sensors

MDPI

Article

Secure Transmission of Cooperative Zero-Forcing Jamming for Two-User SWIPT Sensor Networks

Xuanxuan Tang, Yueming Cai *, Wendong Yang, Weiwei Yang, Dechuan Chen and Junquan Hu

College of Communications Engineering, Army Engineering University of PLA, No. 88 Houbiaoying, Qinhuai District, Nanjing 210007, China; tang_xx@126.com (X.T.); ywd1110@163.com (W.Y.); wwyang1981@163.com (W.Y.); chenchuan927@163.com (D.C.); junquan_hu@163.com (J.H.)

* Correspondence: caiym@vip.sina.com; Tel.: +86-025-8082-9339

Received: 3 January 2018; Accepted: 22 January 2018; Published: 24 January 2018

Abstract: In this paper, the secrecy performance of the two-user simultaneous wireless information and power transfer (SWIPT) sensor networks is studied and a novel secure transmission scheme of cooperative zero-forcing (ZF) jamming is proposed. The two sensors opportunistically conduct the SWIPT and cooperative ZF jamming, respectively, where the energy required for jamming the eavesdropper is provided by the SWIPT operation so as to keep the energy balance at the sensors in the long run. By deriving the exact closed-form expressions of the secrecy outage probability and the secrecy throughout, we provide an effective approach to precisely assess the impacts of key parameters on the secrecy performance of the system. It has been shown that the secrecy outage probability is a monotonically increasing function of the growth of secrecy rate (R_s), and a monotonically decreasing function of the increase of the transmit signal-to-noise ratio (γ_S), and energy conversion efficiency (η). Furthermore, the secrecy throughput could be enhanced when η increases, which becomes especially obvious when a large γ_S is provided. Moreover, the existence of an optimum R_s maximizing the secrecy throughput is depicted, which also grows with the increase of γ_S. Simulations are provided for the validation of the analysis.

Keywords: physical layer security; zero-forcing jamming; secrecy outage probability; secrecy throughput; wireless sensor networks

1. Introduction

Because of the broadcast nature of wireless medium, it is a critical issue to secure the transmission in the design of wireless sensor networks [1]. The security is conventionally tackled through higher layer techniques, e.g., cryptographic protocols, which, however, could not guarantee the required security level alone for the large-scale wireless sensor networks due to the significant increase in the complexity of key distribution and management [2]. In contrast to conventional cryptographic approaches conducted at higher layers, the physical layer security (PLS) tries to secure the wireless networks against eavesdropping by exploiting the inherent channel randomness at the physical layer. Hence, PLS has been widely regarded as an effective supplementary protocol for wireless communications and, thus, has gained much attention in research communities [3–5].

The main idea of PLS is that, by making and enlarging the capacity differences between the legitimate channels and the wiretapping channels, the information could be transmitted at a predefined secrecy rate so that only the authorized receiver can decode the data while the eavesdropper could not [6]. Various advanced techniques have been proposed to further enhance the potential benefits of PLS, such as antenna selection [7], cooperative relaying [8], cooperative jamming [9], etc. Generally speaking, the security of wireless transmission could be significantly increased if jamming signals could be carefully exploited in the legitimate network. As a consequence, the cooperative jamming has been widely applied in the PLS research in numerous systems, such as single-input-multiple-output (SIMO)

networks [10], two-way relay scenarios [11], multiple-input-multiple-output (MIMO) wiretap-channel settings [12], etc.

More recently, the simultaneous wireless information and power transfer (SWIPT) has become an appealing technique in wireless communications due to its great potential in tackling the energy bottleneck issue, especially in some energy-constrained cases [13–15]. Authors in [16] investigated the safeguarding approach for SWIPT systems with both the eavesdropper and the friendly jammer harvesting energy from the wireless signals, and the optimal power allocation strategy based on the Lagrange method was then proposed. In [17], a cooperative jamming aided robust secure transmission for SWIPT multiple-input-single-output (MISO) networks was presented, where the objective of the source and the jammer was to maximize the secrecy rate and also supply wireless power to the energy receiver and the destination. However, an additional jammer must be deployed in literature [16,17], which is practically costly in the construction and upgrading of current wireless systems, especially in the wireless sensor networks.

There has been some research investigating the security issue of scenarios where no additional jammer is available and the user harvests the energy and also acts as the jammer itself [18–20]. Work [18] studied the secrecy performance of full-duplex SWIPT networks, where the two-antenna user received information and energy with one of its antennae by applying the power-splitting SWIPT protocol, and sent the jamming signal to confuse the eavesdropper with the other antenna. Under a similar system of deployment, the security of the time-switching SWIPT protocol was examined in [19], where the secrecy outage performance and the secrecy energy efficiency were formulated. The author in [20] extended the research in the cognitive networks, where the energy collected by the receiving antenna via the power-splitting SWIPT protocol was used for producing jamming signals by the transmitting antenna. However, the shortage of [18–20] is obvious. On the one hand, an effective self-interference cancellation (SIC) method at the users is required to guarantee the validity of the secure schemes, as the users in this literature all work in the full-duplex mode. On the other hand, both the power-splitting and the time-switching approaches applied in these literature will definitely increase the complexity of realization significantly. As a result, the practical value of these schemes in wireless sensor networks is greatly limited.

Motivated by the above observations, we present a novel secure transmission scheme for the proposed two-user SWIPT sensor networks where the two sensors conduct the cooperative zero-forcing (ZF) jamming opportunistically and mutually with the harvested energy. We note that the proposed two-user cooperative pair model is rather practical because each sensor in actual sensor networks can choose another sensor nearby to form this pair and then conduct cooperative jamming in turn. It is also highlighted that the sensors are generally energy-constrained, which again reveals the advantage of the proposed cooperative jamming scheme because it does not consume any energy of the sensors in the long run due to the SWIPT operation. Furthermore, neither the full-duplex and SIC techniques nor the power-splitting and time-switching methods are needed in the proposed scheme, which is of great benefit in practical realization. The remainder of the work is organized as follows: Section 2 characterizes the system model and presents the secure transmission scheme. In Section 3, the exact secrecy analysis of the proposed scheme is carried out. Section 4 conducts the simulations and gives the discussions. Finally, Section 5 summarizes the whole paper.

***Notation*:** Throughout this paper, the boldface uppercase letters are used to denote matrices or vectors. $(\cdot)^T$ and $(\cdot)^H$ are denoted as the transpose operation and the conjugate transpose operation, respectively. $F_\gamma(\cdot)$ and $f_\gamma(\cdot)$ represent the cumulative distribution function (CDF) and the probability density function (PDF) of random variable γ, respectively. $\mathbb{E}[\cdot]$ denotes the expectation operation.

2. System Model

2.1. System Description

We consider a downlink SWIPT sensor network as illustrated in Figure 1, which consists of a source node S, a pair of two sensor nodes D_1 and D_2, and an eavesdropper E. All nodes are equipped with a single antenna, except for the two sensors, which both have only two antennae without having to increase too much complexity of realization [19,20]. In addition, we assume that the channel state information (CSI) of the legitimate links is available, while the CSI of the eavesdropping link is not known by the legitimate nodes. This is a typical passive eavesdropping scenario which is more practical than active eavesdropping [21] and has been widely used in existing literature (see [22–24] and the references therein). It is also assumed that all the channels between two nodes experience quasi-static Rayleigh fading, such that the channel coefficients keep constant during a packet time T_0 but vary independently from one packet time to another. Furthermore, all the channels of $S - D_{i,j}$ and $D_{i,j} - E$ are assumed to be independent and identically distributed (i.i.d), respectively.

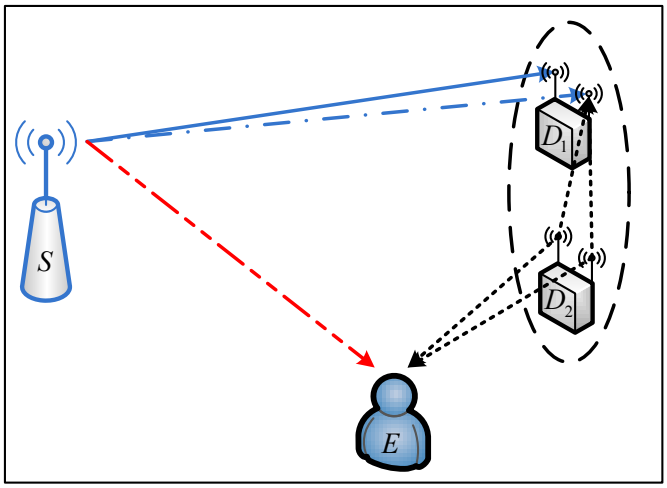

Figure 1. System model.

2.2. Secure Transmission

At each slot, the specific antenna of a certain sensor that maximizes the instantaneous transmission channel capacity is chosen for information receiving (IR). At the same time, the remaining antenna of the selected sensor will be assigned for energy harvesting (EH). In addition, the jamming operation is introduced in order to enhance the security of the transmission. More specifically, the cooperative ZF jamming is applied in this paper by the other sensor, so that the IR process is not interfered.

Without loss of generality, we assume that the D_{i^*,j^*} is selected in a certain slot, namely

$$(i^*, j^*) = \arg \max_{i,j \in \{1,2\}} \left(g_{SD_{i,j}} \right), \tag{1}$$

where $g_{(.)} = \left| h^2_{(.)} \right|$, and $h_{SD_{i,j}}$ represents the channel coefficient between S and the j-th antenna of i-th sensor. At the same time, the antenna $D_{i^*,3-j^*}$ is allocated for collecting energy, and the other sensor D_{3-i^*} is assigned to produce ZF jamming signals in order to increase the security of the transmission. As described above, we can summarize the working mode of all the antennae when D_{i^*,j^*} is determined, which is shown in Table 1 for the better readability.

Table 1. Working mode of the sensors and antennas ($i^*, j^* \in \{1,2\}$).

Sensor	Antenna	Working Mode
D_{i^*}	D_{i^*,j^*}	Information receiving
	$D_{i^*,3-j^*}$	Energy harvesting
D_{3-i^*}	D_{3-i^*,j^*}	Zero-forcing jamming
	$D_{3-i^*,3-j^*}$	

As a result, the signals for IR and EH can be given by Labels (2) and (3), respectively,

$$y_{D_{i^*,j^*}} = \sqrt{P_J}\mathbf{h}^H_{D_{3-i^*}D_{i^*,j^*}}\mathbf{w}_{ZF}x_J + \sqrt{P_S}h_{SD_{i^*,j^*}}x_S + n_{D_{i^*,j^*}}, \tag{2}$$

$$y_{D_{i^*,3-j^*}} = \sqrt{P_J}\mathbf{h}^H_{D_{3-i^*}D_{i^*,3-j^*}}\mathbf{w}_{ZF}x_J + \sqrt{P_S}h_{SD_{i^*,3-j^*}}x_S + n_{D_{i^*,3-j^*}}, \tag{3}$$

where P_S and P_J represent the transmit power of S and the jamming power of sensors, $\mathbf{h}_{D_{3-i^*}D_{i^*,j^*}}$, $\mathbf{h}_{D_{3-i^*}D_{i^*,3-j^*}} \in \mathbb{C}^{2\times 1}$ represent the channel coefficient vectors from D_{3-i^*} to D_{i^*,j^*} and $D_{i^*,3-j^*}$, respectively. x_S and x_J denote the information-bearing signal and the jamming signal, n_a is the additive white Gaussian noise (AWGN) at node a with $a \in \{D_{i,j}\}$, $i,j \in \{1,2\}$. Without loss of generality, the noise power spectral density is assumed the same everywhere within the network and is denoted as N_0, and $\mathbf{w}_{ZF}$ is the normalized vector of the jamming operation.

Now, we will focus on the derivation of $\mathbf{w}_{ZF}$. As pointed out previously, the jamming operation is introduced to increase the security of the transmission. Therefore, three purposes are expected to be achieved by this jamming operation. Firstly, the jamming operation will not affect the receiving performance of the legitimate information receiver. Secondly, the interference received at the eavesdropper should be maximized, so that the eavesdropper is confused as much as possible. Thirdly, the interference received at the legitimate energy receiver should be maximized, so that the legitimate energy receiver could collect as much energy as possible from the jamming signal. Mathematically, the above three ideas can be achieved by Equations (4)–(6), respectively,

$$\left|\mathbf{h}^H_{D_{3-i^*}D_{i^*,j^*}}\mathbf{w}_{ZF}\right| = 0, \tag{4}$$

$$\max_{\mathbf{w}_{ZF}} \left|\mathbf{h}^H_{D_{3-i^*}E}\mathbf{w}_{ZF}\right|, \tag{5}$$

$$\max_{\mathbf{w}_{ZF}} \left|\mathbf{h}^H_{D_{3-i^*}D_{i^*,3-j^*}}\mathbf{w}_{ZF}\right|, \tag{6}$$

where $\mathbf{h}_{D_{3-i^*}E} \in \mathbb{C}^{2\times 1}$ represents the channel coefficient vector from D_{3-i^*} to E. In addition, recall that the jamming vector is normalized, hence we have

$$\|\mathbf{w}_{ZF}\| = 1. \tag{7}$$

Unfortunately, due to the passive eavesdropping assumption, the eavesdropper's CSI, $\mathbf{h}^H_{D_{3-i^*}E}$, is unavailable at the legitimate network, thus it is not possible to maximize the confusing effect to the eavesdropper. As a result, we will try to find an appropriate $\mathbf{w}_{ZF}$ so that Labels (4), (6), and (7) are all satisfied, namely

$$\begin{aligned} &\max_{\mathbf{w}_{ZF}} \left|\mathbf{h}^H_{D_{3-i^*}D_{i^*,3-j^*}}\mathbf{w}_{ZF}\right| \\ &s.t. \left|\mathbf{h}^H_{D_{3-i^*}D_{i^*,j^*}}\mathbf{w}_{ZF}\right| = 0, \|\mathbf{w}_{ZF}\| = 1. \end{aligned} \tag{8}$$

According to [25,26], the solution of Label (8) can be given by

$$\mathbf{w}_{ZF} = \frac{\mathbf{T}\mathbf{h}_{D_{3-i^*}D_{i^*,3-j^*}}}{\left\|\mathbf{T}\mathbf{h}_{D_{3-i^*}D_{i^*,3-j^*}}\right\|}, \tag{9}$$

where $\mathbf{T}$ is the projection idempotent matrix with rank 1, which is given by

$$\mathbf{T} = \mathbf{I} - \mathbf{h}_{D_{3-i^*}D_{i^*,j^*}}\left(\mathbf{h}^H_{D_{3-i^*}D_{i^*,j^*}}\mathbf{h}_{D_{3-i^*}D_{i^*,j^*}}\right)^{-1}\mathbf{h}^H_{D_{3-i^*}D_{i^*,j^*}}. \tag{10}$$

It is easy to see from Labels (9) and (10) that $\mathbf{w}_{ZF}$ is chosen from the null space of the channel direction of $\mathbf{h}_{D_{3-i^*}D_{i^*,j^*}}$ so that the information receiving process is not interfered [27,28].

As can be observed, the CSI knowledge is required for both the selection process and ZF jamming operation. Now, we will elaborate on how this knowledge is obtained. As shown in Figure 2, each time slot could be divided into two parts, namely the pilot duration and the transmission duration. In order to select the best antenna for IR, the antenna $D_{i,j}$ $(i,j \in \{1,2\})$ will send pilot signals during its pilot duration $P_{i,j}$, which can be exploited for channel estimation by S and the other sensor, which acts as a jammer. Hence, S is able to obtain the knowledge of $h_{SD_{i,j}}$ for user/antenna selection, and the sensor that acts as jammer can derive the knowledge of $\mathbf{h}_{D_{3-i^*}D_{i^*,3-j^*}}$ and $\mathbf{h}_{D_{3-i^*}D_{i^*,j^*}}$ to construct the ZF jamming vector.

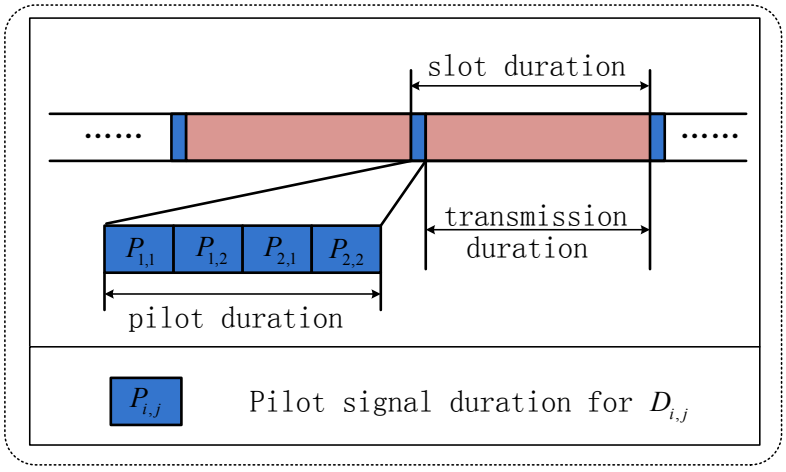

Figure 2. Time slot structure for user/antenna selection.

According to Labels (2) and (8), the receiving signal-to-noise ratio (SNR) for information receiving is given by

$$\gamma_D = \frac{P_S}{N_0}\max_{i,j\in\{1,2\}}\left(g_{SD_{i,j}}\right). \tag{11}$$

At the same time, the amount of collected energy is expressed as

$$\varepsilon_D = \eta T_0\left|y_{D_{i^*,3-j^*}}\right|^2, \tag{12}$$

and denoting $U = \mathbf{h}^H_{D_{3-i^*}D_{i^*,3-j^*}}\mathbf{w}_{ZF}$. According to (Lemma 2 [25]), (Lemma 2 [26]), (Equation (30) [27]), (Equation (52) [28]), the CDF of $U = \mathbf{h}^H_{D_{3-i^*}D_{i^*,3-j^*}}\mathbf{w}_{ZF}$ is a chi-square random variable with $2(L_s-1)$ degrees of freedom, namely $U \sim \chi^2\left(2\left(L_s-1\right)\right)$, where L_s represents the number of ZF antennae.

In this paper, we have $L_s = 2$. Hence, $U \sim \chi^2(2)$, which degenerates into exponentially distributed random variables, namely we have

$$f_U(u) = \frac{1}{\bar{\gamma}_{DD}} e^{-\frac{u}{\bar{\gamma}_{DD}}}, \tag{13}$$

where $\bar{\gamma}_{ab} = \mathbb{E}[g_{ab}]$ represents the average channel gain of link $a-b$, $a, b \epsilon \{S, D, E\}$. Specifically, $\bar{\gamma}_{DD}$ represents the average channel gain between the two sensors. By using the above result, Equation (12) can be readily calculated as (We note that little energy can be harvested from the AWGN in practice, hence is neglected in this paper [14,29].)

$$\varepsilon_D = \eta T_0 \left(P_S \left| h_{SD_{i^*,3-j^*}} \right|^2 + P_J \left| \mathbf{h}^H_{D_{3-i^*} D_{i^*,3-j^*}} \mathbf{w}_{ZF} \right|^2 \right), \tag{14}$$

where η is the energy conversion efficiency. Hence, in order to keep the energy balance at the sensors in the long run, the jamming power can be chosen as (We note that an energy outage would occur by adopting the approach in this paper. Although the probability to occur this can be proven to be very low by the simulations when an appropriate initial energy can be provided, it still should be considered for accurate analysis. In fact, by modeling battery as an energy queue would be a good method to give out the accurate analysis, which however is beyond the scope of this paper and is left for the research in the future.)

$$P_J = \frac{\mathbb{E}[\varepsilon_D]}{T_0} = \eta \left(P_S \bar{\gamma}_{SD} + P_J \bar{\gamma}_{DD} \right). \tag{15}$$

It is readily to know that Label (15) yields to

$$P_J = \frac{\eta \bar{\gamma}_{SD} P_S}{1 - \eta \bar{\gamma}_{DD}}. \tag{16}$$

Similarly, the receiving signal at E is expressed as

$$y_E = \sqrt{P_S} h_{SE} x_S + \sqrt{P_J} \mathbf{h}^H_{D_{3-i^*} E} \mathbf{w}_{ZF} x_J + n_E. \tag{17}$$

Thus, the receiving signal-to-interference-plus-noise ratio (SINR) at E is given by

$$\gamma_E = \frac{P_S g_{SE}}{P_J \left| \mathbf{h}^H_{D_{3-i^*} E} \mathbf{w}_{ZF} \right|^2 + N_0}. \tag{18}$$

3. Secrecy Performance Analysis

In this section, we focus our attention on the secrecy performance of the proposed scheme. Before delving into the details, we present the preliminary of the following two lemmas.

Lemma 1. *The CDF and the PDF of γ_D are given by*

$$F_{\gamma_D}(x) = \left(1 - e^{-\frac{N_0 x}{P_S \bar{\gamma}_{SD}}} \right)^4, \tag{19}$$

$$f_{\gamma_D}(x) = \frac{4 N_0}{P_S \bar{\gamma}_{SD}} \sum_{k=0}^{3} \binom{3}{k} (-1)^k e^{-\frac{(k+1) N_0 x}{P_S \bar{\gamma}_{SD}}}. \tag{20}$$

Proof. According to Label (11) and referring to [5], Equation (19) is readily obtained. By taking the derivation operation, the PDF of γ_D is derived as

$$f_{\gamma_D}(x) = \frac{4N_0}{P_S\bar{\gamma}_{SD}}\left(1 - e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SD}}}\right)^3 e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SD}}}. \tag{21}$$

By using the binomial theorem (Equation (1.111) [30]) in Label (21), the result in Label (20) is readily obtained. □

Lemma 2. *The CDF and PDF of γ_E are given by*

$$F_{\gamma_E}(x) = 1 - \frac{P_S\bar{\gamma}_{SE}}{P_J\bar{\gamma}_{DE}x + P_S\bar{\gamma}_{SE}} e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SE}}}, \tag{22}$$

$$f_{\gamma_E}(x) = \frac{P_S\bar{\gamma}_{SE}P_J\bar{\gamma}_{DE}}{\left(P_J\bar{\gamma}_{DE}x + P_S\bar{\gamma}_{SE}\right)^2} e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SE}}} + \frac{N_0\left(P_J\bar{\gamma}_{DE}x + P_S\bar{\gamma}_{SE}\right)}{\left(P_J\bar{\gamma}_{DE}x + P_S\bar{\gamma}_{SE}\right)^2} e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SE}}}. \tag{23}$$

Proof. Mathematically, the CDF of γ_E can be manipulated as $F_{\gamma_E}(x) = \Pr(\gamma_E < x)$, which can be rewritten as Label (24) according to Label (18)

$$F_{\gamma_E}(x) = \int_0^\infty F_{g_{SE}}\left(\frac{(P_J v + N_0)\, x}{P_S}\right) f_V(v)\, dv, \tag{24}$$

where $V = \left|\mathbf{h}_{D_{3-i^*}E}^H \mathbf{w}_{ZF}\right|^2$. As shown in Label (8), $\mathbf{w}_{ZF} = [w_1, w_2]^T$ is a normalized vector, i.e., $|w_1|^2 + |w_2|^2 = 1$. Thus, $\left|\mathbf{h}_{D_{3-i^*}E}^H \mathbf{w}_{ZF}\right|$ is a unitary transformation of $\mathbf{h}_{D_{3-i^*}E}^H$. In addition, it is obvious that $\mathbf{w}_{ZF}$ is independent of $\mathbf{h}_{D_{3-i^*}E}^H$, and the two elements of $\mathbf{h}_{D_{3-i^*}E}^H$, namely $h_{D_{3-i^*,1}E}$ and $h_{D_{3-i^*,2}E}$ are both Gaussian variables. In other words, we have $h_{D_{3-i^*,1}E}, h_{D_{3-i^*,2}E} \sim \mathcal{N}(0, \bar{\gamma}_{DE})$. Therefore, $w_1 h_{D_{3-i^*,1}E} \sim \mathcal{N}\left(0, |w_1|^2\bar{\gamma}_{DE}\right)$ and $w_2 h_{D_{3-i^*,2}E} \sim \mathcal{N}\left(0, |w_2|^2\bar{\gamma}_{DE}\right)$ can be concluded. Hence, $(w_1 h_{D_{3-i^*,1}E} + w_2 h_{D_{3-i^*,2}E}) \sim \mathcal{N}\left(0, \left(|w_1|^2 + |w_2|^2\right)\bar{\gamma}_{DE}\right) = \mathcal{N}(0, \bar{\gamma}_{DE})$, which means that $V = \left|w_1 h_{D_{3-i^*,1}E} + w_2 h_{D_{3-i^*,2}E}\right|^2$ is also an exponentially distributed random variables with the mean of $\bar{\gamma}_{DE}$. We note that V has the same distribution with $h_{D_{3-i^*,1}E}$ and $h_{D_{3-i^*,2}E}$, and this has verified the conclusion that the unitary transformation does not change the distribution of the transformed variables. As a result, we have

$$f_V(v) = \frac{1}{\bar{\gamma}_{DE}} e^{-\frac{v}{\bar{\gamma}_{DE}}}. \tag{25}$$

In addition, the CDF of g_{SE} is given by

$$F_{g_{SE}}(x) = 1 - e^{-\frac{x}{\bar{\gamma}_{SE}}}. \tag{26}$$

Substituting Labels (25) and (26) into Label (24) and after some calculations, the CDF of γ_E is easily obtained as in Label (22). By taking the derivation operation in Label (22), we finally derive the result in Label (23). □

3.1. Secrecy Outage Probability

The secrecy outage probability is defined as the probability that the instantaneous secrecy capacity falls below a predefined secrecy rate R_s (The design of R_s falls into the construction of the wiretap coding, which has been elaborated abundantly in the literature [31,32], and thus is omitted in this paper.), which can be equivalently expressed as [5,28]

$$P_{out} = \int_0^\infty F_{\gamma_D}\left(\gamma_{th}^s + \gamma_{th}^s y - 1\right) f_{\gamma_E}(y)\, dy, \tag{27}$$

where $\gamma_{th}^{s} = 2^{R_s}$.

Theorem 1. *The secrecy outage probability for the proposed system is given by*

$$P_{out}\left(\gamma_{th}^{s}\right) = \sum_{k=0}^{4} \binom{4}{k} (-1)^{k} e^{-\frac{kN_0\left(\gamma_{th}^{s}-1\right)}{P_S \bar{\gamma}_{SD}}} \left(\mathcal{I}_{1,k} + \mathcal{I}_{2,k}\right), \tag{28}$$

where

$$\mathcal{I}_{1,k} = 1 + \frac{N_0}{P_J \bar{\gamma}_{DE} \bar{\gamma}_{SD}} \left(\bar{\gamma}_{SD} + k\gamma_{th}^{s} \bar{\gamma}_{SE}\right) \exp\left(\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_J \bar{\gamma}_{DE} \bar{\gamma}_{SD}}\right) Ei\left(-\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_J \bar{\gamma}_{DE} \bar{\gamma}_{SD}}\right), \tag{29}$$

$$\mathcal{I}_{2,k} = -\frac{N_0}{P_J \bar{\gamma}_{DE}} \exp\left(\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_J \bar{\gamma}_{DE} \bar{\gamma}_{SD}}\right) Ei\left(-\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_J \bar{\gamma}_{DE} \bar{\gamma}_{SD}}\right). \tag{30}$$

Proof. Replacing x with $\left(\gamma_{th}^{s} + \gamma_{th}^{s} y - 1\right)$ in Label (19), we derive

$$F_{\gamma_D}\left(\gamma_{th}^{s} + \gamma_{th}^{s} y - 1\right) = \left(1 - \exp\left(-\frac{N_0\left(\gamma_{th}^{s} + \gamma_{th}^{s} y - 1\right)}{P_S \bar{\gamma}_{SD}}\right)\right)^{4}. \tag{31}$$

With the help of binomial theorem, Label (31) can be rewritten as

$$F_{\gamma_D}\left(\gamma_{th}^{s} + \gamma_{th}^{s} y - 1\right) = \sum_{k=0}^{4} \binom{4}{k} (-1)^{k} \exp\left(-\frac{kN_0\left(\gamma_{th}^{s} + \gamma_{th}^{s} y - 1\right)}{P_S \bar{\gamma}_{SD}}\right). \tag{32}$$

By substituting Labels (23) and (32) into Label (27), and letting $t = y - \frac{1-\gamma_{th}^{s}}{\gamma_{th}^{s}}$, we obtain

$$P_{out} = \sum_{k=0}^{4} \binom{4}{k} (-1)^{k} \exp\left(-\frac{kN_0\left(\gamma_{th}^{s} - 1\right)}{P_S \bar{\gamma}_{SD}}\right) \left(\mathcal{I}_{1,k} + \mathcal{I}_{2,k}\right), \tag{33}$$

where

$$\mathcal{I}_{1,k} = \int_0^{\infty} \frac{P_S \bar{\gamma}_{SE} P_J \bar{\gamma}_{DE}}{\left(P_J \bar{\gamma}_{DE} y + P_S \bar{\gamma}_{SE}\right)^2} \exp\left(-\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_S \bar{\gamma}_{SE} \bar{\gamma}_{SD}} y\right) dy, \tag{34}$$

$$\mathcal{I}_{2,k} = \int_0^{\infty} \frac{N_0}{P_J \bar{\gamma}_{DE} y + P_S \bar{\gamma}_{SE}} \exp\left(-\frac{N_0 \bar{\gamma}_{SD} + kN_0 \gamma_{th}^{s} \bar{\gamma}_{SE}}{P_S \bar{\gamma}_{SE} \bar{\gamma}_{SD}} y\right) dy. \tag{35}$$

By using $\int_0^{\infty} \left(e^{-px} \Big/ (a+x)^2\right) dx = pe^{ap} Ei\left(-ap\right) + 1/a$ (Equation (3.353.3) [30]), Label (34) leads to Label (29). Similarly, by using $\int_0^{\infty} \left(e^{-\mu x} / (x+\beta)\right) dx = -e^{\beta\mu} Ei\left(-\beta\mu\right)$ (Equation (3.352.4) [30]), Label (35) results in Label (30). □

3.2. Secrecy Throughput

The secrecy throughput can be defined as the secrecy rate multiplied by the probability of a reliable and secure transmission, which is mathematically written as [33]

$$\varsigma = R_s\left(1 - P_{out}\right). \tag{36}$$

By substituting the result in Theorem 1 into Label (36), the secrecy throughput can be easily deduced.

4. Simulation Results and Discussion

In this section, some representative simulations are provided to examine the impacts of the system parameters on the cooperative zero-forcing jamming scheme for the two-user SWIPT networks. The transmit SNR is defined as $\gamma_S = P_S/N_0$. As can be readily observed, the theoretical results are in exact agreement with the simulations, validating the correctness of the analysis. Without loss of generality, we set $N_0 = 1$.

Figure 3 illustrates the secrecy outage probability P_{out} versus the secrecy rate R_s with different $\bar{\gamma}_{SD}$ and η. As it is shown, the secrecy outage probability monotonically increases with the growth of R_s. In addition, we see from Figure 3 that larger $\bar{\gamma}_{SD}$ and η both lead to a better secrecy outage performance. It is not difficult for comprehension because a larger secrecy rate is much harder to support for a given channel condition, thus leading to a greater secrecy outage. In addition, a larger $\bar{\gamma}_{SD}$ indicates a greater amount of harvested energy and a better receiving SNR performance at the receiver. In other words, by increasing $\bar{\gamma}_{SD}$, the receiving SNR performance at the receiver is promoted while the receiving SNR performance at the eavesdropper becomes poor because a larger jamming power could be provided. Furthermore, although it is not a benefit to the receiver by increasing η, it still improves the amount of harvested energy, and thus can confuse the eavesdropper better. Therefore, increasing $\bar{\gamma}_{SD}$ and η both contribute to a better secrecy outage performance.

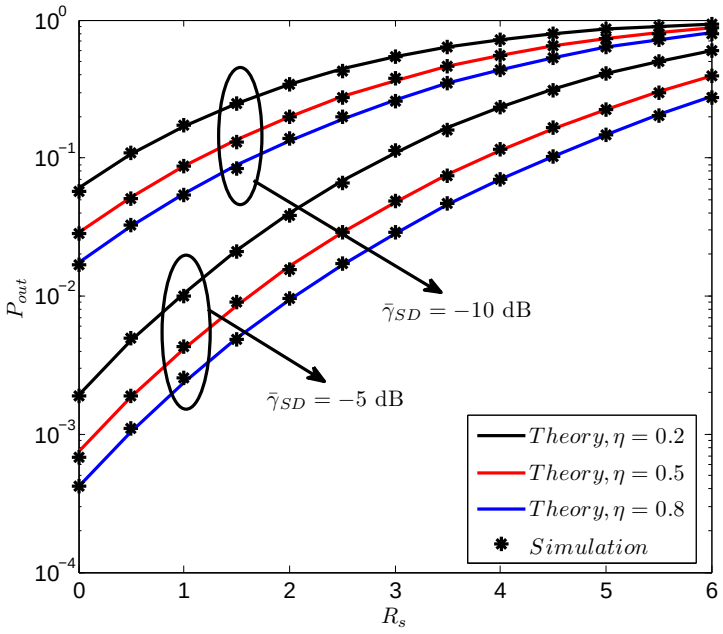

Figure 3. P_{out} vs. R_s with different $\bar{\gamma}_{SD}$ and η. $\gamma_S = 30$ dB, $\bar{\gamma}_{SE} = -10$ dB, $\bar{\gamma}_{DE} = -10$ dB, $\bar{\gamma}_{DD} = -5$ dB.

Figure 4 plots the secrecy outage probability P_{out} versus the transmit SNR γ_S for various R_s. As can be seen, the secrecy outage probability is a monotonically increasing function with R_s, which coincides with the finding in Figure 3. In addition, a lower secrecy outage probability is observed when a larger γ_S is provided, regardless of the value of R_s. As a matter of fact, the changing of γ_S will have two effects on the performance. On the one hand, increasing γ_S will benefit the receiving performance of both the receiver's and the eavesdropper's. One the other hand, the performance of the eavesdropper will be degraded by the jamming operation while the performance of the information receiver will not. We note that, when a larger γ_S is provided, the confusing effect to the eavesdropper will become better because more energy will be harvested, so that the user can jam the eavesdropper at a greater power. Overall, the receiving performance of the information receiver is much more improved than that of the eavesdropper. Therefore, the secrecy outage probability becomes a decreasing function with γ_S.

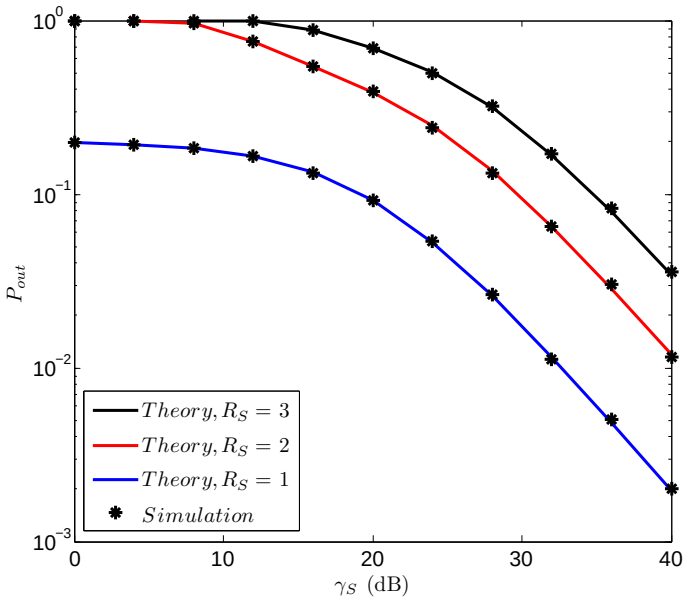

Figure 4. P_{out} vs. γ_S with various R_s. $\bar{\gamma}_{SD} = -10$ dB, $\bar{\gamma}_{SE} = -10$ dB, $\bar{\gamma}_{DE} = -10$ dB, $\bar{\gamma}_{DD} = -5$ dB, $\eta = 0.8$.

Figure 5 compares the secrecy throughput ς versus the secrecy rate R_s with different γ_S and η. It is shown that the secrecy throughput improves significantly when a larger γ_S is provided. Moreover, it is also beneficial to boost the secrecy throughput if η could be increased. In addition, this is especially useful in the high SNR region, as the enhancement of secrecy throughput is much more notable when γ_S is large. Furthermore, it is noted that the variation tendency of the secrecy throughput in each line indicates the existence of an optimum R_s which can maximize the secrecy throughput. This phenomenon is comprehensible. On the one hand, increasing R_s will directly contribute to the enhancement of secrecy throughput, as more secrecy message is transmitted. On the other hand, a larger secrecy rate will also lead to a greater secrecy outage probability, which will result in the decline of the secrecy throughput. As a result, an optimum R_s that maximizes the secrecy throughput is observed.

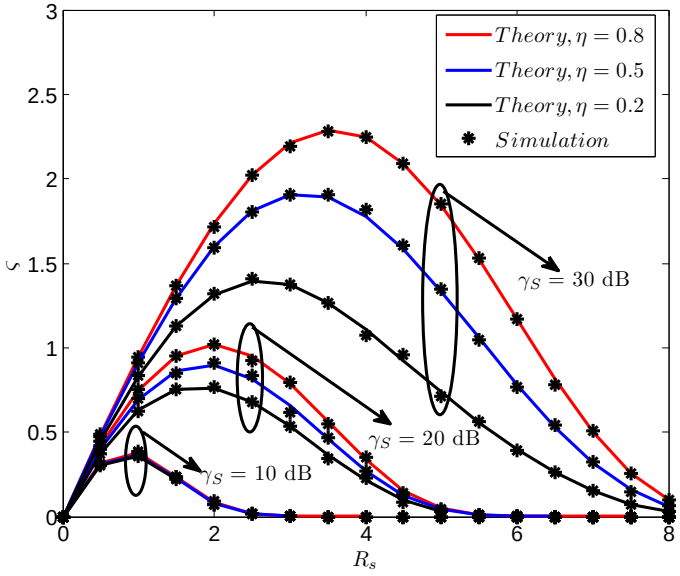

Figure 5. P_{out} vs. R_s with different γ_S and η. $\gamma_S = 30$ dB, $\bar{\gamma}_{SD} = -10$ dB, $\bar{\gamma}_{SE} = -10$ dB, $\bar{\gamma}_{DE} = -10$ dB, $\bar{\gamma}_{DD} = -5$ dB.

5. Conclusions

This paper presented a novel secure transmission scheme for the two-user SWIPT sensor networks where the cooperative zero-forcing jamming was conducted to confuse the eavesdropper. It is highlighted that the cooperative jamming does not require any energy of the sensors due to the SWIPT operation, and thus can be well applied to the energy-constrained wireless sensor networks. The exact closed-form expressions of the secrecy outage probability and the secrecy throughout were derived, which depicted the impacts of the system parameters on the system secrecy performance intuitively. The results illustrated that the secrecy outage probability monotonically increases with the growth of R_s, and monotonically decreases with the increase of γ_S and η. Moreover, the secrecy throughput could be further boosted if η increases, which is especially notable when γ_S is large enough. In addition, it was indicated that an optimum value of R_s maximizing the secrecy throughput exists, which also grows with the increase of γ_S. All of the findings are of great importance in guiding the secure design of practical wireless sensor networks.

Acknowledgments: This work was supported by the National Natural Science Foundation of China under Grant Nos. 61771487, 61471393, and 61371122. The authors would like to extend their gratitude to the anonymous reviewers for their valuable and constructive comments, which have largely improved and clarified this paper.

Author Contributions: Xuanxuan Tang, Yueming Cai, Wendong Yang and Weiwei Yang conceived of the main proposal of the secure transmission schemes, conducted system modeling, and derived analysis and numerical simulation of the proposed schemes. Xuanxuan Tang and Yueming Cai wrote the manuscript. Dechuan Chen and Junquan Hu provided considerable comments and technique review of the proposed scheme and contributed to the revision of the paper. Yueming Cai read and approved the final manuscript.

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

References

1. Zheng, J.; Cai, Y.; Shen, X.; Zheng, Z.; Yang, W. Green energy optimization in energy harvesting wireless sensor networks. *IEEE Commun. Mag.* **2015**, *53*, 150–157.
2. Hu, J.; Yang, W.; Yang, N.; Zhou, X.; Cai, Y. On-off-based secure transmission design with outdated channel state information. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6075–6088.
3. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573.
4. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27.
5. Tang, X.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W.; Yang, W. Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems. *IEEE Trans. Veh. Technol.* **2017**, doi:10.1109/TVT.2017.2695500.
6. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Physical layer network security in the full-duplex relay system. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 574–583.
7. Hu, J.; Cai, Y.; Yang, N.; Yang, W. A new secure transmission scheme with outdated antenna selection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2435–2446.
8. Zou, Y.; Wang, X.; Shen, W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2099–2111.
9. Yang, M.Q.; Zhang, B.N.; Huang, Y.Z.; Yang, N.; Guo, D.X.; Gao, B. Secure multiuser communications in wireless sensor networks with TAS and cooperative jamming. *Sensors* **2016**, *16*, 1908, doi:10.3390/s16111908.
10. Wang, C.; Wang, H.M.; Xia, X.G.; Liu, C. Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 2596–2612.
11. Zhang, R.; Song, L.; Han, Z.; Jiao, B. Physical layer security for two-way untrusted relaying with friendly jammers. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3693–3704.
12. Yun, S.; Park, J.; Im, S.; Ha, J. On the secrecy rate of artificial noise assisted MIMOME channels with full-duplex receiver. In Proceedings of the IEEE Wireless Communications and Networking Conference, San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
13. Liu, H.; Kim, K.J.; Kwak, K.S.; Poor, H.V. Power splitting-based SWIPT with decode-and-forward full-duplex relaying. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 7561–7577.

14. Zhou, X. Training-based SWIPT: Optimal power splitting at the receiver. *IEEE Trans. Veh. Technol.* **2015**, *64*, 4377–4382.
15. Krikidis, I.; Timotheou, S.; Nikolaou, S.; Zheng, G.; Ng, D.W.K.; Schober, R. Simultaneous wireless information and power transfer in modern communication systems. *IEEE Commun. Mag.* **2014**, *52*, 104–110.
16. Liu, M.; Liu, Y. Power allocation for secure SWIPT systems with wireless-powered cooperative jamming. *IEEE Commun. Lett.* **2017**, *21*, 1353–1356.
17. Zhang, Q.; Huang, X.; Li, Q.; Qin, J. Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels. *IEEE Trans. Commun.* **2015**, *63*, 906–915.
18. Tang, X.; Yang, W.; Cai, Y.; Yang, W.; Cao, K.; Yuan, P. Secrecy analysis of full-duplex power-splitting SWIPT networks with artificial noise. In Proceedings of the International Workshop on Computer Science and Engineering, Beijing, China, 25–27 June 2017; pp. 950–955.
19. Yang, W.; Mou, W.; Xu, X.; Yang, W.; Cai, Y. Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques. *IET Commun.* **2016**, *10*, 1712–1720.
20. Zhang, J.; Pan, G.; Wang, H.M. On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system. *IEEE Access* **2016**, *4*, 3887–3893.
21. Zhou, X.; Maham, B.; Hjorungnes, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907.
22. Wang, H.M.; Zheng, T.; Mu, P. Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading. In Proceedings of the IEEE International Conference on Communications, Sydney, NSW, Australia, 10–14 June 2014; pp. 5396–5401.
23. Hu, J.; Yang, N.; Zhou, X.; Yang, W.; Cai, Y. A versatile secure transmission strategy in the presence of outdated CSI. *IEEE Trans. Veh. Technol.* **2016**, *65*, 10084–10090.
24. Bi, Y.; Chen, H. Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1538–1550.
25. Afana, A.; Asghari, V.; Ghrayeb, A.; Affes, S. On the performance of cooperative relaying spectrum-sharing systems with collaborative distributed beamforming. *IEEE Trans. Commun.* **2014**, *62*, 857–871.
26. Afana, A.; Asghari, V.; Ghrayeb, A.; Affes, S. Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints. In Proceedings of the 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Cesme, Turkey, 17–20 June 2012; pp. 429–433.
27. Zhang, T.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W. Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes. *IEEE Trans. Commun.* **2017**, *65*, 335–346.
28. Zhang, T.; Huang, Y.; Cai, Y.; Zhong, C.; Yang, W.; Karagiannidis, G. Secure multi-antenna cognitive wiretap networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 4059–4072.
29. Zeng, Y.; Zhang, R. Full-duplex wireless-powered relay with self-energy recycling. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 201–204.
30. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier/Academic Press: Amsterdam, The Netherlands, 2007.
31. Xu, X.; Yang, W.; Cai, Y.; Jin, S. On the secure spectral-energy efficiency tradeoff in random cognitive radio networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 2706–2722.
32. Yan, S.; Yang, N.; Geraci, G.; Malaney, R.; Yuan, J. Optimization of code rates in SISOME wiretap channels. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 6377–6388.
33. Wang, L.; Cai, Y.; Zou, Y.; Yang, W.; Hanzo, L. Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6259–6274.