information

MDPI

Article

Beamforming and Antenna Grouping Design for the Multi-Antenna Relay with Energy Harvesting to Improve Secrecy Rate

Weijia Lei and Meihui Zhan *

Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; leiwj@cqupt.edu.cn

* Correspondence: zhanmhcqupt@163.com

Academic Editor: Lorenzo Mucchi

Received: 27 April 2016; Accepted: 1 July 2016; Published: 13 July 2016

Abstract: The physical security strategy in the wireless network with a single-antenna eavesdropper is studied. The information transmits from a single-antenna source to a single-antenna destination, and an energy-limited multi-antenna relay is employed to forward information. The antennas of the relay are divided into two groups. One group receives and forwards information, and the other converts the received signal into energy. Beamforming is used by the relay to prevent the eavesdropper from intercepting confidential information. For the purpose of maximizing the secrecy rate, antenna grouping and beamforming vectors are designed. A low complexity scheme of antenna grouping is presented. The simulation results show that the secrecy rate can be significantly improved by arranging part of the antennas for energy harvesting, and part for forwarding and optimizing the beamforming vector at the relay. The antenna grouping scheme significantly reduces the computational complexity at the cost of acceptable performance loss.

Keywords: physical layer security; energy harvesting; multi-antenna relay; beamforming; antenna grouping; secrecy rate

1. Introduction

Due to the openness of the wireless transmission medium, information faces serious security threats in wireless networks. Physical layer security, based on information theory, utilizes the physical characteristics of channels to achieve secure transmission [1,2]. Secrecy rate is an important parameter to measure the confidential performance of a secure system [3]. Much literature has showed that relay cooperation can enhance the performance of physical layer security effectively. The cooperation protocols include amplify-and-forward (AF), decode-and-forward (DF), and cooperative jamming (CJ). In [4], the security performances of three cooperation protocols have been analyzed when there are one or more eavesdroppers. In [5], AF and artificial noise (AN) are simultaneously employed to improve the secrecy rate under the condition of imperfect channel state information (CSI). In [6], multiple relays are used, one of which is selected for CJ relay and others for AF relay. In [7], two cooperation schemes are proposed in AF relay networks, in which jamming signals can be sent by the destination or a relay.

With the rapid development of wireless network technology, energy consumption in wireless communication networks is also increasing. Energy harvesting is an effective way to prolong the lifetime of wireless nodes. Furthermore, wireless energy transmission is a method to realize energy harvesting and overcome the limitation of energy stored in the battery of a node [8]. Some references have researched the application of wireless energy transmission in relay networks, e.g., [9–12]. In [9,10], an energy cooperation protocol is proposed to promote throughput. In [11], a multi-antenna relay uses different antennas to receive information and harvest energy simultaneously. The throughput maximization of a wireless powered communication network with cooperation is studied in [12].

The issue of the secure information transmission also exists in energy harvesting networks, and some researchers have studied the physical layer security in them. Two kinds of receivers, i.e., energy receiver and information receiver, are considered in [13,14] and [15]. In these articles, energy and secrecy information are transmitted simultaneously, and energy receivers are treated as eavesdroppers. Some strategies of optimizing secrecy rates have been proposed when the CSIs are both perfect and imperfect. Ref. [16] is an overview of the security problem in wireless powered systems, and the physical security techniques for wireless information and power transfer in relaying systems are reviewed. The security problem in wireless powered relaying systems is studied in [17,18]. Ref. [17] focuses on the beamforming of signal and artificial noise. Ref. [18] studies the wireless transmission for both secure information and power in a large-scale relaying system with imperfect CSI.

In this paper, we focus on the physical layer security in an energy harvesting relay network. There are two receivers in the network, and the information sent to a receiver needs to be kept secret from the other receiver, so each is the eavesdropper of the other. When there are some obstacles between the source and the receivers, since no direct communication link exists, the information should be forwarded by a relay. The power supply of the relay is limited because of its location, so it needs to harvest energy from the received RF signals to increase the forwarding power. In our scheme, the relay's antennas are divided into two groups, with one group amplifying and forwarding the source's signal, and the other converting the received signal to energy for the forwarding. With the constraint of the source transmitting power, we propose a low complexity antenna grouping scheme, and optimize the beamforming vector of AF to achieve the maximal secrecy rate.

The remainder of this paper is organized as follows. The second section describes the system model. In the third section, we give the mathematical model of the optimization problem, antenna grouping schemes and the beamforming vector. The simulation results are given in the fourth section. The last section is the conclusion.

2. System Model

A source (s) transmits information to two receiving nodes, but the information transmitted to one node needs to be kept secret from the other node. Hence, for one receiver, the other receiver is an eavesdropper. Without loss of generality, in a timeslot, the node that receives information is called the destination (d), and the other node is called eavesdropper (e). Since obstacles are present between the source and the receivers, there is no direct link between the source and any receiving node, and, as a result, the information must be forwarded by a relay (r). The system model is shown in Figure 1. The relay is equipped with M antennas. Since the signal sent to both receivers needs to be forwarded by the relay, and the relay may ask them to feedback CSI, we assume that the relay can obtain all the CSIs. All channels are unrelated to each other, and they are quasi-static, memoryless, and undergo flat Rayleigh fading. In addition, the noise at any node is additive white complex Gaussian noise with zero-mean and variance σ^2.

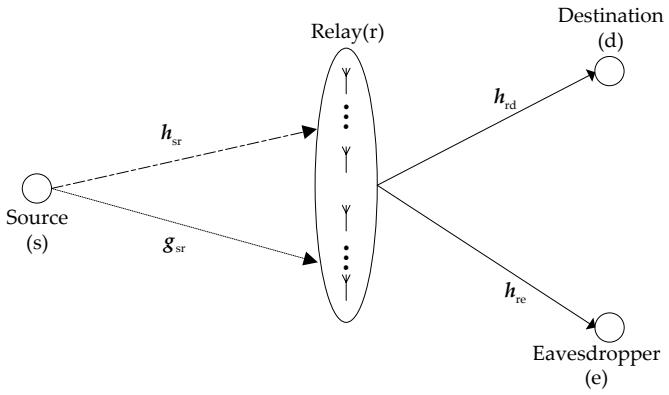

Figure 1. System model.

With the constraints of location and environment, in our model, the relay cannot be powered by power lines. Because the energy stored in relay's battery is limited, the power used for information forwarding is very small, so the data rate will be very low. The rate system will be restricted by the rate of the second hop, in spite of the high achievable rate of the first hop. To alleviate the limit of power supply, we propose an "energy harvesting-AF" strategy. The process of transmission from the source to the destination is divided into two stages. In the first stage, the source sends information; one group of the relay's antennas receives the confidential information, while the other group receives RF signals and converts it into energy. In the second stage, the relay amplifies and forwards signals with the energy both harvested in the first stage and stored in its battery. In this way, more power is focused on the antennas that are better for forwarding. Although the achievable rate of the first hop will decrease, the rate of the second hop will obviously increase, so that the rate of the system will be promoted.

$\boldsymbol{\Psi}$ is defined as the set of relay antennas and $|\boldsymbol{\Psi}| = M$, wherein $|\cdot|$ represents the amount of antennas in the set. The set is divided into two subsets of $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$, and satisfies $\boldsymbol{\Psi} = \boldsymbol{\Theta} \cup \boldsymbol{\Omega}$, $|\boldsymbol{\Theta}| = N$, and $|\boldsymbol{\Omega}| = M - N$. The antennas in the subset $\boldsymbol{\Theta}$ are used to relay information, while the antennas in the subset $\boldsymbol{\Omega}$ are used to harvest energy. We denote the channel coefficient vector between the source and the antennas in the subset $\boldsymbol{\Theta}$ as $\boldsymbol{h}_{\mathrm{sr}}$, and the channel coefficient vector between the source and the antennas in the subset $\boldsymbol{\Omega}$ as $\boldsymbol{g}_{\mathrm{sr}}$. The channel coefficient vectors from the antennas in the subset $\boldsymbol{\Theta}$ to the destination and the eavesdropper are denoted by $\boldsymbol{h}_{\mathrm{rd}}$ and $\boldsymbol{h}_{\mathrm{re}}$, respectively: $\boldsymbol{h}_{\mathrm{sr}} \in \mathbb{C}^{N\times 1}$, $\boldsymbol{g}_{\mathrm{sr}} \in \mathbb{C}^{(M-N)\times 1}$, $\boldsymbol{h}_{\mathrm{rd}} \in \mathbb{C}^{N\times 1}$, $\boldsymbol{h}_{\mathrm{re}} \in \mathbb{C}^{N\times 1}$.

In the first stage, the source transmits symbol x with unit power, i.e., $E\left[|x|^2\right] = 1$, where $E[\cdot]$ denotes expectation. The source has a transmit power constraint P_{s}. The received signal of the relay can be expressed as:

$$\boldsymbol{y}_{\mathrm{r}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}_{\mathrm{sr}}x + \boldsymbol{n}_{\mathrm{r}} \tag{1}$$

where $\boldsymbol{n}_{\mathrm{r}} \sim CN(0, \sigma^2\boldsymbol{I}_N)$ are the additive noises received by the antennas in the subset $\boldsymbol{\Theta}$. Meanwhile, the relay harvests energy through the antennas in the subset $\boldsymbol{\Omega}$. We assume that P_{r} is the power constraint of the relay when only the energy stored in its battery can be used. When $\boldsymbol{\Omega} = \varnothing$, all antennas of the relay are used to forward signals. In this case, the practical power constraint of the relay is $P_{\mathrm{r}}{}' = P_{\mathrm{r}}$. If $\boldsymbol{\Omega} \neq \varnothing$, the received signal of the i-th ($i = 1, 2, \cdots, M-N$) antenna in the subset $\boldsymbol{\Omega}$ can be expressed as:

$$r_i = \sqrt{P_{\mathrm{s}}}\boldsymbol{g}_{\mathrm{sr},i}x + n'_{r,i} \tag{2}$$

where $n'_{r,i}$ denotes the additive noise received by antenna i. Assume that the signal is converted to energy with the efficiency of α, and $\alpha \in (0, 1]$. As the harvested energy is also used in AF, the total power of forwarding signals in the second stage will be:

$$\begin{aligned} P_{\mathrm{r}}{}' &= P_{\mathrm{r}} + \alpha \sum_{i=1}^{M-N} |r_i|^2 \\ &= P_{\mathrm{r}} + \alpha \sum_{i=1}^{M-N} \left(P_{\mathrm{s}} \left|g_{\mathrm{sr},i}\right|^2 + \sigma^2\right) \\ &= P_{\mathrm{r}} + \alpha P_{\mathrm{s}} ||\boldsymbol{g}_{\mathrm{sr}}||^2 + \alpha (M-N)\sigma^2 \end{aligned} \tag{3}$$

In the second stage, the relay forwards information by the antennas in the subset $\boldsymbol{\Theta}$. The transmitted signal of the relay is denoted by $\boldsymbol{x}_{\mathrm{r}} = \boldsymbol{W}\boldsymbol{y}_{\mathrm{r}}$, where $\boldsymbol{W}$ is a diagonal matrix composed of a beamforming vector $\boldsymbol{w} = [w_1, w_2, \cdots, w_N]^{\mathrm{T}}$, i.e. $\boldsymbol{W} = \mathrm{diag}(\boldsymbol{w})$. $\boldsymbol{x}_{\mathrm{r}}$ can be rewritten as:

$$\begin{aligned} \boldsymbol{x}_{\mathrm{r}} &= \boldsymbol{W}\boldsymbol{y}_{\mathrm{r}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{sr}}x + \boldsymbol{W}\boldsymbol{n}_{\mathrm{r}} \\ &= \sqrt{P_{\mathrm{s}}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}x + \mathrm{diag}(\boldsymbol{w})\boldsymbol{n}_{\mathrm{r}} \end{aligned} \tag{4}$$

The transmission power of the relay should satisfy the constraint Equation (5) as follows:

$$||\boldsymbol{x}_{\mathrm{r}}||^2 = P_{\mathrm{r}}{}' \tag{5}$$

The received signals at the destination and the eavesdropper are:

$$\begin{array}{c} y_{\mathrm{d}} = \boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\boldsymbol{x}_{\mathrm{r}} + n_{\mathrm{d}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)\boldsymbol{w}x + \boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{w}\right)\boldsymbol{n}_{\mathrm{r}} + n_{\mathrm{d}} \\ = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)\boldsymbol{w}x + \boldsymbol{n}_{\mathrm{r}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}\right)\boldsymbol{w} + n_{\mathrm{d}} \\ y_{\mathrm{e}} = \boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\boldsymbol{x}_{\mathrm{r}} + n_{\mathrm{e}} = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)\boldsymbol{w}x + \boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{w}\right)\boldsymbol{n}_{\mathrm{r}} + n_{\mathrm{e}} \\ = \sqrt{P_{\mathrm{s}}}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)\boldsymbol{w}x + \boldsymbol{n}_{\mathrm{r}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}\right)\boldsymbol{w} + n_{\mathrm{e}} \end{array} \tag{6}$$

where the superscript T denotes matrix transpose, n_{d} and n_{e}, respectively, represent the noise at the destination and the eavesdropper. The SNRs (Signal to Noise Ratios) at the destination and the eavesdropper can be calculated as:

$$\begin{array}{l} \gamma_{\mathrm{rd}} = \frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{rd}}^{*}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{rd}})\boldsymbol{w}+\sigma^2} \\ \gamma_{\mathrm{re}} = \frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{re}}^{*}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{re}})\boldsymbol{w}+\sigma^2} \end{array} \tag{7}$$

3. Optimization Analysis

In information-theoretical security, the secrecy rate is defined as $\max\{R_{\mathrm{d}} - R_{\mathrm{e}}, 0\}$, where R_{d} and R_{e} are, respectively, the rates at the destination and the eavesdropper. In our model, they can be formulated as:

$$\begin{array}{l} R_{\mathrm{d}} = \frac{1}{2}\log\left(1+\gamma_{\mathrm{rd}}\right) = \frac{1}{2}\log\left(1+\frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{rd}}^{*}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{rd}})\boldsymbol{w}+\sigma^2}\right) \\ R_{\mathrm{e}} = \frac{1}{2}\log\left(1+\gamma_{\mathrm{re}}\right) = \frac{1}{2}\log\left(1+\frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{re}}^{*}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{re}})\boldsymbol{w}+\sigma^2}\right) \end{array} \tag{8}$$

In the formulae, the coefficient $1/2$ means the relay forwards data in half the time of a time slot. Thus, the secrecy rate is:

$$\begin{array}{rl} R_{\mathrm{s}} = & \frac{1}{2}\log\left(1+\frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{rd}}^{*}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{rd}})\boldsymbol{w}+\sigma^2}\right) \\ & -\frac{1}{2}\log\left(1+\frac{P_{\mathrm{s}}\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}}^{*})\boldsymbol{h}_{\mathrm{re}}^{*}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}(\boldsymbol{h}_{\mathrm{sr}})\boldsymbol{w}}{\sigma^2\boldsymbol{w}^{\mathrm{H}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}^{*}\right)\mathrm{diag}(\boldsymbol{h}_{\mathrm{re}})\boldsymbol{w}+\sigma^2}\right) \end{array} \tag{9}$$

The beamforming vector $\boldsymbol{w}$ is constrained by Equation (10) as follows:

$$\boldsymbol{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}^{*}\right)\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)+\sigma^2\boldsymbol{I}_N\right)\boldsymbol{w} = P_{\mathrm{r}}{}' \tag{10}$$

where $\boldsymbol{I}_N$ is an $N \times N$ identity matrix. The optimization problem can be formulated as:

$$\begin{array}{ll} \max\limits_{N,\Theta,\Omega,\boldsymbol{w}} & R_{\mathrm{s}} \\ \text{s.t.} & \boldsymbol{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}^{*}\right)\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)+\sigma^2\boldsymbol{I}_N\right)\boldsymbol{w} = P_{\mathrm{r}}{}' \end{array} \tag{11}$$

As the channels are quasi-static, the channel coefficients over a period of time will be constant. The maximum R_{s} can be obtained by optimizing four optimization variables: N, $\boldsymbol{\Theta}$, $\boldsymbol{\Omega}$, and $\boldsymbol{w}$. The first three variables determine the antenna grouping. If the antenna grouping has been determined, i.e., the variables N, $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$ are known, the original optimization problem can be simplified into the optimization of the beamforming vector $\boldsymbol{w}$. Therefore, the original optimization problem of formula (11) can be split into two parts. The first part is the optimization of $\boldsymbol{w}$ under a certain N, $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$, and the second is to determine the antenna grouping. An exhaustive antenna grouping scheme, which tries all the possible combinations of N, $\boldsymbol{\Theta}$, and $\boldsymbol{\Omega}$ and obtains corresponding $\boldsymbol{w}$ and secrecy

rate R_s, can be used to get the optimal solution. This scheme has the optimal performance, but with a very high complexity. Therefore, we propose a low complexity antenna grouping scheme. $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$ are determined according to an antenna choosing rule at a given N, and then $\boldsymbol{w}$ is calculated. M secrecy rate R_s will be obtained as N increases from 1 to M. The N, $\boldsymbol{\Theta}$, $\boldsymbol{\Omega}$ and $\boldsymbol{w}$ that correspond to the maximum R_s are the optimized antenna grouping and beamforming scheme we are looking for. The performance of this scheme is sub-optimal because we have not tried all the possible grouping of the antennas, but its computational complexity is significantly lower than that of the previous grouping scheme.

3.1. Beamforming Design

In this section, we optimize the beamforming vector at a given antenna grouping. The original problem of formula (11) can be rewritten as:

$$\begin{array}{ll} \max\limits_{\boldsymbol{w}} & \frac{1}{2}\log\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{A}\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{B}\boldsymbol{w}+\sigma^2}\right)-\frac{1}{2}\log\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{C}\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{D}\boldsymbol{w}+\sigma^2}\right) \\ \text{s.t.} & \boldsymbol{w}^{\mathrm{H}}\boldsymbol{R}\boldsymbol{w}=P_{\mathrm{r}}{}' \end{array} \tag{12a}$$

where

$$\begin{array}{ll} \boldsymbol{A}=P_{\mathrm{s}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}^{*}\right)\boldsymbol{h}_{\mathrm{rd}}^{*}\boldsymbol{h}_{\mathrm{rd}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right), & \boldsymbol{B}=\sigma^2\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}^{*}\right)\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{rd}}\right) \\ \boldsymbol{C}=P_{\mathrm{s}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}^{*}\right)\boldsymbol{h}_{\mathrm{re}}^{*}\boldsymbol{h}_{\mathrm{re}}^{\mathrm{T}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right), & \boldsymbol{D}=\sigma^2\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}^{*}\right)\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{re}}\right) \\ \boldsymbol{R}=P_{\mathrm{s}}\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}^{*}\right)\mathrm{diag}\left(\boldsymbol{h}_{\mathrm{sr}}\right)+\sigma^2\boldsymbol{I}_N & \end{array} \tag{12b}$$

This problem only involves variable $\boldsymbol{w}$. $\boldsymbol{A}$ and $\boldsymbol{C}$ are positive semi-definite matrices with size $N \times N$, and $\boldsymbol{B}$, $\boldsymbol{D}$, $\boldsymbol{R}$ are positive definite matrices with size $N \times N$. The objective function of optimization can be further organized as:

$$\begin{array}{ll} \max\limits_{\boldsymbol{w}} & \frac{1}{2}\log\left(f_1 f_2\right) \\ \text{s.t.} & \boldsymbol{w}^{\mathrm{H}}\boldsymbol{R}\boldsymbol{w}=P_{\mathrm{r}}{}' \end{array} \tag{13a}$$

where

$$\begin{array}{cc} f_1=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{A}'\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{C}'\boldsymbol{w}}, & f_2=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{D}'\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{B}'\boldsymbol{w}} \\ \boldsymbol{B}'=\boldsymbol{B}+\sigma^2/P_{\mathrm{r}}{}'\boldsymbol{R}, & \boldsymbol{D}'=\boldsymbol{D}+\sigma^2/P_{\mathrm{r}}{}'\boldsymbol{R} \\ \boldsymbol{A}'=\boldsymbol{A}+\boldsymbol{B}', & \boldsymbol{C}'=\boldsymbol{C}+\boldsymbol{D}' \end{array} \tag{13b}$$

$\boldsymbol{A}'$, $\boldsymbol{B}'$, $\boldsymbol{C}'$ and $\boldsymbol{D}'$ are positive definite matrices with size $N \times N$. Since $\log(\cdot)$ is a monotonically increasing function, formula (13a) is equivalent to maximizing $f_1 f_2$.

The overall optimization of $f_1 f_2$ is difficult. However, the maximum of f_1 and f_2 can be respectively obtained by solving the maximal generalized eigenvalues of $(\boldsymbol{A}', \boldsymbol{C}')$ and $(\boldsymbol{D}', \boldsymbol{B}')$. However, these two generalized eigenvectors corresponding to the two maximal generalized eigenvalues may not be equal. Therefore, we use a local optimal beamforming design. We find that $\boldsymbol{h}_{\mathrm{sr}}$, $\boldsymbol{h}_{\mathrm{rd}}$ and $\boldsymbol{h}_{\mathrm{re}}$ have a more comprehensive impact on f_1, so we will maximize f_1 by solving the maximal generalized eigenvalue of $(\boldsymbol{A}', \boldsymbol{C}')$ to get the generalized eigenvector, and use it as beamforming vector $\boldsymbol{w}$.

We have $f_1^{\max} = \sup\left\{\lambda \middle| \det(\lambda \boldsymbol{C}' - \boldsymbol{A}') = 0\right\}$, where λ represents eigenvalues. Denote the generalized eigenvector corresponding to $f_1^{\max}$ as $\boldsymbol{w}_1$. The local optimal beamforming vector based on the power constraints of the relay is:

$$\boldsymbol{w}_{\mathrm{o}}=\sqrt{\frac{P_{\mathrm{r}}{}'}{\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{R}\boldsymbol{w}_1}}\boldsymbol{w}_1 \tag{14}$$

The secrecy rate can be obtained by formula (9) when $\boldsymbol{w}$ is substituted by $\boldsymbol{w}_{\mathrm{o}}$.

f_2 may not be maximal when f_1 is maximal, so the value range of $f_1 f_2$ should be $\left[f_1^{\max} f_2^{\min}, f_1^{\max} f_2^{\max}\right]$, the superscripts max and min represent the maximum and minimum of f_1

and f_2. Since the two matrices in f_2 are diagonal matrices, based on the generalized eigenvalues of $(\boldsymbol{D}', \boldsymbol{B}')$, the maximum and minimum of f_2 can be formulated as:

$$\begin{aligned} f_2^{\max} &= \max_k \left(1 + \frac{P_r'\left(|h_{re,k}|^2 - |h_{rd,k}|^2\right)}{P_s|h_{sr,k}|^2 + P_r'|h_{rd,k}|^2 + \sigma^2}\right) \\ f_2^{\min} &= \min_k \left(1 + \frac{P_r'\left(|h_{re,k}|^2 - |h_{rd,k}|^2\right)}{P_s|h_{sr,k}|^2 + P_r'|h_{rd,k}|^2 + \sigma^2}\right) \end{aligned} \tag{15}$$

where k represents the number of antennas in subset $\boldsymbol{\Theta}$.

3.2. Antenna Grouping Scheme

As the number of relay antennas is limited, the optimal antenna grouping scheme can be obtained by trying all possible subsets $\boldsymbol{\Theta}$. The number of the subset $\boldsymbol{\Theta}$ is C_M^N when $|\boldsymbol{\Theta}| = N$. The total number of subset $\boldsymbol{\Theta}$ is $\sum_{N=1}^{M} C_M^N = 2^M - 1$ when N varies from 1 to M. A subset $\boldsymbol{\Theta}$ corresponds to a beamforming vector $\boldsymbol{w}_o$ and secrecy rate R_s. The N, $\boldsymbol{\Theta}$, $\boldsymbol{\Omega}$ and $\boldsymbol{w}_o$ corresponding to the maximal R_s are the solutions of the optimization problem. The computation amount of $\boldsymbol{w}_o$ and R_s is also $2^M - 1$. Although this antenna grouping scheme can obtain the optimal solution, its computation complexity is too high. Here, we give a low complexity antenna grouping scheme with the acceptable performance loss.

We find that the change of $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$ will lead to the change of channel coefficients $\boldsymbol{h}_{sr}$, $\boldsymbol{h}_{rd}$, $\boldsymbol{h}_{re}$ and $\boldsymbol{g}_{sr}$ in Equation (9). Thus, we design a rule to determine $\boldsymbol{\Theta}$ and $\boldsymbol{\Omega}$ in a given N. Define $h_{sr,k}$ as the channel coefficient between the source and the k-th antenna of the relay, $h_{rd,k}$ and $h_{re,k}$, respectively, as the channel coefficients from the k-th antenna of the relay to the destination and the eavesdropper, $k = 1, 2, \cdots, M$. $h_{rd,k}$ and $h_{re,k}$ have a great impact on the secrecy transmission performance in the second stage. Obviously, in order to enhance security performance, we should choose the antenna that has a preferable channel performance to the destination but a poorer channel performance to eavesdropper to receive and forward information. Thus, we use $|h_{re,k}| / |h_{rd,k}|$ as a metric to choose the AF antennas. Antenna k with a lower value of $|h_{re,k}| / |h_{rd,k}|$ is more suitable for the forwarding. On the other hand, the amount of the energy harvested in the first stage will determine the transmitting power in the second stage, which has significant impact on secrecy performance, and it is determined by $|h_{sr,k}|$. Therefore, in theory, we should give priority to the antenna with large $|h_{sr,k}|$ to harvest energy and the antenna with small $|h_{sr,k}|$ to forward information.

From the two aspects above, the antennas of the relay can be grouped according to the channel parameter $p = |h_{sr,k}| |h_{re,k}| / |h_{rd,k}|$. We sort the antennas according to the descending order of p. The first $M - N$ antennas are the members of subset $\boldsymbol{\Omega}$, and remaining antennas are the members of subset $\boldsymbol{\Theta}$. As N varies from 1 to M, there are M subsets $\boldsymbol{\Omega}$, $\boldsymbol{\Theta}$, and corresponding $\boldsymbol{w}_o$. The N and antenna grouping corresponding to the maximum of M secrecy rates will be the sub-optimal antenna grouping scheme.

Here, we compare the complexity between the optimal and the sub-optimal antenna grouping schemes. The former searches and computes $2^M - 1$ times, and the latter computes only M times. The sub-optimal antenna grouping scheme has evidently lower computational complexity.

4. Simulation Results

The performance of the proposed scheme is simulated in this section. The coordinates of the nodes are shown in Figure 2. We set the source (s), the destination (d) and the eavesdropper (e), respectively, at $(0, 0)$, $(200, 150)$, $(200, -150)$ (Unit: m). For all channels, path loss and small-scale fading that obey Rayleigh distribution are considered, i.e. $h = \beta d^{-c/2}$. Where, $c = 3$ is the path loss exponent, d (unit: m) represents the distance between two nodes, and $d^{-c/2}$ is the path loss (amplitude). In addition, β is the zero-mean complex Gaussian variable with unit variance, and it represents the small-scale fading factor. We set the variance of noise at all nodes to $\sigma^2 = -120$ dBm. In the process of energy

harvesting, the received signal power is converted to DC power with the efficiency $\alpha = 0.7$ [19]. The results showed in this section are the average values of the data obtained in 5000 independent trials.

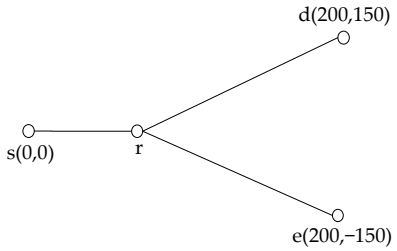

Figure 2. Model used for simulation.

We compare our strategy with the traditional AF relay strategy, where the relay uses all antennas to forward information. Furthermore, the same beamforming as that in our strategy is used in the traditional AF strategy.

Figure 3 shows the relationship between the relay position and secrecy rate. We set $P_s = 1$ mW, $P_r = 0.01$ mW and $M = 6$. The simulation results show that the security performance of the proposed "energy harvesting–AF" strategy is better than the traditional AF strategy. In the traditional AF strategy, the relay forwards information only with the battery energy, so the forwarding power will be very low. Although the relay uses all antennas to forward information, the secrecy rate is still limited. In the proposed "energy harvesting–AF" strategy, the relay can supplement energy through energy harvesting; therefore, it will have higher forwarding power. Because of the logarithmic relationship between the transmission rate and SNR, the increase of transmission power can bring significant improvement of the transmission rate in the low power region. On the other hand, with the increase of distance between the source and the relay, the path loss is also increasing, so the harvested energy is exponentially decreasing, and, consequently, the secrecy rate of the system decreases. Although the relay is closer to the destination, its influence is far less than that of the decrease of the relay forwarding power, so the secrecy rate of the system declines. It also can be seen from Figure 3 that the secrecy rate of the optimal antenna grouping scheme is higher than that of the sub-optimal one, but the gap is not obvious. Therefore, the sub-optimal antenna grouping scheme significantly reduces the computational complexity at only the cost of acceptable performance loss.

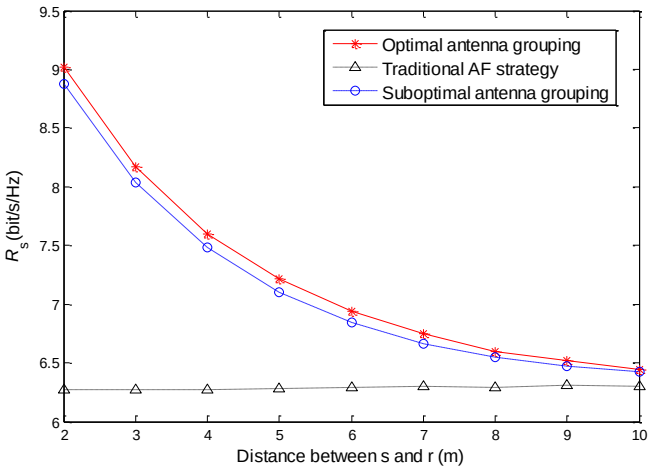

Figure 3. Relationship between relay's position and secrecy rate.

Figure 4 shows the secrecy rate with different source transmission power. We also set $P_r = 0.01$ mW and $M = 6$, while the coordinate of the relay is fixed at $(5, 0)$. The source transmission

power P_s increases from 0.1 mW to 1 mW. We find that the secrecy rates of the proposed strategy with two antenna grouping schemes are both increasing when the source transmission power gets higher. This is because the increase of source transmission power on the one hand is beneficial to the improvement of the receiving SNR of the relay, and, on the other hand, can increase the harvested energy of the relay. However, in the traditional AF strategy, although the receiving SNR of the relay can also be improved by increasing source transmission power, the secrecy rate is not obviously improved due to the low forwarding power of the relay. In addition, it can also be found that the secrecy rate gap between the two antenna grouping schemes increases with the increase of source transmission power. The increase of the source transmission power leads to the increase of the receiving SNR and the harvested energy of the relay. The sub-optimal antenna grouping scheme prefers the antennas with better link quality to the source to harvest energy, and the effect of receiving signal SNR of the relay is not considered adequately. This will not have an obvious influence when source transmission power is low, but it will become serious when source transmission power is high. We also give the secrecy rate when the location of the eavesdropper is $(100, -75)$, closer to the relay than the destination. As the eavesdropper only receives a signal in the second stage, where the secure beamforming is used, the secrecy rates are nearly the same.

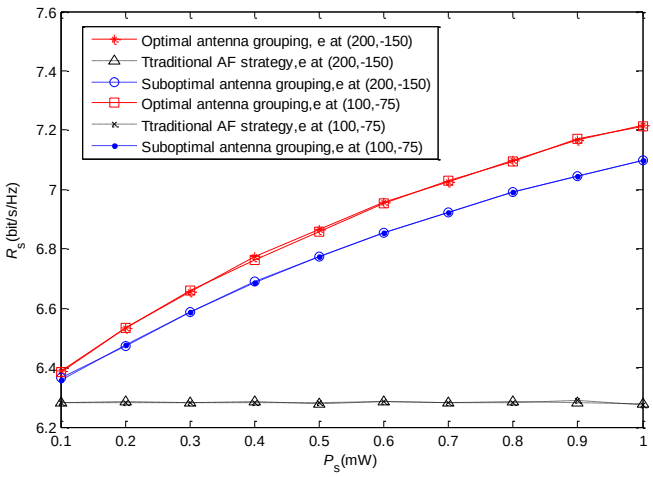

Figure 4. Relationship between source transmission power and secrecy rate.

The relationship between antenna number of the relay and secrecy rate is shown in Figure 5. We set the coordinate of the relay at $(5, 0)$, and set $P_s = 1$ mW and $P_r = 0.01$ mW. M increases from four to 10. For the traditional AF strategy, the increase of M will enhance beamforming gain, so the achievable secrecy rate can be improved. However, in the proposed "energy harvesting–AF" strategy, the increase of M has two benefits. One is that more antennas can be selected into the subset $\boldsymbol{\Theta}$, which means that there are more antennas receiving and forwarding signals. In this case, the beamforming gain of the second stage will improve. The other is that more antennas can be assigned to the subset $\boldsymbol{\Omega}$. Thus, the forwarding power will increase because more energy is harvested by the relay. They are both conducive to enhancing the security performance of the system. Therefore, with the increase of M, the secrecy rate of "energy harvesting–AF" strategy increases significantly. In addition, the "energy harvesting-AF" strategy can use the antennas more flexibly, so its performance is higher than that of the traditional AF strategy.

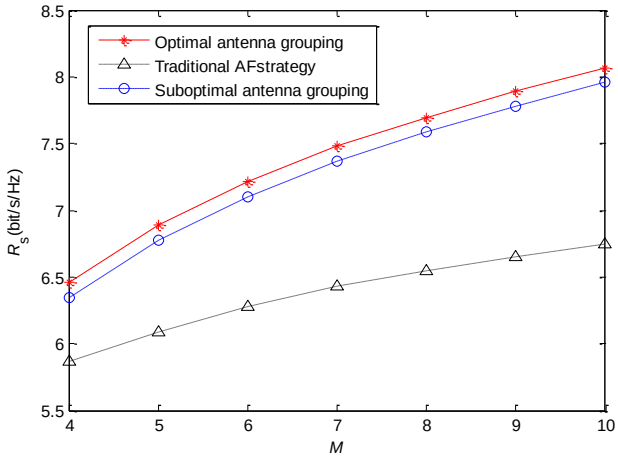

Figure 5. Relationship between antenna number of relay and secrecy rate.

Figure 6 illustrates the relationship between P_r and secrecy rate. We set the coordinate of the relay at $(5, 0)$, and set $P_s = 1$mW and $M = 6$. P_r increases from 0.01 mW to 0.1 mW. Obviously, the forwarding power of the relay affects directly the receiving SNR of the destination. Although the receiving SNR of the eavesdropper is also affected, its promotion is less than that at the destination due to the beamforming. Thus, the secrecy rate increases with the raise of P_r. From Figure 6, we find that the gap of the secrecy rate between the "energy harvesting–AF" strategy and the traditional AF strategy is reduced when P_r increases. Due to the logarithmic relationship between transmission rate and SNR, the performance improvement induced by energy harvesting becomes less evident when P_r becomes higher.

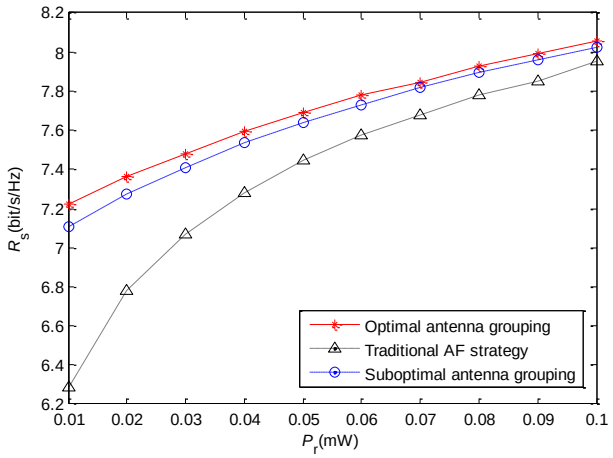

Figure 6. Relationship between P_r and secrecy rate.

5. Conclusions

This paper studies the security transmission in wireless powered relaying systems. In the system model, the source, the destination, and the eavesdropper are respectively equipped with an antenna, and the relay is equipped with multiple antennas to amplify and forward information. The transmission process of confidential information was divided into two stages. In the first stage, the relay converts the received signals in some antennas into energy. In order to avoid the leakage of information, beamforming is used by the relay when it forwards the information to the destination in the second stage. We divide the antennas of the relay into two groups. The antennas in one group forward the received signals with beamforming, and those in the other convert the received signal

to energy for the signal forwarding. We optimize the antenna grouping scheme and beamforming vector to promote the achievable secrecy rate. Since the overall optimal beamforming vector is difficult to obtain, we use a local optimal beamforming vector. We also propose a low complexity antenna grouping scheme at only the cost of acceptable performance loss. The simulation results show that the proposed "energy harvesting–AF" strategy has better security performance than the traditional AF strategy, especially when the battery power of the relay is low.

Acknowledgments: We gratefully acknowledge the detailed and helpful comments of the anonymous reviewers, who have enabled us to considerably improve this paper. This work was supported by the National Natural Science Foundation of China (61471076, 61301123), the fund of the Changjiang Scholars and Innovative Team Development Plan (IRT1299), and the Special Fund of Chongqing Key Laboratory (CSTC).

Author Contributions: Weijia Lei and Meihui Zhan conceived and designed the experiments; Meihui Zhan performed the experiments; Weijia Lei and Meihui Zhan analyzed the data; Meihui Zhan wrote the paper; Weijia Lei revised the paper. .

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

References

1. 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. Tut.* **2014**, *16*, 1550–1573. [CrossRef]
2. Liang, Y.; Poor, H.V. Information theoretic security. *Found. Trends Commun. Inf. Theory* **2009**, *5*, 355–580. [CrossRef]
3. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
4. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
5. Li, Q.; Yang, Y.; Ma, W.K.; 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]
6. Wang, H.M.; Liu, F.; Yang, M. Joint cooperative beamforming, jamming and power allocation to secure AF relay systems. *IEEE Trans. Veh. Technol.* **2015**, *64*, 4893–4898. [CrossRef]
7. 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]
8. Bi, S.; Ho, C.K.; Zhang, R. Wireless powered communication: Opportunities and challenges. *IEEE Commun. Mag.* **2015**, *53*, 117–125. [CrossRef]
9. Gurakan, B.; Ozel, O.; Yang, J.; Ulukus, S. Energy cooperation in energy harvesting wireless communications. In Proceedings of IEEE International Symposium on Information Theory, Cambridge, MA, USA, 1–6 July 2012; pp. 965–969.
10. Gurakan, B.; Ozel, O.; Yang, J.; Ulukus, S. Energy cooperation in energy harvesting communications. *IEEE Trans. Commun.* **2013**, *61*, 4884–4898. [CrossRef]
11. Zhou, Z.; Peng, M.; Zhao, Z.; Li, Y. Joint power splitting and antenna selection in energy harvesting relay channels. *IEEE Signal Process. Lett.* **2015**, *22*, 823–827. [CrossRef]
12. Ju, H.; Zhang, R. User cooperation in wireless powered communication networks. In Proceedings of IEEE Global Communications Conference, Austin, TX, USA, 7–11 December 2014; pp. 1430–1435.
13. Liu, L.; Zhang, R.; Chua, K.C. Secrecy wireless information and power transfer with MISO beamforming. *IEEE Trans. Signal Process.* **2014**, *62*, 1850–1863. [CrossRef]
14. Feng, R.; Li, Q.; Zhang, Q.; Qin, J. Robust secure transmission in MISO simultaneous wireless information and power transfer system. *IEEE Trans. on Veh. Tech.* **2015**, *64*, 400–405. [CrossRef]
15. Wu, W.; Wang, B. Robust downlink beamforming design for multiuser MISO communication system with SWIPT. In Proceedings of IEEE International Conference on Communications, London, UK, 8–12 June 2015; pp. 4751–4756.
16. Chen, X.; Ng, D.W.K.; Chen, H.H. Secrecy wireless information and power transfer: Challenges and opportunities. *IEEE Wirel. Commun.* **2016**, *23*, 54–61. [CrossRef]

17. Zhang, G.; Li, X.; Cui, M.; Li, G.; Yang, L. Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple-output relaying systems. *IET Commun.* **2016**, *10*, 796–804. [CrossRef]
18. Chen, X.; Chen, J.; Liu, T. Secure wireless information and power transfer in large-scale MIMO relaying systems with imperfect CSI. In Proceedings of IEEE Global Communications Conference, Austin, TX, USA, 7–11 December 2014; pp. 4131–4136.
19. Valenta, C.R.; Durgin, G.D. Harvesting wireless power: Survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems. *IEEE Microw. Mag.* **2014**, *15*, 108–120.