electronics

MDPI

Article

Trust-Degree-Based Secure Relay Selection in SWIPT-Enabled Relay Networks

Ran Gao [1], Ling Xu [2], Dan Xu [3] and Jianrong Bao [2,4,*]

[1] State-Owned Assets and Laboratory Management Office, Hangzhou Dianzi University, Hangzhou 310018, China
[2] School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
[3] Zhejiang Dahua Technology Co., Ltd., Hangzhou 310053, China
[4] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
* Correspondence: baojr@hdu.edu.cn

Abstract: In this paper, we investigate the trust-degree-based secure relay selection in simultaneous wireless information and power transfer (SWIPT)-enabled relay networks. In particular, we optimize the interference power by selecting the appropriate relay and time division ratio on the condition of both the secure transmission and trust degree. First, by applying the security capacity constraint, we derive the expressions of the time division ratio and relay interference power concerning the trust degree. Then, we discuss the different results for different trust degrees and determine the set of trust degrees to guarantee secure communications. Finally, according to the different trust degrees, we compute the needed interference power for each relay and make a selection to obtain the optimal performance under relay networks. Simulation results show that with the known trust degree the proposed algorithm obtains the appropriate relay and time division ratio, reduces energy consumption, and guarantees an achievable security rate.

Keywords: relay networks; simultaneous wireless information and power transfer (SWIPT); trust degree; security; power control

check for updates

Citation: Gao, R.; Xu, L.; Xu, D.; Bao, J. Trust-Degree-Based Secure Relay Selection in SWIPT-Enabled Relay Networks. *Electronics* **2023**, *12*, 429. https://doi.org/10.3390/electronics12020429

Academic Editors: Dimitra I. Kaklamani and Flavio Canavero

Received: 23 October 2022
Revised: 5 December 2022
Accepted: 10 January 2023
Published: 13 January 2023

1. Introduction

Motivated by the development of the Internet of Things (IoT), the use of wireless devices, such as smartphones, wearable gadgets, or connected vehicles, has increased exponentially. It has led to a vast amount of information being exchanged and posed great challenges to meet capacity and performance demands [1,2], which have made it more difficult, especially for a long-distance wireless transmitting system due to the terrible channel conditions. Cooperative relays can potentially improve the coverage and system capacity without increasing power consumption; thus, it has become an efficient approach to solve the aforementioned problems [3]. However, in addition to the traffic capacity and coverage, the limited energy has also become a bottleneck, limiting the development of mobile applications [4]. Fortunately, the simultaneous wireless information and power transfer (SWIPT) has emerged as a promising way to alleviate the energy shortage by allowing the relay to act as an information forward as well as an energy receiver, thereby achieving a trade-off between information transmission (IT) and energy harvesting (EH) [4].

Security relay selection was investigated to maximize the average rate or secrecy capacity and improve the secure outage probability (OP). It was modeled as a restless bandit optimization problem to maximize the average rate, while considering the credibility of each relay node. Then, it was solved by using the priority-index heuristic method effectively [5]. To maximize secrecy capacity, the optimal time allocation and power splitting ratio adaptively adjusted according to instantaneous channel state information are proposed in a high signal-to-noise ratio regime through a split-step iterative method [6]. Given trust degrees and channel conditions, a relay selection strategy was proposed to maximize the expected achievable rate. So, a cooperative transmission strategy of relays with an optimal cooperative beamforming vector was derived to maximize the expected achievable rate. Finally, a mixed strategy between the relay selection and cooperative transmission was obtained with respect to the trust degrees [7]. The secrecy performance was investigated, and closed-form expressions of outage probability (OP) and secrecy OP for dynamic or static-power-splitting-based relaying schemes were derived with the lower bound of secrecy OP under the infinity source's transmit power [8]. Generally, there were two modes in a SWIPT-enabled cooperative relay system, which were the time switching (TS) and the power splitting (PS) modes with the objective of secrecy rate and secure energy efficiency maximization [9]. In the former, the relay node was allocated a particular time slot for the EH and IT. The TS mode was easier to realize than the PS one due to the receiver complexity; thus, the former was widely applied in these application processes [10]. To improve the spectrum efficiency of the system, a two-way communication protocol for SWIPT-enabled cognitive radio networks was designed with two data-driven relay selection methods by the neural network for the fixed number of relays and the variable number of relays, respectively [11]. Thus, in this work, we adopt the TS mode to harvest energy from the received radio frequency (RF) signals at the relay node. Another key challenge faced in these SWIPT-enabled relay networks was the security. In most studies of the SWIPT-enabled cooperative systems, the relay was considered completely trustworthy. However, there were many unbelievable relays unwilling to help forward messages and even eavesdropped on them, leading to a decrease in the expected secrecy rate. Therefore, physical security technology [12,13] was applied to hamper the eavesdroppers. Furthermore, the trust degree of relays has been taken into account during the relay selection. Trust degree [14] is generally defined as a belief level that a node can perform a specific operation according to a plan, and it can be evaluated based on previous behaviors [15] or quantified by the physical distance [16]. In this paper, the trust degree is interpreted as the degree to which the relay is willing to help forward the messages, i.e., the probability that the relay forwards the information.

In this paper, we mainly investigate the trust-degree-based secure relay selection in SWIPT-enabled relay networks. The secure relay selection in SWIPT-enabled relay networks has been investigated in [17,18], which aimed to enhance the rate-energy trade-off while assuring transmission security. Unlike the aforementioned works, in this paper, we consider not only the rate–energy trade-off, but also the security performance of the trust degree of the relay node, which is still an open issue. Furthermore, the harvesting energy by the relay is only used to interfere with eavesdropping on the information, and the energy to relay information to the next hop is provided by the relay itself. In particular, we optimize the interference power by selecting the appropriate relay and time division ratio on the condition of both the secure transmissions and trust degrees in a SWIPT-enabled relay network. By applying the security capacity constraint, we first derive the expressions of the time division ratio and relay interference power with respect to the trust degree. Then, we discuss the different results for different trust degrees and determine the set of trust degrees that can guarantee the security communications. Finally, according to the different trust degrees, we can compute the needed interference power and make an optimal relay selection.

The rest of this paper is organized as follows. In Section 2, we introduce and analyze the system model with respect to the secure relay selection in relay networks. Subsequently, the optimization algorithm of the trust-degree-based secure relay selection is proposed for the SWIPT-enabled relay networks in Section 3. Then, in Section 4, we evaluate the performance of the proposed algorithm. Finally, we conclude the entire paper in Section 5.

2. Secure Relay Selection System Model

In this paper, we mainly investigate the SWIPT-enabled secure relay selection network. It consists of a source (s), a destination (d), an eavesdropper (e), and M relays, which are represented by a collection $\Re$, i.e., $\Re = \{r_1, r_2, \cdots, r_M\}$. A decode-and-forward (DF) relaying protocol is adopted in the system. Here, we denote the trust degree of the relay i as $\alpha_i, \alpha_i \in [0,1]$. Finally, the system model is shown in Figure 1 with situations of (a) first time slot and (b) second time slot.

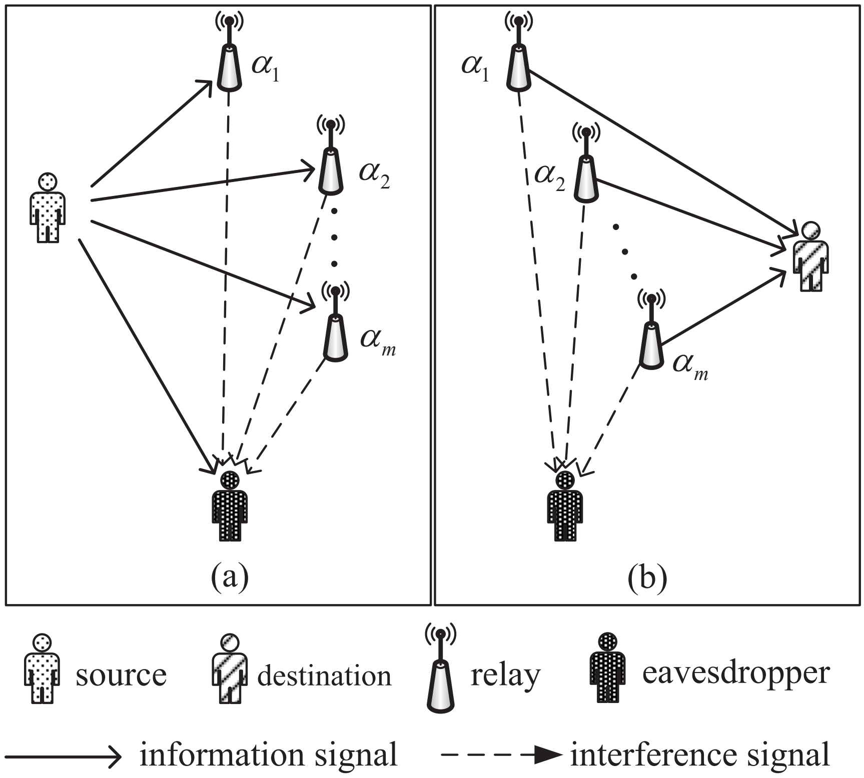

Figure 1. Secure relay selection system model: (**a**) first time slot; (**b**) second time slot.

2.1. TS Model

In the network model, each information transmission cycle is divided into two-time slots, as shown in Figure 2. In the first time slot, a time slot T is divided into two parts by the time division ratio $\gamma, \gamma \in [0,1]$. Within the first interval γT, the source first transmits the energy signals to the relay with power P_s, and the relay harvests the energy from the received signals. In the latter interval $(1-\gamma)T$, the source transmits the messages to the relay with power P_s. Simultaneously, the relay uses the energy collected in the previous interval to send interference signals to hamper the eavesdropper. In the second time slot, the relay forwards the message with power P_s, and it uses the residual energy collected in the first time slot to send the interference signals to hamper the eavesdropper.

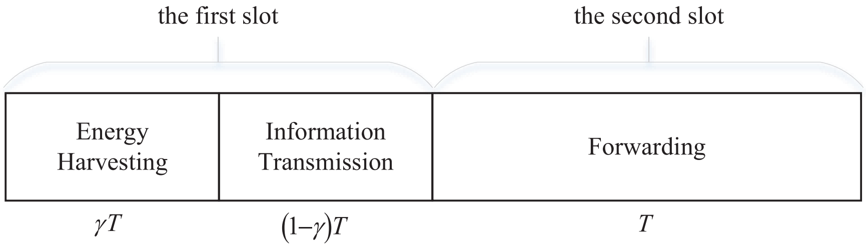

Figure 2. Slot-splitting model.

2.2. Signal Model

Within the interval γT, the source S transmits the energy signals to the relay with power P_s, and the signals received at the i-th relay R_i are given by

$$y_{i1} = \sqrt{P_s g_{si}} x_1 + n_i, \tag{1}$$

where y_{i1} and x_1 denote the transmitted and received signals within the interval γT , respectively; g_{si} represents the channel coefficient between the source s and the i-th relay; n_i is the additive white Gaussian noise at the i-th relay; and its variance is σ_i^2. The total energy collected is given by

$$W = \eta \gamma T P_s g_{si}, \tag{2}$$

where η indicates the energy conversion efficiency [12] and it is assumed that the noise energy is negligible. During the remaining $(1-\gamma)T$ time, the signals received at the i-th relay are given by

$$y_{i2} = \sqrt{P_s g_{si}} x_2 + n_i, \tag{3}$$

where x_2 denotes the transmitted signals from the source, and y_{i2} denotes the received signals at the i-th relay within the interval $(1-\gamma)T$, respectively. The achievable rate at the i-th relay is

$$R_{si} = \log_2\left(1 + \frac{P_s g_{si}}{\sigma_i^2}\right), \tag{4}$$

where R_{si} is the achievable information rate on the source-relay link s-i. At the same time, the i-th relay uses the energy collected in the previous stage to send interference signals. Therefore, the signal received at the eavesdropper is as

$$y_{e1} = \sqrt{P_s g_{se}} x_2 + \sqrt{P_i^j g_{ie}} x_i^j + n_e, \tag{5}$$

where P_i^j and x_i^j are the interference power and interference signals transmitted by the i-th relay; g_{se} and g_{ie} denote the channel coefficients between the source–eavesdropper link s–e and relay–eavesdropper link i–e, respectively; n_e is additive Gaussian white noise at the eavesdropper, and the variance is σ_e^2. Within the second time slot T, the receiver can eliminate the interference signals sent by the relay, and the received signals at the destination d are

$$y_{id} = \sqrt{P_s g_{id}} x_c + n_d, \tag{6}$$

where $y_i d$ denotes the received signals from the i-th relay to the destination d, g_{id} represents the channel coefficient between the i-th relay and destination d, x_c represents the message signal sent by the relay in the second time slot, and n_d is the additive white Gaussian noise at destination d, and its variance is σ_d^2. The achievable rate R_{id} at the destination d is written as

$$R_{id} = \log_2\left(1 + \frac{P_s g_{id}}{\sigma_d^2}\right). \tag{7}$$

According to [19], assuming that the channel conditions and noise in two consecutive time slots are unchanged, the signal intercepted by eavesdroppers can be obtained as

$$y_{e2} = \sqrt{P_s g_{ie}} x_c + \sqrt{P_i^j g_{ie}} x_i^j + n_e. \tag{8}$$

Because the relay uses the DF transmission protocol, the achievable rate at the eavesdropper is given by

$$R_e = \log_2\left(1 + \frac{P_s g_{se}}{P_i^j g_{ie} + \sigma_e^2} + \frac{P_s g_{ie}}{P_i^j g_{ie} + \sigma_e^2}\right). \tag{9}$$

The interference power P_i^j of the relay is related to the interference time. The interference time in the first time slot is equal to $(1-\gamma)T$. During the second time slot, the relay sends interference signals until the message forwarding is complete. Thus, the total transmitting time "t" in the second time slot satisfies

$$(1-\gamma)T\log_2\left(1+\frac{P_s g_{si}}{\sigma_i^2}\right)=t\log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right). \tag{10}$$

It means that the relay needs to send out all packets from the source in the last time slot. This case is reasonable because the source still needs to spend time charging the relay during the last time slot. From Equation (10), we can obtain the time during which the relay sends the interference messages in the second time slot, which is equal to the total transmitting time t.

$$t=(1-\gamma)T\frac{\log_2\left(1+\frac{P_s g_{si}}{\sigma_i^2}\right)}{\log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right)}. \tag{11}$$

Combining Equations (2) and (11), the expression of the relay interference power can be obtained as

$$\begin{aligned}P_i^j&=\frac{W}{(1-\gamma)T+t}\\&=\frac{\gamma}{(1-\gamma)}\cdot\frac{\eta P_s g_{si}\log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right)}{\log_2\left[\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right)\left(1+\frac{P_s g_{si}}{\sigma_i^2}\right)\right]}\end{aligned}. \tag{12}$$

From Equation (12), the relay interference power P_i^j is an increasing function of the time division ratio γ. By the basic conception of the relay interference power and the slot-splitting model with slot allocation by the energy harvesting and the information transmission, the relay interference power P_i^j is first represented in the first-line expression of Equation (12). Then, by substituting "W" with the expression in Equation (2) and "T/t" with the transformed expression in Equation (11), the detailed expression of relay interference power P_i^j is easily derived in the second line of Equation (12). According to [20], in a two-hop relay network, the maximum achievable rate at the destination is $\min(R_{si}, R_{id})$. If the trust degree of the i-th relay is represented by α_i, the relay forwarding probability is α_i. According to the definition of physical layer security [12,13], we have

$$\alpha_i[\min(R_{si},R_{id})-R_e]\geq\bar{R}, \tag{13}$$

where $\bar{R}$ is the expected secrecy rate. Equation (13) is the security rate constraint, which means that the attainable secrecy rate needs to be larger than the expected secrecy rate $\bar{R}$.

2.3. Problem Formulation

In this paper, we aim to minimize the interference power consumption P_i^j by selecting the appropriate relay i and the time division ratio γ on the constraint of the secure transmission and trust degree. The optimization model can be formulated as

$$\begin{array}{ll}\min\limits_{i,\gamma} & P_i^j\\ \text{s.t.} & P_i^j=\frac{\gamma}{(1-\gamma)}\cdot\frac{\eta P_s g_{si}\log_2(1+P_s g_{id}/\sigma_d^2)}{\log_2[(1+P_s g_{id}/\sigma_d^2)(1+P_s g_{si}/\sigma_i^2)]},\\ & \alpha_i[\min(R_{si},R_{id})-R_e]\geq\bar{R},\\ & 0\leq P_i^j\leq 1,\\ & \gamma\in[0,1],\\ & \alpha_i\in[0,1],\\ & i\in\{1,2,\ldots,M\}.\end{array}, \tag{14}$$

where $0\leq P_i^j\leq 1$ is the interference power constraint to limit the impact of interference.

In (14), the appropriate relay and the time division ratio are chosen to optimize the interference power on the condition of considering the secure transmission and trust degree, and it is mainly implemented by the time division ratio and relay interference power with respect to trust degree. Then, the different results are analyzed for different trust degrees, and the set of trust degrees are found to guarantee the security communications. Finally, according to the different trust degrees, the required interference power is simulated and analyzed for each relay and make a selection.

3. Proposed Optimization Algorithm of the Trust-Degree-Based Secure Relay Selection

3.1. Trust-Degree-Based Secure Relay Selection

To solve Equation (14), we first simplify the first constraint Equation (13).

The maximum achievable rate is $\min(R_{si}, R_{id})$, so we can divide it into two cases: (1) $R_{si} > R_{id}$ and (2) $R_{si} \le R_{id}$. Since R_{si} and R_{id} are only related to the channel coefficients and noises, the following analysis focuses on Case (1), and Case (2) is similarly available.

Case (1):

Equation (13) can be transformed as

$$\log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right) - \frac{\bar{R}}{\alpha_i} \ge \log_2\left(1+\frac{P_s(g_{se}+g_{ie})}{P_i^j g_{ie} + \sigma_e^2}\right) > 0. \tag{15}$$

It can be derived from Equation (15) that only when Equation (14) can hold, can we obtain

$$P_i^j \ge \frac{2^{\bar{R}/\alpha_i}\sigma_d^2 P_s(g_{se}+g_{ie})}{\left(\sigma_d^2+P_s g_{id} - 2^{\bar{R}/\alpha_i}\sigma_d^2\right)g_{ie}} - \frac{\sigma_e^2}{g_{ie}}. \tag{16}$$

Let $P_L = \frac{2^{\bar{R}/\alpha_i}\sigma_d^2 P_s(g_{se}+g_{ie})}{\left(\sigma_d^2+P_s g_{id}-2^{\bar{R}/\alpha_i}\sigma_d^2\right)g_{ie}} - \frac{\sigma_e^2}{g_{ie}}$ and $\alpha_i^1 = \frac{\bar{R}}{\log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right)}$. Since the optimization goal is to minimize the interference power, we have

$$P_i^j = \begin{cases} P_L, & \alpha_i > \alpha_i^1; \\ 0, & \alpha_i \le \alpha_i^1. \end{cases} \tag{17}$$

Because constraints $0 \le P_L \le 1$ should hold, we have

$$\frac{\bar{R}}{\log_2\left[\frac{\left(g_{ie}+\sigma_e^2\right)\left(\sigma_d^2+P_s g_{id}\right)}{\sigma_d^2\left(g_{ie}+\sigma_e^2+P_s\left(g_{se}+g_{ie}\right)\right)}\right]} \le \alpha_i \le \frac{\bar{R}}{\log_2\left[\frac{\sigma_e^2\left(\sigma_d^2+P_s g_{id}\right)}{\sigma_d^2\left(\sigma_e^2+P_s\left(g_{se}+g_{ie}\right)\right)}\right]} . \tag{18}$$

By combining Equations (12) and (17) together, there is

$$\gamma = \frac{P_L}{P_L + N}, \tag{19}$$

where there is $N = \eta P_s g_{si} \log_2\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right) \Big/ \log_2\left[\left(1+\frac{P_s g_{id}}{\sigma_d^2}\right)\left(1+\frac{P_s g_{si}}{\sigma_i^2}\right)\right]$.

Define $\alpha_i^2 = \bar{R} \Big/ \log_2\left[\frac{\sigma_e^2\left(\sigma_d^2+P_s g_{id}\right)}{\sigma_d^2\left(\sigma_e^2+P_s\left(g_{se}+g_{ie}\right)\right)}\right]$ and $\alpha_i^3 = \bar{R} \Big/ \log_2\left[\frac{\left(g_{ie}+\sigma_e^2\right)\left(\sigma_d^2+P_s g_{id}\right)}{\sigma_d^2\left(g_{ie}+\sigma_e^2+P_s\left(g_{se}+g_{ie}\right)\right)}\right]$. By combining Equations (17) and (18), there are some conclusions drawn as follows.

- When $\alpha_i > \alpha_i^1$, the constraint Equation (13) is satisfied.
- When $\alpha_i > \alpha_i^3$, the constraint of the interference power in the optimization problem is satisfied.
- When $\alpha_i \ge \alpha_i^2$, although the relay does not send the interference power, the network can also achieve confidential communication, i.e., the source could directly transmit information without charging to the relay in advance.

- When $\alpha_i < \alpha_i^2$, the relay must send a certain interference signal to ensure the safety of the communication.

According to the different values $\alpha_i^1, \alpha_i^2, \alpha_i^3, 0, 1$, there are 30 cases. The following 10 cases can ensure confidential communications as

$$\begin{array}{ll} 0 < \alpha_i^1 < \alpha_i^3 < 1 < \alpha_i^2; & 0 < \alpha_i^1 < \alpha_i^3 < \alpha_i^2 < 1; \\ 0 < \alpha_i^3 < \alpha_i^1 < 1 < \alpha_i^2; & 0 < \alpha_i^3 < \alpha_i^1 < \alpha_i^2 < 1; \\ 0 < \alpha_i^1 < \alpha_i^2 < \alpha_i^3 < 1; & 0 < \alpha_i^3 < \alpha_i^2 < \alpha_i^1 < 1; \\ 0 < \alpha_i^2 < \alpha_i^1 < \alpha_i^3 < 1; & 0 < \alpha_i^2 < \alpha_i^3 < \alpha_i^1 < 1; \\ \alpha_i^2 < 0 < \alpha_i^1 < \alpha_i^3 < 1; & \alpha_i^2 < 0 < \alpha_i^3 < \alpha_i^1 < 1. \end{array} . \tag{20}$$

Here, we take the case "$0 < \alpha_i^1 < \alpha_i^3 < \alpha_i^2 < 1$", for example, to analyze specifically as follows, and the other cases can be derived in the same way.

- When $0 < \alpha_i < \alpha_i^1$, constraints of the expected secrecy rate and the interference power cannot be satisfied; that is to say, confidential communication is impossible.
- When $\alpha_i^1 < \alpha_i < \alpha_i^3$, if the expected secrecy rate constraint is satisfied, the interference power constraint cannot be satisfied; thus, confidential communication also cannot be guaranteed.
- When $\alpha_i^3 < \alpha_i < \alpha_i^2$, the relay needs to send a certain interference signal to ensure the safety of communication, and the interference power is equal to Equation (12).
- When $\alpha_i^2 < \alpha_i < 1$, confidential communication is guaranteed without interference signals.

Case (2):

Since the values of R_{si} and R_{id} are only related to the channel coefficients and noises, the above analysis on Case (1) is still suitable for Case (2). To avoid repetition and save space, it is not described in this article.

Until now, the minimum interference power needed for different relays can be computed with different trust degrees and channel conditions. After comparing the power values, the best relay to forward the packets can be determined.

3.2. Evaluation and Analysis of the Trust-Degree-Based Secure Relay Selection

The performance of the proposed trust-degree-based secure relay selection is mainly evaluated by the expected secure achievable rate [7], short for the expected secure rate. Then, there are mainly three class of such relay selection schemes, such as the trust-degree-based relay selection, cooperative transmission, and hybrid cooperation schemes. In the first relay selection scheme, the transmitter chooses a single relay node, and the chosen relay node forwards the received data from source to destination according to trust degrees. In the relay selection, the transmitter selects the relay node by considering both the trust degrees of the relay nodes and the channel conditions. In the second cooperative transmission, the source transmits the data to all relay nodes, and then the relay nodes forward the data to the destination with the cooperative transmission. In this case, the participation of the relay nodes in the cooperation is determined by the trust degrees. In the third hybrid cooperation scheme, the source selects the best scheme between the trust-degree-based relay selection and the cooperative transmission by both channel conditions and trust degrees. This scheme totally adopts all parameters for the optimization of the expected achievable rate, and it obtains the best performance among these three schemes. The main difference between our scheme and that in [7] is that our scheme extends the latter by increasing the influence of the eavesdropper. As shown in Figure 1, the expected achievable rate from the relay node to the destination is subtracted by R_e in Equation (13). Finally, with similar definitions and analyses in [7], we obtain the expected achievable secrecy rate of the above three relay selection cooperation schemes as follows.

The transmission is divided into two stages: Stage I for the links of source to relays and Stage II for the links of relays to destination. The source and relay node i have the transmit power budgets P_T and $P_i (i = 1, 2)$, respectively, and the source is supposed to know the channel state information (CSI) of the connected channel to relay node i denoted by $\mathbf{h}_i(i = 1, 2)$. The trust degree represents the extent of the relay node trusted for cooperation.

3.2.1. Trust-Degree-Based Relay Selection Scheme

In this scheme, one relay node is chosen for secure signal forwarding with low complexity [7]. In Stage I, by channel capacity form information theory, the expected achievable rate of relay $R_i^{[1]}$ is represented as

$$R_i^{[1]} = \log(1 + \rho_T \cdot \|\mathbf{h}_i\|), \tag{21}$$

where $\rho_T = \frac{P_T}{\sigma^2}$ is the SNR of the transmit node, P_T is the transmit power, σ^2 is the variance of noises, and $\|\mathbf{h}_i\|$ is the norm of the i-th channel coefficient vector.

In Stage II, by channel capacity form information theory, the expected achievable rate of relay $R_i^{[2]}$ is represented as

$$\bar{R}_i^{[2]} = \alpha_i \cdot R_i^{[2]} - R_e = \alpha_i \cdot \log(1 + \rho_i \cdot |g_i|^2) - R_e, \tag{22}$$

where $\rho_i = \frac{P_i}{\sigma^2}$ is the SNR of the relay node, P_i is the transmit power, and σ^2 is the variance of noises in the relay node. R_e is defined in Equation (9), and it is caused by the influence of the eavesdropper. Here, α_i and g_i are the trust degree and channel coefficient of link R_i to the destination, respectively.

With the half-duplex mode, the expected secure rate for the link with relay node i is expressed as

$$\bar{R}_i[\delta_I(\mathbf{w}_i)] = \frac{1}{2}\min[R_i^{[1]}, \bar{R}_i^{[2]}], \tag{23}$$

where δ_I represents the scheme I of the trust-degree-based relay selection scheme, and $\mathbf{w_i}$ represents the corresponding beamforming vector.

Therefore, the expected secure rate of this scheme with two relay nodes is expressed as

$$\bar{R}[\delta_I(\mathbf{w}_i^{MRT})] = \max\{\bar{R}_i[\delta_I(\mathbf{w}_1)], \bar{R}_i[\delta_I(\mathbf{w}_2)]\}. \tag{24}$$

where $\mathbf{w}_i^{MRT}$ is the beamforming vector of the maximum ratio transmission (MRT).

3.2.2. Trust-Degree-Based Cooperative Transmission Scheme

In this scheme, all relay nodes are available and combined for optimal secure signal forwarding. In Stage I, the two relay node can decode and forward received data. Because both relay nodes can decode and forward the received data from the source, the achievable rate of the trust-degree-based cooperative transmission is the minimum of the achievable rates of the two relay nodes [7], and it is expressed as

$$\begin{aligned} R^{[1]}(\mathbf{w}) &= \min[R_1^{[1]}(\mathbf{w}), R_2^{[1]}(\mathbf{w})] \\ &= \min[\log(1 + \rho_T \cdot |\mathbf{h}_1^\dagger \mathbf{w}|^2), \log(1 + \rho_T \cdot |\mathbf{h}_2^\dagger \mathbf{w}|^2)] \end{aligned}, \tag{25}$$

where $\mathbf{h}_i^\dagger$ is the i-th channel coefficient vector.

In Stage II, the achievable rate of the trust-degree-based cooperative transmission is represented as

$$\bar{R}^{[2]} = \alpha_1\alpha_2 \log(1 + \rho_1|g_1|^2 + \rho_2|g_2|^2) + \alpha_1(1 - \alpha_2)R_1^{[2]} + \alpha_2(1 - \alpha_1)R_2^{[2]} - R_e, \tag{26}$$

where $R_i^{[2]}$ is expressed the same as Equation (22), and R_e is defined in Equation (9) from the influence of the eavesdropper. Equation (26) can be explained as follows. The first item represents the expected achievable rate of the cooperative data forwarding from two relay nodes to the destination. The second or third item presents the expected achievable rate by Relay Node 1 or 2, respectively.

Finally, given the half-duplex DF relaying, the expected achievable rate of this cooperative transmission scheme is expressed as

$$\bar{R}[\delta_{II}(\mathbf{w})] = \frac{1}{2}\min\{R^{[1]}(\mathbf{w}), \bar{R}^{[2]}\}, \tag{27}$$

where δ_{II} represents Scheme II as the trust-degree-based relay selection scheme.

3.2.3. Hybrid Cooperative Transmission Scheme

In this subsection, the trust-degree-based hybrid cooperation scheme is proposed by an optimized scheme between the joint relay selection and the cooperative transmission. By using the proposed hybrid cooperation scheme, we obtain the optimal transmission to maximize the expected achievable rate in terms of both the trust degrees and channel conditions. It is implemented with different schemes [7] adopted by some constraints, and it is expressed as

$$\delta_{III}(\mathbf{w}_{opt}) = \begin{cases} \delta_{II}(\mathbf{w}) \;, & given \quad \frac{R^{[1]}(\mathbf{w})}{R_1^{[2]}} \geq \alpha_1, \frac{R^{[1]}(\mathbf{w})}{R_2^{[2]}} \geq \alpha_2 \\ \delta_I(\mathbf{w}), & otherwise \end{cases} \quad . \tag{28}$$

When the channel gains from the source to the relay nodes are larger than those from the relay nodes to the destination such as $R^{[1]}(\mathbf{w}) > \max\{R_1^{[2]}, R_2^{[2]}\}$, there are $\frac{R^{[1]}(\mathbf{w})}{R_1^{[2]}} \geq 1$ and $\frac{R^{[1]}(\mathbf{w})}{R_2^{[2]}} \geq 1$. Hence, the cooperative transmission becomes the optimal strategy regardless of trust degrees. In this case, the source can transmit the data, and it can be decoded at both of the relay nodes without any rate loss. Therefore, the cooperative transmission yields a larger expected achievable rate than that of the relay selection for any α_1 and α_2. Otherwise, the optimal transmission is mainly decided by the trust degrees. When the trust degree of one relay node is relatively larger than that of another one, the first relay selection scheme becomes the optimal transmission scheme.

4. Numerical Simulation Results and Analyses

In this section, we present simulations to evaluate the performance and characteristics of the proposed methods. We assume that the additive white Gaussian noise at the relays, receiver, and eavesdroppers is equal, and its value is −40 dB. Set the energy conversion efficiency $\eta = 0.99$ and the confidential information
rate threshold to $\overline{R} = 0.5$ bit/s. Due to some factors, such as the efficiency of the power amplifier and the transmission loss in SWIPT energy reception, the energy conversion efficiency cannot be obtained for 100%. In addition, the confidential information rate threshold is set as 0.5 bit/s as a typical example of the confidential information rate (normalized information achievable rate), which is commonly used in the SWIPT experiment on our simulation occasions. Then, the aforementioned parameters are chosen properly to perform the simulations and validation of the proposed trust-degree-based secure relay selection in SWIPT-enabled relay networks. Finally, we simulate the time division ratio and the relay interference power concerning different trust degrees under distinct transmission power and channel conditions, respectively.

Figures 3 and 4 show the conditions where the transmission power $P_s = 0.5$ W and the channel gain g_{ie} are equal to −15 dB, −35 dB, and −45 dB, respectively. They show the relationships of trust degree with respect to the time division ratio and the relay interference power, respectively. When the trust degree is near zero, the time division ratio and the relay interference power are both equal to zero because no relay can be selected to guarantee the achievable security rate $\overline{R}$. Then, with the increase of the trust degree, the time division ratio decreases because the needed interference power decreases, and the relay needs less charging time. When the trust degree has a very high value, this system is safe enough, and it does not even need interference to guarantee security, which is shown in the later parts with the blue and green lines. However, when the eavesdropping channel g_{ie} is too weak, for example −45 dB, even if the relay has a high trust degree, the relay still needs to send interference power to degrade the eavesdropping capacity. Under the same trust degree, the better the eavesdropping channel is, the more interference power is needed. This phenomenon can be explained as follows. We need to use interference to decrease the attainable eavesdropping capacity. By solving Equation (14), we first simplify the first constraint Equation (13) at the destination to obtain the maximum achievable rate, i.e., $\min(R_{si}, R_{id})$, with minimization of interference power consumption. With the known trust degrees for each relay, we can compute the minimum interference power it needs, so we can decide which one to select to forward the messages.

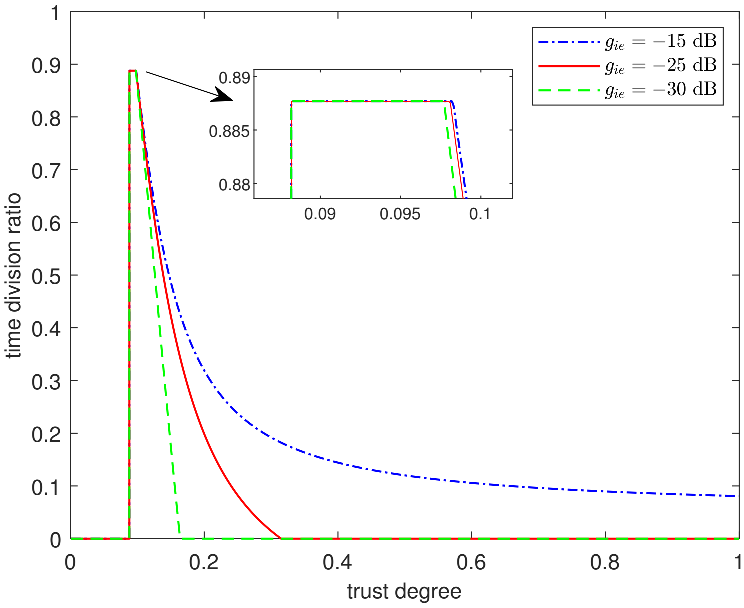

Figure 3. Time division ratio versus trust degree.

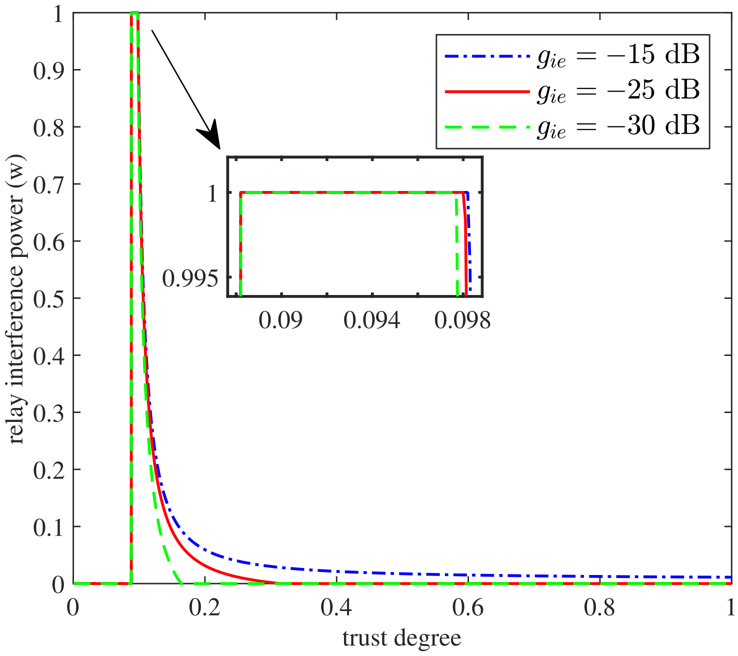

Figure 4. Relay interference power versus trust degree.

Figures 5 and 6 are operated on the conditions that the channel gain g_{ie} is equal to −35 dB and the transmit power P_s is equal to 0.1 W, 0.5 W and 0.9 W, respectively. The variation trends of the time division ratio and the relay interference power concerning trust degree in Figures 5 and 6 are almost the same as in Figures 3 and 4, respectively. By combining Equations (17) and (18), there are some conclusions drawn as follows. When the eavesdropping channel g_{ie} is small, the relay with a high trust degree still needs to send interference power to degrade the eavesdropping capacity. Therefore, with the decrease of the transmission power, the capacity gap between the legitimate channel and the eavesdropping one becomes smaller. The relay needs to enlarge the charging time and interference power to keep the capacity gap larger than the achievable security capacity $\overline{R}$.

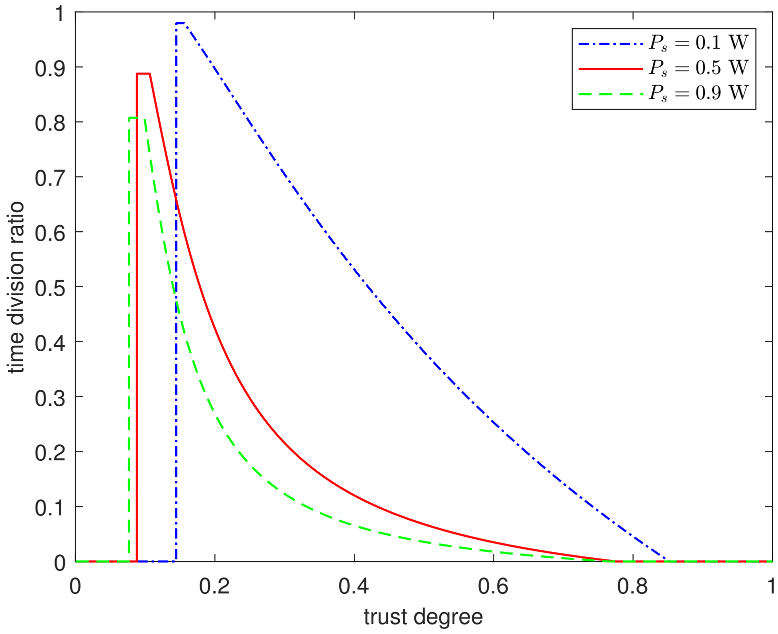

Figure 5. Time division ratio versus trust degree.

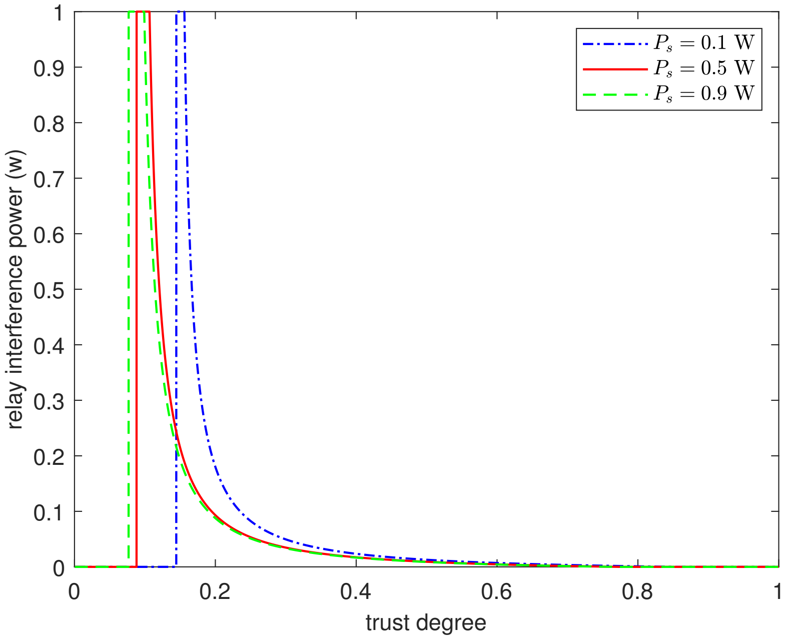

Figure 6. Relay interference power versus trust degree.

Given trust degrees and channel conditions, a relay selection strategy was proposed to maximize the expected achievable rate. So, a cooperative transmission strategy of relays with an optimal cooperative beamforming vector was derived to maximize the expected achievable rate [7]. Finally, a mixed strategy between the relay selection and cooperative transmission was obtained with respect to the trust degrees. In our scheme, the interference power is optimized by selecting the appropriate relay and time division ratio on the condition of both the secure transmission and trust degree, so our scheme possesses good transmission and power allocation performance by the trust-degree-based secure relay selection in SWIPT-enabled relay networks.

We also present the expected achievable rate for the trust-degree-based relay selection, cooperative transmissions, and the hybrid cooperation schemes. The proposed schemes are mainly compared with the conventional relay selection scheme, which chooses a relay only according to the channel conditions. Then, the conventional-channel-based one and the simulation result are shown in Figure 7. The expected secure achievable rate is increased with the growth of the transmit SNR. The performance of the trust-degree-based hybrid cooperative transmission outperforms that of the conventional-channel-based relay selection by about 2.62 dB at the expected secure achievable rate of 0.6. In addition, the hybrid cooperation scheme outperforms both the trust-degree-based relay selection and cooperative transmissions by about 1.22 dB and 1.03 dB at the expected secure achievable rate of 0.6, respectively. The phenomenon can be explained as follows. In the conventional relay selection, relay nodes are selected according to the channel conditions. However, in the trust-degree-based relay selection, by evaluating both trust degree and channel conditions, the proper relay node is preferentially selected; thus, the trust-degree-based relay selection increases the expected secure achievable rate over that of the conventional relay selection. In addition, the hybrid cooperation scheme outperforms the trust-degree-based relay selection and cooperative transmissions since the hybrid cooperation is the optimal combination of the two above schemes shown in Equation (28). Therefore, the proposed trust-degree-based scheme outperforms the traditional one, and it can be efficiently applied in wireless secure IoT communications.

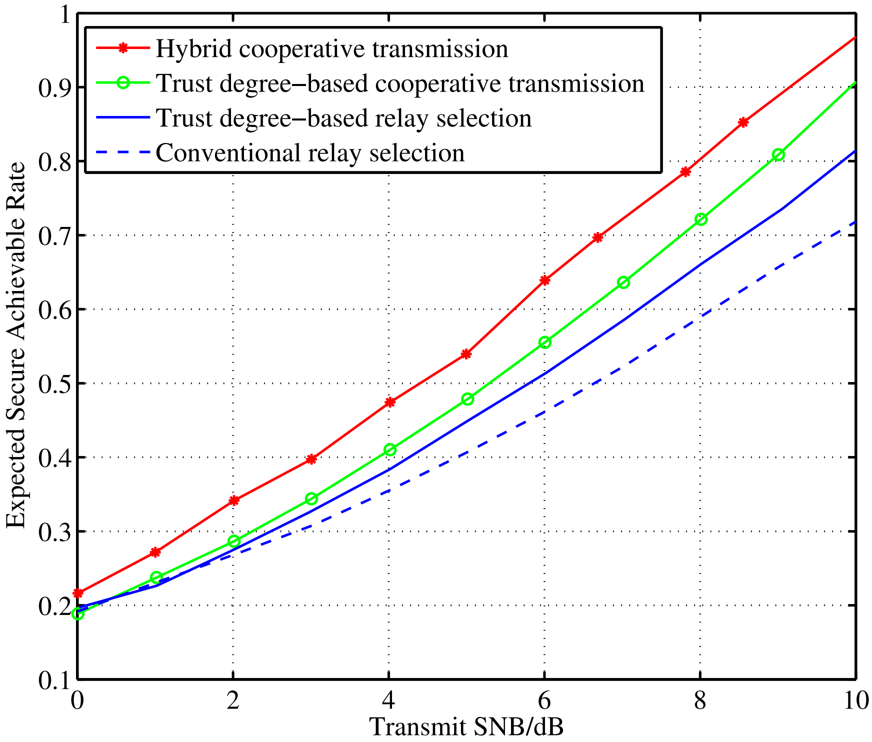

Figure 7. Expected achievable rate versus transmit SNR (α_1 = 0.6, α_2 = 0.3).

5. Conclusions

In this paper, we mainly optimize the interference power by selecting the appropriate relay and time division ratio on the condition of considering the secure transmission and trust degree in a SWIPT-enabled relay network. In the deriving process, the expressions of the time division ratio and relay interference power concerning trust degree are deduced, and the optimal time division ratio is derived. With known trust degrees of relays, we can choose the best relay to deliver the packets and try our best to guarantee the transmission security.

Author Contributions: Conceptualization: R.G., J.B.; methodology: R.G., L.X., D.X., and J.B.; software: L.X. and D.X.; formal analysis: J.B.; investigation: R.G., L.X., D.X., and J.B.; resources: R.G., L.X., D.X., and J.B.; data curation: L.X. and D.X.; writing—original draft preparation: R.G. and J.B.; writing—review and editing: J.B.; visualization: R.G. and J.B.; supervision: J.B.; project administration: J.B.; funding acquisition: J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Natural Science Foundation of China under Grant U1809201, Fundamental Research Funds for the Provincial Universities of Zhejiang under Grant GK209907299001-003, Zhejiang Provincial Natural Science Foundation of China under Grant No. LY19F010011, Scientific research projects of the Zhejiang Provincial Department of Education under Grant Y202044430, 2022 Zhejiang provincial Higher Education Research Project under Grant KT2022009 and Higher Education Reform Project of Hangzhou Dianzi University under Grant SYYB202212.

Acknowledgments: The authors would like to thank National Natural Science Foundation of China (NSFC), Zhejiang Provincial Natural Science Foundation of China (ZPNSFC), Zhejiang Provincial Education Department (ZPED) and Hangzhou Dianzi University for support this work.

Conflicts of Interest: The authors declare that there is no conflict of interests regarding the publication of this paper.

References

1. Gautam, S.; Vu, T.X.; Chatzinotas, S.; Ottersten, B. Cache-aided simultaneous wireless information and power transfer (SWIPT) with relay selection. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 187–201. [CrossRef]
2. Yan, Z.; Kong, H.; Wang, W.; Liu, H.-L.; Shen, X. Reliability benefit of location-based relay selection for cognitive relay networks. *IEEE Internet Things J.* **2022**, *9*, 2319–2329. [CrossRef]
3. Chen, J.; Liu, C.; Qian, M. A selection-based cooperative SWIPT scheme with energy-preserving DF relays. In Proceedings of the 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP), Hangzhou, China, 18–20 October 2018.
4. Gautam, S.; Lagunas, E.; Sharma, S.K.; Chatzinotas, S.; Ottersten, B. Relay selection strategies for SWIPT-enabled cooperative wireless systems. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'2017), Montreal, QC, Canada, 8–13 October 2017.
5. Wu, D.; Zhu, G.; Zhu, L.; Ai, B. Trust-based relay selection in relay-based networks. *KSII Trans. Internet Inf. Syst.* **2012**, *6*, 2587–2600.
6. Zhang, Y.; Zhao, X.; Xie, Y. Secure communications in SWIPT-enabled two-way relay networks. *IEEE Access* **2019**, *7*, 111890–111896. [CrossRef]
7. Ryu, J.Y.; Lee, J.H. Trust degree-based MISO cooperative communications with two relay nodes. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 7927358. [CrossRef]
8. Phan, V.-D.; Nguyen, T.N.; Le, A.V.; Voznak, M. A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting. *Sensors* **2021**, *21*, 5692. [CrossRef] [PubMed]
9. Zhang, J.; Tao, X.; Wu, H.; Zhang, X. Secure transmission in SWIPT-powered two-way untrusted relay networks. *IEEE Access* **2018**, *6*, 10508–10519. [CrossRef]
10. Gupta, A.; Singh, K.; Sellathurai, M. Time-switching EH-based joint relay selection and resource allocation algorithms for multi-user multi-carrier AF relay networks. *IEEE Trans. Green Commun. Netw.* **2019**, *3*, 505–522. [CrossRef]
11. Zhang, Z.; Lu, Y.; Huang, Y.; Zhang, P. Network-based relay selection in two-way SWIPT-enabled cognitive radio networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6264–6274. [CrossRef]
12. Ma, R.; Wu, H.; Ou, J.; Yang, S.; Gao, Y. Power splitting-based SWIPT systems with full-duplex jamming. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9822–9836. [CrossRef]
13. Jameel, F.; Chang, Z.; Jäntti, R. Secrecy limits of energy harvesting IoT networks under channel imperfections. In Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom'2020 Workshops), Austin, TX, USA, 23–27 March 2020.
14. Glendenning, B.; Kiefer, R.; Patel, A. Ziggurat: A framework for providing scalability and security in IoT blockchains. In Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI'2021), Las Vegas, NV, USA, 15–17 December 2021.

15. Rivera, A.V.; Refaey, A.; Hossain, E. A blockchain framework for secure task sharing in multi-access edge computing. *IEEE Netw.* **2019**, *3*, 176–183. [CrossRef]
16. Coon, J.P.A. Modelling trust in random wireless networks. In Proceedings of the 2014 11th International Symposium on Wireless Communications Systems (ISWCS'2014), Barcelona, Spain, 26–29 August 2014.
17. Hu, Z.; Xie, D.; Jin, M.; Zhou, L.; Li, J. Relay cooperative beamforming algorithm based on probabilistic constraint in SWIPT secrecy networks. *IEEE Access* **2020**, *8*, 173999–174008. [CrossRef]
18. Alageli, M.; Ikhlef, A.; Alsifiany, F.; Abdullah, M.A.M.; Chen, G.; Chambers, J. Optimal downlink transmission for cell-free SWIPT massive MIMO systems with active eavesdropping. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1983–1998. [CrossRef]
19. Cirik, A.C.; Rong, Y.; Hua, Y. Achievable rates of full-duplex MIMO radios in fast fading channels with imperfect channel estimation. *IEEE Trans. Signal Process.* **2014**, *62*, 3874–3886. [CrossRef]
20. Laneman, J.N.; Tse, D.N.C.; Wornell, G.W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Trans. Inf. Theory* **2004**, *50*, 3062–3080. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.