Article

Robust Security Beamforming for SWIPT-Assisted Relay System with Channel Uncertainty

Ruijie Guo 1, Chunling Fu 2,*, Yong Jin 1, Zhentao Hu 1 and Lin Zhou 1

1 School of Artificial Intelligence, Henan University, Zhengzhou 450046, China; guorj@vip.henu.edu.cn (R.G.); jy@henu.edu.cn (Y.J.); hzt@henu.edu.cn (Z.H.); zhoulin@henu.edu.cn (L.Z.)
2 School of Physics and Electronics, Henan University, Kaifeng 475004, China
* Correspondence: fuchunling@henu.edu.cn

Abstract: This paper considers the physical layer security (PLS) of a simultaneous wireless information and power transfer (SWIPT) relay communication system composed of a legitimate source–destination pair and some eavesdroppers. Supposing a disturbance of channel status information (CSI) between relay and eavesdroppers in a bounded ellipse, we intend to design a robust beamformer to maximum security rate in the worst case on the constraints of relay energy consumption. To handle this non-convex optimization problem, we introduce a slack variable to transform the original problem into two sub-problems firstly, then an algorithm employing a semidefinite relaxation (SDR) technique and S-procedure is proposed to tackle above two sub-problems. Although our study was conducted in the scene of a direct link among source, destination, and eavesdroppers that is non-existing, we demonstrate that our conclusions can be easily extended to the scene for which a direct link among source, destination and eavesdroppers exist. Numerical simulation results compared with the benchmark scheme are provided to prove the effectiveness and superior performance of our algorithm.

Keywords: physical layer security; energy harvest; robust optimization; SWIPT; worst case optimization

1. Introduction

The future Wireless Sensor Network (WSN) or Internet of Things (IoT) network is composed of billions of energy-limited devices. Since it is frequently deployed in harsh environments, those energy-limited devices are usually difficult to charge. How to give a stable energy supply to those energy-limited devices and thus prolong the life cycle of WSNs is a hot research topic today. Simultaneous wireless information and power transfer (SWIPT) have been proposed as a promising technology to provide power as well as to transmit information for wireless devices, thus it can effectively prolong the life of the energy-limited devices [1]. Moreover, since wireless charging techniques are employed, SWIPT may be flexibly used in electronic devices embedded in building structures or human bodies. Therefore, SWIPT technology in WSN has aroused extensive interest [2].

Due to the dynamic topology of mobile WSN and the open nature of wireless channels, information transmission in WSN may be easy to be intercepted and eavesdropped. At present, the security of wireless communication systems is commonly protected by a cryptographic encryption method which is based on multi-layer protocols. However, the complicated encryption system may induce huge computing challenges at base stations and users, while secure transmission of keys is still difficult to be guaranteed [3]. The physical layer security (PLS) technique is proposed to handle the above problem; since it is free from computational burden caused by encryption and decryption and works well even if the eavesdropper has strong computing power, the foreground of PLS in security of WSN is nice [4].

Traditionally, the cooperative relay technique widely used in WSN is employed to achieve spatial diversity gain as well as to expand WSN coverage [5]. PLS of cooperative
relay WSN is a noteworthy issue too. More specifically, to improve PLS is to improve the confidentiality rate of the signal received by users. PLS methods of cooperative relay WSN are divided roughly into two categories. The first is the cooperative jammer (CJ) method, in which the relay transmits artificial noise (AN) to interfere with eavesdroppers. In [6], the relay cluster is divided into two parts, one amplifies and forwards the signal, the other produces AN to interfere with eavesdroppers. In [7], the received signal of each relay is divided into two parts, one is used to forward the signal, and the other is used to harvest energy and then use harvested energy to generate AN to interfere to eavesdroppers. However, generating AN may consume additional energy of energy-limited services embedded in the relay as well as interfere with the legitimate receiver. The other way related to PLS in cooperative relay WSN is the secure beamforming. Security rate and computation complexity of some schemes including maximum secure rate and the zero-space beamforming at total power constraints and individual power constraints of the relay are discussed in [8]. Li proposed the secure relay beamforming algorithm based on concave convex optimization at the power constraints of relay transmitter and energy collector in a multi-antenna SWIPT relay network [9]. The joint optimization of beamformer and energy division ratio in a multi-antenna relay network is also proposed [10]. In an energy-limited full-duplex (FD) relay network, time allocation ratio, energy, and information beamformer are jointly optimized to achieve the maximum secrecy rate [11]. Assuming the channel status information (CSI) of eavesdropper and CSI of legitimate are uncorrelated, Yang proposed a zero-space beamforming algorithm to force the confidential signal into zero space of the eavesdropper to enhance information security [12].

Although much work has been done on secure beamforming, the above research is merely carried out by supposing the CSI of the legitimate receiver and eavesdropper fully known, which is not realistic in the actual scenario. Since eavesdroppers may keep silent to hide themselves, the relay may have difficulty obtaining the accurate CSI between relay and eavesdropper, leading performance of the above algorithms to deterioration. Therefore, how to design a robust beamforming algorithm with tolerance for CSI disturbance to improve the security of SWIPT-assisted communication system is challenging work. Supposing CSI error follows Gaussian distribution, the optimal security rate is achieved by the joint optimization of relay beamformer and power allocation factors [13]. Assuming the CSI error between the base station and the user in a bounded ellipsoid region, a robust beamforming scheme based on S-procedure is proposed to achieve the minimum base station transmission power [14]. The robust sum rate optimization in non-orthogonal multiple access (NOMA) amplifying and forwarding (AF) relay networks is considered in [15], and the power allocation scheme and beamforming matrix are jointly optimized to achieve the maximum rate at the quality of service (QoS) constraints and relay transmission power constraints. In addition, a joint information beamforming and energy beamforming scheme based on semidefinite relaxation (SDR) and successive convex approximation (SCA) techniques is proposed to achieve the maximum secrecy rate of the multiple input single output (MISO) network [16], in which the CSI error is also restrained in a bounded elliptic region.

It is worth noting that the difference between our work and the above works are the following. Different from [13], we discussed the bounded ellipsoid model of the channel error instead of the Gaussian distribution model, which is widely used in the literature [14–18]. Although the bounded ellipsoid channel error model is discussed in [14–18], the point to point algorithm proposed in [14,16,17] can not be directly generalized to our SWIPT relay network. The security problem of two-tier downlink heterogeneous network is studied in [18], since channel error between the base station and the eavesdropper is not involved in [18], and their system models are too different from ours, and its conclusions could not be directly extended to SWIPT WSN. The research in [15] only focuses on how to obtain the best quality of service for users, while ignoring the problem of user information leakage. Our research can effectively prevent information leakage while maximizing user transmission rate.

The main contributions of our work are summarized as follows:
- We propose the robust optimization method to maximize the security rate of the destination under the constraints such as transmission power of relay, signal to interference plus noise power ratio (SINR) of receiver, and CSI error between relay and eavesdroppers. Our method solves the problem that the performance of existing methods deteriorates sharply when the relay fails to obtain perfect CSI. Since perfect CSI is difficult to obtain in practical scenarios, our method has better performance.

- To circumvent the non-convexity of the original optimization problem, the original problem is decoupled into two subproblems by introducing a slack variable, and thus can be iteratively solved by an SDR technique and bisection method, respectively.

- For simplicity, the scene without a direct connection between the source, the legitimate destination and the eavesdropper are mainly involved in the proposed algorithm; however, we have proved that the proposed algorithm can be generalized to SWIPT WSN with a direct connection between the source, the legitimate destination and the existing eavesdropper.

- Extensive numerical results are presented to demonstrate the system parameters impacting the performance of the proposed scheme and the superior performance of the proposed scheme against three other benchmark schemes.

The rest of this paper is organized as follows: the system model and the problem formulation are presented in Section 2. Then, we design an effective iterative algorithm to achieve the maximum secrecy rate in the worst case in Section 3. Section 4 presents numerical results to validate the proposed scheme. Finally, Section 5 concludes the paper and extends the future research work.

Notations: Bold lowercase letters and capital letters represent column vectors and matrices, respectively. The transpose, conjugate transpose, trace, and rank of a matrix $S$ are denoted by $S^T$, $S^H$, $\text{Tr}(S)$, and $\text{rank}(S)$, respectively. $[S]_{i,j}$ signals the $(i,j)$ term of the matrix $S$. The modulus of a complex scalar $s$ and euclidean norm of a vector $s$ are denoted by $|s|$ and $\|s\|_2$, respectively. $I_N$ denotes the N-dimensional identity matrix. $\text{diag}(s)$ is the diagonal matrix whose diagonal elements are the vector $s$. $E[\cdot]$ representing mathematical expectation. $[x]^+$ is the abbreviation of $\max\{x,0\}$.

2. System Model and Problem Formulation

Consider the SWIPT-assisted relay communications system shown in Figure 1, which consists of a source (S), a legitimate destination (D), K eavesdroppers (Eve), and N energy limited relays (R). Each piece of the equipment is equipped with a single antenna. Furthermore, we assume that there is no direct link among S, D, and Eve (The algorithm proposed by this paper is also applicable to the case of direct link. Refer to Remark 1 at the end of Section 3 [19]), which usually occurs at the long-distance path loss or heavy channel fading [20–25]. For example, in a long range missile detection system, the satellite can act as a relay to forward information to the control center without a direct link between monitoring nodes. Here, we consider the fact that relay uses the power splitting (PS) scheme to harvest energy from the Radio Frequency (RF) signal transmitted by S to forward the confidential information to D in the meantime (There are two well-known practical receiver schemes (i.e., time switching (TS) and power splitting PS). PS scheme can process information and harvest energy at the same time to avoid interruption of information transmission, so we adopt PS scheme).

Following by SWIPT-AF relay protocol, relay employs cascading two stages to process the signal received by $i$-th relay [7]. In the first stage, namely the receiving stage, the signal received by $i$-th relay can be expressed as

$$y_{r_i} = h_{sr_i}x_s + n_{a_i}, \forall i,$$

where $x$ represents the transmit signal at S with power $E(|x_s|^2) = P_s$. $P_s$ represents the transmitted power of S. $h_{sr_i}$ represents the channel complex coefficient from S to $i$-th R,
and \( n_{a,i} \sim \mathcal{CN}(0, \sigma_{a,i}^2) \) is the additive white Gaussian noise with 0 mean and \( \sigma_{a,i}^2 \) variance received by the \( k \)-TH relay.

![Figure 1](image-url)  
Figure 1. The SWIPT-assisted relay communication network model.

Each AF relay adopts a PS receiver shown in Figure 2 to process signals. Specifically, the relay divides the received signal into two parts. One part \((\sqrt{1-\alpha_i}y_{ri})\) is used for information decoding (ID); the other part \((\sqrt{\alpha_i}y_{ri})\) is used for energy harvest, where \( \alpha_i \) is the power splitting ratio. In general, the energy harvested from the received RF power may be modeled by a nonlinear equation. However, since there is currently no widely accepted nonlinear model related to energy harvest, we employ the linear energy collection model here [26]. Thus, the energy harvested by the relay is modeled as

\[
E_R = \eta \alpha_i P_s \| h_{sr} \|_2^2, \quad (2)
\]

where \( \eta (0 < \eta < 1) \) represents the EH efficiency and \( h_{sr} = \left[ h_{sr,i} \right]_{i=1}^N \).

![Figure 2](image-url)  
Figure 2. Power splitting receiver architecture.

In the second stage, called the amplification and forwarding stage, linear amplification of the signal received by the \( i \)-th relay can be described as

\[
x_{ri} = \beta_i \left( \sqrt{1-\alpha_i}y_{ri} + n_{c,i} \right), \quad \forall i, \quad (3)
\]

where \( n_{c,i} \sim \mathcal{CN}(0, \sigma_{c}^2) \) is baseband conversion noise of the RF signal. \( \beta_i \) is a complex coefficient given by

\[
\beta_i = \sqrt{\frac{\eta \alpha_i |h_{sr,i}|^2 P_s}{(1-\alpha_i)|h_{sr,i}|^2 P_s + (1-\alpha_i)\sigma_a^2 + \sigma_c^2 e^{j\theta_i}}}. \quad (4)
\]
Due to limited energy in the relay, the energy of the relay output signal must be less than the energy harvested by the relay, viz., the following constraints must be satisfied:

$$|x_r|^2 \leq E_R.$$  \hspace{1cm} (5)

To sum up, transmitting signals of relays can be described as

$$x_r = Q_{ba} h_{sr} \sqrt{P_s} x_s + Q_{ba} n_a + Q_{ba} n_c,$$  \hspace{1cm} (6)

where $Q_{ba}$ and $Q_{b}$ are the diagonal matrix with diagonal elements are $(\beta_1 \sqrt{1-a_1}, \ldots, \beta_N \sqrt{1-a_N})^T$ and $(\beta_1, \ldots, \beta_N)^T$, respectively. $n_a \sim \mathcal{CN}(0, \sigma_a^2)$ is the additive white Gaussian noise received by R, where $\sigma_a^2$ represents the variance of $n_a$. $n_c \sim \mathcal{CN}(0, \sigma_c^2)$ is the baseband conversion noise of the RF signal, where $\sigma_c^2$ represents the variance of $n_c$. Thus, signals received by the legitimate destination can be described as

$$y_d = h_{rd}^H x_r + n_d.$$  \hspace{1cm} (7)

where $n_d \sim \mathcal{CN}(0, \sigma_d^2)$ is the additive white Gaussian noise received by D, where $\sigma_d^2$ represents the variance of $n_d$. $h_{rd} = |h_{rd}|^N_{k=1}$ represents the channel complex coefficient from relay to legitimate destination. Substituting (6) into (7), we can obtain

$$y_d = h_{rd}^H Q_{ba} h_{sr} \sqrt{P_s} x_s + h_{rd}^H Q_{ba} n_a + h_{rd}^H Q_{ba} n_c + n_d.$$  \hspace{1cm} (8)

Meanwhile, the signal received by each eavesdropper is expressed as

$$y_{e,k} = \bar{h}_{re,k}^H x_r + n_{e,k},$$  \hspace{1cm} (9)

where $\bar{h}_{re,k}$ represents the nominal channel complex coefficient from relay to $k$-th eavesdroppers, $n_{e,k} \sim \mathcal{CN}(0, \sigma_{e,k}^2)$ is the additive white Gaussian noise. Substituting (6) into (9), the signal received by the $k$-th eavesdropper can be described as

$$y_{e,k} = \bar{h}_{re,k}^H Q_{ba} h_{sr} \sqrt{P_s} x_s + \bar{h}_{re,k}^H Q_{ba} n_a + \bar{h}_{re,k}^H Q_{ba} n_c + n_{e,k}.$$  \hspace{1cm} (10)

In summary, the SINR of D and Eve can be respectively described as

$$\text{SINRS}_{\text{D}} = \frac{P_s |h_{rd}^H Q_{ba} h_{sr}|^2}{\sigma_d^2 \|h_{rd}^H Q_{ba}\|^2 + \sigma_a^2 \|h_{rd}^H Q_{b}\|^2 + \sigma_c^2},$$  \hspace{1cm} (11)

$$\text{SINRS}_{\text{E},k} = \frac{P_s |\bar{h}_{re,k}^H Q_{ba}|^2}{\sigma_{e,k}^2 \|\bar{h}_{re,k}^H Q_{ba}\|^2 + \sigma_a^2 \|\bar{h}_{re,k}^H Q_{b}\|^2 + \sigma_c^2}.$$  \hspace{1cm} (12)

Supposing CSI disturbance between R and Eve following the elliptical sphere uncertainty model, i.e.,

$$h_{re,k} = \bar{h}_{re,k} + \Delta h_{re,k},$$  \hspace{1cm} (13)

where $h_{re,k}$ represents the actual channel coefficient vector between R and the $k$-th Eve, and $\Delta h_{re,k}$ represents the bounded estimate error described by $\Delta = \{\Delta h_{re,k} \mid \|\Delta h_{re,k}\|^2 \leq \delta^2, \forall k, \delta \geq 0\}$, where $\delta$ is the upper bound on the error. It can be considered that the relay has perfect CSI when $h_{re,k} = \bar{h}_{re,k}$. After introducing the channel error model, the SINR of the received signal of the $k$-th eavesdropper can be re-expressed as

$$\text{SINRS}_{\text{E},k} = \frac{P_s |(\bar{h}_{re,k} + \Delta h_{re,k})^H Q_{ba} h_{sr}|^2}{\sigma_{e,k}^2 \| (\bar{h}_{re,k} + \Delta h_{re,k})^H Q_{ba}\|^2 + \sigma_a^2 \| (\bar{h}_{re,k} + \Delta h_{re,k})^H Q_{b}\|^2 + \sigma_c^2}.$$  \hspace{1cm} (14)
where \( r_{SD} = 1/2 \log (1 + \text{SINR}_{SD}) \) represents the mutual information between S and D. \( r_{SE,k} = 1/2 \log (1 + \text{SINR}_{SE,k}) \) represents the mutual information between the \( k \)-th Eve and S. The coefficient 1/2 is due to the relay working in a half-duplex model.

For convenience, we may convert \( r_{SD} \) and \( r_{SE,k} \) into the following forms:

\[
\begin{align*}
    r_{SD} &= \frac{1}{2} \log_2 \left( 1 + \frac{|h_{SD}^H w|^2}{|g_{SD}^H w|^2 + \sigma_n^2} \right), \\
    r_{SE,k} &= \frac{1}{2} \log_2 \left( 1 + \frac{|h_{SE,k}^H w|^2}{|g_{SE,k}^H w|^2 + \sigma_n^2} \right),
\end{align*}
\]

where \( w = [w_1, w_2, ..., w_N]^T \) is defined as a beamforming vector, and the other parameters are defined as follows:

\[
\begin{align*}
    [h_{sd}]_i &\triangleq h_{sr} h_{rd}^i \left( \frac{\eta a_i (1 - a_i) P_s}{(1 - a_i) \left( |h_{sr}|^2 P_s + \sigma_n^2 \right) + \sigma_n^2} \right), \forall i; \\
    [g_{sd}]_i &\triangleq h_{sr} h_{rd}^i \left( \frac{\eta a_i P_s (1 - a_i) \sigma_n^2 + \sigma_n^2}{(1 - a_i) \left( |h_{sr}|^2 P_s + \sigma_n^2 \right) + \sigma_n^2} \right), \forall i; \\
    [h_{sr}]_i &\triangleq h_{sr} h_{re,k}^i \left( \frac{\eta a_i (1 - a_i) P_s}{(1 - a_i) \left( |h_{sr}|^2 P_s + \sigma_n^2 \right) + \sigma_n^2} \right), \forall i, \forall k; \\
    [g_{sr}]_i &\triangleq h_{sr} h_{re,k}^i \left( \frac{\eta a_i P_s (1 - a_i) \sigma_n^2 + \sigma_n^2}{(1 - a_i) \left( |h_{sr}|^2 P_s + \sigma_n^2 \right) + \sigma_n^2} \right), \forall i, \forall k.
\end{align*}
\]

Considering that the error of CSI can be described by an elliptic bounded model, we intend to design a beamforming vector which may achieve the maximum secrecy rate in all possible eavesdropper CSI errors; thus, the optimization problem mentioned above can be described as

\[
\begin{align*}
    \max_{w} \quad & \min_{\Delta h_{re,k} \in \Delta} \frac{1}{2} \left[ r_{SD} - r_{SE,k} \right]^+ \\
    \text{s.t.} \quad & \text{Tr} \left( \left( \eta a_i P_s |h_{sr}|^2 w w^H \right) E_i \right) \leq \eta a_i P_s |h_{sr}|^2, \forall i \\
    & \Delta = \{\Delta h_{re,k} \| \Delta h_{re,k} \|^2 \leq \delta^2, \forall k\},
\end{align*}
\]

where \( E_i = \text{diag}(e_i) \), \( e_i \) is the vector whose \( i \)-th entry is 1, and the other entries are 0. Considering that the channel error only exists between the eavesdropper and the relay, (21) can be translated into

\[
\begin{align*}
    \max_{w,\Delta h_{re,k} \in \Delta} \quad & \frac{1}{2} \left( r_{SD} - \text{max} r_{SE,k} \right) \\
    \text{s.t.} \quad & \text{Tr} \left( \left( \eta a_i P_s |h_{sr}|^2 w w^H \right) E_i \right) \leq \eta a_i P_s |h_{sr}|^2, \forall i \\
    & \Delta = \{\Delta h_{re,k} \| \Delta h_{re,k} \|^2 \leq \delta^2, \forall k\}.
\end{align*}
\]

Observing (22), we can find that two optimized variables are coupled in objective functions; thus, the original problem is non-convex and hard to handle. We will explore the solution method of this problem in the next section.
3. Robust Beamforming Optimization for Physical Layer Security

In this section, we aim to settle the problem of maximizing the secrecy rate under the bounded CSI error model proposed in Section 2. To settle the above non-convex problem, we introduce a slack variable $\tau$ to convert the original problem into $P_1$:

$$
\begin{align*}
\text{(P1)} & \quad \min_{\tau, w} \frac{1}{2} r_{S,D} - \frac{1}{2} \log \left( \frac{1}{\tau} \right) \\
& \quad \text{s.t. } \max_{\Delta h_{re}, k \in \Delta r_{S,E}, k} r_{S,E,k} \leq \log \left( \frac{1}{\tau} \right), \forall k \\
& \quad \text{Tr} \left( \left( \eta \alpha_i P_s |h_{sr_i}|^2 w w^H \right) E_i \right) \leq \eta \alpha_i P_s |h_{sr_i}|^2, \forall i,
\end{align*}
$$

(23)

Observing $(P1)$, it can be seen that, although the introduced variable $\tau$ solves the maximum and minimum forms of the source problem (22), due to the coupling of $\tau$ and $w$ in the objective function (23) and the form of constraint (24), the problem (23) is still non-convex and unsolvable. To settle this problem, we propose an algorithm to transform it into a two-level optimization problem. Specifically, the lower-level optimization problem can be expressed as the following form $(P2)$:

$$
\begin{align*}
\text{(P2)} & \quad \min_{w} \frac{|h_{sd}^H w|^2}{|g_{sd}^H w|^2 + \sigma_d^2} \\
& \quad \text{s.t. } \max_{\Delta h_{re}, k \in \Delta r_{S,E}, k} r_{S,E,k} \leq \log \left( \frac{1}{\tau} \right), \forall k \\
& \quad \text{Tr} \left( \left( \eta \alpha_i P_s |h_{sr_i}|^2 w w^H \right) E_i \right) \leq \eta \alpha_i P_s |h_{sr_i}|^2, \forall i.
\end{align*}
$$

(26)

which can be regarded as a quadratic programming problem for the variable $w$ when the variable $\tau$ is fixed.

The upper-level optimization problem is determined by the solution of the lower-level optimization problem. Let $R(\tau) = \tau \gamma(\tau)$, where $\gamma(\tau)$ represents the objective function of the optimization problem $(P2)$. The objective function of the optimization problem $(23)$ could be modeled as

$$
\frac{1}{2} \log(1 + \gamma(\tau)) - \frac{1}{2} \log \left( \frac{1}{\tau} \right) = \frac{1}{2} \log(\tau + R(\tau)).
$$

(29)

Consequently, we can describe the upper-level optimization problem $(P3)$ as

$$
\begin{align*}
\text{(P3)} & \quad \max_{\tau} \frac{1}{2} \log(\tau + R(\tau)) \\
& \quad \text{s.t. } \tau_{\min} \leq \tau \leq 1,
\end{align*}
$$

(30)

The meaning of $1/\tau$ in problem $(23)$ is the maximum allowable SINR of channels between relay and eavesdroppers which satisfies the non-zero security rate. $\tau_{\min}$ represents the smallest feasible value of $\tau$ given by the following inequality:

$$
\tau \geq \frac{1}{1 + P_s |h_{sr}|^2 \|w\|^2 / \sigma_d^2} \\
\geq \frac{1}{1 + NP_s |h_{sr}|^2 / \sigma_d^2} = \tau_{\min}.
$$

(31)
where the first inequality is obtained according to Cauchy–Schwarz inequality, and the second inequality is obtained by $|w_i|^2 \leq 1, \forall i$.

Suppose that we can obtain the corresponding $R(\tau)$ for any $\tau$ in the definition domain, and then the optimal solution $\tau^*$ of the (30) can be efficiently solved within the region $[\tau_{\text{min}}, 1]$ through bisection method, etc. Heretofore, we have solved the upper-level problem (30), but, due to the non-convexity of constraint (27), the lower-level problem (26) is still difficult to settle. It is obvious that constraint (27) can be rewritten in the following form:

$$\forall \Delta h_{r,c,k} \in \Delta \Rightarrow \frac{|h_{r,c,k}^H w|^2}{|g_{s,c,k}^H w|^2 + \sigma_{r,c,k}^2} \leq \frac{1}{\tau} - 1, \quad (32)$$

Considering the ellipsoidal uncertainty model, using S-procedure [27], inequation (32) can be expressed in the form of a series of linear matrix inequalities (LMI), which are summarized as the following proposition:

**Proposition 1.** The constraints (32) hold if and only if there exist $\mu_k \geq 0, k = 1, \ldots K$ such that the following LMIs hold:

$$\begin{bmatrix} \mu_k I_N + W & \tilde{W} h_{r,c,k}^H \\ h_{r,c,k} W & \psi_k \end{bmatrix} \succeq 0, \forall k, \quad (33)$$

**Proof.** See Appendix A. \qed

Using Proposition 1, the constraint (27) can be converted to an LMI form, and then problem (26) can be expressed as

$$\begin{align*}
\max_{\mu_k, \psi_k} & \quad \frac{\text{Tr}(\tilde{W} h_{r,c,k}^H)}{\text{Tr}(\tilde{g}_{s,c,k}^H \tilde{g}_{s,c,k} + \sigma_\alpha^2)} \\
\text{s.t.} & \quad W \succeq 0, \mu_k \geq 0, \psi_k \geq 0 \\
& \quad \begin{bmatrix} \mu_k I_N + W & \tilde{W} h_{r,c,k}^H \\ h_{r,c,k} W & \psi_k \end{bmatrix} \succeq 0, \forall k \\
& \quad \text{Tr} \left( \left( \eta_\alpha P_s |h_{sr}|^2 W \right) E_i \right) \leq \eta_\alpha P_s |h_{sr}|^2, \forall i, \quad (34)
\end{align*}$$

where $h_{r,c} \triangleq \text{diag}(1 - \alpha_i) h_{r,c}$, $\tilde{g}_{s,c} \triangleq \text{diag}(1 - \alpha_i) \sigma_\alpha^2 + \sigma_\alpha^2) h_{r,c}$.

At this point, the problem is easy to solve while still not a standard convex optimization problem. In order to settle the fractional form of the above problem, we define $\tilde{W} = \zeta W$, $\zeta = (\text{Tr}(\tilde{g}_{s,c}^H \tilde{g}_{s,c}) + \sigma_\alpha^2)^{-1}$ according to the Charnes–Cooper transformation. By combining the above definitions, we could convert the above problem into a standard convex optimization problem:

$$\begin{align*}
\text{P4} \quad \max_{\tilde{W}, \mu_k, \psi_k} & \quad \text{Tr}(\tilde{h}_{r,c}^H \tilde{W} \tilde{h}_{r,c}) \\
\text{s.t.} & \quad \tilde{W} \succeq 0, \mu_k \geq 0, \psi_k \geq 0 \\
& \quad \text{Tr}(\tilde{g}_{s,c}^H \tilde{W} \tilde{g}_{s,c}) + \sigma_\alpha^2 \tau = \tau \\
& \quad \begin{bmatrix} \mu_k I_N + W & \tilde{W} h_{r,c,k}^H \\ h_{r,c,k} W & \psi_k \end{bmatrix} \succeq 0, \forall k \\
& \quad \text{Tr} \left( \left( \eta_\alpha P_s |h_{sr}|^2 \tilde{W} \right) E_i \right) \leq \mu_k \eta_\alpha P_s |h_{sr}|^2, \forall i. \\
\end{align*} \quad (35)$$

Thus far, we convert the original non-convex problem (22) into two convex problems (P3) and (P4). (P3) can be solved by using the bisection method, and (P4) can be solved by using the interior point method or a convex optimization toolbox such as CVX [27]. If the solution $\hat{W}^*$ of the problem (P4) satisfies $\text{Rank}(\hat{W}^*) = 1$, $w$ could be obtained by EVD, otherwise by Gaussian randomization. In addition, the specific algorithm is summarized in Algorithm 1.
### Algorithm 1 Proposed algorithm for solving P1

1. Initialize relevant basic parameters;
2. Set $s = \tau_{\text{min}}, v = \tau_{\text{max}} = 1$, accuracy $\epsilon > 0$;
3. Repeat
   3.1. $\tau_{\text{cur}} = (s + v)/2$;
   4. Solve (35), get $R(\tau_{\text{cur}})$ and $W$;
   5. Solve (30), get $r_{\text{cur}} = (1/2)\log_2(\tau_{\text{cur}} + R(\tau_{\text{cur}}))$;
   6. Set $\tau_{\text{tem}} = \max(\tau_{\text{cur}} - \Delta \tau, \tau_{\text{min}})$, where $\Delta \tau > 0$ denotes a minimum,
     return $r_{\text{tem}} = (1/2)\log_2(\tau_{\text{tem}} + R(\tau_{\text{tem}}))$;
   7. If $r_{\text{cur}} > r_{\text{tem}}$, $s = \tau_{\text{tem}}$,
     else $v = \tau_{\text{cur}}$;
8. until $|r_{\text{cur}} - r_{\text{tem}}| < \epsilon$
9. $W^* = W$, get $w^*$ by EVD or Gaussian randomization to $W^*$, $r^* = r_{\text{cur}}$.

### Remark 1.

Although the problem described in (22) is modeled without a direct link between $S$, $D$, and Eve, it is can be easily extended to the case direct link between $S$, $D$, and Eve existing. Let a direct link channel coefficient between $S$ and $D$ be defined as $h_{sd-\text{DL}}$ and the direct link channel coefficient vector between $S$ and the $k$-th Eve be defined as $h_{s_{\text{DL}},k}$, respectively. The signals received by $D$ and Eve through the direct link could be respectively defined as

$$
\begin{align*}
y_{S,D-\text{DL}} &= h_{sd-\text{DL}}x + n_{sd-\text{DL}}, \\
y_{S,E,k-\text{DL}} &= h_{s_{\text{DL}},k}x + n_{s_{\text{DL}},k},
\end{align*}
$$

where $n_{sd-\text{DL}} \sim \mathcal{CN}(0,1)$ represents the noise signal received by $D$, $n_{s_{\text{DL}},k} \sim \mathcal{CN}(0,1)$ represents the noise signal received by $Eve$.

By stacking the direct link signals and relay forward signals received by the $D$ and $Eve$ into a $2 \times 1$ vector, respectively, the reception rate of $D$ and $Eve$ can be defined as

$$
\begin{align*}
r_{S,D-\text{DL}} &= \log(1 + P_x ||h_{sd-\text{DL}}||^2 + ||h_{s_{\text{DL}},k}w||^2)/(||s^H_{\text{DL}}w||^2 + \sigma^2) ), \\
r_{S,E,k-\text{DL}} &= \log(1 + P_x ||h_{s_{\text{DL}},k}||^2 + ||h_{s_{\text{DL}},k}w||^2)/(||s^H_{\text{DL}}w||^2 + \sigma^2) ).
\end{align*}
$$

It can be seen that the only difference between (38) and (16) is the additive constant. Similar to a model without a direct link between the $S$, $D$, and $Eve$, supposing a direct link between existing $D$ and $S$, imperfect CSI between relay and eavesdropper can also be modeled as a bounded ellipsoid, i.e., $||h_{s_{\text{DL}},k-\text{DL}} - h_{s_{\text{DL}},k-\text{DL}}||_2 \leq \xi_k$, where $\xi_k$ represents the upper bound of channel error of the $k$-th eavesdropper. Then, the worst-case transmission rate of system is described as

$$
\begin{align*}
\max_{h_{s_{\text{DL}},k-\text{DL}}}
\|h_{s_{\text{DL}},k-\text{DL}} - h_{s_{\text{DL}},k-\text{DL}}\|_2 \leq \xi_k
= \log(1 + P_x (||h_{s_{\text{DL}},k-\text{DL}}|| + \xi_k^2) + ||h_{s_{\text{DL}},k}w||^2)/(||s^H_{\text{DL}}w||^2 + \sigma^2) ),
\end{align*}
$$

which again differs from the no-direct link term in (16) only in some constant term [21]. Hence, our model of direct link non-existing can be straightforwardly extended to the case of direct link existing. However, it is worth noting that, if the direct links between $S$ and $Eve$ are strong, a positive secrecy rate may be achieved with difficulty.

### 4. Complexity Analysis and Numerical Results

In this section, we first derive the complexity of the proposed algorithm. By analyzing Algorithm 1, it can be found that the complexity of the proposed algorithm is concentrated from solved (P2) in each iteration. Due to the LMI form introduced by S-procedure and
SDR, the complexity of the problem in (P2) is mainly derived from solving the following quantitative LMI including $K$ linear matrix inequalities of $N + 1$ dimensions, $N$ linear matrix inequalities of 1 dimension, and $K$ linear matrix inequalities of one dimension. Similar to [28], the complexity of the proposed robust secure beamforming algorithm can be roughly expressed as $\sqrt{K(N+1)K^2N^4 \ln(1/\epsilon)}$.

Next, we present extensive numerical simulation results to prove the performance of the proposed algorithm. Our comparison algorithm comes from similar works presented in [7,12,13]. As shown in Figure 1, we assume that the S is located at the edge of a circular region and the legitimate destination is located at a symmetrical position of the source on the circle. AF relay and eavesdroppers (only existing in the “security zone”) are randomly distributed within a circle of radius $R$. Similar to some related work, we assume that all channel models used in the paper contain large-scale path loss and small-scale multipath fading, the small-scale fading is assumed to be Rician fading, and the path loss model can be described as

$$L = A_0 \left( \frac{d}{d_0} \right)^{-\kappa}.$$

Parameters related to experiments are shown in Table 1.

| Parameters                   | Notation | Typical Value |
|------------------------------|----------|---------------|
| Standard Distance            | $d_0$    | 1 m           |
| Path loss exponent           | $\kappa$ | 2.5           |
| Channel mismatch bound       | $\delta$ | 0.1           |
| Power splitting ratio        | $\alpha$ | 0.5           |
| Fade coefficient             | $A_0$    | $10^{-3}$     |
| Energy collection efficiency | $\eta$   | 50%           |
| Circular area of radius $R$  | $R$      | 50 m          |
| Power of source              | $P_s$    | 30 dBm        |
| Noise variance of relay      | $\sigma^2_d$ | $-80$ dBm |
| Noise variance of baseband   | $\sigma^2_a$ | $-50$ dBm |
| Noise variance of receiver   | $\sigma^2_r$ | $-130$ dBm |
| Noise variance of eavesdropper| $\sigma^2_e$ | $-130$ dBm |

Convergences of the algorithms are plotted in Figure 3. It can be seen that the convergence of the three algorithms is similar, and all converge to the maximum within seven iterations, but the proposed algorithm achieves a higher secrecy rate. The reason is that the cooperative jamming beamforming (CJ-SPS) algorithm [7] only considers the performance in the case of perfect CSI. Although AN is introduced to interfere with eavesdroppers, the security of the system is still deteriorating in the presence of CSI errors. Since designs for CSI error follow Gaussian distribution, the probabilistic constraint beamforming (PC-SPS) algorithm [13] has a certain robustness, and its performance is slightly better than the CJ-SPS algorithm, while the proposed algorithm can achieve a higher security rate at the ellipsoidal bounded CSI error.

In the proposed algorithm, the levels of CSI error impacting the security of the system are plotted in Figure 4a. As can be seen from the figure, the secrecy rate increases with the source transmission power increasing. It is mainly because of harvest energy of relay increasing with source transmission power, resulting in more transmission power of relay. Moreover, the security of system will decrease with CSI error increasing. In addition, Figure 4b shows that the secrecy rate varies with the channel error at the different transmission power of the source, and the conclusion is similar to Figure 4a. With the CSI error increasing, the achieved secrecy rate decreases gradually, and this is because the CSI has greater uncertainty within a larger error bound, leading the worst-case achieved secrecy rate to increases.
The performance of the proposed algorithm is compared with the three benchmark algorithms mentioned in the introduction in Figure 5. Clearly, relay may achieve higher secrecy rate with the transmitting power $P_s$ increasing. In addition, compared with the other benchmark algorithms, the performance of the proposed algorithm is improved as expected. It is worth noting that the PC-SPS algorithm models CSI error as Gaussian distribution, which is inconsistent with actual CSI error, thus leading to the worst performance.

Next, Figure 6a compares the system performance of our scheme at different energy collection efficiency $\eta$. As expected, the security rate increases with the energy collection efficiency $\eta$ at any transmission power. The reason for the above phenomenon is that the relay can obtain more energy with the $\eta$ increasing, thus having more transmission power. However, since SINR obtained by the eavesdropper may also enhance following $\eta$ increasing, the increasing trend of security rate may slow down at the large $\eta$. The security rate of four algorithms at the different $\eta$ are plotted in Figure 6b. Similar to Figure 6a, the secrecy rate of all algorithms increases with $\eta$. Moreover, our proposed algorithm achieves the highest secrecy rate since bounded CSI errors impacting the performance of the system are fully considered.
The number of relays impacting the security rate of system is described in Figure 7. It can be seen that security rate of all algorithms tends to increase with number of relays. This is of course because the ability of system may be enhanced with the number of relays increasing. Moreover, since the bounded CSI error impacting the performance of the system is fully considered, the proposed algorithm achieves the highest security rate among all the algorithms.

Finally, the worst-case secrecy rates at the different power allocation factors are also described in Figure 8a. Similar to Figure 6, with the power allocation factor $\alpha$ increasing, the relay can obtain more energy, which leads to a higher secrecy rate. However, the secrecy rate drops sharply once $\alpha$ is greater than 0.9, since there is little signal to be forwarded. The security rate of four schemes at the different power allocation factor $\alpha$ are also compared in Figure 8b. Similar to Figure 8a, the secrecy rate of all algorithms increases with $\alpha$. Moreover, our proposed algorithm achieves the highest secrecy rate since bounded CSI errors impacting the performance of the system are fully considered. It should be pointed out that, with the $\alpha$ increasing, the growth of the secrecy rate gradually tends to be flat, so using large $\alpha$ may be unadvisable and energy wasting.
5. Conclusions and Future Research

The robust beamforming design related to the secrecy rate of SWIPT WSN with relay is deeply discussed in this paper. Assuming bounded ellipsoid of CSI error between the relay and the eavesdropper, a maximum secrecy rate algorithm of the system at the constraints of relay power and bounded CSI error is proposed. By introducing slack variables, the original non-convex optimization is converted into a two-level coupled optimization problems. In addition, using S-procedure and SDR techniques, the non-convex constraints of lower-level problem are transformed into a series of LMI forms and iterative bisection methods are introduced to tackle the above decouple problem. The effectiveness of the proposed algorithm is verified by comparing it with PC-SPS, CJ-SPS, and ZF-SPS algorithms.

In this paper, we focus on the impact of channel errors on physical layer security, and we adopt a linear EH model at the relay. There are also many nonlinear EH models in the literature, and it is also necessary to study the influence of the nonlinear EH model on the network. However, because of the complexity of the nonlinear EH model, this is a challenging problem. In addition, the common relay cooperation technology is adopted in this paper, and the emerging intelligent reflecting surface technology is expected to replace relay in short-distance communication because of its excellent energy-saving effect. The
The SWIPT network of intelligent reflecting surface cooperation is also a subject of concern. We will also continue to pay attention to the above issues in the follow-up work.

**Author Contributions:** Conceptualization, Y.J. and R.G.; methodology, C.F.; software, R.G.; validation, C.F. and R.G.; writing—original draft preparation, R.G.; writing—review and editing, Y.J., L.Z. and C.F.; funding acquisition, Y.J. and Z.H. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Science Foundation Council of China (61771006, 61976080), Key Research Projects of University in Henan Province of China (19A413006, 20B510001), First-class Discipline Training Foundation of Henan University (2018yltd04), the Programs for Science and Technology Development of Henan Province (192102210254), and the Talent Program of Henan University (SYL1906110).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data presented in this study are available on request from the first author.

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

**Appendix A**

**Proof of Proposition 1.** Let $\tilde{\omega} = \sqrt{\frac{\nu a B_0}{(1-a)((|\nu|\rho_0\sigma^2+\nu_0^2)+\nu_0^2)}} \text{diag}(h_{sr})w$, The constraint (27) can be expressed as

$$\|\Delta h_{re,k}\|^2 \leq \delta^2 \tag{A1}$$

$$(h_{re,k} + \Delta h_{re,k})^H \tilde{\omega} \tilde{\omega}^H (h_{re,k} + \Delta h_{re,k}) + \frac{\sigma_{e,k}^2}{(1-a)\sigma^2 + \sigma_e^2 - \frac{1-a}{1+a}} \geq 0, \forall k. \tag{A2}$$

Then, according to SDR, let $W = \tilde{\omega} \tilde{\omega}^H$, (A2) converts to

$$(h_{re,k} + \Delta h_{re,k})^H W (h_{re,k} + \Delta h_{re,k}) + \frac{\sigma_{e,k}^2}{(1-a)\sigma^2 + \sigma_e^2 - \frac{1-a}{1+a}} \geq 0, \forall k. \tag{A3}$$

**Lemma A1.** Let $Q_1, Q_2 \in \mathbb{C}^{N \times N}$, $b_1, b_2 \in \mathbb{C}^{N \times 1}$, $c_1, c_2 \in \mathbb{C}$ and $x \in \mathbb{C}^{N \times 1}$, and then the inequality $x^H Q_1 x + 2 \Re\{b_1^H x\} + c_1 \leq 0 \Rightarrow x^H Q_2 x + 2 \Re\{b_1^H x\} + c_2 \leq 0$ hold if and only if there exists a $\mu \geq 0$ such that

$$\mu \left[ \begin{array}{cc} Q_1 & b_1 \\ b_1^H & c_1 \end{array} \right] - \left[ \begin{array}{cc} Q_2 & b_2 \\ b_2^H & c_2 \end{array} \right] \succeq 0, \tag{A4}$$

provided there exists a point $\tilde{x}$ with $x^H Q_1 \tilde{x} + 2 \Re\{b_1^H \tilde{x}\} + c_1 \leq 0$ [4].

By applying Lemma A1, let $x = \tilde{h}_{re,k}$, $Q_1 = I_N$, $b_1 = 0$, $c_1 = -\delta^2$, $Q_2 = -W$, $b_2 = -W\tilde{h}_{re,k}$, $c_2 = -\tilde{h}_{re,k}^H W\tilde{h}_{re,k} - \frac{\sigma_e^2}{(1-a)\sigma^2 + \sigma_e^2 - \frac{1-a}{1+a}}$, the inequations (A1) and (A2) can be transformed into

$$\left[ \begin{array}{cc} \mu_k I_N + W & W\tilde{h}_{re,k} \\ \tilde{h}_{re,k}^H W & \psi_k \end{array} \right] \succeq 0, \forall k, \tag{A5}$$

where $\psi_k \triangleq \tilde{h}_{re,k}^H W\tilde{h}_{re,k} + \frac{\sigma_e^2}{(1-a)\sigma^2 + \sigma_e^2 - \frac{1-a}{1+a}} - \delta^2$. 

**References**

1. Lu, X.; Wang, P.; Niyato, D.; Kim, D.I.; Han, Z. Wireless Networks With RF Energy Harvesting: A Contemporary Survey. *IEEE Commun. Surv. Tutor.* 2015, 17, 757–789. [CrossRef]
2. Yang, Y.; Li, Q.; Ma, W.; Ge, J.; Ching, P.C. Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers. *IEEE Trans. Signal Process.* 2012, 60, 1696–1707. [CrossRef]

3. Wang, D.; Bai, B.; Chen, W.; Han, Z. Achieving High Energy Efficiency and Physical-Layer Security in AF Relaying. *IEEE Trans. Veh. Technol.* 2016, 65, 4455–4469. [CrossRef]

4. Huang, J.; Swindlehurst, A.L. Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization. *IEEE Trans. Veh. Technol.* 2013, 62, 12140–12155. [CrossRef]

5. Dong, L.; Han, Z.; Petroplu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* 2010, 58, 1875–1888. [CrossRef]

6. Ding, Z.; Leung, K.K.; Goeckel, D.L.; Towsley, D. Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting. *IEEE Trans. Wirel. Commun.* 2011, 10, 1725–1729. [CrossRef]

7. Zhou, X.; Li, Q. Energy Efficiency for SWIPT in MIMO Two-Way Amplify-and-Forward Relay Networks. *IEEE Trans. Veh. Technol.* 2018, 67, 4910–4924. [CrossRef]

8. Zhao, S.; Tian, M.; Li, Q. Robust Transmission in Non-Orthogonal Multiple Access AF Relay Networks. *IEEE Trans. Veh. Technol.* 2016, 65, 35–38. [CrossRef]

9. Li, Q.; Zhang, Q.; Qin, J. Secure Relay Beamforming for Simultaneous Wireless Information and Power Transfer in Nonregenerative Relay Networks. *IEEE Trans. Veh. Technol.* 2014, 63, 2462–2467. [CrossRef]

10. Li, Q.; Zhang, Q.; Qin, J. Robust AN-Aided Beamforming and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT. *IEEE Trans. Veh. Technol.* 2019, 68, 6784–6794. [CrossRef]

11. Zhou, X.; Li, Q.; Ma, W.; Ge, J.; Ching, P.C. Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers. *IEEE Trans. Signal Process.* 2016, 64, 4910–4924. [CrossRef]

12. Xing, H.; Kong, K.; Nallanathan, A.; Zhang, R. Wireless Powered Cooperative Jamming for Secrecy Multi-AF Relaying Networks. *IEEE Trans. Wirel. Commun.* 2016, 15, 7971–7984. [CrossRef]

13. 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]

14. Zhou, F.; Li, Z.; Cheng, J.; Li, Q.; Si, J. Robust AN-Aided Beamforming and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT. *IEEE Trans. Veh. Technol.* 2017, 66, 2450–2459. [CrossRef]

15. Zhao, S.; Tian, M.; Li, Q. Robust Transmission in Non-Orthogonal Multiple Access AF Relay Networks. *IEEE Trans. Veh. Technol.* 2018, 67, 567–579. [CrossRef]

16. Joshi, S.K.; Wijewardhana, U.L.; Codreanu, M.; Latva-aho, M. Maximization of Worst-Case Weighted Sum-Rate for MISO Downlink Systems With Imperfect Channel Knowledge. *IEEE Trans. Commun.* 2015, 63, 3671–3685. [CrossRef]

17. Li, Q.; Ma, W. Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming. *IEEE Trans. Signal Process.* 2011, 59, 3799–3812. [CrossRef]

18. Ren, Y.; Lv, T.; Gao, H.; Li, Y. Secure Wireless Information and Power Transfer in Heterogeneous Networks. *IEEE Access* 2017, 5, 4967–4979. [CrossRef]

19. Li, Q.; Yang, Y.; Ma, W.; Lin, M.; Ge, J.; Lin, J. Robust Cooperative Beamforming and Artificial Noise Design for Physical-Layer Secrecy in AF Multi-Antenna Multi-Relay Networks. *IEEE Trans. Signal Process.* 2015, 63, 206–220. [CrossRef]

20. Mukherjee, A.; Swindlehurst, A.L. Detecting passive eavesdroppers in the MIMO wiretap channel. In *Proceedings of the 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*; Kyoto, Japan, 25 March 2012; pp. 2809–2812. [CrossRef]

21. Hasan, A.; Andrews, J.G. The Guard Zone in Wireless Ad hoc Networks. *IEEE Trans. Wirel. Commun.* 2007, 6, 897–906. [CrossRef]

22. Wang, X.; Wang, K.; Zhang, X. Secure Relay Beamforming With Imperfect Channel Side Information. *IEEE Trans. Veh. Technol.* 2013, 62, 2140–2155. [CrossRef]

23. Xing, H.; Kong, K.; Chu, Z.; Nallanathan, A. To Harvest and Jam: A Paradigm of Self-Sustaining Friendly Jammers for Secure AF Relaying. *IEEE Trans. Signal Process.* 2015, 63, 6616–6631. [CrossRef]

24. Salari, S.; Amirani, M.Z.; Kim, I.; Kim, D.I.; Yang, J. Distributed Beamforming in Two-Way Relay Networks With Interference and Imperfect CSI. *IEEE Trans. Wirel. Commun.* 2016, 15, 4455–4469. [CrossRef]

25. Li, X.; Wang, W.; Zhang, M.; Zhou, F.; Al-Dhahir, N. Robust Secure Beamforming for SWIPT-Aided Relay Systems With Full-Duplex Receiver and Imperfect CSI. *IEEE Trans. Veh. Technol.* 2020, 69, 1867–1878. [CrossRef]

26. Feng, Y.; Yang, Z.; Zhu, W.; Li, Q.; Lv, B. Robust Cooperative Secure Beamforming for Simultaneous Wireless Information and Power Transfer in Amplify-and-Forward Relay Networks. *IEEE Trans. Veh. Technol.* 2017, 66, 2354–2366. [CrossRef]