entropy

MDPI

*Article*

# Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing

**Shuai Chang [1], Jialun Li [2], Xiaomei Fu [1,*] and Liang Zhang [1]**

[1] School of Marine Science and Technology, Tianjin University, Tianjin 300072, China; shuai.chang@tju.edu.cn (S.C.); liangzhang@tju.edu.cn (L.Z.)

[2] School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China; Li_five@tju.edu.cn

* Correspondence: fuxiaomei@tju.edu.cn; Tel.: +86-22-87370655

Received: 20 July 2017; Accepted: 25 August 2017; Published: 1 September 2017

**Abstract:** Energy harvesting (EH) has attracted a lot of attention in cooperative communication networks studies for its capability of transferring energy from sources to relays. In this paper, we study the secrecy capacity of a cooperative compressed sensing amplify and forward (CCS-AF) wireless network in the presence of eavesdroppers based on an energy harvesting protocol. In this model, the source nodes send their information to the relays simultaneously, and then the relays perform EH from the received radio-frequency signals based on the power splitting-based relaying (PSR) protocol. The energy harvested by the relays will be used to amplify and forward the received information to the destination. The impacts of some key parameters, such as the power splitting ratio, energy conversion efficiency, relay location, and the number of relays, on the system secrecy capacity are analyzed through a group of experiments. Simulation results reveal that under certain conditions, the proposed EH relaying scheme can achieve higher secrecy capacity than traditional relaying strategies while consuming equal or even less power.

**Keywords:** secrecy capacity; cooperative wireless communication; energy harvesting; compressed sensing; physical layer security

## 1. Introduction

Physical-layer security approaches can enhance the security of wireless sensor networks (WSNs) against eavesdroppers by exploiting the physical characteristics of wireless channels, such as noise and multipath fading [1]. The secrecy capacity is the maximum rate of secret information that can be sent from the source to the destination in the presence of eavesdroppers. The cooperative relaying strategy has recently been used as a practical technology to provide transmission secrecy [2–5], to break through the limitation on the channel conditions that the main channel (from the source to the destination) must be better than the eavesdropper channel (from the source to the eavesdropper). Many kinds of approaches have been proposed to enhance the physical-layer security under cooperative communication framework conditions, such as amplify-and-forward (AF) [6,7], decode-and-forward (DF) [8], compress-and-forward (CF) [8], noise-forwarding (NF) [9], etc.

In the past few years, radio frequency (RF) energy harvesting (EH) has becomes a research hotspot in wireless communications, especially in applications where the battery-limited devices are difficult to replace or recharge [10]. Simultaneous wireless information and power transfer (SWIPT) [11–13] was proposed to improve the energy utilization efficiency of wireless networks. Under this scheme, the nodes in wireless networks can be energy self-sufficient by harvesting RF signals from the surrounding environment.

Cooperative communication is exploited for its capability to further improve the efficiency of SWIPT systems [14]. As the RF signals can carry information and energy concurrently, thereby in such wireless networks, the cooperative relays are able to harvest energy and process information simultaneously [11]. There are two kinds of relaying protocols: power splitting relaying (PSR) protocols and time switching relaying (TSR) protocols [11,15–17]. In a PSR protocol, the received signals are divided by a power-splitting ratio to operate EH and information processing (AF or DF), and the EH and information processing are performed simultaneously [10,11,15,16], while, in a TSR protocol, the EH is performed first, and the information processing is performed in the remainder of the total transmission period [10,11,15,17,18]. Comparison studies between PSR and TSR are conducted in [10,15], and the PSR approach is proved to be better than the TSR in EH-based multi-antenna AF relaying networks. Especially in [15], an eavesdropper is considered in the network, and the destination transmits noise information to interrupt the eavesdropper. In [16], the EH-AF and EH-DF schemes with a single EH relay and single eavesdropper are compared based on TSR protocol, concluding that the EH-DF protocol outperforms the EH-AF protocol in terms of secrecy capacity. In [18], the authors consider an underlay cognitive radio network (CRN) with a pair of primary nodes, a couple of secondary nodes, and one eavesdropper. The EH is performed on the secondary transmitter. Experimental results show that the EH nodes could improve both energy efficiency and spectral efficiency.

Compressed sensing (CS) technology has recently become an effective solution to improve the physical layer security in cooperative wireless networks. CS could represent the compressible signals at a rate below the Nyquist rate, and the information could be retrieved from a small number of linear measurements [19–21]. The application of CS in the field of information-theoretic secrecy has attracted researchers' attention and a series of studies have been conducted. In [22,23], the authors consider the scenario of one source node, one receiver and one eavesdropper (i.e., a point-to-point scheme). In [22], the measurement matrix is treated as an encryption key which is unknown to the eavesdroppers. It can provide computational secrecy with unbounded eavesdropper computation capability. In [23], perfect secrecy is achievable under the condition that the number of source messages goes to infinity. Different from these methods, the authors in [24] considered the situation of keyless physical-layer security, and indicated that the eavesdropper could not decode the information successfully in terms of the Wolfowitz secrecy. In [25], the CS matrix is used to encode the messages. If the wire-tap channels are strictly worse than the main channels, the eavesdroppers can learn almost nothing, thereby, in this situation, it is unnecessary for us to know the channel state information (CSI) of eavesdroppers.

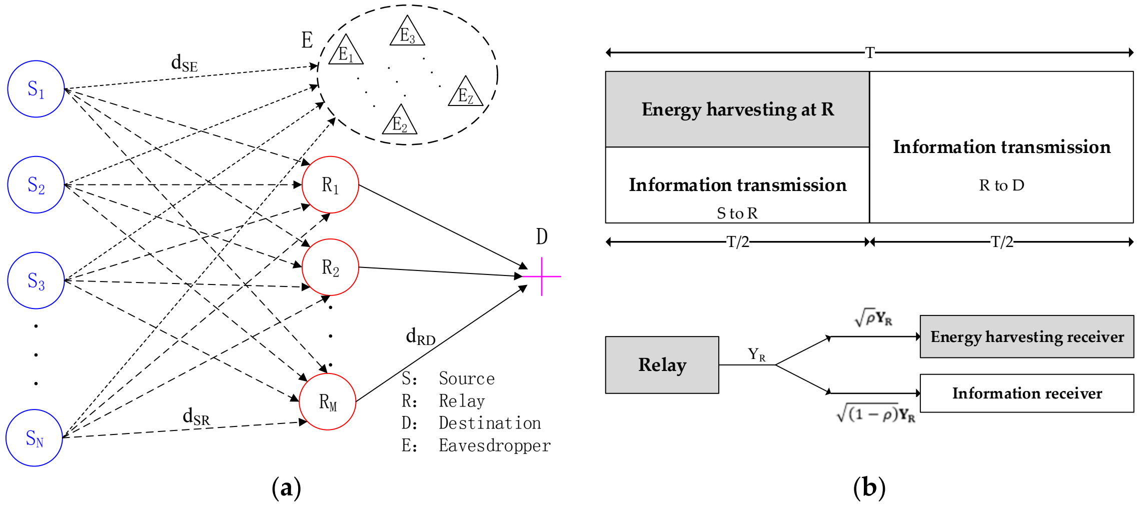
However, the transmitting methods with CS in point-to-point communication scenarios cannot be directly applied to WSNs, because WSNs possess the property of decentralization [26]. The CS-AF scheme was first proposed and applied in wireless networks in [27], and the channel capacity of the CS-AF scheme was investigated in [28]. It is a novel approach in that the channel matrix from sources to relays is the compressive matrix in CS technology, and thus can help to achieve security. It has been proved that the recovery probability of the eavesdroppers under a CS-AF scheme can be arbitrarily small. No more researches considering the channel matrixes as the compressed matrix have been found, and the study of EH in this kind of networks is still a new area.

In this paper, we study the secrecy capacity of the CCS-AF wireless network based on the EH protocol. In this model, the sources send their information to the relays simultaneously, and the relays harvest energy from the radio-frequency signals of sources based on the PSR protocol. Through this protocol, the energy harvested is used by the cooperative relays to amplify and forward the received information to the destination. A group of simulation experiments is conducted to analyze the impacts of some key parameters (such as power splitting ratio, EH efficiency, relay location, and the number of relays) on the system secrecy capacity. Simulation results reveal that under certain conditions, the EH relaying scheme in this paper can achieve higher secrecy capacity than traditional relaying strategies while costing the same or even less power.

The rest of this paper is organized as follows: in Section 2, the CCS-AF model is proposed and introduced in detail. Then a brief introduction of PSR protocol is presented in Section 3. Simulations with analysis are presented in Section 4. Finally, conclusions are drawn in Section 5.

## 2. System Model

Figure 1 shows the communication network of CCS-AF with eavesdroppers and the scheme of the PSR protocol. This network contains $N$ source nodes $(S_1, \ldots, S_N)$, $M$ relays $(R_1, \ldots, R_M)$, $Z$ eavesdroppers $(E_1, \ldots, E_Z)$ and one destination $(D)$. In the first time slot, the sources transmit their information to the relays simultaneously with a fixed transmission power $P_S$, thereby, the power shared by each source node is $P_S/N$. In the second time slot, the relays harvest energy from the RF signals to amplify and forward (AF) the information received to the destination. The channel state information (CSI) is known to all legitimate users.



(**a**) (**b**)

**Figure 1.** Schemes of CCS-AF network and PSR protocol. (**a**) CCS-AF network; (**b**) PSR protocol.

The channels in the CCS-AF network are represented as follows. We denote the matrix $\mathbf{H}_{SR} \in \mathbf{R}^{M \times N}$ as the source-to-relay channel matrix; the vector $\mathbf{H}_{DR} \in \mathbf{R}^{M \times 1}$ is the relay-to-destination channel vector; the matrix $\mathbf{H}_{SE} \in \mathbf{R}^{Z \times M}$ is the source-to-eavesdropper channel matrix. The distances from the sources to relays, from relays to the destination and from sources to eavesdroppers are denoted by $d_{SR}$, $d_{RD}$, and $d_{SE}$, respectively.

To measure the security level of the communication network, the secrecy capacity is usually defined as the maximum difference between the mutual information of the main channels and eavesdropper channels [21], and could be formulated as Equation (1):

$$C_S = \max[I(x;y) - I(x;z)]^+ = (C_D - C_E)^+ \tag{1}$$

in which $C_S$ is the secrecy capacity, $x$ is the input signal at sources, $y$ and $z$ are output signals at destination and eavesdroppers, respectively. $I(x;y)$ is the mutual information of the sources and destination; $I(x;z)$ is the mutual information of the sources and eavesdroppers; $C_D$ is the capacity for the transmission between sources and destination; and $C_E$ is the capacity at eavesdropper.

*CCS-AF Scheme*

In the first time slot, denote $\mathbf{X} = [x_1,\ x_2,\ \ldots,\ x_N]$ as the original signals to be transmitted by the source nodes. The power constraints of the sources and relays are $P_S$ and $P_R$, respectively. The channel fading between sources and relays is $\mathbf{H}_{SR} \in \mathbf{R}^{M \times N}$, where $[\mathbf{H}_{SR}]_{i,j} \sim \mathcal{N}(0, M^{-1})$. This is incoherent with the identity matrix and satisfies the restricted isometry property (RIP) with a high probability as long as $M \geq \mathrm{c} \cdot K \log(N/K)$ [15], where $M$ is the number of relays, $c$ is a small constant, $K$ is the sparsity, $N$ is the number of sources. $\mathbf{H} = \boldsymbol{\alpha}_{SR}\mathbf{H}_{SR}$ is the $M \times N$ transmission matrix of the source-to-relay channels, the matrix $\boldsymbol{\alpha}_{SR}$ represents the path loss the channels. The element $\alpha_{SR}^{i,j}$ indicates the path loss from the $j$th source node to the $i$th relay and can be calculated as $\alpha_{SR}^{i,j} = d_{S_j\ R_i}^{-u/2}$, where $d_{S_j\ R_i}$ is the distance between the $S_j$ and $R_i$, and $\mu$ is the path loss component. The signals received by the relays is represented by $\mathbf{Y}_R = \mathbf{H}\cdot\mathbf{X} + \mathbf{N}_0$, where $\mathbf{N}_0 \in \mathbf{R}^{M\times 1}$ is an additive white Gaussian noise (AWGN) vector with variance $\sigma_{n_0}^2$.

In the second time slot, the selected relays cooperate to amplify and forward the received signals to the destination. $\mathbf{H}_{RD} \in \mathbf{R}^M$ indicates the channel between relays and the destination, then $\mathbf{H} = \boldsymbol{\alpha}_{RD}\mathbf{H}_{RD}$ is the transmission matrix between relays and destination, and $\boldsymbol{\alpha}_{RD}$ is the path loss of the relay-to-destination channels. Therefore, the signal received at the destination could be represented by Equation (2):

$$\mathbf{Y}_D = \boldsymbol{\beta}\cdot\mathbf{G}\cdot\mathbf{Y}_R + \mathbf{W}_0 = \boldsymbol{\beta}\cdot\mathbf{G}(\mathbf{H}\cdot\mathbf{X} + \mathbf{N}_0) + \mathbf{W}_0 \tag{2}$$

where $\boldsymbol{\beta}$ is a diagonal matrix, the entry $\beta_{ii} = \sqrt{\frac{P_R/M}{\frac{P_S}{N}\cdot\sum_{j=1}^{N}\left|A_{ij}\right|^2 + \sigma_{\mathrm{n}_0}^2}}$ in $\boldsymbol{\beta}$ denotes the amplification coefficient of the $i$th relay. The noise between relays and destination is $\mathbf{W}_0 \in \mathbf{R}^{M\times 1}$, which is a AWGN vector with variance $\sigma_{w_0}^2$.

Let $\boldsymbol{\Phi} = (\boldsymbol{\beta}\cdot\mathbf{G})\cdot\mathbf{H}$, then Equation (2) can be rewritten as $\mathbf{Y}_D = \boldsymbol{\Phi}\cdot\mathbf{X} + (\boldsymbol{\beta}\cdot\mathbf{G}\mathbf{N}_0 + \mathbf{W}_0)$. As the channel matrix $\mathbf{H}$ satisfies the RIP property and $\boldsymbol{\beta}\cdot\mathbf{G}$ is a diagonal matrix, therefore, $\boldsymbol{\Phi}$ satisfies the requirements of the RIP property and can be used as the secure measurement matrix to encrypt the transmitted information. The channel matrix from sources to the destination is the compressive matrix in CS theory, and also it is the measurement matrix.

The destination recovers the source signals $\mathbf{X}$ from $\mathbf{Y}_D$ by solving the convex optimization problem:

$$\min||\hat{\mathbf{X}}||_{l_1} \text{ s.t. } ||\mathbf{Y}_D - \boldsymbol{\Phi}\hat{\mathbf{X}}||_{l_2} \le \varepsilon \tag{3}$$

where $\varepsilon$ is the upper bound of the noise magnitude and $\hat{\mathbf{X}}$ are the signals reconstructed at the destination.

## 3. Power Splitting Relaying Protocol

In the power splitting relaying protocol, the total transmission time $T$ from sources to the destination is divided into two equal parts, i.e., $T/2$. During the first slot, the relays harvest energy and process information simultaneously. The RF power $P$ received at each relay is divided by the power splitting ratio $\rho$ $(0 < \rho < 1)$, which means $\rho P$ is allocated for EH and $(1-\rho)P$ is used for information processing. In the second slot, the relays amplify and forward the received signal to the destination using the harvested energy. The channel matrix between the sources and relays is:

$$\mathbf{H} = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots \mathbf{h}_M]^{\mathrm{T}} \tag{4}$$

where $\mathbf{h}_i = \left[h_{i,1}, h_{i,2}, \ldots, h_{i,j}, \ldots, h_{i,N}\right]$, $1 \le i \le M$, and $h_{i,j}$ $(1 \le j \le N)$ indicates the channel between $S_j$ and $R_i$.

In the first slot, denoting the signals received by the EH receiver as $\mathbf{Y}_{RH}$, then it can be expressed as Equation (5):

$$\mathbf{Y}_{RH} = \sqrt{\rho}(\mathbf{H}\mathbf{X} + \mathbf{N}_0) \tag{5}$$

The energy harvested by the EH receiver is as follows:

$$E_{R_i} = \frac{T}{2}\eta\rho\left[\frac{P_S}{N}||\mathbf{h}||_i^2 1 + \sigma_{n_0}^2\right] \tag{6}$$

Thereby, the power of the harvested energy at $R_i$ could be obtained and shown in Equation (7):

$$P_{R_i} = \eta\rho\left[\frac{P_S}{N}||\mathbf{h}||_i^2 1 + \sigma_{n_0}^2\right] \tag{7}$$

Denoting he signals at the information receiver as $\mathbf{Y}_{RI}$, then it can be computed as Equation (8).

$$\mathbf{Y}_{RI} = \sqrt{(1-\rho)}(\mathbf{HX} + \mathbf{N}_0) \tag{8}$$

Now, the signals received at the eavesdroppers in the first slot can be written as:

$$\mathbf{Y}_E = \mathbf{H}_{SE}\mathbf{X} + \mathbf{N}_0 \tag{9}$$

In the second slot, the signal transmitted by the relays is $\mathbf{X}_R = \boldsymbol{\beta}\mathbf{Y}_R$, where $\boldsymbol{\beta}$ is a diagonal matrix. The diagonal elements in $\boldsymbol{\beta}$ can be represented as Equation (10):

$$\beta_{ii} = \sqrt{\frac{P_{R_i}}{(1-\rho)\left(\frac{P_S}{N} \cdot ||\mathbf{h}||_i^2 1 + \sigma_{n_0}^2\right)}} \tag{10}$$

where $\beta_{ii}$ is the amplification coefficient of the $i$th relay. The noise between relays and destination is $\mathbf{W}_0 \in \mathbf{R}^{M\times 1}$, which is a AWGN vector with variance $\sigma_{w_0}^2$.Thereby, the signal received at the destination can be formulated as:

$$\mathbf{Y}_{\mathrm{D}} = \boldsymbol{\beta G}\mathbf{Y}_{\boldsymbol{RI}} + \mathbf{W_0} = \sqrt{\boldsymbol{(1-\rho)}}\, \boldsymbol{\beta G}(\mathbf{HX} + \mathbf{N_0}) + \mathbf{W_0} \tag{11}$$

The secrecy capacity is the difference between the capacity of main channels and the eavesdropper channels, and could be calculated as the sum of the reliable information received by the destination. In order to obtain the channel capacity, we transform the $M \times N$ channel matrix $\mathbf{H}$ to a $M \times 1$ parallel channel vector by using singular value decomposition (SVD) approach [16]. Let $\mathbf{H} = \boldsymbol{U\Lambda}\mathbf{V^H}$, then we get $\mathrm{Y}_{RI} = \sqrt{(1-\rho)}\big(\boldsymbol{U\Lambda}\mathbf{V^H}\cdot\mathbf{X} + \mathbf{N}_0\big)$, where $\boldsymbol{\Lambda}$ is a diagonal matrix, $\mathbf{U} \in \mathbf{C}^{M\times M}$ and $\mathbf{V}\in \mathbf{C}^{M\times N}$ are both unitary matrixes, and $\mathbf{V^H}$ is the conjugate transpose of $\mathbf{V}$. Let $\mathbf{Y}'_{RI} = \mathbf{U^H}\cdot\mathbf{Y}_{RI}$, $\mathbf{X}' = \mathbf{V^H}\cdot\mathbf{X}$, $\mathbf{N}'_0 = \mathbf{U^H}\cdot\mathbf{N}_0$, then the information received by relays is equivalent to $\mathbf{Y}'_{RI} = \sqrt{(1-\rho)}(\boldsymbol{\Lambda X'} + \mathbf{N}'_0)$. Thereby, Equation (11) can be rewritten as:

$$\mathbf{Y}'_{\boldsymbol{D}} = \boldsymbol{\beta G}\mathbf{Y}'_{\boldsymbol{RI}} + \mathbf{W_0} = \sqrt{\boldsymbol{(1-\rho)}}\, \boldsymbol{\beta G\Lambda X} + \sqrt{\boldsymbol{(1-\rho)}}\boldsymbol{\beta G}\mathbf{N}'_{\mathbf{0}} + \mathbf{W_0} \tag{12}$$

According to the property of the unitary matrix, $\mathbf{U}$ and $\mathbf{V}$ won't change the power of $\mathbf{Y}_{\mathrm{RI}}$, $\mathbf{X}$, $\mathbf{N}_0$, which means $\mathrm{P}_{\mathrm{X}'} = P_{\mathrm{X}}$, $\mathrm{P}_{\mathrm{N}'_0} = \mathrm{P}_{\mathrm{N}_0}$, $\mathrm{P}_{\mathrm{Y}'_R} = \mathrm{P}_{\mathrm{Y}_R}$. Thereby, the power matrixes of the received information and signal noise at the destination can be easily obtained after SVD, and could be formulated as Equations (13) and (14):

$$P_i = \frac{(1-\rho)P_S}{N}\cdot|G_{ii}|^2\beta_{ii}^2\Lambda_i^2 \tag{13}$$

$$\sigma_i^2 = \sigma_{w_0}^2 + (1-\rho)\sigma_{n_0}^2|G_{ii}|^2\beta_{ii}^2 \tag{14}$$

where $i$ indicates the $i$th parallel Gaussian channel, $\Lambda_i$ is the $i$th diagonal entry of $\boldsymbol{\Lambda}$.

Then the channel capacity $C$ of the main channel could be computed by Equation (5):

$$\begin{aligned} C &= \frac{1}{2}\sum_{i=1}^{M}\log_2\left(1 + P_i/\sigma_i^2\right) \\ &= \frac{1}{2}\sum_{i=1}^{M}\log_2\left(1 + \frac{\frac{P_S}{N}\cdot|G_{ii}|^2\Lambda_i^2}{\frac{\sigma_{w_0}^2}{(1-\rho)\beta_{ii}^2} + \sigma_{n_0}^2|G_{ii}|^2}\right) \\ &= \frac{1}{2}\sum_{i=1}^{M}\log_2\left(1 + \frac{\frac{P_S}{N}\cdot|G_{ii}|^2\Lambda_i^2}{\frac{\sigma_{w_0}^2}{\eta\rho} + \sigma_{n_0}^2|G_{ii}|^2}\right) \end{aligned} \tag{15}$$

in which, $\sigma_{n_0}^2$ and $\sigma_{w_0}^2$ are the noise powers of two time slots.

The signal received by eavesdropper $E_t$ could be expressed as:

$$\mathbf{Y}_{E_t} = \mathbf{B}_t\mathbf{X} + \mathbf{N}_{E_t} \tag{16}$$

where $\mathbf{B}_t$ is the channel matrix between the sources and $E_t$, $\mathbf{N}_{E_t}$ is the noise at $E_t$. The power of the signals and noise received by $E_t$ is $P_t^e = \frac{P_S}{N} \cdot |B_{j,t}|^2$ and $\sigma_{E_t}^2$, respectively.

The channel capacity of the eavesdropper channel (from $S_j$ to $E_t$) is:

$$C_{j,t}^e = \frac{1}{2}\log_2\left(1 + \frac{\frac{P_S}{N} \cdot |B_{j,t}|^2}{\sigma_{E_t}^2}\right) \tag{17}$$

where $B_{j.t}$ is the path loss between $S_j$ and $E_t$. The security loss caused by the eavesdroppers is as follows:

$$C_E = \sum_{j=1}^{N} C_j^e \tag{18}$$

where $C_j^e = \max\,(\hat{C}_{j,1}^e, \ldots, \hat{C}_{j,t}^e, \ldots, \hat{C}_{j,Z}^e)$, and $\hat{C}_{j,t}^e$ $(1 \le t \le Z)$ indicates the capacity of the channel from $S_j$ to $E_t$. Thereby, the secrecy capacity of the CCS-AF network can be obtained by Equation (1) and represented as $C_S = C - C_E$.

Our scheme can achieve perfect secrecy under the condition of bounded computation capability of eavesdroppers.

## 4. Simulations and Analysis

In this section, we consider a CCS-AF wireless network with 15 sources, four relays, two eavesdroppers and one destination. The parameters are set as follows: the path loss of the channels is $\mu = 4$; the noises are assumed to be Gaussian with variances $\sigma_{n_0}^2 = \sigma_{w_0}^2 = 10$ dbm. In order to simplify the simulation and study the impact of the relays' position on the system secrecy capacity, a simple model is shown in Figure 2, where all nodes are set on a straight line. All the source nodes are considered to be located at the same position, thereby the effect on the secrecy capacity caused by the distances among the source nodes is ignored. The relays and eavesdroppers are treated in the same way. The distance between sources and destination are normalized to a unit value, thereby, the coordinates of the source nodes, relays, eavesdroppers, and destination are (0, 0), $(d_{SR}, 0)$, $(d_{SE}, 0)$ and (1, 0), respectively.

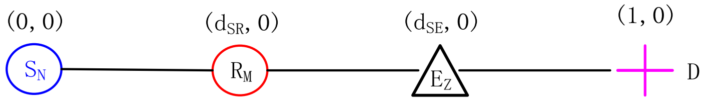


**Figure 2.** Simplified model of CCS-AF network.

In the first simulation, we study how the secrecy capacity changes with $d_{SR}$. The power splitting ratio $\rho$ is 0.5, the energy conversion efficiency $\eta$ is 1, and $d_{SR}$ varies from 0 to 1. Three conditions that the $P_S$ is $10^{-4}$ W, $10^{-3}$ W and $10^{-2}$ W, are considered, respectively. Figure 3 shows the simulation results. The secrecy capacity under each $P_S$ decreases monotonously and approaches to 0 with the increase of $d_{SR}$. This could be explained that when $d_{SR}$ increases, the EH power and information received by relays decrease rapidly, which obeys Equations (6) and (8). The reason for why does the network achieves the higher secrecy capacity when $P_S = 10^{-3}$ W than the other two conditions will be analyzed in the fourth simulation.

In the second simulation, we study how the secrecy capacity changes with the power-splitting ratio $\rho$ under several conditions of $d_{SR}$. The sources' power is $P_S = 10^{-2}$ W, $\eta = 1$, and $d_{SR}$ is set to

0.3, 0.5 and 0.8, respectively. The secrecy rates of the networks are calculated and plotted in Figure 4. On the one hand, for each situation of $d_{SR}$, the system secrecy capacity with $\rho$ increases first and then decreases, and achieves the highest at a certain point.

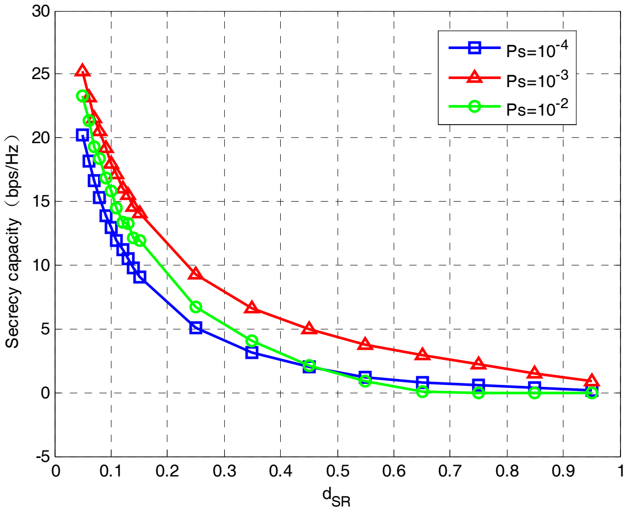


**Figure 3.** Secrecy capacity versus $d_{SR}$ when $M = 4$, $\eta = 1$, and $\rho = 0.5$.

This is because when $\rho$ is small, the relays get little power for energy harvesting, which makes the transmission power at relays un-enough and results in lower secrecy capacity. In contrary, when $\rho$ is too large, the power for the information transmission will be too little and much harvested power will be wasted. This could well explain that the secrecy capacity achieves the highest when $\rho$ takes a moderate value. The reason for why the model with smaller $d_{SR}$ could get higher secrecy rate has been explained in the first simulation.

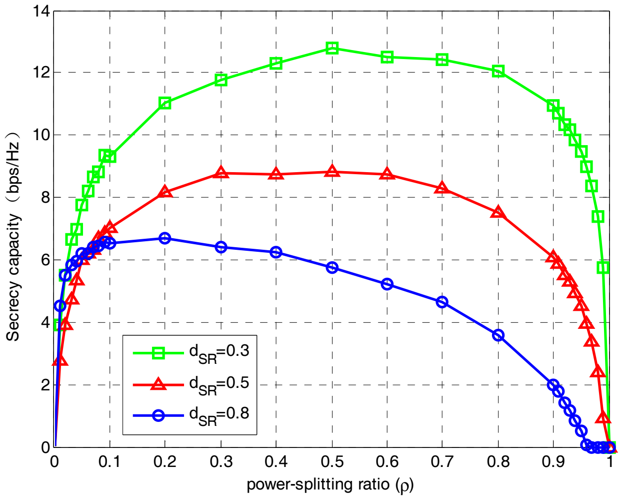


**Figure 4.** Secrecy capacity versus $\rho$ with various values of $d_{SR}$.

In the third simulation, we study the change of the secrecy capacity with the energy conversion efficiency $\eta$. $\eta$ varies from 0 to 1, $\rho$ is set to 0.5, and the other parameters are set the same as the first simulation. The simulation results are shown in Figure 5. It is obvious that for each $d_{SR}$, the secrecy capacity of the EH-AF protocol increases with $\eta$, and approaches to a constant when $\eta$ is high enough. This is easy to explain, higher energy conversion efficiency means higher energy could be obtained without improving the power splitting ratio. Thereby more energy can be obtained to transmit the received information to the destination. We can also see that the secrecy rates increase slowly with $\eta$ when $\eta$ is higher than 0.7, 0.5 and 0.1 under the conditions that $d_{SR}$ is 0.3, 0.5 and 0.8, respectively. This phenomenon has an important instructive meaning in engineering, as it means we do not have to seek EH devices with high $\eta$ with an unnecessarily high economic cost.

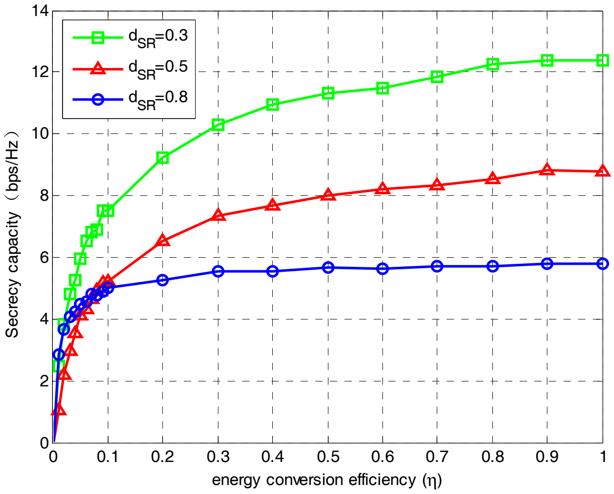


**Figure 5.** Secrecy capacity versus $\eta$ with different $d_{SR}$ when $M$ = 4, and $\rho = 0.5$.

The effect of relay number on the system secrecy capacity is studied in the fourth simulation, and three scenarios are considered, where $P_S$ is set to $10^{-4}$ W, $10^{-3}$ W, and $10^{-2}$ W, respectively. $d_{SR} = 0.5$, $\eta = 1$, $\rho = 0.5$, and the relay number varies from 3 to 13. The simulation result is shown in Figure 6. It could be seen that when $P_S$ is large enough, the model that contains more relays will presents a significant advantage. As shown in Figure 6, when the relay number $M > 6$, the higher $P_S$ is, the higher secrecy capacity will be obtained. This is because the number of eavesdroppers is fixed, though higher $P_S$ will improve the channel capacity of eavesdroppers, but the increased relays will obtain more secrecy capacity for the main channels under enough energy. Thereby higher secrecy capacity could be obtained. It could be seen in Figure 6 that when the relay number $M = 4$, the network achieves the highest secrecy capacity when $P_S = 10^{-3}$ W, which could explain why the network achieves the highest secrecy rate when $P_S = 10^{-3}$ W in the first simulation.

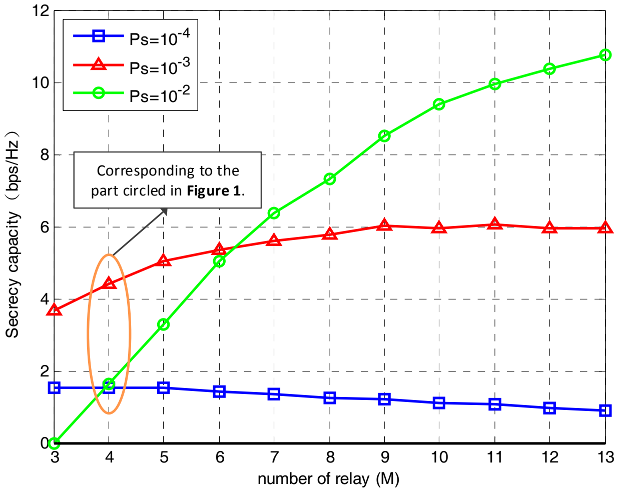


**Figure 6.** Secrecy capacity versus $M$ with different $P_S$ when $\eta = 1$, and $\rho = 0.5$.

In the last simulation, we study the change of secrecy capacity with $P_S$. To test the efficiency of the PSR protocol sufficiently, the AF protocols in [28] is taken as a comparison. In both approaches, the $P_S$ varies from $10^{-3}$ W to $10^{-2}$ W, and the simulation is operated under three conditions where $d_{SR}$ is 0.3, 0.5, and 0.8, respectively. The total power in the AF protocol is $P = 10^{-2}$ W, and the energy conversion efficiency in PSR protocol is $\eta = 1$. Figure 7 presents the simulation results. Under each circumstance of $d_{SR}$, the secrecy capacity of PSR increases with $P_S$ and approaches to a constant. As we can see, when $d_{SR} = 0.3$, the PSR protocol in this paper always outperforms the AF protocol. When $d_{SR} = 0.5$ and 0.8, the PSR protocol performs the better only when $P_S$ is higher than $2 \times 10^{-3}$ W and $8.5 \times 10^{-3}$ W, respectively. Though the PSR protocol is not so good as the AF protocol in some stages when $d_{SR}$ is 0.5 and 0.8, the inferiority is very small. This means the PSR protocol proposed in this paper could get a similar or much higher secrecy capacity by consuming less power than AF, though this advantage will be weakened with the increase of $d_{SR}$.

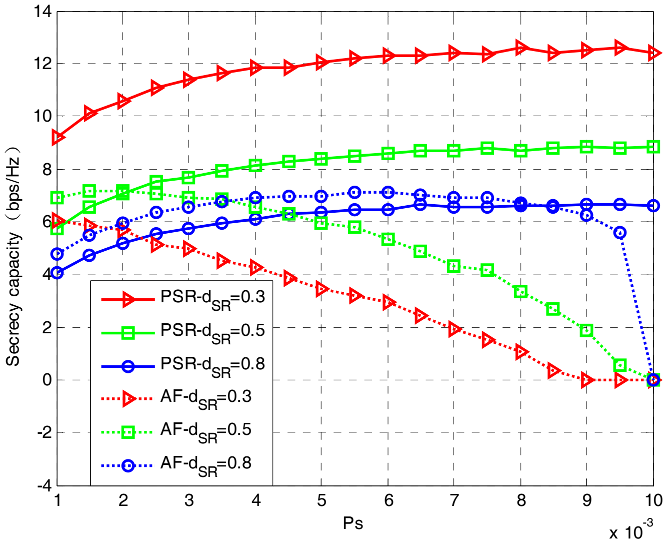


**Figure 7.** Secrecy capacity versus the $P_S$ when total power $P = 10^{-2}$ W and $M = 4$.

## 5. Conclusions

CS technology is a novel approach to enhance the physical-layer security of cooperative communication networks in the presence of eavesdroppers, and EH can help relays work in continuous mode in specific environments. In this paper, we analyze the secrecy capacity of the CCS-AF wireless networks with EH relays using the PSR protocol. Five simulations revealed how the secrecy capacity reacts to the change of some key factors in this network, and verified the EH is to be capable of improve the energy utilization efficiency. Thus, they have great guiding significance for researchers to obtain the highest secrecy capacity or design the most appropriate solution in related researches. Our future work will focus on how to improve the physical-layer security of multi-hop communication networks through applying EH approaches.

**Acknowledgments:** This work is supported by the National Natural Science Foundation of China under Grant No. 61571323.

**Author Contributions:** Shuai Chang and Xiaomei Fu conceived the study; Jialun Li performed the experiments; Shuai Chang and Jialun Li analyzed the data; Shuai Chang, Jialun Li, and Liang Zhang wrote the paper.

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

## References

1. Khodakarami, H.; Lahouti, F. Link adaptation for physical layer security over wireless fading channels. *IET Commun.* **2012**, *6*, 353–362. [CrossRef]
2. Zhuang, W.; Ismail, M. Cooperation in wireless communication networks. *IEEE Wirel. Commun.* **2012**, *19*, 10–20. [CrossRef]
3. Zou, Y.; Wang, X.; Shen, W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2099–2111. [CrossRef]
4. Jing, Y.; Jafarkhani, H. Single and multiple relay selection schemes and their achievable diversity orders. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1414–1423. [CrossRef]
5. Lai, L.; El Gamal, H. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theor.* **2008**, *54*, 4005–4019. [CrossRef]
6. Zhang, R.; Song, L.; Han, Z.; Jiao, B. Physical layer security for two-way untrusted relaying with friendly jammers. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3693–3704. [CrossRef]
7. Zhang, J.; Gursoy, M.C. Relay beamforming strategies for physical-layer security. In Proceedings of the 2010 44th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 17–19 March 2010; pp. 1–6.
8. Ju, P.; Song, W.; Zhou, D. Survey on cooperative medium access control protocols. *IET Commun.* **2013**, *7*, 893–902. [CrossRef]
9. Popovski, P.; Simeone, O. Wireless secrecy in cellular systems with infrastructure-aided cooperation. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 243–256. [CrossRef]
10. Nasir, A.A.; Zhou, X.; Durrani, S.; Kennedy, R.A. Relaying protocols for wireless energy harvesting and information processing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 3622–3636. [CrossRef]
11. Zhou, X.; Zhang, R.; Ho, C.K. Wireless information and power transfer: Architecture design and rate-energy tradeoff. *IEEE Trans. Commun.* **2013**, *61*, 4754–4767. [CrossRef]
12. Varshney, L.R. Transporting information and energy simultaneously. In Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT), Toronto, ON, Canada, 6–11 July 2008; pp. 1612–1616.
13. Zhang, M.; Liu, Y. Energy harvesting for physical-layer security in OFDMA networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 154–162. [CrossRef]
14. Zhang, R.; Ho, C.K. MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 1989–2001. [CrossRef]
15. Salem, A.; Hamdi, K.A.; Rabie, K.M. Physical layer security with RF energy harvesting in AF multi-antenna relaying networks. *IEEE Trans. Commun.* **2016**, *64*, 3025–3038. [CrossRef]
16. Son, P.N.; Kong, H.Y. Cooperative communication with energy-harvesting relays under physical layer security. *IET Commun.* **2015**, *9*, 2131–2139. [CrossRef]
17. Hoang, T.M.; Duong, T.Q.; Vo, N.S.; Kundu, C. Physical layer security in cooperative energy harvesting networks with a friendly jammer. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 174–177. [CrossRef]
18. Lei, H.; Xu, M.; Ansari, I.S.; Pan, G.; Qaraqe, K.A.; Alouini, M.S. On Secure Underlay MIMO Cognitive Radio Networks with Energy Harvesting and Transmit Antenna Selection. *IEEE Trans. Green Commun. Netw.* **2017**, *1*, 192–203. [CrossRef]
19. Patterson, S.; Eldar, Y.C.; Keidar, I. Distributed compressed sensing for static and time-varying networks. *IEEE Trans. Signal Process.* **2014**, *62*, 4931–4946. [CrossRef]
20. Martinez, J.; Mejia, J.; Mederos, B. Compress sensing for wireless sensor networks using gossip pairwise algorithm and optimization algorithms. In Proceedings of the IEEE Ecuador Technical Chapters Meeting, Guayaquil, Ecuador, 12–14 October 2016; pp. 1–5.
21. Candes, E.J.; Romberg, J.K.; Tao, T. Stable signal recovery from incomplete and inaccurate measurements. *Commun. Pure Appl. Math.* **2006**, *59*, 1207–1223. [CrossRef]
22. Rachlin, Y.; Baron, D. The secrecy of compressed sensing measurements. In Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, USA, 23–26 September 2008; pp. 813–817.
23. Mayiami, M.R.; Seyfe, B.; Bafghi, H.G. Perfect secrecy using compressed sensing. *Mathematics* **2010**. [CrossRef]

24. Agrawal, S.; Vishwanath, S. Secrecy using compressive sensing. In Proceedings of the 2011 IEEE Information Theory Workshop, Paraty, Brazil, 16–20 October 2011; pp. 563–567.
25. Reeves, G.; Goela, N.; Milosavljevic, N.; Gastpar, M. A compressed sensing wire-tap channel. In Proceedings of the 2011 IEEE Information Theory Workshop, Paraty, Brazil, 16–20 October 2011; pp. 548–552.
26. Barcelo-Llado, J.E.; Morell, A.; Seco-Granados, G. Amplify-and-forward compressed sensing as an energy-efficient solution in wireless sensor networks. *IEEE Sens. J.* **2014**, *14*, 1710–1719. [CrossRef]
27. Barcelo-Llado, J.E.; Morell, A.; Seco-Granados, G. Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 839–850. [CrossRef]
28. Fu, X.; Cui, Y. Multi-source and multi-relay cooperative system based on compressed sensing. *Electron. Lett.* **2015**, *51*, 1828–1830. [CrossRef]