviously, the secondary transmission may make the event happen when $S \neq \varnothing$. Thus, we obtain

$$\mathrm{P_{out}} = \Pr\{S = \emptyset\}\Pr\{\Omega_{\mathrm{P}}|S = \emptyset\} + \sum_{l=1}^{2^{K-1}-1}\Pr\{S = S_l\}\Pr\{\Omega_{\mathrm{P}}|S = S_l\} \tag{17}$$

and

$$\Pr\{S = \emptyset\} = \prod_{i=1, i\neq o}^{K}\Pr\{C_{\mathrm{P}} < R_{\mathrm{P}}\} = \prod_{i=1, i\neq o}^{K}\Pr\left\{\frac{P_{\mathrm{P}}|h_{\mathrm{P}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{P}}|^2 + N_0} < 2^{R_{\mathrm{P}}} - 1\right\}, \tag{18}$$

where $C_{\mathrm{P}}^{S=\emptyset}$ is given by Equation (3). Since $|h_{\mathrm{P}}|^2$ and $|h_{\mathrm{S}_i\mathrm{P}}|^2$ are i.i.d. exponential distribution with parameters $1/\sigma_{\mathrm{P}}^2$ and $1/\sigma_{\mathrm{S}_i\mathrm{P}}^2$, respectively, letting $X_1 = |h_{\mathrm{P}}|^2$ and $X_2 = |h_{\mathrm{S}_i\mathrm{P}}|^2$, Equation (18) can be rewritten as

$$\begin{aligned}\Pr\{S = \emptyset\} &= \prod_{i=1, i\neq o}^{K}\Pr\{C_{\mathrm{P}} < R_{\mathrm{P}}\} = \prod_{i=1, i\neq o}^{K}\Pr\left\{\frac{P_{\mathrm{P}}X_1}{P_{\mathrm{S}}X_2 + N_0}\right\} \\ &= \prod_{i=1, i\neq o}^{K}\int_0^{\infty}\frac{1}{\sigma_{\mathrm{S}_i\mathrm{P}}^2}e^{-\frac{x_2}{\sigma_{\mathrm{S}_i\mathrm{P}}^2}}\int_0^{\rho_{\mathrm{P}}(P_{\mathrm{S}}x_2+N_0)/P_{\mathrm{P}}}\frac{1}{\sigma_{\mathrm{P}}^2}e^{\frac{x_1}{\sigma_{\mathrm{P}}^2}}dx_1dx_2 \\ &= \prod_{i=1, i\neq o}^{K}\left(1 - \frac{\sigma_{\mathrm{P}}^2P_{\mathrm{P}}e^{-\frac{\rho_{\mathrm{P}}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^2}}}{\sigma_{\mathrm{P}}^2P_{\mathrm{P}} + \rho_{\mathrm{P}}P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^2}\right).\end{aligned} \tag{19}$$

Furthermore, $\Pr\{\Omega_{\mathrm{P}}|S = \emptyset\}$ and $\Pr\{S = S_l\}$ can be calculated as follows:

$$\Pr\{\Omega_{\mathrm{P}}|S = \emptyset\} = \Pr\left\{\log_2\left(1 + P_{\mathrm{P}}|h_{\mathrm{P}}|^2\right) < R_{\mathrm{P}}\right\} = 1 - e^{-\frac{\rho_{\mathrm{P}}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^2}} \tag{20}$$

and

$$\begin{aligned}\Pr\{S = S_l\} &= \prod_{i\in\bar{S}_l}\Pr\{C_{\mathrm{P}} < R_{\mathrm{P}}\}\prod_{j\in S_l}\Pr\{C_{\mathrm{P}} \geq R_{\mathrm{P}}\} \\ &= \prod_{i\in\bar{S}_l}\left(1 - \frac{\sigma_{\mathrm{P}}^2P_{\mathrm{P}}}{\sigma_{\mathrm{P}}^2P_{\mathrm{P}} + \rho_{\mathrm{P}}P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^2}e^{-\frac{\rho_{\mathrm{P}}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^2}}\right)\prod_{j\in S_l}\frac{\sigma_{\mathrm{P}}^2P_{\mathrm{P}}}{\sigma_{\mathrm{P}}^2P_{\mathrm{P}} + \rho_{\mathrm{P}}P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^2}e^{-\frac{\rho_{\mathrm{P}}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^2}},\end{aligned} \tag{21}$$

where $\rho_{\mathrm{P}} = 2^{R_{\mathrm{P}}} - 1$. According to the definition of the set S_l, we can see that $\Pr\{\Omega_{\mathrm{P}}|S = S_l\}$ equals to zero in OSTS and OCJS. Thus, the expression of the outage probability for the primary system is obtained by substituting Equations (19)–(21) and $\Pr\{\Omega_{\mathrm{P}}|S = S_l\} = 0$ into Equation (17).

3.2. The Outage Probability of the Secondary System

We use Ω_{S} to denote an event, which represents an occurrence of outage of the channel ST → SR. If $C_{\mathrm{S}}^{S=S_l} < R_{\mathrm{S}}$, then the event Ω_{S} occurs. Therefore, we have

$$\mathrm{S_{out}} = \Pr\{S = \emptyset\}\Pr\{\Omega_{\mathrm{S}}|S = \emptyset\} + \sum_{l=1}^{2^{K-1}-1}\Pr\{S = S_l\}\Pr\{\Omega_{\mathrm{S}}|S = S_l\} \tag{22}$$

and

$$\begin{aligned}\Pr\{\Omega_{\mathrm{S}}|S = S_l\} &= \min_{\mathrm{ST}_i\in S_l}\Pr\left\{C_{\mathrm{S}}^{S=S_l} < R_{\mathrm{S}}\right\} \\ &= \Pr\left\{\max_{\mathrm{ST}_i\in S_l}\frac{P_{\mathrm{S}}|h_{\mathrm{S}_i}|^2}{P_{\mathrm{P}}|h_{\mathrm{PS}}|^2 + N_0} < 2^{R_{\mathrm{S}}} - 1\right\} \\ &= \prod_{i=1}^{L-1}\Pr\left\{\frac{P_{\mathrm{S}}|h_{\mathrm{S}_i}|^2}{P_{\mathrm{P}}|h_{\mathrm{PS}}|^2 + N_0} < 2^{R_{\mathrm{S}}} - 1\right\}.\end{aligned} \tag{23}$$

Furthermore, $|h_{\mathrm{S}_i}|^2$ and $|h_{\mathrm{PS}}|^2$ are i.i.d. exponential distribution with parameters $1/\sigma_{\mathrm{S}_i}^2$ and $1/\sigma_{\mathrm{PS}}^2$, respectively. Let $Z_1 = |h_{\mathrm{S}_i}|^2$ and $Z_2 = |h_{\mathrm{PS}}|^2$, thus Equation (23) can be rewritten as

$$\begin{aligned}\Pr\left\{\Omega_{\mathrm{S}}|S=S_l\right\} &= \prod_{i=1}^{L-1}\Pr\left\{\frac{P_{\mathrm{S}}Z_1}{P_{\mathrm{P}}Z_2+N_0}<\rho_{\mathrm{S}}\right\}\\ &= \prod_{i=1}^{L-1}\int_0^{\infty}\frac{1}{\sigma^2_{\mathrm{PS}_i}}e^{-\frac{z_2}{\sigma^2_{\mathrm{PS}_i}}}\int_0^{\rho_{\mathrm{S}}(P_{\mathrm{P}}z_1+N_0)/P_{\mathrm{S}}}\frac{1}{\sigma^2_{\mathrm{S}_i}}e^{-\frac{z_1}{\sigma^2_{\mathrm{S}_i}}}dz_1dz_2\\ &= \prod_{i=1}^{L-1}\left(1-\frac{\sigma^2_{\mathrm{S}_i}P_{\mathrm{S}}e^{-\frac{\rho_{\mathrm{S}}N_0}{P_{\mathrm{S}}\sigma^2_{\mathrm{S}_i}}}}{\sigma^2_{\mathrm{S}_i}P_{\mathrm{S}}+\rho_{\mathrm{S}}P_{\mathrm{P}}\sigma^2_{\mathrm{PS}_i}}\right),\end{aligned} \tag{24}$$

where $\rho_{\mathrm{S}} = 2^{R_{\mathrm{S}}} - 1$. We can see that $\Pr\{\Omega_{\mathrm{S}}|S = \emptyset\} = 1$. Thus, the expression of the outage probability of the secondary system is obtained by substituting Equations (19), (21), (24) and $\Pr\{\Omega_{\mathrm{S}}|S = \emptyset\} = 1$ into Equation (22).

3.3. The Intercept Probability of the Primary Transmission

The secrecy intercept event for the primary system is denoted by Ω_{int}. Hence, the intercept probability of the primary transmission is equal to the probability of the event Ω_{int} occurrence [33]. In addition, the secrecy intercept event occurs when $C_{\mathrm{P}}^{S=\emptyset} < C_{\mathrm{E}}^{S=\emptyset}$ or $C_{\mathrm{P}}^{S\neq\emptyset} < C_{\mathrm{E}}^{S\neq\emptyset}$. Obviously, the event Ω_{int} occurs only when $S \neq \emptyset$. Therefore, we obtain

$$\mathrm{P}_{\mathrm{int}} = \Pr\left\{S=\emptyset\right\}\Pr\left\{\Omega_{\mathrm{int}}|S=\emptyset\right\} + \sum_{l=1}^{2^{K-1}-1}\Pr\left\{S=S_l\right\}\Pr\left\{\Omega_{\mathrm{int}}|S=S_l\right\}. \tag{25}$$

Moreover, $|h_{\mathrm{PE}}|^2$, $|h_{\mathrm{S}_i\mathrm{E}}|^2$ and $|h_{\mathrm{S}_o\mathrm{E}}|^2$ are exponential variables with parameters $1/\sigma^2_{\mathrm{PE}}$, $1/\sigma^2_{\mathrm{S}_i\mathrm{E}}$ and $1/\sigma^2_{\mathrm{S}_o\mathrm{E}}$, respectively. Let $\hat{X}_3 = |h_{\mathrm{S}_i\mathrm{E}}|^2$, $X_3 = |h_{\mathrm{S}_o\mathrm{E}}|^2$ and $X_4 = |h_{\mathrm{PE}}|^2$. Thus, when $S = \emptyset$, the conditional intercept probability $\Pr\{\Omega_{\mathrm{int}}|S = \emptyset\}$ and $\Pr\{\Omega_{\mathrm{int}}|S = S_l\}$ can be derived as

$$\begin{aligned}\Pr\{\Omega_{\mathrm{int}}|S=\emptyset\} &= \Pr\left\{\frac{P_{\mathrm{P}}|h_{\mathrm{P}}|^2}{N_0}<\frac{P_{\mathrm{P}}|h_{\mathrm{PE}}|^2}{P_{\mathrm{S}}\cdot\max_{o\in\{1,\ldots,K\}}|h_{\mathrm{S}_o\mathrm{E}}|^2+N_0}\right\}\\ &= \prod_{o\in\{1,\ldots,K\}}\Pr\left\{|h_{\mathrm{P}}|^2<\frac{N_0}{P_{\mathrm{S}}}\frac{|h_{\mathrm{PE}}|^2}{|h_{\mathrm{S}_o\mathrm{E}}|^2+N_0/P_{\mathrm{S}}}\right\}\\ &= \prod_{o\in\{1,\ldots,K\}}\Pr\left\{X_1<\frac{N_0}{P_{\mathrm{S}}}\frac{X_4}{X_3+N_0/P_{\mathrm{S}}}\right\}\end{aligned} \tag{26}$$

and

$$\begin{aligned}\Pr\{\Omega_{\mathrm{int}}|S=S_l\} &= \min_{o\in\{1,\ldots,K\}}\Pr\left\{C_{\mathrm{P}}^{S=S_l}<C_{\mathrm{E}}^{S=S_l}\right\}\\ &= \Pr\left\{C_{\mathrm{P}}^{S=S_l}<\min_{o\in\{1,\ldots,K\}}C_{\mathrm{E}}^{S=S_l}\right\}\\ &= \prod_{o=1}^{K}\Pr\left\{C_{\mathrm{P}}^{S=S_l}<C_{\mathrm{E}}^{S=S_l}\right\}\\ &= \prod_{o=1}^{K}\Pr\left\{\frac{P_{\mathrm{P}}|h_{\mathrm{P}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{P}}|^2+N_0}<\frac{P_{\mathrm{P}}|h_{\mathrm{PE}}|^2}{P_{\mathrm{S}}|h_{\mathrm{S}_i\mathrm{E}}|^2+P_{\mathrm{S}}|h_{\mathrm{S}_o\mathrm{E}}|^2+N_0}\right\}\\ &= \prod_{o=1}^{K}\Pr\left\{\frac{X_1}{X_2+N_0/P_{\mathrm{S}}}<\frac{X_4}{X_3+\hat{X}_3+N_0/P_{\mathrm{S}}}\right\}.\end{aligned} \tag{27}$$

Let $\tilde{X}_2 = X_2 + N_0/P_{\mathrm{S}}$, $\tilde{X}_3 = X_3 + \hat{X}_3 + N_0/P_{\mathrm{S}}$, $Y_1 = X_1/\tilde{X}_2$, $Y_2 = X_4/\tilde{X}_3$, and $Y_3 = X_4/(X_3 + N_0/P_{\mathrm{S}})$. Following Equations (A1) and (A9) in Appendix A, the probability density of random variables Y_1, Y_2 and Y_3 can be written as follows:

$$\begin{aligned} f_{Y_1}(y_1) &= \left(\frac{\sigma_{\mathrm{P}}^2/\sigma_{\mathrm{S}_i\mathrm{P}}^2}{\left(\sigma_{\mathrm{P}}^2/\sigma_{\mathrm{S}_i\mathrm{P}}^2 + y_1\right)^2} + \frac{N_0/\left(P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^2\right)}{\sigma_{\mathrm{P}}^2/\sigma_{\mathrm{S}_i\mathrm{P}}^2 + y_1} \right) e^{-\frac{N_0 y_1}{P_{\mathrm{S}}\sigma_{\mathrm{P}}^2}} \\ &= \left(\frac{a_1}{(a_1+y_1)^2} + \frac{a_1 b_1}{a_1+b_1} \right) e^{-b_1 y_1}, \end{aligned} \tag{28}$$

$$\begin{aligned} f_{Y_2}(y_2) &= \left(\frac{1}{\left(\sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2 + y_2\right)^2} + \frac{N_0/\left(P_{\mathrm{S}}\sigma_{\mathrm{PE}}^2\right)}{\sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2 + y_2} \right) \cdot \frac{\sigma_{\mathrm{PE}}^2 e^{-\frac{N_0 y_2}{P_{\mathrm{S}}\sigma_{\mathrm{PE}}^2}}}{\sigma_{\mathrm{S}_o\mathrm{E}}^2 - \sigma_{\mathrm{S}_i\mathrm{E}}^2} \\ &= c\left(\frac{1}{(a_2+y_2)^2} + \frac{b_2}{a_2+y_2} \right) e^{-b_2 y_2}, \end{aligned} \tag{29}$$

and

$$\begin{aligned} f_{Y_3}(y_3) &= \left(\frac{\sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2}{\left(\sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2 + y_3\right)^2} + \frac{N_0/\left(P_{\mathrm{S}}\sigma_{\mathrm{S}_o\mathrm{E}}^2\right)}{\sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2 + y_3} \right) e^{-\frac{N_0 y_3}{P_{\mathrm{S}}\sigma_{\mathrm{PE}}^2}} \\ &= \left(\frac{a_3}{(a_3+y_3)^2} + \frac{a_3 b_3}{a_3+b_3} \right) e^{-b_3 y_3}, \end{aligned} \tag{30}$$

where $a_1 = \sigma_{\mathrm{P}}^2/\sigma_{\mathrm{S}_i\mathrm{P}}^2$, $b_1 = N_0/P_{\mathrm{S}}\sigma_{\mathrm{P}}^2$, $a_2 = a_3 = \sigma_{\mathrm{PE}}^2/\sigma_{\mathrm{S}_o\mathrm{E}}^2$, $b_2 = b_3 = N_0/P_{\mathrm{S}}\sigma_{\mathrm{PE}}^2$, $c = \sigma_{\mathrm{S}_o\mathrm{E}}^2/(\sigma_{\mathrm{S}_o\mathrm{E}}^2 - \sigma_{\mathrm{S}_i\mathrm{E}}^2)$. By using the equalities in Equations (28)–(30), Equations (26) and (27) can be rewritten, respectively, as follows:

$$\begin{aligned} \Pr\{\Omega_{\mathrm{int}}|S=\varnothing\} &= \prod_{o\in\{1,\ldots,K\}} \Pr\{X_1 < (N_0/P_{\mathrm{S}})\,Y_3\} \\ &= \prod_{o\in\{1,\ldots,K\}} \int_0^\infty \left(\frac{a_3}{(a_3+y_3)^2} + \frac{a_3 b_3}{a_3+b_3} \right) e^{-b_3 y_3} \int_0^{\frac{N_0}{P_{\mathrm{S}}}} \frac{1}{\sigma_{\mathrm{P}}^2} e^{-\frac{x_1}{\sigma_{\mathrm{P}}^2}} dx_1 dy_3 \\ &= -\prod_{o\in\{1,\ldots,K\}} a_3 b_1 e^{a_3(b_1+b_3)} \mathrm{Ei}\left(-a_3\left(b_1+b_3\right)\right) \end{aligned} \tag{31}$$

and

$$\begin{aligned} \Pr\{\Omega_{\mathrm{int}}|S=S_l\} &= \prod_{o=1}^{K} \Pr\{Y_1 < Y_2\} \\ &= \prod_{o=1}^{K} \int_0^\infty \frac{c + cb_2\left(y_2+a_2\right)}{\left(y_2+a_2\right)^2} e^{-b_2 y_2} \int_0^{y_2} \frac{a_1 + a_1 b_1\left(y_1+a_1\right)}{\left(y_1+a_1\right)^2} e^{-b_1 y_1} dy_1 dy_2 \\ &= \prod_{o=1}^{K} \left(c - \frac{a_1 a_2 c\left(1+a_1 b_1 - a_2 b_1\right)}{\left(a_1-a_2\right)^2} e^{a_2(b_1+b_2)} \mathrm{Ei}\left(-a_2\left(b_1+b_2\right)\right) \right. \\ &\quad \left. + \frac{a_1 a_2 c\left(1+a_2 b_2 - a_1 b_2\right)}{\left(a_1-a_2\right)^2} e^{a_1(b_1+b_2)} \mathrm{Ei}\left(-a_1\left(b_1+b_2\right)\right) - \frac{a_1 c}{a_1 - a_2} \right), \end{aligned} \tag{32}$$

where $\mathrm{Ei}(x) = \int_{-\infty}^{x} \frac{1}{x} e^x dx = r + \ln(-x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!}$, $x < 0$, r is the Euler's constant. Therefore, the intercept probability of the primary system in proposed protocol is obtained by substituting Equations (19), (21), (31) and (32) into Equation (25).

3.4. The Outage and Intercept Probability for the Conventional No-Security Protocol

Similar to the performance analysis for the proposed protocols, the primary and secondary outage probability and the primary intercept probability are calculated, respectively, as follows:

$$\mathrm{P}_{\mathrm{out}}^{\mathrm{C}} = \Pr\left\{S^{\mathrm{C}} = \varnothing\right\} \Pr\left\{\Omega_{\mathrm{P}}|S^{\mathrm{C}} = \varnothing\right\} + \sum_{l=1}^{2^K-1} \Pr\left\{S^{\mathrm{C}} = S_l\right\} \Pr\left\{\Omega_{\mathrm{P}}|S^{\mathrm{C}} = S_l\right\}, \tag{33}$$

$$\mathrm{S}_{\mathrm{out}}^{C} = \Pr\left\{S^{C} = \varnothing\right\}\Pr\left\{\Omega_{\mathrm{S}}|S^{C} = \varnothing\right\} + \sum_{l=1}^{2^{K}-1}\Pr\left\{S^{C} = S_{l}\right\}\Pr\left\{\Omega_{\mathrm{S}}|S^{C} = S_{l}\right\}, \tag{34}$$

and

$$\mathrm{P}_{\mathrm{int}}^{C} = \Pr\left\{S^{C} = \varnothing\right\}\Pr\left\{\Omega_{\mathrm{int}}|S^{C} = \varnothing\right\} + \sum_{l=1}^{2^{K}-1}\Pr\left\{S^{C} = S_{l}\right\}\Pr\left\{\Omega_{\mathrm{int}}|S^{C} = S_{l}\right\}. \tag{35}$$

We can see that $\Pr\{\Omega_{\mathrm{S}}|S^{C} = \varnothing\} = 1$, $\Pr\{\Omega_{\mathrm{P}}|S^{C} = S_{l}\} = 1$. To encourage STs to aid the transmission of artificial noise, we set $R_{\mathrm{P}_0} \geq R_{\mathrm{P}}$. Therefore, we also have

$$\Pr\left\{S^{C} = \varnothing\right\} = \prod_{i=1}^{K}\Pr\left\{C_{\mathrm{P}}^{C} < R_{\mathrm{P}_0}\right\} = \prod_{i=1}^{K}\left(1 - \frac{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}}}{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}} + \rho_{\mathrm{P}_0}P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^{2}}e^{-\frac{\rho_{\mathrm{P}_0}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^{2}}}\right), \tag{36}$$

$$\begin{aligned}\Pr\left\{S^{C} = S_{l}\right\} &= \prod_{i\in\bar{S}_l}\Pr\left\{C_{\mathrm{P}}^{C} < R_{\mathrm{P}_0}\right\}\prod_{j\in S_l}\Pr\left\{C_{\mathrm{P}}^{C} \geq R_{\mathrm{P}_0}\right\}\\ &= \prod_{i\in\bar{S}_l}\left(1 - \frac{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}}}{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}} + \beta\rho_{\mathrm{P}_0}P_{\mathrm{S}}\sigma_{\mathrm{S}_i\mathrm{P}}^{2}}e^{-\frac{\rho_{\mathrm{P}_0}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^{2}}}\right)\\ &\quad\times\prod_{j\in S_l}\left(1 - \frac{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}}}{\sigma_{\mathrm{P}}^{2}P_{\mathrm{P}} + \beta\rho_{\mathrm{P}_0}P_{\mathrm{S}}\sigma_{\mathrm{S}_j\mathrm{P}}^{2}}e^{-\frac{\rho_{\mathrm{P}_0}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^{2}}}\right),\end{aligned} \tag{37}$$

$$\Pr\left\{\Omega_{\mathrm{P}}|S^{C} = \varnothing\right\} = \Pr\left\{\log_2\left(1 + P_{\mathrm{P}}|h_{\mathrm{P}}|^{2}/N_0\right) < R_{\mathrm{P}_0}\right\} = 1 - e^{-\frac{\rho_{\mathrm{P}_0}N_0}{P_{\mathrm{P}}\sigma_{\mathrm{P}}^{2}}}, \tag{38}$$

$$\Pr\left\{\Omega_{\mathrm{S}}|S^{C} = S_{l}\right\} = \prod_{i=1}^{L}\Pr\left\{C_{\mathrm{S}}^{C} < R_{\mathrm{S}}\right\} = \prod_{i=1}^{L}\left(1 - \frac{\sigma_{\mathrm{S}_i}^{2}P_{\mathrm{S}}}{\sigma_{\mathrm{S}_i}^{2}P_{\mathrm{P}} + \rho_{\mathrm{S}}P_{\mathrm{P}}\sigma_{\mathrm{PS}_i}^{2}}e^{-\frac{\rho_{\mathrm{S}}N_0}{P_{\mathrm{S}}\sigma_{\mathrm{S}_i}^{2}}}\right), \tag{39}$$

$$\begin{aligned}\Pr\left\{\Omega_{\mathrm{int}}|S^{C} = \varnothing\right\} &= \Pr\left\{P_{\mathrm{P}}|h_{\mathrm{P}}|^{2}/N_0 < P_{\mathrm{P}}|h_{\mathrm{PE}}|^{2}/N_0\right\} = \Pr\left\{X_1 < X_4\right\}\\ &= \int_0^{\infty}\frac{1}{\sigma_{\mathrm{PE}}^{2}}e^{-\frac{x_4}{\sigma_{\mathrm{PE}}^{2}}}\int_0^{x_4}\frac{1}{\sigma_{\mathrm{P}}^{2}}e^{-\frac{x_1}{\sigma_{\mathrm{P}}^{2}}}dx_1dx_4\\ &= 1 - \frac{\sigma_{\mathrm{P}}^{2}}{\sigma_{\mathrm{P}}^{2} + \sigma_{\mathrm{PE}}^{2}},\end{aligned} \tag{40}$$

$$\begin{aligned}\Pr\left\{\Omega_{\mathrm{int}}|S^{C} = S_{l}\right\} &= \Pr\left\{C_{\mathrm{P}}^{C} < C_{\mathrm{E}}^{C}\right\}\\ &= \Pr\left\{\frac{P_{\mathrm{P}}|h_{\mathrm{P}}|^{2}}{P_{\mathrm{S}}|h_{\mathrm{S}_o\mathrm{P}}|^{2} + N_0} < \frac{P_{\mathrm{PE}}|h_{\mathrm{P}}|^{2}}{P_{\mathrm{S}}|h_{\mathrm{S}_o\mathrm{E}}|^{2} + N_0}\right\}\\ &= 1 - \frac{a_1}{a_1 - \tilde{a}_2} + c_1\mathrm{Ei}\left(-a_1\left(b_1 + b_2\right)\right)\\ &\quad + c_2\mathrm{Ei}\left(-\tilde{a}_2\left(b_1 + b_2\right)\right)e^{\tilde{a}_2(b_1+b_2)},\end{aligned} \tag{41}$$

where $\rho_{\mathrm{P}_0} = 2^{R_{\mathrm{P}_0}} - 1$, $\tilde{a}_2 = \sigma_{\mathrm{PE}}^{2}/\sigma_{\mathrm{S}_i\mathrm{E}}^{2}$, $c_1 = \beta a_1\tilde{a}_2(1 + \tilde{a}_2b_2 - \beta a_1b_2)/(\tilde{a}_2 - \beta a_1)^{2}$ and $c_2 = \beta a_1\tilde{a}_2(\tilde{a}_2b_1 - \beta a_1b_1 - 1)/(\tilde{a}_2 - \beta a_1)^{2}$.

4. Numerical Results

The simulation results of the proposed protocols are provided in this section. The systems comprise a primary pair (PS-PD), an eavesdropper (E), a secondary receiver (SR) and K secondary transmitters ST_i ($i = 1,\ldots,K$). Since the secondary user can serve as cooperative jammer, the primary user relaxes the interference threshold in return, which decreases the minimum achievable rate of primary user R_{P}. Thus, we set $R_{\mathrm{P}} = 1.5$ Bit/s/Hz and $R_{\mathrm{P}} = 1$ Bit/s/Hz in the conventional model and the proposed model, respectively. If the parameters are not specified, the simulation parameters are settled as follow: $R_S = 1$ Bit/s/Hz; $r_1 = 10\lg(P_P/N_0) = 10$ dB is the average transmit SNR of the primary user. In addition, $\sigma_P^2 = \sigma_{SP}^2 = \sigma_{PS}^2 = \sigma_{PE}^2 = 1$, $\sigma_{S_oE}^2 = 3$, $\sigma_{S_iE}^2 = 1/5$ and $\sigma_S^2 = 4$.

The outage probabilities of the primary user versus r_2 in the conventional model and the proposed model are shown as Figure 2, where $r_2 = 10\lg(P_S/N_0)$. The special parameter is the number of STs, which is fixed as $K = 3; 4; 9$. In Figure 2, the outage probability of primary system increases with increase of the secondary SNR. In the same protocol, the primary outage probability decreases with increase of the number of secondary users. This is because the diversity gain increases with increase of the number of secondary users. Furthermore, the outage probability of primary system in our proposed protocol is less than the conventional protocol, which is because that the secondary user is encouraged to serve as friendly jammer, which decreases the interference threshold.

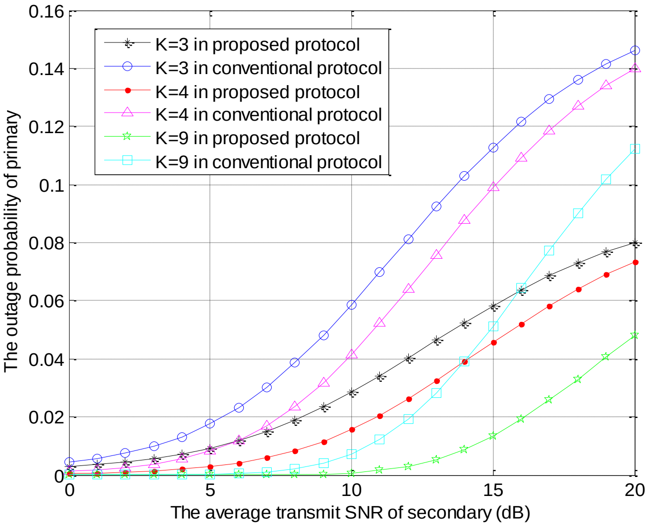

Figure 2. The outage probabilities of primary users versus r_2 with different K values.

The outage probabilities of the secondary user versus r_2 are shown in Figure 3, which is generated by using the same parameters as those in Figure 2. In Figure 3, in the same protocol, the secondary outage performances are improved when the number of STs becomes larger. Moreover, the outage probabilities of secondary decrease firstly, and increase with the increase of the average SNR for secondary in the two protocols. Furthermore, the increasing trend is due to that the interference threshold is always not satisfied by secondary user when the SNR of the secondary user is too large. In the small secondary average SNR range, the outage performance of secondary users in the conventional model is better than the performance in the proposed protocol. This performance is mainly determined by the multi-user diversity gain. In this case, the proposed protocol has a lower multi-user diversity gain than the conventional model due to one secondary transmitter acting as the cooperative jammer. In contrast, the proposed protocol can provide a better secondary outage performance in the high secondary average SNR range because the primary user relaxes the interference threshold.

Figure 4 is generated using the same parameters as those in Figure 2, which shows the intercept probabilities of the primary versus r_2 with different number of STs. In Figure 4, the primary security performance is improved significantly in the proposed protocol and is improved slightly in the conventional model as the number of STs becomes larger due to the multi-user diversity gain. Moreover, compared with the conventional protocol, our protocol can provide better primary security performance. The intercept probabilities of the primary system decrease with the increase of r_2 in the proposed protocol because the interference from ST to eavesdropper increases with the increase of r_2. However, the intercept probabilities of the primary system decrease firstly and increase with the increase of r_2 in the conventional protocol. In the small value range of r_2, the interference threshold is always satisfied, but the interference from ST to eavesdropper increases with the increase of r_2, which causes the decreasing phenomenon. In the large value range of r_2, the interference threshold is hard to satisfy. Thus, the access probability of the secondary transmission decreases and the interference from ST to eavesdropper is reduced with the increase of r_2. This is the cause of the latter increasing phenomenon. These numerical results can also be found in Figures 5–7.

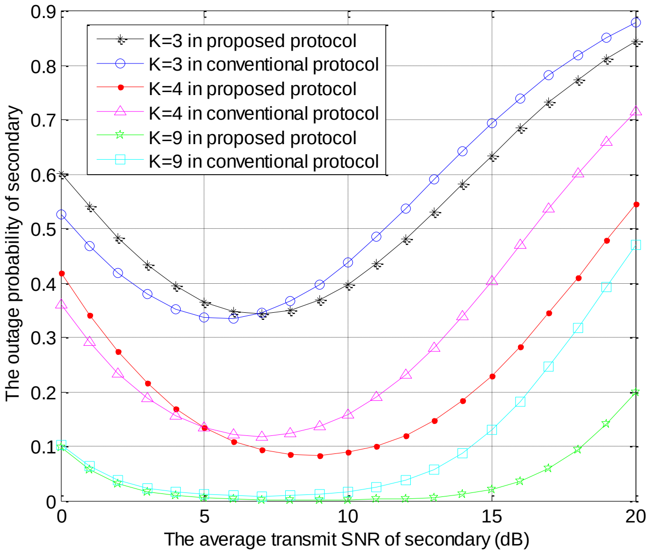

Figure 3. The outage probability of secondary system versus r_2 in the two protocols with different K values.

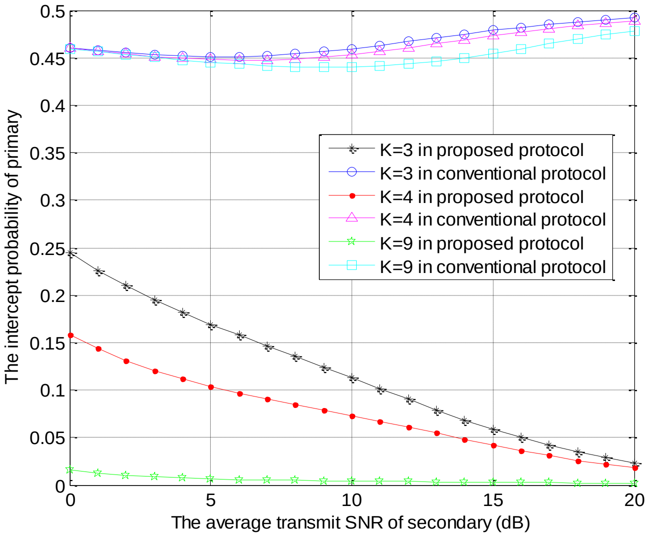

Figure 4. The intercept probabilities of primary users versus r_2 with different K values.

The intercept probabilities of primary users versus r_2 with different values of σ^2_{SE} are shown in Figure 5. Namely, the special parameter is the channel coefficient σ^2_{SE}, which equals 3, 3.5 or 4. As described in Figure 5, the primary security performance is improved significantly in the proposed protocol and is improved slightly in the conventional model as the value of σ^2_{SE} becomes larger. Compared with the conventional protocol, our protocol can provide the better primary security performance because the larger value of $\sigma^2_{\mathrm{S_oE}}$ represents the better channel conditions for links ST_o → E. In other words, the interference from ST_o to eavesdropper increases with the increase of

$\sigma^2_{\mathrm{S}_o\mathrm{E}}$. In addition, the interference to eavesdropper from ST_o is greater than that from ST_i. In proposed protocol, both ST_o and ST_i interfere with the eavesdropping. However, the interference to eavesdropper just comes from ST_i in the conventional model and the probability that i is equal to o is $1/K$.

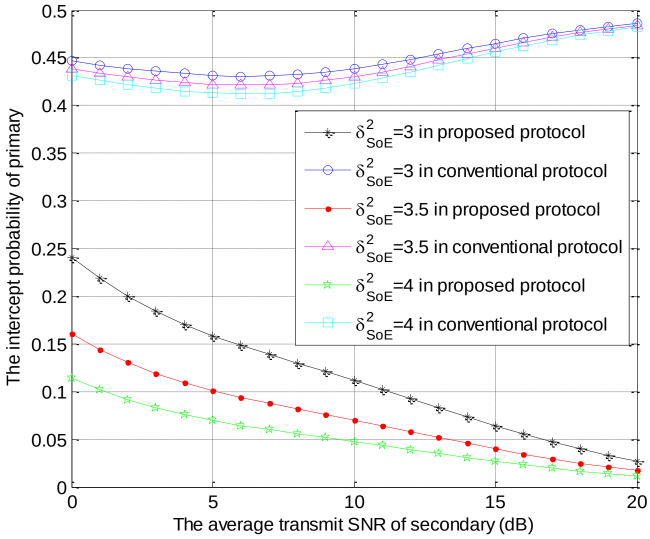

Figure 5. The intercept probabilities of primary users versus r_2 with different σ^2_{SE} values.

The intercept probabilities of primary users versus r_2 with different values of σ^2_{PE} as shown in Figure 6. Namely, the special parameter is the channel coefficient σ^2_{PE}, which equals to 1.2, 1 or 0.8. In Figure 6, a smaller value of σ^2_{PE} can lead to a good primary security performance in the same protocol because a larger value of σ^2_{PE} represents the better channel conditions for links PS → E. In other words, the instantaneous capacity of PS → E increases with the increase of σ^2_{PE}. In the proposed protocol with the larger values of σ^2_{PE}, the primary security performance is enhanced significantly in small value range of r_2 and is enhanced slightly in large value range of r_2. Compared to the conventional protocol, the proposed protocol can provide the better primary security performance. These numerical results are consistent with those in Figures 4 and 5.

The intercept probabilities of primary users versus r_2 with different values of r_1 are shown in Figure 7. Namely, the special parameter is the average SNR of the primary user, which is set as $r_1 = 10\lg(P_{\mathrm{P}}/N_0) = 5$, 10 or 15 dB. In Figure 7, the primary security performance in the proposed protocol is improved as the value of r_1 becomes larger. On the contrary, the primary security performance in the conventional model is reduced as the value of r_1 becomes larger. The valid primary information received by eavesdropper and the interference to eavesdropper are the two main factors related to the security performance of primary system. The more valid primary information is received by the eavesdropper, the worse is primary security performance achieved, and the more interference to he eavesdropper, the greater is primary security performance achieved. In the proposed protocol, the smaller value of r_1 causes the less valid primary information received at eavesdropper, so the smaller intercept probability of the primary system is obtained. In the conventional model, the interference threshold is hard to satisfy with the smaller r_1 and the interference caused by ST_i to eavesdropper is very little, so the larger intercept probability of the primary system is obtained. All of the above numerical results are consistent with the theoretical results in Section 3.

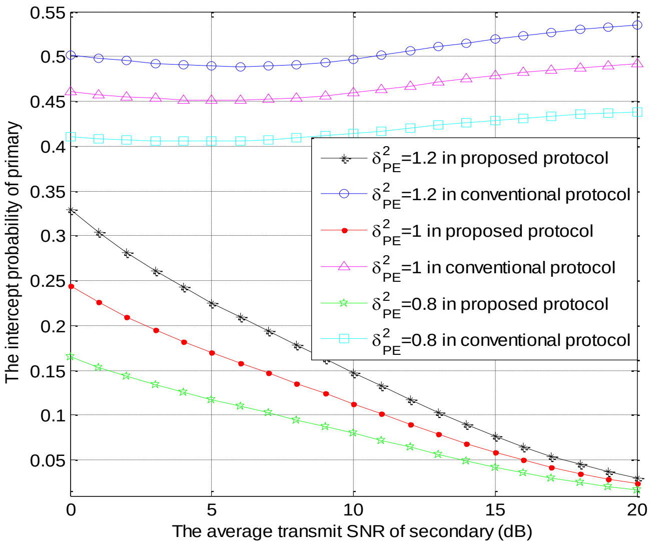

Figure 6. The intercept probabilities of primary users versus r_2 with different σ^2_{PE} values.

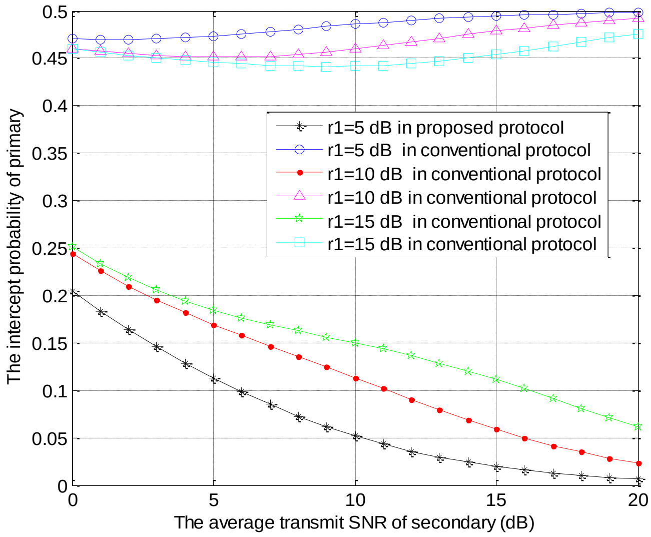

Figure 7. The intercept probabilities of primary users versus r_2 with different r_1 values.

5. Conclusions

In this paper, we have investigated the physical-layer security for a cognitive Internet of things model, which is composed of a primary pair (PS-PD), a secondary receiver (SR), K secondary transmitters and an eavesdropper. To protect the information of primary users against eavesdropping, we have proposed the ST cooperative jammer selection transmission protocol. In return, for the cooperation of ST$_o$, interference threshold for secondary user is relaxed by the primary system compared with the non-security management model. When this interference threshold is satisfied and the best outage performance of secondary users is obtained by selecting ST$_i$, then the secondary user ST$_i$ has access to the licensed spectrum. Due to the cooperation of ST$_o$, the security performance of primary users are enhanced. Due to the cooperation of ST$_o$ and the selection of ST$_i$, the outage performance of secondary users are enhanced in high secondary transmit SNR region. Furthermore, the intercept probability and outage probability of the primary system have been derived. The outage probability of the secondary system has also been obtained. For comparison purposes, the conventional non-security management was also investigated as a baseline. The numerical results have shown that our protocol has better primary secrecy performance than the non-security management model.

In addition, the proposed protocol also has better secondary and primary transmission performance than the conventional model.

Author Contributions: Conceptualization, P.X., L.X., H.W., and I.Y. Formal analysis: P.X. and L.X. Funding acquisition: P.X. and I.Y. Investigation: P.X., L.X., J.T.S., and I.Y. Methodology: P.X., L.X., and I.Y. Performance evaluation: P.X., H.W., and J.T.S. Case study: H.W. and J.T.S. Supervision: P.X. and I.Y. Validation: P.X., L.X., H.W., J.T.S., and I.Y. Visualization: P.X. and L.X. Writing, original draft: P.X., L.X., H.W., J.T.S., and I.Y. Writing, review and editing: P.X., L.X., J.T.S., and I.Y.

Funding: This work was supported by the National Natural Science Foundation of China (NSFC) under Grants No. 61801171 and the Soonchunhyang University Research Fund.

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

Appendix A

Let X_1, X_2, $\hat{X}_3$ and X_4 be exponentially variables with parameters $1/\sigma^2_{\mathrm{P}}$, $1/\sigma^2_{\mathrm{S}_i\mathrm{P}}$, $1/\sigma^2_{\mathrm{S}_o\mathrm{E}}$, $1/\sigma^2_{\mathrm{S}_i\mathrm{E}}$ and $1/\sigma^2_{\mathrm{PE}}$, respectively. Let $\tilde{X}_2 = X_2 + N_0/P_{\mathrm{S}}$, $\tilde{X}_3 = X_3 + \hat{X}_3 + N_0/P_{\mathrm{S}}$, $Y_1 = X_1/\tilde{X}_2$, $Y_2 = X_4/\tilde{X}_3$, and $Y_3 = X_4/(X_3 + N_0/P_{\mathrm{S}})$. Since

$$\begin{aligned} F_{\tilde{X}_2}(\tilde{x}_2) &= \Pr\left\{\tilde{X}_2 < \tilde{x}_2\right\} = \Pr\left\{X_2 < \tilde{x}_2 - N_0/P_{\mathrm{S}}\right\} \\ &= \int_0^{\tilde{x}_2 - N_0/P_{\mathrm{S}}} \frac{1}{\sigma^2_{\mathrm{S}_i\mathrm{P}}} e^{-\frac{x_2}{\sigma^2_{\mathrm{S}_i\mathrm{P}}}} dx_2 = 1 - e^{\frac{N_0}{P_{\mathrm{S}}\sigma^2_{\mathrm{S}_i\mathrm{P}}} - \frac{\tilde{x}_2}{\sigma^2_{\mathrm{S}_i\mathrm{P}}}}, \end{aligned} \tag{A1}$$

we have

$$f_{\tilde{X}_2}(\tilde{x}_2) = \frac{1}{\sigma^2_{\mathrm{S}_i\mathrm{P}}} e^{\frac{N_0}{P_{\mathrm{S}}\sigma^2_{\mathrm{S}_i\mathrm{P}}} - \frac{\tilde{x}_2}{\sigma^2_{\mathrm{S}_i\mathrm{P}}}}. \tag{A2}$$

From Equation (34), we have

$$\begin{aligned} F_{Y_1}(y_1) &= \Pr\left\{X_1/\tilde{X}_2 < y_1\right\} = \Pr\left\{X_1 < \tilde{x}_2 y_1\right\} \\ &= \int_{N_0/P_{\mathrm{S}}}^{\infty} \frac{1}{\sigma^2_{\mathrm{S}_i\mathrm{P}}} e^{-\frac{N_0}{P_{\mathrm{S}}\sigma^2_{\mathrm{S}_i\mathrm{P}}}} e^{-\frac{\tilde{x}_2}{\sigma^2_{\mathrm{S}_i\mathrm{P}}}} \int_0^{\tilde{x}_2 y_1} \frac{1}{\sigma^2_{\mathrm{P}}} e^{-\frac{x_1}{\sigma^2_{\mathrm{P}}}} dx_1 d\tilde{x}_2 \\ &= 1 - \frac{\sigma^2_{\mathrm{P}}}{\sigma^2_{\mathrm{S}_i\mathrm{P}} y_1 + \sigma^2_{\mathrm{P}}} e^{-\frac{N_0}{P_{\mathrm{S}}\sigma^2_{\mathrm{P}}} y_1}. \end{aligned} \tag{A3}$$

Therefore, we obtain

$$f_{Y_1}(y_1) = \left(\frac{\sigma^2_{\mathrm{S}_i\mathrm{P}}\sigma^2_{\mathrm{P}}}{\left(\sigma^2_{\mathrm{P}} + \sigma^2_{\mathrm{S}_i\mathrm{P}} y_1\right)^2} + \frac{N_0/P_{\mathrm{S}}}{\sigma^2_{\mathrm{P}} + \sigma^2_{\mathrm{S}_i\mathrm{P}} y_1} \right) e^{-\frac{N_0 y_1}{P_{\mathrm{S}}\sigma^2_{\mathrm{P}}}}. \tag{A4}$$

Similar to the derivation of the probability density of Y_1, the probability density of random variables Y_3 can obtained by

$$f_{Y_3}(y_3) = \left(\frac{\sigma^2_{\mathrm{S}_o\mathrm{E}}\sigma^2_{\mathrm{PE}}}{\left(\sigma^2_{\mathrm{PE}} + \sigma^2_{\mathrm{S}_o\mathrm{E}} y_3\right)^2} + \frac{N_0/P_{\mathrm{S}}}{\sigma^2_{\mathrm{PE}} + \sigma^2_{\mathrm{S}_o\mathrm{E}} y_3} \right) e^{-\frac{N_0 y_3}{P_{\mathrm{S}}\sigma^2_{\mathrm{PE}}}}. \tag{A5}$$

In addition, since

$$\begin{aligned} F_{\tilde{X}_3}\left(\tilde{x}_3\right) &= \Pr\left\{X_3 < \tilde{x}_3 - \hat{x}_3 - N_0/P_S\right\} \\ &= \int_0^{\infty} \frac{1}{\sigma^2_{S_iE}} e^{-\frac{\hat{x}_3}{\sigma^2_{S_iE}}} \int_0^{\tilde{x}_3 - \hat{x}_3 - N_0/P_S} \frac{1}{\sigma^2_{S_oP}} e^{-\frac{x_3}{\sigma^2_{S_oP}}} dx_3 d\hat{x}_3 \\ &= 1 - \frac{\sigma^2_{S_oE}}{\sigma^2_{S_oE} - \sigma^2_{S_iE}} e^{\frac{N_0}{P_S\sigma^2_{S_oE}} - \frac{\tilde{x}_3}{\sigma^2_{S_oE}}}, \end{aligned} \tag{A6}$$

we have

$$f_{\tilde{X}_3}\left(\tilde{x}_3\right) = \frac{1}{\sigma^2_{S_oE} - \sigma^2_{S_iE}} e^{\frac{N_0}{P_S\sigma^2_{S_oE}} - \frac{\tilde{x}_3}{\sigma^2_{S_oE}}}. \tag{A7}$$

From Equation (A7), we have

$$\begin{aligned} F_{Y_2}\left(y_2\right) &= \Pr\left\{X_4/\tilde{X}_3 < y_2\right\} = \Pr\left\{X_4 < \tilde{x}_3 y_2\right\} \\ &= \int_{N_0/P_S}^{\infty} \frac{1}{\sigma^2_{S_oE} - \sigma^2_{S_iE}} e^{\frac{N_0}{P_S\sigma^2_{S_oE}}} e^{-\frac{\tilde{x}_3}{\sigma^2_{S_oE}}} \int_0^{\tilde{x}_3 y_2} \frac{1}{\sigma^2_{PE}} e^{-\frac{x_4}{\sigma^2_{PE}}} dx_4 d\tilde{x}_3 \\ &= \frac{\sigma^2_{S_oE}}{\sigma^2_{S_oE} - \sigma^2_{S_iE}} \left(1 - \frac{\sigma^2_{PE}}{\sigma^2_{S_oE} y_2 + \sigma^2_{PE}} e^{-\frac{N_0}{P_S\sigma^2_{PE}} y_2}\right). \end{aligned} \tag{A8}$$

Thus, we obtain

$$f_{Y_2}\left(y_2\right) = \frac{e^{-\frac{N_0 y_2}{P_S\sigma^2_{PE}}}}{\sigma^2_{S_oE} - \sigma^2_{S_iE}} \left(\frac{\sigma^2_{PE}}{\left(\sigma^2_{PE}/\sigma^2_{S_oE} + y_2\right)^2} + \frac{\sigma^2_{S_oE} N_0/P_S}{\sigma^2_{PE}/\sigma^2_{S_oE} + y_2}\right). \tag{A9}$$

References

1. Wu, Q.; Ding, G.; Xu, Y.; Feng, S.; Du, Z.; Wang, J.; Long, K. Cognitive Internet of Things: A New Paradigm Beyond Connection. *IEEE Internet Things J.* **2014**, *1*, 129–142. [CrossRef]
2. Song, F.; Ai, Z.; Li, J.; Pau, G.; Collotta, M.; You, I.; Zhang, H. Smart collaborative caching for Information-centric IoT in fog computing. *Sensors* **2017**, *17*, 2512. [CrossRef] [PubMed]
3. Ai, Z.; Liu, Y.; Song, F.; Zhang, H. A smart collaborative charging algorithm for mobile power distribution in 5G networks. *IEEE Access* **2018**, *6*, 28668–28679. [CrossRef]
4. Trihinas, D.; Pallis, G.; Dikaiakos, M. Low-Cost Adaptive Monitoring Techniques for the Internet of Things. *IEEE Trans. Serv. Comput.* **2018**, *99*, 1. [CrossRef]
5. Trihinas, D.; Pallis, G.; Dikaiakos, M. ADMin: Adaptive Monitoring Dissemination for the Internet of Things. In Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017.
6. Tata, S.; Mohamed, M.; Megahed, A. An Optimization Approach for Adaptive Monitoring in IoT Environments. In Proceedings of the 2017 IEEE International Conference on Services Computing (SCC), Honolulu, HI, USA, 25–30 June 2017; pp. 378–385.
7. Lee, Y.-T.; Hsiao, W.-H.; Lin, Y.-S.; Chou, S.-C.T. Privacy-Preserving Data Analytics in Cloud-Based Smart Home with Community Hierarchy. *IEEE Trans. Consum. Electron.* **2017**, *63*, 200–207. [CrossRef]
8. Song, F.; Zhou, Y.; Wang, Y.; Zhao, T.; You, I.; Zhang, H. Smart Collaborative Distribution for Privacy Enhancement in Moving Target Defense. *Inf. Sci.* **2018**. [CrossRef]
9. Ai, Z.; Zhou, Y.; Song, F. A Smart Collaborative Routing Protocol for Reliable Data Diffusion in IoT. *Sensors* **2017**, *18*, 1926. [CrossRef]
10. Uchida, N.; Takeuchi, S.; Ishida, T.; Shibata, Y. Mobile traffic accident prevention system based on chronological changes of wireless signals and sensors. *J. Wirel. Netw. Ubiquitous Comput. Dependable Appl.* **2017**, *8*, 57–66.

11. Kotenko, I.; Saenko, I.; Branitskiy, A. Applying Big Data Processing and Machine Learning Methods for Mobile Internet of Things Security Monitoring. *J. Internet Serv. Inf. Secur.* **2017**, *8*, 54–63.
12. Kotenko, I.; Saenko, I.; Kushnerevich, A. Parallel big data processing for security monitoring in Internet of Things networks. *J. Wirel. Netw. Ubiquitous Comput. Dependable Appl.* **2018**, *8*, 60–74.
13. Afza, A.; Zaidi, S.A.R.; Shakir, M.Z.; Imran, M.A.; Ghogho, M. The Cognitive Internet of Things: A Unified Perspective. *IEEE Mob. Netw. Appl.* **2015**, *20*, 72–85. [CrossRef]
14. Jackson, D.; Zang, W.; Gu, Q.; Yu, M. Robust detection of rogue signals in cooperative spectrum sensing. *J. Internet Serv. Inf. Secur.* **2015**, *5*, 4–23.
15. Mitola, J. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. Ph.D. Thesis, KTH Royal Institute of Technol, Stockholm, Sweden, December 2000.
16. Haykin, S. Cognitive radio: Brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 201–220. [CrossRef]
17. Goldsmith, A.; Jafar, S.; Maric, I.; Srinivasa, S. Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proc. IEEE* **2009**, *97*, 894–914. [CrossRef]
18. Rajesh, K.S.; Danda, B.R. Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1023–1043.
19. Li, J.; Feng, Z.; Feng, Z.; Zhang, P. A Survey of Security Issues in Cognitive Radio Networks. *IEEE J. Mag. China Commun.* **2015**, *12*, 132–150. [CrossRef]
20. Nguyen, V.D.; Hoang, T.M.; Shin, O.S. Secrecy capacity of the primary system in a cognitive radio network. *IEEE Trans. Veh. Technol.* **2015**, *64*, 3834–38435. [CrossRef]
21. Yulong, Z.; Xianbin, W.; Weiming, S. Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks. *IEEE Trans. Commun.* **2013**, *61*, 5103–5113.
22. Zhihui, S.; Yi, Q.; Song, C. On physical layer security for cognitive radio networks. *IEEE Netw.* **2013**, *27*, 28–33. [CrossRef]
23. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
24. Zhang, N.; Lu, N.; Cheng, N.; Mark, J.W.; Shen, X.S. Cooperative spectrum access towards secure information transfer for CRNs. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2453–2464. [CrossRef]
25. Mokari, N.; Parsaeefard, S.; Saeedi, H.; Azmi, P. Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1058–1073. [CrossRef]
26. Xu, D.; Li, Q. Resource allocation for cognitive radio with primary user secrecy outage constraint. *IEEE Syst. J.* **2018**, *12*, 893–904. [CrossRef]
27. Wang, C.; Wang, H.-M. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1814–1827. [CrossRef]
28. Nguyen, V.-D.; Duong, T.Q.; Dobre, O.A.; Shin, O.-S. Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2609–2623. [CrossRef]
29. Elkashlan, M.; Wang, L.; Duong, T.Q.; Karagiannidis, G.K.; Nallanathan, A. On the security of cognitive radio networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 3790–3795. [CrossRef]
30. Yang, L.; Jiang, H.; Vorobyov, S.A.; Chen, J.; Zhang, H. Secure communications in underlay cognitive radio networks: User scheduling and performance analysis. *IEEE Commun. Lett.* **2016**, *20*, 1191–1194. [CrossRef]
31. Zou, Y. Physical-layer security for spectrum sharing systems. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1319–1329. [CrossRef]
32. Pei, Y.; Liang, Y.-C.; Teh, K.C.; Li, K. Secure communication in multiantenna cognitive radio networks with imperfect channel state information. *IEEE Trans. Signal Process.* **2011**, *59*, 1683–1693. [CrossRef]
33. Wang, Z.; Xiao, M.; Skoglund, M.; Poor, H.V. Secure degrees of freedom of wireless networks using artificial noise alignment. *IEEE Trans. Commun.* **2015**, *63*, 2632–2646. [CrossRef]