sensors

MDPI

Article

Secrecy Performance Analysis of Cognitive Sensor Radio Networks with an EH-Based Eavesdropper

Aiwei Sun [1,*,†], Tao Liang [2,†] and Bolun Li [1,†]

1 Institute of Communications Engineering, PLA University of Science and Technology, No. 2 Biaoying, Qinhuai District, Nanjing 210007, China; libolun21@sohu.com
2 Nanjing Telecommunication Technology Institute, No. 18 Houbiaoying, Qinhuai District, Nanjing 210007, China; liangt61@sina.cn
* Correspondence: sunaw0610@126.com; Tel.: +86-137-7063-9680
† These authors contributed equally to this work.

Academic Editors: Yuanyuan Yang and Songtao Guo
Received: 14 January 2017; Accepted: 23 March 2017; Published: 4 May 2017

Abstract: Security and privacy are crucial for cognitive sensor radio networks (CSRNs) due to the possible eavesdropping between secondary sensors and the secondary fusion center. Motivated by this observation, we investigate the physical layer security performance of CSRNs with an external energy harvesting (EH)-based eavesdropper. Considering the underlay working paradigm of CSRNs, the transmit power of the secondary sensor node must be adjusted to guarantee the quality-of-service (*QoS*) of the primary user. Hence, two different interference power constraint scenarios are studied in this paper. To give an intuitive insight into the secrecy performance of the considered wiretap scenarios, we have derived the closed-form analytical expressions of secrecy outage probability for both of the considered cases. Monte Carlo simulation results are also performed to verify the theoretical analysis derived, and show the effect of various parameters on the system performance.

Keywords: physical layer security; cognitive sensor radio networks; secrecy outage performance; Monte Carlo simulations

1. Introduction

Wireless sensor networks (WSNs), which often operate on the unlicensed spectrum (e.g., Industrial, Scientific, Medical (ISM) band), have been widely used in various areas such as environmental monitoring and event detection. However, with the growing proliferation of wireless technologies, the spectrum for WSNs is becoming more and more overcrowded. One promising solution to address this problem is spectrum sharing technologies via cognitive radio (CR). To date, a large number of works have been devoted to the evolution of various aspects of spectrum prediction [1], spectrum sensing [2], and resource management [3]. The above observations provide motivation to study cognitive sensor radio networks (CSRNs) [4,5], which integrate the advantages of CR and WSNs, and have also been considered as an opportunity to realize reliable and low-cost remote monitoring systems.

On the other hand, with the rapid growth of wireless services, energy consumption issues for CSRNs have, in recent years, become increasingly critical, and different energy-efficient optimization algorithms for CSRNs have been investigated [6,7]. However, the sensors are often deployed in remote areas, which makes it inconvenient and infeasible to recharge or replace the batteries frequently. In this situation, energy harvesting (EH) technology has attracted significant interest from industry and the academic community [8,9] because it can effectively alleviate the energy scarcity of WSNs and low-power-consuming equipment. In particular, ambient radio signal can be another safe and convenient energy source since it carries energy and information simultaneously. Consequently, the idea of wireless information and power transfer (WIPT) has been proposed recently, and it has

been studied in different communication scenarios (see, e.g., [10–20] and the references therein). To investigate the energy scarcity problem in energy-constraint wireless networks, the authors of [10] firstly proposed a capacity-energy function to characterize the fundamental tradeoffs in WIPT systems. In [11], the authors extended the work in [10] to include frequency-selective single antenna additive white Gaussian noise (AWGN) channels with the average power constraint. In addition, various beam-forming technologies have been proposed in diverse scenarios such as broadcast channels [12–16], relaying channels [17,18], interference channels [19,20], to optimize the transmission performance at the information decoding (ID) users and the harvested energy at the EH users simultaneously.

Moreover, due to the openness of the wireless medium, the dual purposes of energy and information transmission, and the dynamic architecture of the CR system, the wireless information in CSRNs is more susceptible to eavesdropping [21]. Besides, owing to its capability of both information decoding and energy harvesting, the confidential information of secondary transmission can be easily overheard by the EH-based eavesdropper. However, traditional cryptographic techniques will face great challenges, since the eavesdropper can decode the confidential information with the development of the computational ability of a computer. Thus, physical layer security is now emerging as a complementary secure communication method to defend against eavesdroppers, which can effectively enhance the secrecy performance of wireless channels [22–24]. Moreover, physical layer security has also been studied in various multi-antenna WIPT systems [25–27].

Note that the aforementioned works mainly focus on the aspects of transmission strategy design [28], performance optimization algorithm [29,30], resource management [31–33], and few works have investigated the secrecy performance analysis of CSRNs. Different from [23,34], this paper investigates the physical layer security performance of CSRNs with an EH-based enemy fusion center, wherein, due to the PU's interference temperature constraint, the transmit power of the secondary sensor transmitter (ST) is largely restrained, which has greatly affected the system transmission performance of the secondary sensor network. In addition, the EH-based enemy fusion center has the capability to overhear the confidential message of ST if they do not harvest energy as presumed. In this context, we investigate the impact of an EH-based eavesdropper on the physical layer security performance of the CSRNs. The main contributions of this paper can be summarized as follows:

(1) Considering the interference temperature issues of PU, the closed-form expressions of the secrecy outage probability (SOP) and the average secrecy rate (ASR) are derived, which are validated by Monte Carlo simulations;
(2) Two different scenarios are studied: Case 1, the transmit power of the ST is only affected by the interference power constraint of the PU, and Case 2, the transmit power of the ST is limited by the maximal transmit power of ST itself and the interference power constraint for PU simultaneously;
(3) The effects of various parameters, (such as power splitting factor, link power gain ratio, target secrecy rate), on the physical layer secrecy performance of the CSRNs are investigated, which can give an intuitive insight into the secrecy performance of the considered system.

The remainder of this paper is organized as follows. System model and channel model are introduced in Section 2. In Section 3, we investigate the secrecy performance of the considered system, and derive the closed-form expressions of the secrecy performance metrics for two cases. Numerical results are presented to illustrate the proposed solutions in Section 4. Finally, Section 5 provides some concluding remarks.

2. System Model

We consider an underlay CSRN as shown in Figure 1, which consists of an unlicensed secondary user (SU) system, a licensed primary user (PU) system, and an external eavesdropper. The SU system consists of a secondary source sensor (S) and a secondary information fusion center (D), which share the same spectrum band with the licensed PU system. Here, we assume that the PU system consists of a single antenna primary receiver (P) as in [35]. The primary transmitter is located far away from

the CSRN. Thus, it causes no interference to the SUs. An EH-based enemy fusion center (E) acts as a potential eavesdropper to overhear the SUs' confidential information. All communication nodes are equipped with one antenna, they also operate in time slot mode for easy implementation. We further assume an independent and quasi-static Rayleigh fading channel model, such that the channel state information remain unchanged during each packet duration, but independently vary from one block to another block. We denote h_{ab} as the instantaneous link power gain of the link '$a \rightarrow b$', where, a denotes the transmitter S, and b denotes the corresponding receivers, with $b \in \{\mathrm{P}, \mathrm{D}, \mathrm{E}\}$, all link power gains are random variables (RVs) and subject to exponential distribution with parameter, $\lambda_{ab} = 1/\Omega_{ab}$, Ω_{ab} denotes the variances of h_{ab}. Specifically, h_{sp}, h_{sd} and h_{se} are denoted as the channel gains of the link S→P, S→D and S→E, respectively.

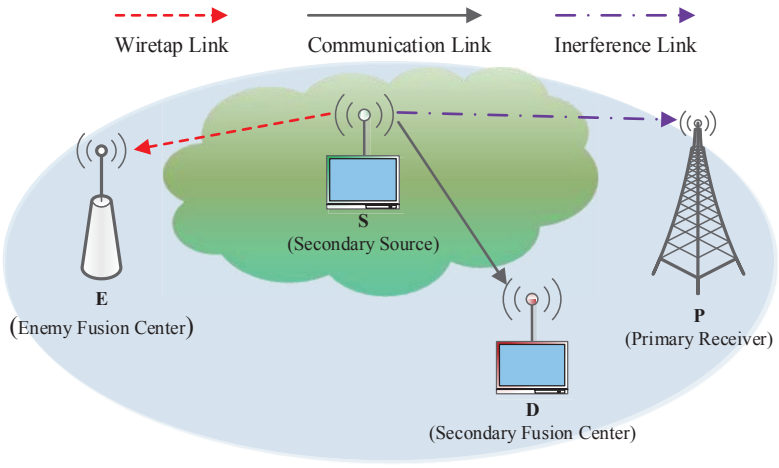

Figure 1. Cognitive sensor radio network system model.

In this paper, the basic power splitting architecture of the EH receiver is shown in Figure 2. This was initially proposed in [12]. The received radio frequency (RF) signal at the EH receiver is then split into a dynamic power splitter (DPS), no noise is assumed to be induced at the DPS. After the DPS, one part of the received power is used for information decoding, which takes about a $\rho\,(t)$ portion of the total received power; the other $1-\rho\,(t)$ part is used for energy harvesting. For the eavesdropper, the received signal will be converted to baseband signal after a series of standard operations. As a result, the signal will be corrupted by another noise $n_{\mathrm{p}}(t)$, which is assumed to be AWGN with variance σ_{p}^2.

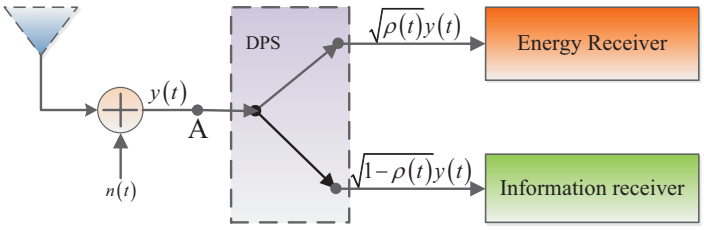

Figure 2. Power splitting architecture of the energy harvesting (EH)-based enemy fusion center.

By denoting $x(t)$ as the data packet transmitted to Y at time t, with $E\left(|x\,(t)|^2\right) = 1$, the signals received at the D and E (potential eavesdropper) can be given as

$$y_D = \sqrt{P_{\mathrm{t}} \cdot h_{\mathrm{sd}}(t)}x(t) + n_D(t), \tag{1}$$

$$y_E = \sqrt{\rho\,(t)}\sqrt{P_{\mathrm{t}} \cdot h_{\mathrm{se}}(t)}x(t) + n_E(t) + n_{\mathrm{p}}(t), \tag{2}$$

respectively, where, P_{t} is the transmit power of the S, $n_D(t)$ and $n_E(t)$ are the signal processing noise at the D and E, with noise power N_0. The time index t is ignored below unless necessary in the sequel for notational convenience.

3. Secrecy Performance Analysis

In this section, physical layer security issues of the considered cognitive sensor system are investigated, and we concentrate on the performance metrics, including secrecy outage probability and average secrecy rate, which can provide an intuitive insight into the impact of the various system parameters on the transmission security. Then, considering the underlay working mode of the CSRN, two cases are considered. Case 1: we consider that the transmit power of the S is only affected by the interference power constraint of the primary users, and Case 2, we consider that the transmit power of the S is limited by the maximal transmit power of itself and the interference power constraint for P simultaneously, which will be investigated separately in the follow-up work.

3.1. Case 1: Interference Power Constraint for the Secondary Transmitter

Considering the interference temperature constraint of the P, the transmit power of S is mainly limited by interference power to the P, which is a common assumption [36]. Thus, the transmit power of the S can be given as

$$P_{\mathrm{t}} = \frac{P_{\mathrm{th}}}{h_{\mathrm{sp}}}, \tag{3}$$

where, P_{th} is the predefined interference power threshold, which denotes the maximal interference power that S are allowed to cause to the P. After this, the signal-to-noise ratios (SNRs) at D and E are given as

$$\psi_D = \frac{P_{\mathrm{th}} h_{\mathrm{sd}}}{N_0 h_{\mathrm{sp}}}, \tag{4}$$

$$\psi_E = \frac{\rho P_{\mathrm{th}} h_{\mathrm{se}}}{\left(\rho N_0 + \sigma_p^2\right) h_{\mathrm{sp}}}, \tag{5}$$

respectively. By denoting: $u = h_{\mathrm{sp}}$, $x = \psi_D$, $y = \psi_E$, ψ_D and ψ_E are also subject to expontional distribution with parameters λ_{ψ_D} and λ_{ψ_E}, and their probability density functions (PDFs) can be expressed as

$$f_{\psi_D}(x) = \lambda_{\psi_D} \exp\left(-\lambda_{\psi_D} x\right), \tag{6}$$

$$f_{\psi_E}(y) = \lambda_{\psi_E} \exp\left(-\lambda_{\psi_E} y\right), \tag{7}$$

where,

$$\lambda_{\psi_D} = \frac{\lambda_{\mathrm{sd}} N_0 u}{P_{\mathrm{th}}}, \tag{8}$$

$$\lambda_{\psi_E} = \frac{\left(\rho N_0 + \sigma_p^2\right) \lambda_{\mathrm{se}} u}{\rho P_{\mathrm{th}}}, \tag{9}$$

respectively.

Based on the above analysis, the instantaneous secrecy capacity of secondary transmission link can be further given as follows:

$$C_{\mathrm{sec}}(u) = \left[\log_2(1+\psi_D) - \log_2(1+\psi_E)\right]^+, \tag{10}$$

here, $[x]^+ = \max\{x, 0\}$.

3.1.1. Secrecy Outage Probability

As in previous works [22–25], the SOP is defined as the probability that instantaneous secrecy rate is below a predefined threshold value R_s.

Lemma 1. *The secrecy outage probability of the considered system under the predefined R_s for the first case can be calculated as,*

$$\mathrm{SOP}\left(R_s\right) = 1 - \frac{K\lambda_{sp}P_{th}}{L + \lambda_{sp}P_{th}}, \tag{11}$$

where,

$$K = \frac{\left(\rho N_0 + \sigma_p^2\right)\lambda_{se}}{\rho N_0 \lambda_{sd} 2^{R_s} + \left(\rho N_0 + \sigma_p^2\right)\lambda_{se}}, L = N_0\lambda_{sd}\left(2^{R_s} - 1\right). \tag{12}$$

Based on Equations (11) and (12), the exact SOP value for Case 1 can be calculated under arbitrary predefined target secrecy rate R_s and arbitrary interference power threshold P_{th}, which can effectively show the physical layer security performance of the considered system.

Proof. From Equation (10), the SOP conditioned on u can be expressed as

$$\begin{aligned} \mathrm{SOP}\left(R_s\,|u\right) &= \Pr\left(C_{sec}\left(u\right) < R_s\right) \\ &= \Pr\left(\log_2\left(\frac{1+\psi_D}{1+\psi_E}\right) < R_s\right) \\ &= \Pr\left(\psi_D - \alpha\psi_E < \alpha - 1\right), \end{aligned} \tag{13}$$

where, $\Pr\left(\cdot\right)$ denotes the probability of the closed. For notational convenience, we denote, $\alpha = 2^{R_s}$. Recall from Equation (7), the PDF of $\alpha\psi_E$ should be firstly obtained as

$$f_{\alpha\psi_E}\left(x\right) = \frac{\lambda_{\psi_E}}{\alpha}\exp\left(-\frac{\lambda_{\psi_E}}{\alpha}x\right). \tag{14}$$

□

Further, let us denote $z = \psi_D - \alpha\psi_E$, combining Equations (6) and (13), the PDF of z can be calculated as follows:

$$f_Z(z) = \begin{cases} \int_0^\infty f_{\psi_D}(z+x)\cdot f_{\alpha\psi_E}(x)dx = A, & z \geq 0 \\ \int_{-z}^\infty f_{\psi_D}(z+x)\cdot f_{\alpha\psi_E}(x)dx = B, & z < 0 \end{cases}. \tag{15}$$

After some multiplications and transformations, A and B are easy to be calculated as

$$A = \frac{\lambda_{\psi_D}\lambda_{\psi_E}}{\alpha\lambda_{\psi_D} + \lambda_{\psi_E}}\exp\left(-\lambda_{\psi_D}z\right), \tag{16}$$

$$B = \frac{\lambda_{\psi_D}\lambda_{\psi_E}}{\lambda_{\psi_E} + \alpha\lambda_{\psi_D}}\exp\left(\frac{\lambda_{\psi_E}z}{\alpha}\right). \tag{17}$$

Based on the aforementioned analysis, the SOP $(R_s\,|u\,)$ can be further calculated as Equation (18).

$$\begin{aligned}\mathrm{SOP}\,(R_s\,|u\,) &= \int_{-\infty}^{0} B dz + \int_{0}^{\alpha-1} A dz \\ &= \int_{-\infty}^{0} \frac{\lambda_{\psi_D}\lambda_{\psi_E}}{\lambda_{\psi_E}+\alpha\lambda_{\psi_D}} \exp\left(\frac{\lambda_{\psi_E} z}{\alpha}\right) dz \\ &\quad + \int_{0}^{\alpha-1} \frac{\lambda_{\psi_D}\lambda_{\psi_E}}{\alpha\lambda_{\psi_D}+\lambda_{\psi_E}} \exp\left(-\lambda_{\psi_D} z\right) dz \\ &= 1 - \frac{\lambda_{\psi_E}\exp\left(-\lambda_{\psi_D}\alpha+\lambda_{\psi_D}\right)}{\alpha\lambda_{\psi_D}+\lambda_{\psi_E}}\end{aligned} \tag{18}$$

Substitute Equations (8) and (9) into Equation (18), the SOP $(R_s\,|u\,)$ can also be denoted as

$$\mathrm{SOP}\,(R_s\,|u\,) = 1 - K\exp\left(-\frac{Lu}{P_{\mathrm{th}}}\right), \tag{19}$$

where, K and L have been denoted in Equation (12).

Under PU's interference temperature constraint, the closed-form expressions for SOP (R_s) of secondary transmission can be calculated as

$$\mathrm{SOP}\,(R_s) = \int_{0}^{\infty} \mathrm{SOP}\,(R_s\,|u\,)\, f_{h_{sp}}(u)\, du, \tag{20}$$

where, $f_{h_{sp}}(u)$ is the PDF of h_{sp}, with $f_{h_{sp}}(u) = \lambda_{sp}\exp\left(-\lambda_{sp}u\right)$, the link power gain between S and P, which is also a exponential variable according to previous assumptions [37].

After some multiplications, combining Equation (18) with Equation (20), the SOP (R_s) for Case 1 can be calculated as

$$\begin{aligned}\mathrm{SOP}\,(R_s) &= \int_{0}^{\infty}\left[1 - K\exp\left(-\frac{uL}{P_{\mathrm{th}}}\right)\right]\lambda_{sp}\exp\left(-\lambda_{sp}u\right) du \\ &= 1 - \frac{K\lambda_{sp}P_{\mathrm{th}}}{L+\lambda_{sp}P_{\mathrm{th}}}\end{aligned} \tag{21}$$

Thus, we have Equations (11) and (12).

3.1.2. Average Secrecy Rate

As defined in previous works [25–34], secrecy capacity is the maximum rate at which the destination can decode the packets, while the eavesdropper's bit error probability of decodes approaches one. Here, we will derive the closed-form expressions of average secrecy rate (ASR) based on the fading characteristic of the Rayleigh fading channel. Under the predefined interference value P_{th} of P, the ASR can be given as

$$C_{\mathrm{sec}}^{\mathrm{ave}}\,(P_{\mathrm{th}}) = \int_{0}^{\infty} C_{\mathrm{sec}}^{\mathrm{ave}}\,(P_{\mathrm{th}}\,|u\,)\, f_{h_{sp}}(u)\, du, \tag{22}$$

and

$$\begin{aligned}C_{\mathrm{sec}}^{\mathrm{ave}}\,(P_{\mathrm{th}}\,|u\,) &= \int_{0}^{\infty}\int_{0}^{\infty} C_{\mathrm{sec}}\,(P_{\mathrm{th}}\,|u\,) \\ &\quad \times f_{\psi_D}(\psi_D)\, f_{\psi_E}(\psi_E)\, d_{\psi_D} d_{\psi_E},\end{aligned} \tag{23}$$

where, $f_{\psi_D}(\psi_D)$, and $f_{\psi_E}(\psi_E)$ are the probability density function of ψ_D, and ψ_E, respectively, which have been given in Equations (6) and (7).

By using the fact that all channels are assumed to suffer the independent and identical Rayleigh distribution, the ASR can also be calculated as

$$C_{\text{sec}}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=\frac{1}{\ln 2}C_{s1}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)-\frac{1}{\ln 2}C_{s2}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right) \tag{24}$$

where, $C_{s1}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)$ and $C_{s2}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)$ can be calculated as Equations (25) and (26), respectively.

$$\begin{aligned}C_{s1}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=&\int_0^{\infty}\int_0^{\psi_D}\ln\left(1+\psi_D\right)f_{\psi_D}\left(\psi_D\right)\\&\times f_{\psi_E}\left(\psi_E\right)d\psi_D d\psi_E,\end{aligned} \tag{25}$$

$$\begin{aligned}C_{s2}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=&\int_0^{\infty}\int_{\psi_E}^{\infty}\ln\left(1+\psi_E\right)f_{\psi_D}\left(\psi_D\right)\\&\times f_{\psi_E}\left(\psi_E\right)d_{\psi_D}d_{\psi_E},\end{aligned} \tag{26}$$

For easy calculation, we denote: $x=\psi_D$, $y=\psi_E$, combining with Equations (6) and (7), and by using Equation (27) in [38],

$$\int_0^{\infty}e^{-\mu x}\ln\left(1+\beta x\right)dx=-\frac{1}{\mu}\exp\left(\frac{\mu}{\beta}\right)\text{Ei}\left(-\frac{\mu}{\beta}\right), \tag{27}$$

the $C_{s1}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)$ and $C_{s2}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)$ can be further given as follows:

$$\begin{aligned}C_{s1}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=&\int_0^{\infty}\ln\left(1+x\right)f_x\left(x\right)dx\int_0^{x}f_y\left(y\right)dy\\=&\frac{\lambda_{\psi_D}}{\lambda_{\psi_D}+\lambda_{\psi_E}}\exp\left(\lambda_{\psi_D}+\lambda_{\psi_E}\right)\text{Ei}\left(-\lambda_{\psi_D}-\lambda_{\psi_E}\right)\\&-\exp\left(\lambda_{\psi_D}\right)\text{Ei}\left(-\lambda_{\psi_D}\right),\end{aligned} \tag{28}$$

$$\begin{aligned}C_{s2}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=&\int_0^{\infty}\ln\left(1+y\right)f_y\left(y\right)dy\int_y^{\infty}f_x\left(x\right)dx\\=&-\frac{\lambda_{\psi_E}}{\lambda_{\psi_E}+\lambda_{\psi_D}}\exp\left(\lambda_{\psi_E}+\lambda_{\psi_D}\right)\\&\times\text{Ei}\left(-\lambda_{\psi_E}-\lambda_{\psi_D}\right),\end{aligned} \tag{29}$$

respectively, where, $\text{Ei}\left(x\right)$ is the exponential integral function [38]. Substituting Equations (28) and (29) into Equation (24), the ASR conditioned on u can be calculated as

$$\begin{aligned}C_{\text{sec}}^{\text{ave}}\left(P_{\text{th}}\left|u\right.\right)=&\frac{1}{\ln 2}\exp\left(\lambda_{\phi_D}+\lambda_{\phi_E}\right)\text{Ei}\left(-\lambda_{\phi_D}-\lambda_{\phi_E}\right)\\&-\frac{1}{\ln 2}\left(\exp\left(\lambda_{\phi_D}\right)\text{Ei}\left(-\lambda_{\phi_D}\right)\right).\end{aligned} \tag{30}$$

From Equations (22) and (30), the ASR can be given as Equation (31).

$$\begin{aligned}C_{\text{sec}}^{\text{ave}}\left(P_{\text{th}}\right)=&\frac{\lambda_{\text{sp}}}{\ln 2}\int_0^{\infty}\exp\left(-\lambda_{\text{sp}}u\right)\exp\left(\frac{\rho N_0\left(\lambda_{\text{sd}}+\lambda_{\text{se}}\right)+\sigma^2\lambda_{\text{se}}}{\rho P_{\text{th}}}u\right)\\&\times\text{Ei}\left(-\frac{\rho N_0\left(\lambda_{\text{sd}}+\lambda_{\text{se}}\right)+\sigma^2\lambda_{\text{se}}}{\rho P_{\text{th}}}u\right)du\\&-\frac{\lambda_{\text{sp}}}{\ln 2}\int_0^{\infty}\exp\left(-\lambda_{\text{sp}}u\right)\exp\left(\frac{N_0\lambda_{\text{sd}}}{P_{\text{th}}}u\right)\text{Ei}\left(-\frac{N_0\lambda_{\text{sd}}}{P_{\text{th}}}u\right)du\end{aligned} \tag{31}$$

Based on the aforementioned analysis, by using the following Equation (32) in [38],

$$\int_0^\infty \mathrm{Ei}\left(-\beta x\right)\exp\left(-\mu x\right)\mathrm{d}x = -\frac{1}{\mu}\ln\left(1+\frac{\mu}{\beta}\right), \tag{32}$$

and performing some simple mathematical manipulations, we obtain the final closed-form expressions of the ASR for Case 1 as

$$\begin{aligned} C_{\mathrm{sec}}^{\mathrm{ave}}\left(P_{\mathrm{th}}\right) &= \frac{\lambda_{\mathrm{sp}}}{\ln 2}\int_0^\infty \exp\left(-\Xi_1 x\right)\mathrm{Ei}\left(-\Xi_2 x\right)dx \\ &\quad - \frac{\lambda_{\mathrm{sp}}}{\ln 2}\int_0^\infty \exp\left(-\Xi_3 x\right)\mathrm{Ei}\left(-\Xi_4 x\right)dx \\ &= \frac{\lambda_{\mathrm{sp}}}{\ln 2}\left[\frac{1}{\Xi_3}\ln\left(1+\frac{\Xi_3}{\Xi_4}\right) - \frac{1}{\Xi_1}\ln\left(1+\frac{\Xi_1}{\Xi_2}\right)\right] \end{aligned} \tag{33}$$

where,

$$\begin{aligned} \Xi_1 &= \frac{\lambda_{\mathrm{sp}}\rho P_{\mathrm{th}} - \rho N_0\lambda_{\mathrm{se}} - \sigma^2\lambda_{\mathrm{se}} - \rho N_0\lambda_{\mathrm{sd}}}{\rho P_{\mathrm{th}}}, \\ \Xi_2 &= \frac{\rho N_0\lambda_{\mathrm{se}} + \sigma^2\lambda_{\mathrm{se}} + \rho N_0\lambda_{\mathrm{sd}}}{\rho P_{\mathrm{th}}}, \\ \Xi_3 &= \frac{\lambda_{\mathrm{sp}}P_{\mathrm{th}} - N_0\lambda_{\mathrm{sd}}}{P_{\mathrm{th}}}, \\ \Xi_4 &= \frac{N_0\lambda_{\mathrm{sd}}}{P_{\mathrm{th}}}. \end{aligned} \tag{34}$$

Based on Equations (33) and (34), the exact ASR value for Case 1 can be easily calculated under arbitrary interference power threshold P_{th}.

3.2. Case 2: Maximum Source Power Constraint and Interference Power Constraint for the Secondary Transmitter

In this section, we consider the case that the transmit power of the secondary sensor is limited not only by the interference constraint of the PU system, but also the maximal source power of the S itself. The adoption of this assumption is not intended to complicate the system model, but to address a more practical scenario in wireless communication system. In this case, the transmit power of S can be given as

$$P_{\mathrm{t}} = \min\left(P_{\max}, \frac{P_{\mathrm{th}}}{h_{\mathrm{sp}}}\right), \tag{35}$$

where, $P_{\max}$ is the allowable power of S, $\min\left(\cdot,\cdot\right)$ denotes the minimum value of the two variables in the parentheses. The SNRs at D and E are given as

$$\phi_D = \frac{\min\left(P_{\max}, P_{\mathrm{th}}/h_{\mathrm{sp}}\right)h_{\mathrm{sd}}}{N_0}, \tag{36}$$

$$\phi_E = \frac{\rho\min\left(P_{\max}, P_{\mathrm{th}}/h_{\mathrm{sp}}\right)h_{\mathrm{se}}}{\rho N_0 + \sigma_p^2}, \tag{37}$$

respectively. By denoting: $v = h_{\mathrm{sp}}$, the ϕ_D and ϕ_E are also subject to expontional distribution with parameter λ_{ϕ_D} and λ_{ϕ_E}, where,

$$\lambda_{\phi_D} = \frac{N_0}{\min\left(P_{\max}, P_{th}/v\right)}\lambda_{\mathrm{sd}}, \tag{38}$$

$$\lambda_{\phi_E} = \frac{\rho N_0 + \sigma_p^2}{\rho\min\left(P_{\max}, P_{\mathrm{th}}/v\right)}\lambda_{\mathrm{se}}. \tag{39}$$

Here, we adopt the same calculation procedure as that from Equation (6) to Equation (19). After performing some mathematical manipulations, the SOP $(R_s\,|v\,)$ can also be obtained as

$$\mathrm{SOP}\,(R_\mathrm{s}\,|v\,) = 1 - K\exp\left(-\frac{L}{\min\left(P_\mathrm{max}, P_\mathrm{th}/v\right)}\right). \tag{40}$$

Under PU's interference temperature constraint, the closed-form expressions for the SOP (R_s) can be calculated as

$$\mathrm{SOP}\,(R_\mathrm{s}) = \int_0^\infty \mathrm{SOP}\,(R_\mathrm{s}\,|v\,)\, f_{h_\mathrm{sp}}\,(v)\, dv, \tag{41}$$

After some calculation, the final closed-form expressions of the SOP for Case 2 can be expressed as Equation (42) at the top of the next page.

$$\begin{aligned}\mathrm{SOP}\,(R_\mathrm{s}) = &\int_0^{\frac{P_\mathrm{th}}{P_\mathrm{max}}}\left[1 - K\exp\left(-\frac{L}{\min\left(P_\mathrm{max}, P_\mathrm{th}/x\right)}\right)\right]\lambda_\mathrm{sp}\exp\left(-\lambda_\mathrm{sp}x\right)dx\\ &+\int_{\frac{P_\mathrm{th}}{P_\mathrm{max}}}^{+\infty}\left[1 - K\exp\left(-\frac{L}{\min\left(P_\mathrm{max}, P_\mathrm{th}/x\right)}\right)\right]\lambda_\mathrm{sp}\exp\left(-\lambda_\mathrm{sp}x\right)dx\\ &= 1 - K\left[\exp\left(-\frac{L+\lambda_\mathrm{sp}P_\mathrm{th}}{P_\mathrm{max}}\right) + \exp\left(-\frac{L}{P_\mathrm{max}}\right)\right]\\ &-\frac{\lambda_\mathrm{sp}KP_\mathrm{th}}{L + P_\mathrm{th}\lambda_\mathrm{sp}}\exp\left(-\frac{L+\lambda_\mathrm{sp}P_\mathrm{th}}{P_\mathrm{max}}\right),\end{aligned} \tag{42}$$

Equations (11) and (42) give the analytical expressions of the SOP for two distinct scenarios, which can effectively measure the secrecy performance of the considered system, and show the impact of various parameters on the secrecy performance. In the following sections, we will validate the accuracy of the analytical expressions derived through Monte Carlo simulations.

4. Discussions

For a cognitive radio sensor network with EH function for the eavesdropper, two conflicting goals exist: the power of the received signal at the eavesdropper is needs to be large for efficient energy harvesting, but it is also needs to be sufficient to decode more confidential information. The performance boundary of the two goals is mainly determined by the ratio of power splitting, which has a great effect on the secrecy performance of the information transmission. In this subsection, we will investigate the average amount of the harvested power under specified system and channel condition. According to the previous assumptions, the instantaneous harvested power can be calculated as follows:

$$\begin{aligned}P_\mathrm{EH} &= (1-\rho)\times P_\mathrm{t}\times h_\mathrm{se}\\ &= (1-\rho)\times h_\mathrm{se}\times\min\left(P_\mathrm{max}, P_\mathrm{th}/h_\mathrm{sp}\right).\end{aligned} \tag{43}$$

Let us denote: $x = h_\mathrm{sp}$, and $y = h_\mathrm{se}$, the average harvested power can be given as

$$\begin{aligned}P_\mathrm{EH}^\mathrm{ave} &= \int_0^\infty\int_0^\infty P_\mathrm{EH}\times f_{h_\mathrm{sp}}\,(x)\, f_{h_\mathrm{se}}\,(y)dxdy\\ &= (1-\rho)\times\lambda_\mathrm{se}\lambda_\mathrm{sp}\int_0^\infty xe^{-\lambda_\mathrm{se}x}dx\\ &\times\int_0^\infty\min\left(P_\mathrm{max}, P_\mathrm{th}/y\right)e^{-\lambda_\mathrm{sp}y}dy.\end{aligned} \tag{44}$$

With the help of the expressions in [38]

$$\int_1^\infty\frac{e^{-\mu x}}{x}dx = -\mathrm{Ei}\,(-\mu). \tag{45}$$

After some multiplications, the final closed-form expressions of average harvested power can be given as

$$P_{\mathrm{EH}}^{\mathrm{ave}} = \frac{(1-\rho)\times P_{\max}}{\lambda_{\mathrm{se}}}\left(1-\exp\left(-\frac{\lambda_{\mathrm{sp}}P_{\mathrm{th}}}{P_{\max}}\right)\right) - \frac{(1-\rho)\times \lambda_{\mathrm{sp}}P_{\mathrm{th}}}{\lambda_{\mathrm{se}}}\mathrm{Ei}\left(-\frac{\lambda_{\mathrm{sp}}P_{\mathrm{th}}}{P_{\max}}\right), \tag{46}$$

where, $\mathrm{Ei}(x)$ is the same exponential integral function as in Equation (27).

5. Simulation Results and Analysis

We have given system model and channel characteristic description in Section 2. Here, numerical results are presented to highlight the impact of various parameters on secure performance of CSRNs. Recall that all channels experience independent and identical Rayleigh fading. Unless otherwise specified, the relevant simulation parameter can be set as follows: $\Omega_{\mathrm{sp}} = 10\,\mathrm{dB}$, $\lambda_{\mathrm{sp}} = 1/\Omega_{\mathrm{sp}}$, $\Omega_{\mathrm{sd}} = 30\,\mathrm{dB}$, $\lambda_{\mathrm{sd}} = 1/\Omega_{\mathrm{sd}}$, $\tau = \Omega_{\mathrm{se}}/\Omega_{\mathrm{sd}}$, $N_0 = 1$, $\sigma_p^2 = 0.9$. For the EH-based eavesdropper, ρ portion of the total received power is used for information decoding, and the other remaining $1-\rho$ portion is used for energy harvesting. All communication nodes have a single antenna, and work in time slot mode.

5.1. Simulation Results for Case 1

For the case 1, considering the quality-of-service (QoS) of the PU system, the transmit power of the secondary sensor is limited by the interference constraint effect. the analytical curves of the SOP are obtained from Equations (11) and (12).

Figure 3 gives the SOP performance versus the ratio τ for various power splitting factor ρ, under different interference power threshold P_{th} for P. For all cases, the derived analytical expressions are in great agreement with the simulation results. We can easily see that: (1) the SOP will decrease with the increase of the τ, which is an expected result, since the main channel has better quality than the wiretap channel; (2) with the same P_{th} and τ, if we increase the value of ρ, the SOP will be decreased, due to the fact that, higher values of ρ mean more power for the information decoding, which can lead to better secrecy performance; (3) with the same value of τ and ρ, if P_{th}, the interference power threshold is enlarged, and the secrecy performance can be further improved.

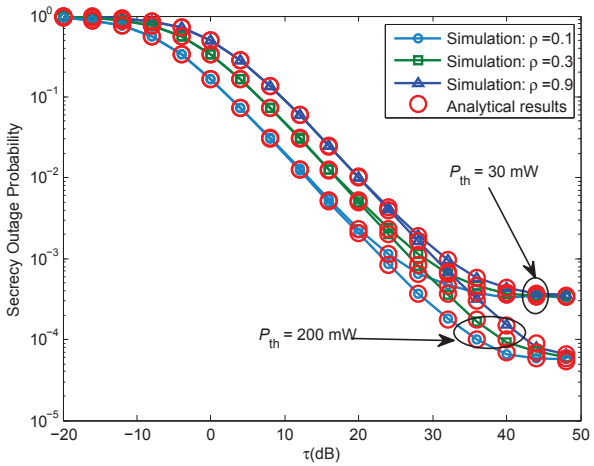

Figure 3. Case 1: Secrecy outage probability versus τ, when P_{th} = [30, 200] mW, R_{s} = 1 bits/Hz/s, ρ = [0.1, 0.3, 0.9].

Figure 4 gives the SOP performance of the considered system versus τ and various ρ of the EH receiver. For easy implantation, only analytical results are showed in this figure. As can be seen, the SOP apparently decreases with the increase of the EH receiver's harvested power. These are the expected results since the two goals represent a conflict between the amount of the harvested energy and the rate of the wiretapped information, and they all have a relationship with ρ, the power-splitting factor of the EH-based eavesdropper, if the eavesdropper prefers to harvest more energy through EH function, then less power remains to decode the information, and the secrecy rate of the secondary receiver will decrease, and vice versa.

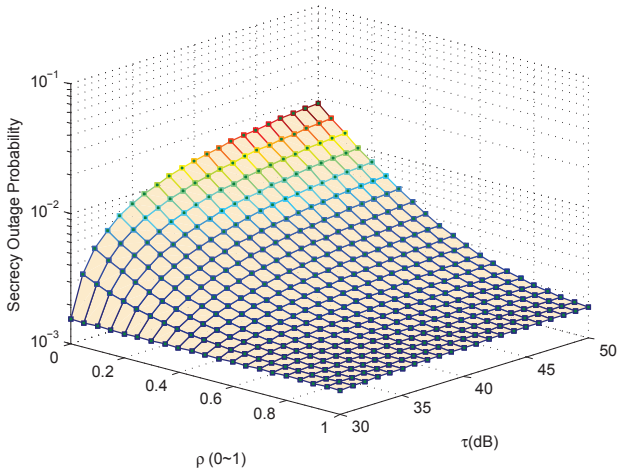

Figure 4. Case 1: Secrecy outage probability versus τ and ρ, when P_{th} = 200 mW, R_{s} = 5 bits/Hz/s.

Figure 5 gives the ASR versus the ratio τ for various ρ, under different interference power thresholds, P_{th} =[10, 100] dBW is provided. For all cases, we can observe that the proposed analytical expressions of ASR given by Equations (33) and (34) are in great agreement with the simulation results, which corroborates the accuracy of the analytical expressions. In addition, the ASR will increase with the increase of the ratio τ, and then converge to a relatively fixed value, since the system performance is limited by the interference power constraint of PR in the high τ region. In addition, as expected, under the same value of τ and ρ, if we enlarge P_{th}, the interference power threshold, the ASR can be further increased.

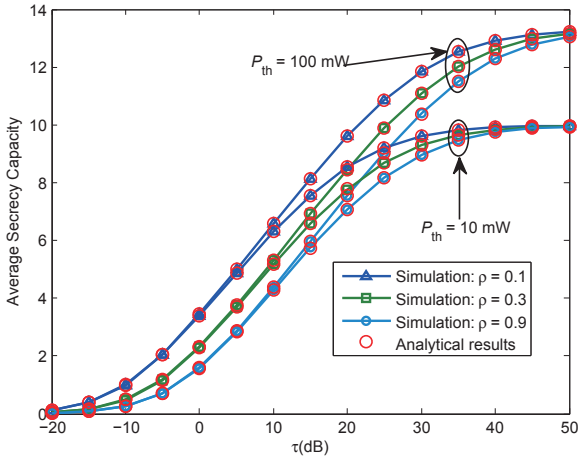

Figure 5. Case 1: Average secrecy rate versus τ, when P_{th} = 100 mW, R_{s} = 5 bits/Hz/s, ρ = 0.9.

5.2. Simulation Results for Case 2

In this section, we will consider the second case, the analytical curves of the SOP are obtained from Equation (42), the simulation results are presented as follows:

Figure 6 gives the SOP performance versus the ratio τ for various ρ, $\rho = [0.1, 0.3, 0.9]$, under different interference power threshold of P, P_{th} = [10, 30] dB. The curves for both the analytical results and Monte Carlo simulations are presented for Case 2 scenario. We can observe that the secrecy performance curve shown in Figure 6 for Case 2 has a similar trend to that in Figure 3 for Case 1. Under the same parameters set, the main difference is that the secrecy performance for Case 1 performs better than that for Case 2, due to the fact that the SOP for Case 2 is affected by the maximal transmit power constraint of the ST and the interference temperature constraint simultaneously.

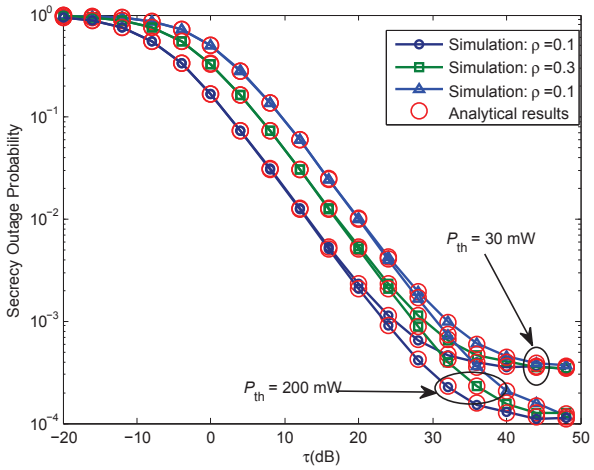

Figure 6. Case 2: Secrecy outage probability versus τ, when P_{th} = 30 mW, $P_{\max}$ = 10 mW, R_{s} = 1 bits/Hz/s, ρ = 0.9.

Figure 7 provides the SOP versus the ratio τ, under different target secrecy rate R_{s}. Only analytical results obtained from Equations (11) and (42) are plotted here, τ ranges from –10 dB to 60 dB. As can be seen, the SOP for case 1 performs better than that for case 2. This is intuitive, since for case 2, the SOP is affected by the maximum power of the secondary source itself additionally, which will somewhat depress the transmit performance.

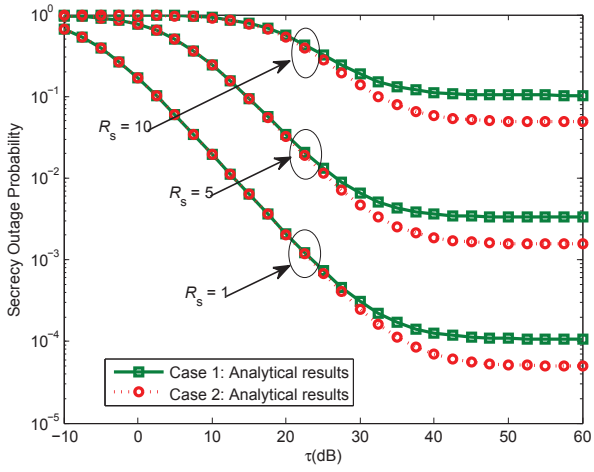

Figure 7. Comparison of secrecy outage probability for the two proposed cases, when when R_{s} = [1, 5, 10] bits/Hz/s, ρ = 0.1, P_{th} = 200 mW.

6. Conclusions

This paper has investigated the physical layer security performance of cognitive sensor radio networks. In contrast to conventional security issues, we consider the energy harvesting (EH) function for the eavesdropper. New closed-form expressions of secrecy outage probability for two different cases have been derived, and the impacts of various parameters on secure performance have also been studied. The precise matching between the simulation results and the derived closed-form expressions also validates the theoretical analysis presented in this paper. Furthermore, the proposed analytical models can be readily applied to practical energy harvesting wireless sensor networks design such as power allocation, and transmission policy. As a final remark, this work can be served as an important step for investigating different physical layer security enhancement technologies, e.g., multi-antenna scenarios and full-duplex scenarios, etc., to provide more secrecy transmission methods for cognitive sensor radio networks. Moreover, security in the time switching (TS)-based energy harvesting scheme will be a fundamental and significant research field, which will involve more sophisticated settings and practical considerations in the near future.

Acknowledgments: This research was supported in part by the National Nature Science Foundation of China under grant 61471392 and grant 61501507, by Jiangsu Provincial National Science Foundation under grant BK20150719.

Author Contributions: Aiwei Sun and Tao Liang conceived and designed the experiments; Aiwei Sun performed the experiments; Bolun Li and Tao Liang analyzed the data; Aiwei Sun wrote the paper.

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

References

1. Zhao, Y.; Hong, Z.; Wang, G.; Huang, J. High-Order Hidden Bivariate Markov Model: A Novel Approach on Spectrum Prediction. In Proceedings of the 25th International Conference on Computer Communications and Networks (2016 ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–7.
2. Zhao, Y.; Pradhan, J.; Wang, G.; Huang, J. Experimental approach: Two-stage spectrum sensing using GNU radio and USRP to detect primary user's signal. In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC 2016), Pisa, Italy, 4–8 April 2016; pp. 2165–2170.
3. Zhao, Y.; Anjum, M.N.; Song, M.; Xu, X.; Wang, G.; Huang, J. Optimal Resource Allocation for Delay Constrained Users in Self-coexistence WRAN. In Proceedings of the IEEE Globecom Workshops, San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
4. Akan, O.B.; Karli, O.B.; Ergul, O. Cognitive radio sensor networks. *IEEE Netw.* **2009**, *23*, 34–40.
5. Goh, H.G.; Kwong, K.H.; Shen, C.; Michie, C.; Andonovic, I. CogSeNet: A Concept of Cognitive Wireless Sensor Network. In Proceedings of the 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010; pp. 1–2.
6. Ren, J.; Zhang, Y.; Zhang N.; Zhang, D.; Shen, X. Dynamic Channel Access to Improve Energy Efficiency in Cognitive Radio Sensor Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3143–3156.
7. Zheng, M.; Liang, W.; Yu, H.; Sharif, H. Utility-based opportunistic spectrum access for cognitive radio sensor networks: Joint spectrum sensing and random access control. *IET Commun.* **2016**, *10*, 1044–1052.
8. Nobar, S.K.; Mehr, K.A.; Niya, J.M.; Tazehkand, B.M. Cognitive Radio Sensor Network With Green Power Beacon. *IEEE Sens. J.* **2016**, *17*, 1549–1561.
9. Zhang, D.; Chen, Z.; Ren, J.; Zhang, N.; Awad, M.K.; Zhou, H.; Shen, X. Energy-Harvesting-Aided Spectrum Sensing and Data Transmission in Heterogeneous Cognitive Radio Sensor Network. *IEEE Trans. Veh. Technol.* **2017**, *66*, 831–843.
10. Varshney, L.R. Transporting information and energy simultaneously. In Proceeding of the IEEE International Symposium on Information Theory (ISIT), Toronto, ON, Canada, 6–11 July 2008; pp. 1612–1616.
11. Grover, P.; Sahai, A. Shannon meets Tesla: Wireless information and power transfer. In Proceeding of the IEEE International Symposium on Information Theory (ISIT), Austin, TX, USA, 13–18 June 2010; pp. 2363–2367.

12. Zhang, R.; Ho, C.K. MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 1989–2001.
13. Xing, C.; Wang, N.; Ni, J. MIMO beam-forming designs with partial CSI under energy harvesting constraints. *IEEE Signal Process. Lett.* **2013**, *20*, 363–366.
14. Xiang, Z.; Tao, M. Robust beamforming for wireless information and power transmission. *IEEE Wirel. Commun. Lett.* **2012**, *1*, 372–375.
15. Zhou, X.; Zhang, R.; Ho, C.K. Wireless information and power transfer: Architecture design and rate-energy tradeoff. *IEEE Trans. Commun.* **2013**, *61*, 4754–4765.
16. Shi, Q.; Liu, L.; Xu, W.; Zhang, R. Joint transmit beam-forming and receive power splitting for MISO SWIPT systems. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 3269–3280.
17. Huang, J.; Li, Q.; Zhang, Q.; Zhang, G.; Qin, J. Relay beamforming for amplify-and-forward multi-antenna relay networks with energy harvesting constraint. *IEEE Signal Process. Lett.* **2014**, *21*, 454–458.
18. Chalise, B.K.; Ma, W.K.; Zhang, Y.D.; Himal, A.S. Optimum performance boundaries of OSTBC-based AF-MIMO relay system with energy harvesting receiver. *IEEE Trans. Signal Process.* **2013**, *61*, 4199–4231.
19. Shen, C.; Li, W.; Chang, T. Wireless information and energy transfer in multi-antenna interference channel. *IEEE Trans. Signal Process.* **2014**, *62*, 6249–6264.
20. Park, J.; Clerckx, B. Joint wireless information and energy transfer in a two-user MIMO interference channel. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 4210–4221.
21. Soosahabi, R.; Naraghi-Pour, M. Scalable PHY-layer security for distributed detection in wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1118–1126.
22. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: New York, NY, USA, 2004.
23. Lee, J.-H.; Sohn, I.; Kim, Y.-H. Transmit Power Allocation for Physical Layer Security in Cooperative Multi-Hop Full-Duplex Relay Networks. *Sensors* **2016**, *16*, 1726–1739.
24. Deng, Y.; Wang, L.; Elkashlan, M.; Nallanathan, A.; Mallik, R.K. Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1128–1138.
25. Hong, Y.W.P.; Lan, P.C.; Kuo, C.C.J. Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches. *IEEE Signal Process. Mag.* **2013**, *30*, 29–40.
26. Yang, J.; Kim, I.M.; Kim, D.I. Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2840–2852.
27. Liu, L.; Zhang, R.; Chua, K.C. Secrecy wireless information and power transfer with MISO beam-forming. *IEEE Trans. Signal Process.* **2014**, *62*, 1850–1863.
28. Hung, S.-C.; Xiao, Y.; Chen, K.-C. Transmission Strategy With Cooperative Sensors in Cognitive Radio Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3416–3429.
29. Ding, G.; Wang, J.; Wu, Q.; Song, F.; Chen, Y. Spectrum Sensing in Opportunity–Heterogeneous Cognitive Sensor Networks: How to Cooperate? *IEEE Sens. J.* **2013**, *13*, 4247–4255.
30. Zheng, M.; Chen, L.; Liang, W.; Yu, H.; Wu, J. Energy-efficiency Maximization for Cooperative Spectrum Sensing in Cognitive Sensor Networks. *IEEE Trans. Green Commun. Netw.* **2016**, doi:10.1109/TGCN.2016.2646819.
31. Chiti, F.; Fantacci, R.; Tani A. Performance Evaluation of An Adaptive Channel Allocation Technique for Cognitive Wireless Sensor Networks. *IEEE Trans. Veh. Technol.* **2016**, doi:10.1109/TVT.2016.2621140.
32. Sun, Y. Distributed fast channel allocation in cognitive wireless sensor networks. *IET Signal Process.* **2016**, *10*, 471–477.
33. Wang, D.; Ren, P.; Du, Q.; Sun, L.; Wang, Y. Optimal Power Allocation for Cognitive Radio Sensor Networks under Primary Secrecy Outage Constraint. In Proceedings of the IEEE International Conference on Communication Systems (ICCS), Shenzhen, China, 14–16 December 2016; pp. 1–5.
34. Pan, G.; Tang, C.; Li, T.; Chen, Y. Secrecy Performance Analysis for SIMO Simultaneous Wireless Information and Power Transfer Systems. *IEEE Trans. Wirel. Commun.* **2015**, *63*, 3423–3433.
35. 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.
36. Duong, T.Q.; da Costa, D.B.; Elkashlan, M.; Bao, V.N.Q. Cognitive Amplify-and-Forward Relay Networks Over Nakagami-*m* Fading. *IEEE Trans. Veh. Technol.* **2012**, *61*, 2368–2374.

37. Grinstead, C.M.; Snell, J.L. *Introduction to Probability*, 2nd ed.; American Mathmatical Society: Providence, RI, USA, 1991.
38. Gradshteyn, I.S.; Ryzhir, I.M. *Tables of Integrals, Series and Products*, 7th ed.; Academic Press: NewYork, NY, USA, 2007.