This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

Adaptive Wireless-powered Relaying schemes with Cooperative Jamming for Two-hop Secure Communication

Kisong Lee, *Member, IEEE*, Jun-Pyo Hong, *Member, IEEE*, Hyun-Ho Choi, *Member, IEEE*, and Marco Levorato, *Member, IEEE*

***Abstract*—A two-hop relay network is considered, in which an eavesdropper can overhear the relaying signal. To prevent the eavesdropper from decoding this signal, a destination transmits a jamming noise while a source transmits the data signal to the relay. At the same time, the relay can harvest energy from both the source signal and the jamming noise, and use this harvested energy to forward the received signal to the destination. In such a wireless-powered relay system with cooperative jamming, we propose two adaptive relaying schemes based on power splitting and time switching techniques. In the proposed power splitting-based relaying (PSR) and time switching-based relaying (TSR) schemes, the relay controls the power splitting ratio (ρ) and time switching ratio (α), respectively, in order to achieve a balance between signal processing and energy harvesting. We find analytically the optimal values of ρ and α in each scheme to maximize the secrecy capacity under the assumption of high signal-to-noise ratio. Interestingly, although the eavesdropper's channel state information (CSI) is used in the derivation of the optimal control parameters (ρ and α), they are shown not to be affected by the eavesdropper's CSI in a high SNR regime. This implies that the proposed schemes can be effective even for practical environments where there is no eavesdropper's CSI. Furthermore, simulation results show that they well coincide with the exact solutions in practical environments even though the closed-form solutions are obtained with a high SNR assumption. Moreover, the comparisons of PSR and TSR in various scenarios show that the two relaying schemes have complementary performances depending on the network conditions. Specifically, PSR achieves greater secrecy capacity than TSR when the channel condition is unfavourable to the eavesdropper for wiretapping.**

***Index Terms*—Energy harvesting, physical layer security, secrecy capacity, cooperative jamming, power splitting, time switching**

I. Introduction

Recent technological advances in smart devices capable of wireless communication have been key in speeding up the realization of the Internet of Things (IoT). As an essential building block for IoT, mobile communication systems are required to fulfill additional performance indicators: long-range communication and long device life time [1]. For example, NarrowBand IoT (NB-IoT), Long range (LoRa), and Sigfox share the same key design objectives of long-range communication and long device lifetime although these systems have different specifications based on different techniques. On top of these design objectives, the communication security is considered as an essential requirement due to their wide scopes encompassing commercial, industrial, governmental, and military applications [2], [3]. Considering the limited hardware, low-complexity, and severe energy constraints of IoT devices, physical layer security methods are attracting great attention as alternatives to the conventional cryptography-based methods in IoT systems [4]–[9].

In the presence of an eavesdropper, 'secrecy capacity' is defined as the difference between the link capacity from the source to the destination (i.e., the main link) and that from the source to the eavesdropper (i.e., the wiretap link), such that a negative secrecy capacity indicates that the eavesdropper can successfully interpret the source signal [4]. One of the most common strategies used to increase the secrecy capacity is cooperative jamming [5]–[9], where friendly jammers transmit jamming signals to prevent the eavesdropper from decoding information from the source signal. In [5], the beamforming vector of multiple relays for cooperative jamming was optimized to maximize the secrecy rate with the power constraint of an individual relay. In [6], a joint cooperative beamforming and jamming strategy was studied to try to improve the security of cooperative relay networks without the instantaneous channel state information (CSI) of the eavesdropper. In [7], optimal relay selection and power allocation for the data signal and the jamming noise were jointly considered to maximize secrecy rate, while in [8], the jamming noise from the destination was considered, and jamming power allocation strategies were proposed, to minimize the outage probability of the secrecy rate. In [9], a criterion to select intermediate nodes as relays for forwarding messages or jammers for broadcasting noise was investigated to minimize the secrecy outage probability in cooperative wireless networks.

At the same time, the energy deficiency of battery-powered devices remains a bottleneck in the improvement of the operational time and reliability of IoT. To address the problem of energy shortage, energy harvesting (EH) from radio frequency (RF) signals is suggested as a promising solution. A number of studies of RF EH have been investigated by various research groups [10]–[16]. In [10]–[12], the concept of simultaneous

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2016R1C1B1016261) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2016R1C1B2012173). *(Corresponding author: Hyun-Ho Choi.)*

K. Lee is with the School of Information and Communication Engineering, Chungbuk National University, Cheongju, 28644, Korea (e-mail: kslee851105@gmail.com).

J.-P. Hong is with the Department of Information and Communications Engineering, Pukyoung National University, Busan, 48513, Korea (e-mail: jp_hong@pknu.ac.kr).

H.-H. Choi is with the Department of Electrical, Electronic and Control Engineering, and the Institute for Information Technology Convergence, Hankyong National University, Anseong 17579, Korea, (e-mail: hhchoi@hknu.ac.kr).

M. Levorato is with the Donald Bren School of Information and Computer Sciences, University of California at Irvine, Irvine, CA 92617, USA (e-mail: levorato@uci.edu)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

wireless information and power transfer (SWIPT) was advanced, and two mode switching techniques of *opportunistic time switching* and *dynamic power splitting* were proposed. Based on this concept, several relay schemes capable of RF EH have been investigated [13]–[16]. In [13], two amplify-and-forward (AF) relaying schemes based on time switching and power splitting were proposed to perform both EH and information processing at the relay, and the outage probability and the ergodic capacity were then analyzed. In [14], time switching-based AF and decode-and-forward (DF) relaying schemes were considered, and an achievable throughput for each scheme was derived. In [15], a 'harvest-and-forward' relaying strategy, which optimizes the antenna selection and power splitting techniques jointly, was proposed to improve the achievable rate for a wireless-powered relay with multiple antennas. Moreover, a hybrid scheme combining power splitting and time switching was also suggested to maximize network throughput for both AF and DF relaying [16].

Because of security vulnerability and energy scarcity at the relay in IoT, there have been some attempts recently to consider both physical layer security and EH in relay networks [17]–[21]. In [17], a wireless-powered jammer was considered for secure communication between source and destination in the presence of an eavesdropper, and the rate parameters regarding the codeword and secret information were optimized to maximize throughput subject to a secrecy outage probability constraint. In [18], multiple wireless-powered jammers were used to guarantee secure two-hop relay networks, and the covariance matrices for cooperative jamming and the beamforming matrix for AF relaying were jointly optimized. In [19], an 'accumulate-and-jam' scheme using a wireless-powered full-duplex jammer was proposed, and secrecy performance metrics were investigated. In [20], EH-enabled AF relays performing both relaying and jamming were considered, and the optimal beamforming vectors were derived to maximize the achievable secrecy rate. In [21], an untrusted relay capable of EH was considered, and destination-assisted jamming was applied to maintain information confidentiality from the relay node. Both the secrecy outage probability and the ergodic secrecy rate were derived analytically.

In this paper, we propose two wireless-powered two-hop relaying schemes for improving secrecy capacity in the presence of an eavesdropper. The proposed schemes are based on two popular schemes for SWIPT problem: power splitting and time switching, and additionally considers the jamming noise transmission at the destination to prevent the eavesdropper from decoding the relaying signal. This jamming noise can also be utilized for harvesting energy at the wireless-powered relay. Since our system model is based on the well-known SWIPT schemes, it is easy to see the effect of security constraint on the optimal control parameters (power splitting ratio and time switching ratio) and the secrecy performance through the comparisons with the conventional schemes. In addition, to the best of our knowledge, this is the first work that derives the closed-form expressions of optimal power splitting ratio and time switching ratio in a secure relaying model based on both RF energy harvesting and jamming noise. Although there have been several previous works on the secure relay communications with RF energy harvesting [17]–[21], they have not explicitly explained the behaviors and performances of the schemes in closed-form expressions. The main contributions of the paper can be summarized as follows.

- We propose two relaying schemes for a wireless-powered relay in the presence of an eavesdropper: *power splitting-based relaying* (PSR) and *time switching-based relaying* (TSR). They adaptively control the power splitting ratio (ρ) and time switching ratio (α), respectively, by considering EH, signal processing, and eavesdropping.
- For both proposed schemes, we prove the concavity of the secrecy capacity with respect to the control parameters and derive the closed-form expressions of the optimal control parameters for maximizing secrecy capacity under the high signal-to-noise ratio (SNR) assumption.[1]
- Numerical results demonstrate that the proposed PSR and TSR schemes using the optimized values of ρ and α achieve near-optimal performance in terms of secrecy capacity. Notably, it is revealed that the optimal ρ and α do not depend on the relay-to-eavesdropper link in a high SNR regime, which means that near-optimal secrecy capacity can be achieved regardless of the location of the eavesdropper. Furthermore, intensive simulations in various scenarios reveal that the two proposed relaying schemes can be used complementarily according to the network environments.

The remainder of this paper is organized as follows. In Section II, we present the system model of the considered relay network. In Sections III and IV, we describe the proposed PSR and TSR schemes, we obtain the optimal values of ρ and α analytically, and we verify their optimality in terms of the secrecy capacity. In Section V, we compare the proposed PSR and TSR schemes and investigate their behaviors in various scenarios. Finally, we set out our conclusions in Section VI.

II. System Model

We consider a two-hop relay network consisting of a source, a relay, a destination, and an eavesdropper, as shown in Fig. 1. We consider a scenario where the eavesdropper sets the relay as a target and wiretaps the transmit signal of the relay with its directional antenna. Since the directional antenna provides a high receive sensitivity for the direction of the relay but a low sensitivity for the other directions, the eavesdropper cannot receive the signal from the source. For this reason, the source-to-eavesdropper and destination-to-eavesdropper links are ignored in the system model. Such secure relay network model has also been considered in [8], [9], [18], [20]. The channel gains for source-to-relay, relay-to-destination, and relay-to-eavesdropper links are denoted by h_{sr}, h_{rd}, and h_{re}, respectively. Here, we assume that h_{sr} and h_{rd} can be known at the relay through the channel estimation because they are the channels of reliable wireless links among legitimate nodes.

[1]The high SNR assumption can be justified by the fact that the energy harvesting technology is generally operated in a high SNR due to its low power sensitivity. For example, information reception and RF energy harvesting work on very different power sensitivity, e.g., -10 dBm for energy harvesters while -60 dBm for information receivers [22], [23].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

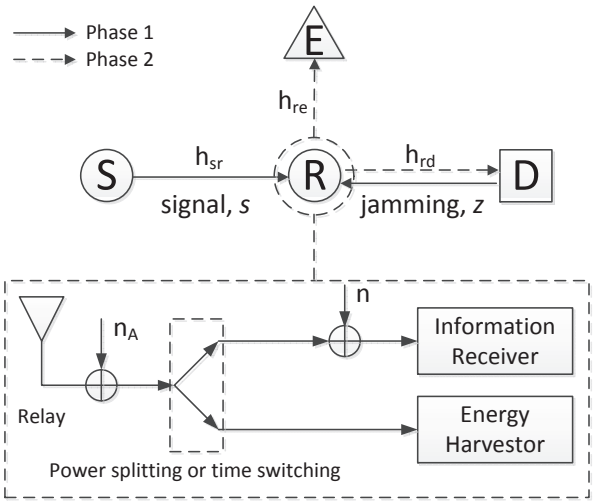


Fig. 1. System model of the considered relay network

However, h_{re} is unknown at the relay because it is difficult to estimate h_{re} in a practical environment where we do not know the location of eavesdropper. The channel reciprocity is assumed. We consider a quasi-static frequency non-selective channel, so that the channel gains remain constant over the block time of T and change independently every block.

The block time T is divided into two phases of the same length [13]–[21].[2] Both the proposed PSR and TSR are based on amplify-and-forward (AF) method, i.e., the relay does not need to decode the source signal and just amplifies and forwards the received signals using the harvested energy. The only difference between them is the way to split the received signal for harvesting energy and transferring data signal, e.g., PSR and TSR split the received signal with respect to power and time, respectively. Both of them follow the procedures given below. During the first phase, the source and destination transmit a data signal s and a jamming noise z, respectively, while the relay receives the data signal s together with the jamming noise z. The relay is assumed to have not enough power supply for transmission. Hence, the relay harvests energy from some power/time portion of the received signal and amplifies the remaining portion of the received signal with the harvested energy in the first phase. During the second phase, the relay forwards the amplified signal containing s and z using the harvested energy. Although the decoding at the eavesdropper is interfered by the jamming noise z, the destination is able to cancel out z from its received signal by using successive interference cancellation (SIC). Consequently, the jamming noise z only degrades the received signal of the eavesdropper, which has no prior knowledge on z. The differences from the standard SWIPT schemes are the existence of eavesdropper and the jamming signal transmitted by destination. The reason that we have considered simple variations of the standard model is to focus on the effect of eavesdropper in the wireless-powered relay network.

[2]The lengths of two phases can be flexibly determined according to the environments, but the phase length optimization is beyond the scope of this paper.

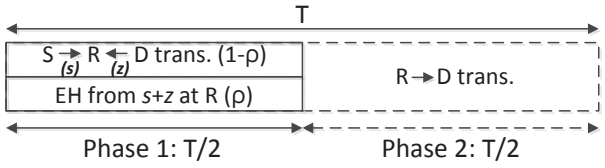


Fig. 2. Power splitting-based relaying scheme

Note that there are two types of noise, namely antenna noise and baseband noise. Antenna noise n_A is generated at the receiving antenna while the baseband noise n is produced at the information detector during the signal processing stage. In general, n_A is much smaller than n and is usually ignored [10], [12]. We assume that the baseband noise in the received signal of each node follows complex Gaussian distribution with zero-mean and variance σ^2, In other words, the baseband noise at the relay n_r, destination n_d, and eavesdropper n_e follows $\mathcal{CN}\left(0, \sigma^2\right)$.

As a performance measure for secure communications, we consider the achievable secrecy capacity [24]. The secrecy capacity is defined as the maximum achievable data rate while preventing the eavesdropper from recovering any information of transmitted signal. Hence, a higher secrecy capacity means that we can successfully transfer more information bits to the destination without any information leakage to the eavesdropper.

III. Power Splitting-based Relaying scheme

A. scheme Description

Fig. 2 illustrates the proposed PSR scheme. During the first phase of length $\frac{T}{2}$, the relay receives information and harvests energy simultaneously from the received RF signal with power splitting technique [12]. In other words, the received RF signal is split into two portions. The portion of ρ is used for harvesting energy and the remaining $1-\rho$ is used for amplifying and forwarding the data signal, $0 \leq \rho \leq 1$. After the RF energy harvesting, the received signal at the relay is represented by

$$y_r = \sqrt{(1-\rho)P_s}h_{sr}s + \sqrt{(1-\rho)P_z}h_{rd}z + n_r \qquad (1)$$

where P_s denotes the transmit power for signal s at the source and P_z denotes the transmit power for jamming noise z at the destination. Here, s and z have a normalized power, i.e., $\mathbb{E}[|s|^2] = \mathbb{E}[|z|^2] = 1$. At the same time, the harvested energy at the relay, E_h, is expressed as

$$E_h = \frac{T\eta\rho(P_s|h_{sr}|^2 + P_z|h_{rd}|^2)}{2} = \frac{T\eta\rho E_r}{2} \qquad (2)$$

where η is an energy conversion efficiency and E_r is defined as $P_s|h_{sr}|^2 + P_z|h_{rd}|^2$.

During the second phase with the remaining $\frac{T}{2}$, the relay forwards the amplified signal using the harvested energy, E_h.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

Thus, the transmitted signal from the relay, x_r, is described as

$$x_r = \frac{\sqrt{P_r}y_r}{\sqrt{(1-\rho)(P_s|h_{sr}|^2 + P_z|h_{rd}|^2) + \sigma^2}} = \frac{\sqrt{P_r}y_r}{\sqrt{(1-\rho)E_r + \sigma^2}} \quad (3)$$

where the denominator $\sqrt{(1-\rho)E_r + \sigma^2}$ is the power constraint factor at the relay, and P_r is the transmission power at the relay, which is given by

$$P_r = \frac{E_h}{T/2} = \eta\rho E_r. \quad (4)$$

Then, the received signal at the destination, y_d, is obtained as

$$\begin{aligned} y_d &= h_{rd}x_r + n_d \\ &= \frac{\sqrt{(1-\rho)P_sP_r}h_{sr}h_{rd}s + \sqrt{P_r}h_{rd}n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} \\ &\quad + \underbrace{\frac{\sqrt{(1-\rho)P_zP_r}h_{rd}^2 z}{\sqrt{(1-\rho)E_r + \sigma^2}}}_{\text{self-cancellation}} + n_d \\ &= \frac{\sqrt{(1-\rho)P_sP_r}h_{sr}h_{rd}s + \sqrt{P_r}h_{rd}n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + n_d \end{aligned} \quad (5)$$

where the part related to the jamming noise, $\frac{\sqrt{(1-\rho)P_zP_r}h_{rd}^2 z}{\sqrt{(1-\rho)E_r+\sigma^2}}$, can be removed by a self-interference cancellation at the destination. Here, we assume that the self-interference cancellation is perfect [8]. On the other hand, the received signal at the eavesdropper, y_e, is represented by

$$\begin{aligned} y_e &= h_{re}x_r + n_e \\ &= \frac{\sqrt{(1-\rho)P_sP_r}h_{sr}h_{re}s + \sqrt{P_r}h_{re}n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} \\ &\quad + \frac{\sqrt{(1-\rho)P_zP_r}h_{rd}h_{re}z}{\sqrt{(1-\rho)E_r + \sigma^2}} + n_e \end{aligned} \quad (6)$$

where the jamming noise z acts as interference to prevent the eavesdropper from decoding s, thereby ensuring secure communication.

B. Optimal Power Splitting Ratio

We seek an optimal power splitting ratio, ρ^*, for maximizing the secrecy capacity. From (5), the SNR at the destination, Γ_d, is obtained as

$$\begin{aligned} \Gamma_d &= \frac{\frac{(1-\rho)P_sP_r|h_{sr}|^2|h_{rd}|^2}{(1-\rho)E_r + \sigma^2}}{\frac{P_r|h_{rd}|^2\sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} \\ &= \frac{\eta\rho(1-\rho)E_rP_s|h_{sr}|^2|h_{rd}|^2}{\eta\rho E_r|h_{rd}|^2\sigma^2 + \sigma^2((1-\rho)E_r + \sigma^2)}. \end{aligned} \quad (7)$$

From (6), the SNR at the eavesdropper, Γ_e, is calculated as

$$\begin{aligned} \Gamma_e &= \frac{\frac{(1-\rho)P_sP_r|h_{sr}|^2|h_{re}|^2}{(1-\rho)E_r + \sigma^2}}{\frac{(1-\rho)P_rP_z|h_{rd}|^2|h_{re}|^2}{(1-\rho)E_r + \sigma^2} + \frac{P_r|h_{re}|^2\sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} \\ &= \frac{\eta\rho(1-\rho)E_rP_s|h_{sr}|^2|h_{re}|^2}{\eta\rho E_r|h_{re}|^2((1-\rho)P_z|h_{rd}|^2 + \sigma^2) + \sigma^2((1-\rho)E_r + \sigma^2)}. \end{aligned} \quad (8)$$

Then, the achievable rates at the destination and the eavesdropper are given by $R_d = \frac{T}{2}\log_2(1+\Gamma_d)$ and $R_e = \frac{T}{2}\log_2(1+\Gamma_e)$, respectively. The achievable secrecy capacity is defined as the difference between R_d and R_e, as follows.

$$\begin{aligned} C_S &\triangleq [R_d - R_e]^+ \\ &= \left[\frac{T}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_e}\right)\right]^+ \quad (9) \\ &\approx \left[\frac{T}{2}\log_2\left(\frac{\Gamma_d}{\Gamma_e}\right)\right]^+ \quad \text{(in high SNR)} \quad (10) \end{aligned}$$

where the approximation is based on the assumption of high SNR (i.e., $\Gamma_d \gg 1$ and $\Gamma_e \gg 1$). Note that we will discuss the effect of this approximation on the performance in detail in sub-section III-C. As shown in (9) and (10), the achievable secrecy capacity is zero if $\Gamma_d \leq \Gamma_e$. This implies that it is unable to ensure the secure communication without any information leakage to the eavesdropper. For this reason, we assume $\Gamma_d > \Gamma_e$ to derive a practically meaningful solution. This condition of $\Gamma_d > \Gamma_e$ can be practically satisfied by using a directional antenna at the relay because the directional antenna provides a high receive sensitivity for the target direction (i.e., toward the destination) than the other directions (i.e., toward the eavesdropper).

Now, we define $\Gamma_s \triangleq \frac{\Gamma_d}{\Gamma_e}$ and find an optimal ρ for maximizing Γ_s instead of C_s in closed-form under the assumption of high SNR. Thus, Γ_s is given by

$$\begin{aligned} \Gamma_s &\triangleq \frac{\Gamma_d}{\Gamma_e} \\ &= \frac{|h_{rd}|^2\{\eta\rho E_r|h_{re}|^2((1-\rho)P_z|h_{rd}|^2 + \sigma^2) + \sigma^2((1-\rho)E_r + \sigma^2)\}}{|h_{re}|^2\{\eta\rho E_r|h_{rd}|^2\sigma^2 + \sigma^2((1-\rho)E_r + \sigma^2)\}} \\ &= \frac{|h_{rd}|^2\{-\rho^2 A + \rho(A+B) + D\}}{|h_{re}|^2\{\rho C + D\}} \end{aligned} \quad (11)$$

where

$$\begin{aligned} A &= \eta E_rP_z|h_{re}|^2|h_{rd}|^2, \\ B &= E_r(\eta|h_{re}|^2 - 1)\sigma^2, \\ C &= E_r(\eta|h_{rd}|^2 - 1)\sigma^2, \\ D &= \sigma^2(E_r + \sigma^2). \end{aligned} \quad (12)$$

The second derivative of Γ_s with respect to (w.r.t.) ρ is calculated as

$$\frac{\partial^2\Gamma_s}{\partial\rho^2} = -\frac{2|h_{rd}|^2D\{A(C+D) + C(B-C)\}}{|h_{re}|^2(\rho C + D)^3}. \quad (13)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

With $A(C+D) = \eta P_z E_r^2 \sigma^2 |h_{re}|^2 |h_{rd}|^2 \left(\eta |h_{rd}|^2 + \frac{\sigma^2}{E_r}\right)$ and $C(B-C) = \eta E_r^2 \sigma^4 \left(\eta |h_{rd}|^2 - 1\right) \left(|h_{re}|^2 - |h_{rd}|^2\right)$, the ratio of these two can be represented by

$$\frac{A(C+D)}{C(B-C)} = \frac{|h_{rd}|^2 P_z}{\sigma^2} \frac{|h_{re}|^2 \left(\eta |h_{rd}|^2 + \frac{\sigma^2}{E_r}\right)}{(\eta |h_{rd}|^2 - 1)\left(|h_{re}|^2 - |h_{rd}|^2\right)}. \quad (14)$$

From the high SNR assumption, e.g., $\frac{|h_{rd}|^2 P_z}{\sigma^2} \gg 1$, it is confirmed that $\left|\frac{A(C+D)}{C(B-C)}\right|$ is greater than 1. This implies that $|C(B-C)|$ is smaller than $A(C+D)$ because $A(C+D)$ is a positive value. Based on the above derivations and the fact that $(\rho C + D) > 0$, we can conclude that $\frac{\partial^2 \Gamma_s}{\partial \rho^2} < 0$, and therefore, Γ_s is a concave function of ρ.

Then, we can find ρ for maximizing Γ_s from the following condition.

$$\frac{\partial \Gamma_s}{\partial \rho} = -\frac{|h_{rd}|^2 \{AC\rho^2 + 2AD\rho - (A+B-C)D\}}{|h_{re}|^2 (\rho C + D)^2} = 0. \quad (15)$$

From the quadratic formula, the solutions of (15) can be obtained as

$$\begin{aligned} \rho^* &= \frac{-AD \pm \sqrt{(AD)^2 + ACD(A+B-C)}}{AC} \\ &= \frac{-AD \pm \sqrt{AD\{A(C+D) + C(B-C)\}}}{AC}. \end{aligned} \quad (16)$$

In (16), $C < 0$ because $\eta |h_{rd}|^2 < 1$ in C. Thus, the following inequality, $A(C+D) < AD$, holds. In addition, $|C(B-C)|$ is rather smaller than $A(C+D)$ as mentioned in (13). In consequence, $\sqrt{AD(A(C+D) + C(B-C))}$ has a value between 0 and AD. Furthermore, $\frac{-AD - \sqrt{AD(A(C+D)+C(B-C))}}{AC}$ is always larger than 1 because $|D| > |C|$ and $C < 0$, while $0 < \frac{-AD + \sqrt{AD(A(C+D)+C(B-C))}}{AC} < 1$. Therefore, ρ^* is finally obtained as

$$\rho^* = \frac{-AD + \sqrt{AD\{A(C+D) + C(B-C)\}}}{AC}. \quad (17)$$

Furthermore, the high SNR approximation can eliminate those equations of order σ^4. Thus, $C(B-C)$ approaches zero and $D \approx \sigma^2 E_r$ so that ρ^* in (17) can be simplified as

$$\begin{aligned} \rho^* &\approx \frac{-AD + \sqrt{AD\{A(C+D)\}}}{AC} \\ &= \frac{-D + \sqrt{D(C+D)}}{C} \\ &\approx \frac{-\sigma^2 E_r + \sqrt{\sigma^2 E_r (E_r(\eta |h_{rd}|^2 - 1)\sigma^2 + \sigma^2 E_r)}}{E_r(\eta |h_{rd}|^2 - 1)\sigma^2} \\ &= \frac{1}{1 + \sqrt{\eta |h_{rd}|^2}}. \quad \text{(in high SNR)} \end{aligned} \quad (18)$$

From the numerical result of (18), we make the following two remarks.

Remark 1 (Effective range of ρ^*)**.** *In a high SNR regime, the range of ρ^* is determined as $\frac{1}{2} < \rho^* < 1$, regardless of channel conditions on h_{sr}, h_{rd}, and h_{re}. In the PSR scheme, it is desirable for the relay to allocate more power to energy harvesting rather than to information reception.*

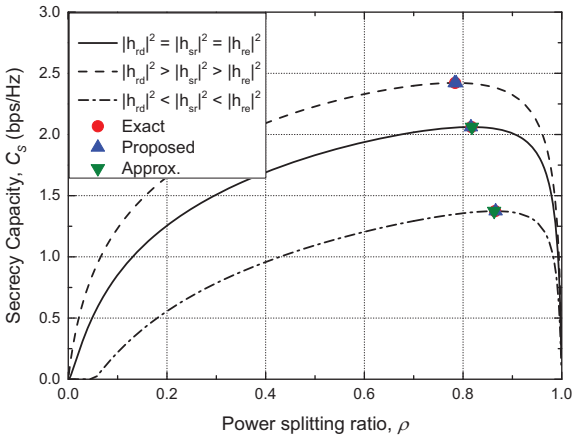


Fig. 3. Secrecy capacity vs. power splitting ratio

Remark 2 (Channel dependency of ρ^*)**.** *In a high SNR regime, ρ^* is only affected by h_{rd}. This implies that the PSR can be optimized without the knowledge of CSI related to the eavesdropper (i.e., h_{re}). Consequently, the proposed scheme is effective even for practical environments where there is no eavesdropper's CSI.*

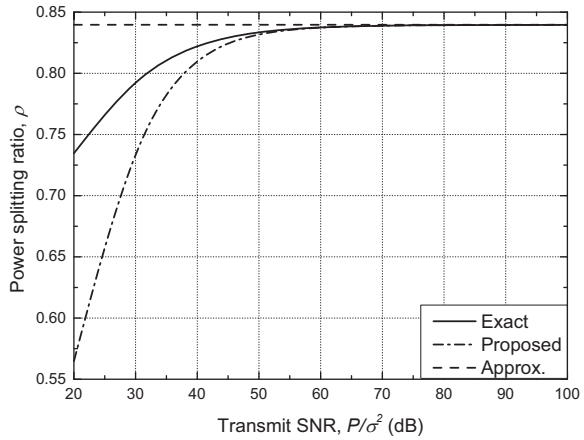
C. Evaluation of Optimality

We evaluate the accuracy of the derived power splitting ratio and its achievable secrecy capacity. The default parameters used are $T = 1$, $P_s = P_z = P = 1$, $\sigma^2 = 10^{-4}$, and $\eta = 0.5$ [23].

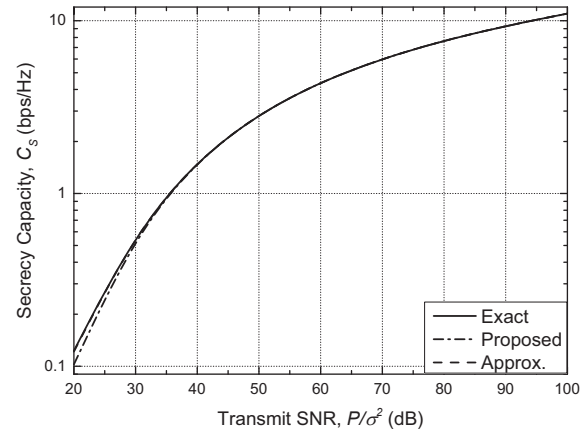
Fig. 3 shows the secrecy capacity (C_S) versus the power splitting ratio (ρ). Here, consider three cases with specific channel parameters as follows: i) $|h_{rd}|^2 = |h_{sr}|^2 = |h_{re}|^2 = 0.1$, ii) $|h_{rd}|^2 = 0.15 > |h_{sr}|^2 = 0.1 > |h_{re}|^2 = 0.05$, and iii) $|h_{rd}|^2 = 0.05 < |h_{sr}|^2 = 0.1 < |h_{re}|^2 = 0.15$. Note that the exact ρ is obtained by an exhaustive search for a solution to maximize (9) while the proposed ρ and the approximated ρ are analytical results obtained from (17) and (18), respectively. As previously shown, C_S is concave w.r.t. ρ, so that the exact ρ for maximizing C_S exists. It is verified that the proposed ρ and approximated ρ are in good agreement with the exact ρ, which indicates that the high SNR approximation in (10) is reasonable. Moreover, they are observed at the point between $\frac{1}{2}$ and 1 for all cases, as mentioned in Remark 1.

Fig. 4 shows the power splitting ratio (a) and the secrecy capacity (b) versus the transmit SNR ($\frac{P}{\sigma^2}$). Here, we used an exponential random variable with a mean of 0.1 to generate h_{sr}, h_{rd}, and h_{re}, and performed 10,000 experiments to obtain an average. As shown in Fig. 4(a), there is little difference among the proposed ρ, the approximated ρ, and the exact ρ in the high SNR regime, but the differences increase as the transmit SNR decreases. Specifically, the proposed ρ and the approximated ρ start to differ from the exact ρ as $\frac{P}{\sigma^2} \leq 50$ dB and $\frac{P}{\sigma^2} \leq 70$ dB, respectively. Nevertheless, in terms of secrecy capacity as shown in Fig. 4(b), the performance gap of each ρ is small even in the low SNR regime. In other words, the C_S of the proposed ρ and the approximated ρ differ slightly from that of the exact ρ when $\frac{P}{\sigma^2} \leq 30$ dB.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal



(a) Power splitting ratio vs. transmit SNR



(b) Secrecy capacity vs. transmit SNR

Fig. 4. Performances against transmit SNR

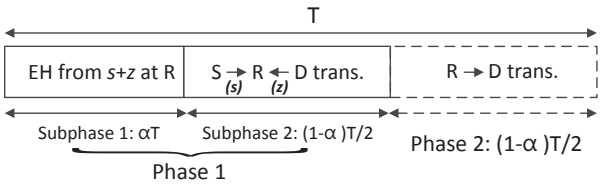


Fig. 5. Time switching-based relaying scheme

IV. Time Switching-based Relaying scheme

A. scheme Description

Fig. 5 shows the considered TSR scheme. The time block is generally divided into two phases according to the functions of reception and transmission. The first phase for reception consists of two subphases. The first subphase with length αT is used for harvesting energy from both the source signal and the jamming noise at the relay and the second subphase with length $\frac{(1-\alpha)T}{2}$ is used for amplifying the received signals from the source and the destination. The second phase with length $\frac{(1-\alpha)T}{2}$ is utilized for the relay to transmit the received signal to the destination [13], [14], [21].

In the first subphase, the harvested energy at the relay, E_h, is represented by

$$E_h = T\eta\alpha(P_s|h_{sr}|^2 + P_z|h_{rd}|^2) = T\eta\alpha E_r \tag{19}$$

where E_r is defined as $P_s|h_{sr}|^2 + P_z|h_{rd}|^2$. In the second subphase, the received signal at the relay, y_r, is obtained as

$$y_r = \sqrt{P_s}h_{sr}s + \sqrt{P_z}h_{rd}z + n_r. \tag{20}$$

Then, in the second phase, the transmitted signal from the relay, x_r, consuming E_h is given by

$$\begin{aligned} x_r &= \frac{\sqrt{P_r}y_r}{\sqrt{P_s|h_{sr}|^2 + P_z|h_{rd}|^2 + \sigma^2}} \\ &= \frac{\sqrt{P_r}y_r}{\sqrt{E_r + \sigma^2}} \end{aligned} \tag{21}$$

where the denominator $\sqrt{E_r + \sigma^2}$ is the power constraint factor at the relay. Here, the transmission power at the relay, P_r, is found as

$$P_r = \frac{E_h}{(1-\alpha)T/2} = \frac{2\eta\alpha E_r}{1-\alpha}. \tag{22}$$

Then, the received signal at the destination, y_d, is expressed as

$$\begin{aligned} y_d &= h_{rd}x_r + n_d \\ &= \frac{\sqrt{P_sP_r}h_{sr}h_{rd}s + \sqrt{P_r}h_{rd}n_r}{\sqrt{E_r + \sigma^2}} + \underbrace{\frac{\sqrt{P_zP_r}h_{rd}^2 z}{\sqrt{E_r + \sigma^2}}}_{\text{self-cancellation}} + n_d \\ &= \frac{\sqrt{P_sP_r}h_{sr}h_{rd}s + \sqrt{P_r}h_{rd}n_r}{\sqrt{E_r + \sigma^2}} + n_d. \end{aligned} \tag{23}$$

Similar to the PSR scheme, the factors relevant to z, $\frac{\sqrt{P_zP_r}h_{rd}^2 z}{\sqrt{E_r+\sigma^2}}$, can be eliminated by self-interference cancellation at the destination. At the same time, the received signal at the eavesdropper, y_e, is given by

$$\begin{aligned} y_e &= h_{re}x_r + n_e \\ &= \frac{\sqrt{P_sP_r}h_{sr}h_{re}s + \sqrt{P_r}h_{re}n_r}{\sqrt{E_r + \sigma^2}} + \frac{\sqrt{P_zP_r}h_{rd}h_{re}z}{\sqrt{E_r + \sigma^2}} + n_e. \end{aligned} \tag{24}$$

As shown, the jamming noise, z, plays a key role in enhancing physical layer security by disrupting the eavesdropper's attempts to decode the source signal, s.

B. Optimal Time Switching Ratio

First, we reveal that the secrecy capacity is concave w.r.t. α under a high SNR environment, in order to show the existence and uniqueness of an optimal time splitting ratio. From (23), the SNR at the destination, Γ_d, is found as

$$\begin{aligned} \Gamma_d &= \frac{\frac{2\eta\alpha E_r P_s|h_{sr}|^2|h_{rd}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r|h_{rd}|^2\sigma^2}{(1-\alpha)(E_r+\sigma^2)} + \sigma^2} \\ &= \frac{2\eta\alpha E_r P_s|h_{sr}|^2|h_{rd}|^2}{2\eta\alpha E_r|h_{rd}|^2\sigma^2 + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \end{aligned} \tag{25}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

At the same time, from (24), the SNR at the eavesdropper, Γ_e, is obtained as

$$\Gamma_e = \frac{\frac{2\eta\alpha E_r P_s |h_{sr}|^2 |h_{re}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r P_z |h_{rd}|^2 |h_{re}|^2}{(1-\alpha)(E_r+\sigma^2)} + \frac{2\eta\alpha E_r |h_{re}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)} + \sigma^2} = \frac{2\eta\alpha E_r P_s |h_{sr}|^2 |h_{re}|^2}{2\eta\alpha E_r |h_{re}|^2 (P_z|h_{rd}|^2+\sigma^2) + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (26)$$

Then, the achievable rates at the destination and the eavesdropper are given by $R_d = \frac{(1-\alpha)T}{2}\log_2(1+\Gamma_d)$ and $R_e = \frac{(1-\alpha)T}{2}\log_2(1+\Gamma_e)$, respectively. Thus, the achievable secrecy capacity is defined as

$$C_S \triangleq [R_d - R_e]^+ = \left[\frac{(1-\alpha)T}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_e}\right)\right]^+ \quad (27)$$

$$\approx \left[\frac{(1-\alpha)T}{2}\log_2\left(\frac{\Gamma_d}{\Gamma_e}\right)\right]^+ \quad \text{(in high SNR)} \quad (28)$$

where the high SNR approximation is utilized in a similar way to the PSR scheme. Here, we define Γ_s as

$$\Gamma_s \triangleq \frac{\Gamma_d}{\Gamma_e} = \frac{|h_{rd}|^2\{2\eta\alpha E_r|h_{re}|^2(P_z|h_{rd}|^2+\sigma^2)+\sigma^2(1-\alpha)(E_r+\sigma^2)\}}{|h_{re}|^2\{2\eta\alpha E_r|h_{rd}|^2\sigma^2+\sigma^2(1-\alpha)(E_r+\sigma^2)\}} = \frac{|h_{rd}|^2(A\alpha+(1-\alpha)D)}{|h_{re}|^2(B\alpha+(1-\alpha)D)} \quad (29)$$

where

$$A = 2\eta E_r|h_{re}|^2(P_z|h_{rd}|^2+\sigma^2),$$
$$B = 2\eta E_r|h_{rd}|^2\sigma^2,$$
$$D = \sigma^2(E_r+\sigma^2). \quad (30)$$

To show the concavity of C_S w.r.t. α, we define $h(\alpha) \triangleq f(\alpha)\cdot g(\alpha)$, where $h(\alpha) \triangleq C_S$, $f(\alpha) \triangleq \frac{(1-\alpha)T}{2}$, and $g(\alpha) \triangleq \log_2(\Gamma_s)$. Then, the second derivative of $h(\alpha)$ w.r.t. α is derived as

$$h''(\alpha) = f''(\alpha)g(\alpha) + 2f'(\alpha)g'(\alpha) + f(\alpha)g''(\alpha) = 2f'(\alpha)g'(\alpha) + f(\alpha)g''(\alpha). \quad (\because f''(\alpha)=0) \quad (31)$$

Here, $f'(\alpha)$, $g'(\alpha)$, and $g''(\alpha)$ are calculated as

$$f'(\alpha) = -\frac{T}{2},$$
$$g'(\alpha) = \frac{D(A-B)}{\ln 2 X_1 X_2},$$
$$g''(\alpha) = \frac{-D(A-B)\{(B-D)X_1+(A-D)X_2\}}{\ln 2 X_1^2 X_2^2} \quad (32)$$

where we define $X_1 \triangleq A\alpha+(1-\alpha)D$ and $X_2 \triangleq B\alpha+(1-\alpha)D$. Finally, $h''(\alpha)$ is represented by

$$h''(\alpha) = \frac{-TD(A-B)\left\{X_1X_2+\frac{1-\alpha}{2}(B-D)X_1+\frac{1-\alpha}{2}(A-D)X_2\right\}}{\ln 2 X_1^2X_2^2} = \frac{-TD(A-B)\left\{\left(\left(\frac{1+\alpha}{2}\right)B+\left(\frac{1-\alpha}{2}\right)D\right)X_1+\frac{1-\alpha}{2}(A-D)X_2\right\}}{\ln 2 X_1^2X_2^2}. \quad (33)$$

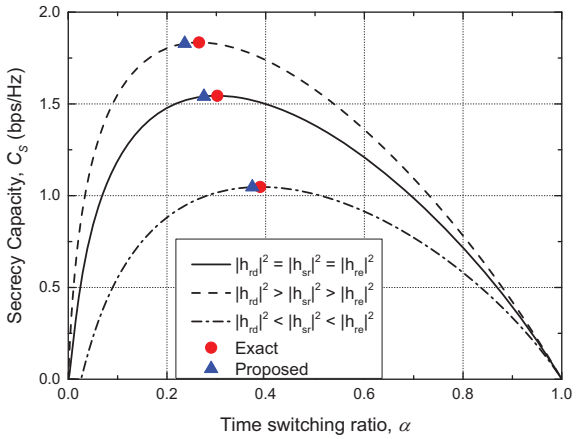


Fig. 6. Secrecy capacity vs. time switching ratio

Since $A > B$ and $A > D$ hold in the high SNR regime, we conclude that $h''(\alpha) < 0$ and C_S is concave w.r.t. α for $0 \le \alpha \le 1$.

Based on this proof of concavity, we can find the optimal value of α to maximize C_S from the following condition.

$$\frac{\partial C_S}{\partial \alpha} = \frac{T}{2\ln 2}\left(\frac{A}{(A-D)\alpha+D} - \frac{B}{(B-D)\alpha+D} - \ln\frac{|h_{rd}|^2}{|h_{re}|^2} - \ln((A-D)\alpha+D) + \ln((B-D)\alpha+D)\right) = 0. \quad (34)$$

With the assumption of high SNR, $A \gg D$, $A \gg B$, and $D \gg B$ all hold. Thus, (34) can be simplified as follows.

$$\frac{\partial C_S}{\partial \alpha} = \frac{1}{\alpha} + \ln\frac{1-\alpha}{\alpha} - \ln\frac{A|h_{rd}|^2}{D|h_{re}|^2} = 0. \quad (35)$$

By solving (35), the optimal α^* is found as

$$\alpha^* = \frac{1}{\mathbb{W}\left(\frac{A|h_{rd}|^2}{D|h_{re}|^2\cdot e}\right)+1} \approx \frac{1}{\mathbb{W}\left(\frac{2\eta|h_{rd}|^2(P_z|h_{rd}|^2+\sigma^2)}{\sigma^2\cdot e}\right)+1} \quad \text{(in high SNR)} \quad (36)$$

where $\mathbb{W}(\cdot)$ denotes the Lambert W-function.

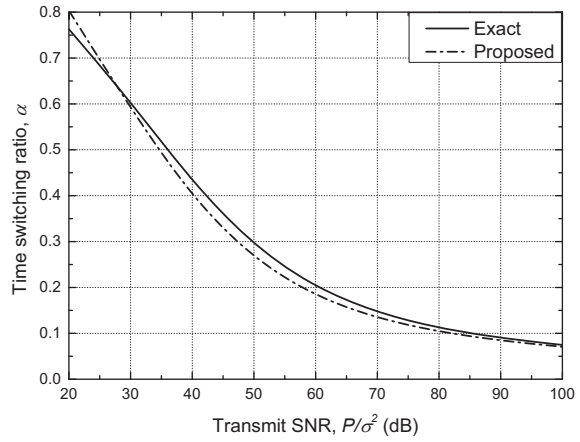
Remark 3 (Channel dependency of α^*)**.** *In a high SNR regime, α^* is only influenced by h_{rd}. TSR can achieve asymptotically the same secrecy capacity performance even if there is no eavesdropper's CSI.*[3]

C. Evaluation of Optimality

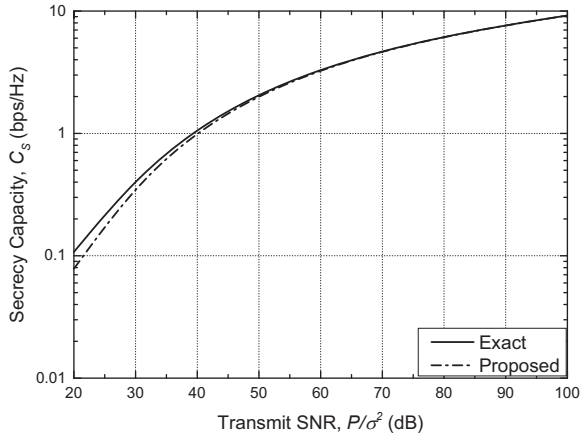
To evaluate the optimality of the proposed α, we use the same parameters used in III-C. Fig. 6 shows the secrecy capacity (C_S) versus the time switching ratio (α). Here, the exact α is a solution obtained by exhaustive search to

[3]In Remarks 2 and 3, h_{rd} can be easily obtained using existing channel estimation methods [25], [26] with regard to derive ρ^* and α^*.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal



(a) Time switching ratio vs. transmit SNR



(b) Secrecy capacity vs. transmit SNR

Fig. 7. Performances against transmit SNR

maximize (27) while the proposed α is obtained from (36). As previously shown, C_S is concave w.r.t. α, and there is an optimal α to maximize C_S. There is a slight difference between the exact α and the proposed α because the proposed α is derived under the assumption of high SNR. As the relay-to-destination channel $|h_{rd}|^2$ decreases, the optimal α increases, similar to the PSR scheme. This is because the relay needs to spend more time on EH rather than on information processing in order to improve C_S as the relay-to-destination channel deteriorates.

Fig. 7 shows the time switching ratio (a) and the secrecy capacity (b) versus the transmit SNR ($\frac{P}{\sigma^2}$), respectively. Due to the high SNR approximation, there is a slight difference between the exact α and the proposed α, as shown in Fig. 7(a). Nevertheless, the C_S of the proposed α approaches that of the exact α when $\frac{P}{\sigma^2}$ is greater than 40 dB, as shown in Fig. 7(b).

V. Comparison of PSR and TSR schemes

We compare the secrecy capacity of the PSR and TSR schemes according to the changes in wireless channel and other system parameters. Unless otherwise stated, we consider

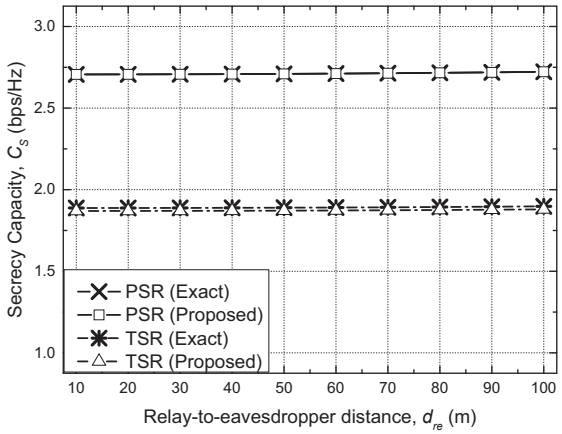


Fig. 8. Secrecy capacity vs. relay-to-eavesdropper distance (d_{re}) when $d_{sd} =$ 200 m and $d_{sr} = 100$ m

the following system parameters: $T = 1$ [17][4], $\eta = 0.5$ [23], $P_s = P_z = P = 43$ dBm [14], [20], and $\sigma^2 = -93$ dBm [14], [17]. For the generation of wireless channels, we define the channel between node i and j as $h_{ij} = \frac{g_{ij}}{d_{ij}^m}$, where d_{ij} is the physical distance between two nodes, m is a path-loss exponent, and g_{ij} is a fading coefficient. Here, g_{ij} is an exponential random variable with mean λ_{ij}. We set $\lambda_{sr} = \lambda_{rd} = \lambda_{re} = 1$ [11]–[13] and $m = 2.7$ assuming an urban cellular network environment [27].

A. Effects of Wireless Channels

First, we investigate the performance of the PSR and TSR schemes according to the channel variation of each link. Fig. 8 shows the secrecy capacity versus the relay-to-eavesdropper distance (d_{re}) when $d_{sd} = 200$ m and $d_{sr} = 100$ m. Both PSR and TSR show constant secrecy capacity regardless of d_{re}. This is because ρ^* and α^* are not affected by h_{re} in the high SNR environment as mentioned in Remarks 2 and 3. Here, $\rho^* = 0.94$ and $\alpha^* = 0.28$ are maintained regardless of d_{re}. These behaviours are key to ensuring the proposed schemes remain operational in real environments because the location of the eavesdropper is generally unknown, therefore it is impossible to obtain the CSI of the eavesdropper.

Fig. 9 shows the secrecy capacity versus the source-to-destination distance (d_{sd}) when the relay is placed in the middle of d_{sd} and $d_{re} = 50$ m. As d_{sd} increases, the signal strength from the source to the destination is attenuated, and thus the C_S of the two schemes decreases. This result shows that PSR achieves a higher C_S than TSR when d_{sd} is less than 500 m. In other words, PSR performs better than TSR as the channel between the source and the destination improves.

Fig. 10 shows the secrecy capacity versus the source-to-relay distance (d_{sr}) when $d_{re} = 50$ m and $d_{sd} = 500$ m. Both schemes yield an increasing C_S as d_{sr} increases because

[4]The amount of harvested energy depends on the block time length, T, so the relay can harvest a sufficient energy for forwarding signals by adjusting T. Note that we considered $T = 1$ in our work because the optimal ρ and α that we derived are irrelevant to T, but the amount of harvested energy at the relay can be practically increased by extending T.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal

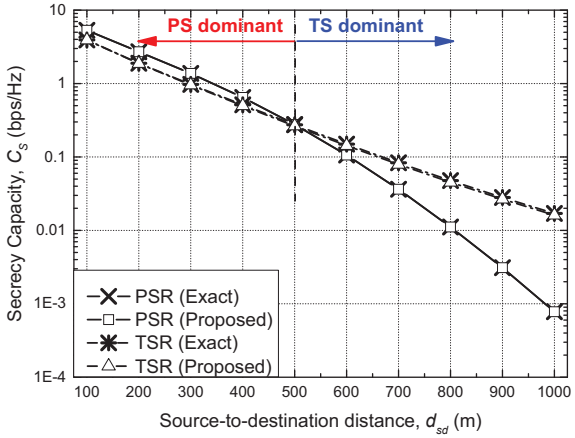


Fig. 9. Secrecy capacity vs. source-to-destination distance (d_{sd}) when $d_{re} = 50$ m and $d_{sr} = \frac{d_{sd}}{2}$

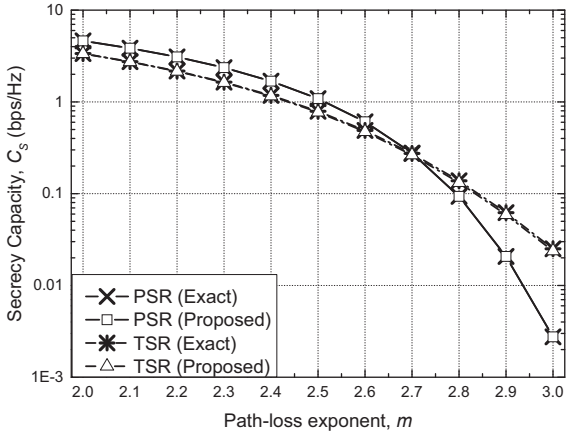


Fig. 11. Secrecy capacity vs. path-loss exponent (m)

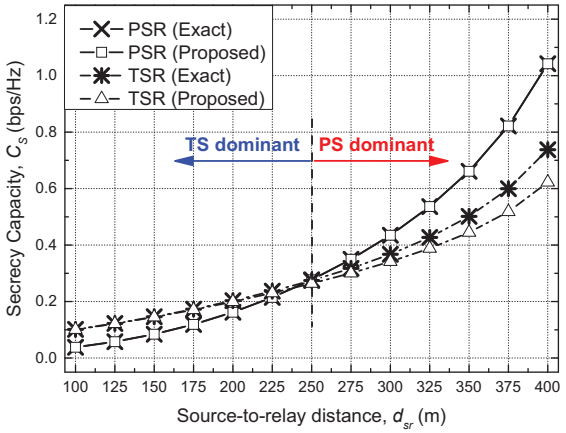


Fig. 10. Secrecy capacity vs. source-to-relay distance (d_{sr}) when $d_{re} = 50$ m and $d_{sd} = 500$ m

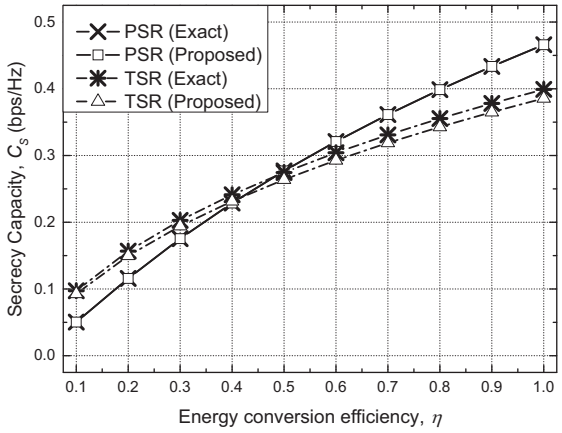


Fig. 12. Secrecy capacity vs. energy conversion efficiency (η)

the jamming noise has more of an effect in decreasing Γ_e when the relay is close to the destination. We also observe that the difference in C_S between the proposed and exact TSR increases as d_{sr} increases. This is because the increase in d_{sr} violates the condition $D \gg B$, which is required to derive (36). Considering the variance of d_{sr}, PSR yields a higher C_S than TSR as d_{sr} increases (i.e., the channel condition is too bad for the eavesdropper to wiretap).

B. Effects of Other System Parameters

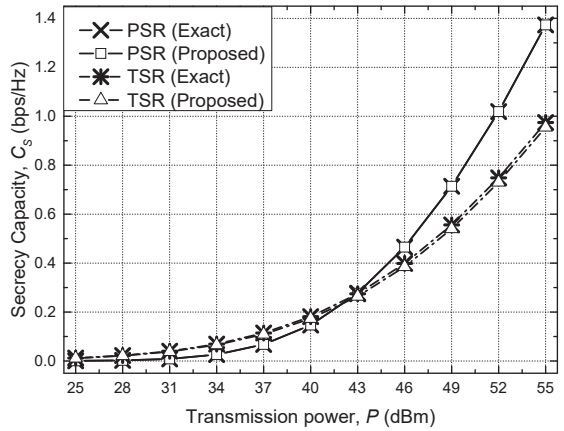
Additionally, we investigate the performances of PSR and TSR to assess the effects of other system parameters, such as path-loss exponent, energy conversion efficiency, and transmission power. To exclude the effects of wireless channel, we use $d_{re} = 50$ m, $d_{sd} = 500$ m, and $d_{sr} = \frac{d_{sd}}{2}$ for this evaluation, based on the previous results in Figs. 9 and 10.

Fig. 11 shows the secrecy capacity versus the path-loss exponent (m). The increase in path-loss exponent results in a decrease in C_S for both schemes due to the attenuated signal strength. It is observed that C_S of PSR is greater than that of TSR at smaller m, e.g., $m < 2.7$.

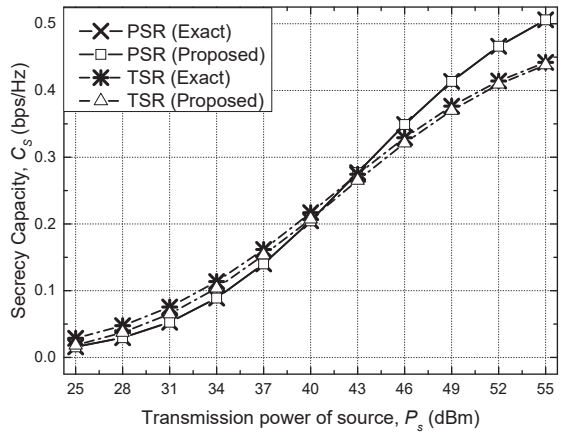
Fig. 12 shows the secrecy capacity versus the energy conversion efficiency (η). A larger η leads to an increase in C_S for both schemes because the relay can harvest more energy from the source signal and jamming noise and thus use a greater power to forward the received signal to the destination. We also confirm that the C_S of PSR starts to exceed that of TSR when η is greater than 0.5.

Fig. 13 shows the secrecy capacity versus the transmission power (P). Fig. 13(a) shows the result when the source and the destination use identical transmission power ($P_s = P_z = P = 43$ dBm) while Fig. 13(b) shows the result when the transmission power of the destination is fixed at $P_z = 43$ dBm while that of the source is varied from 25 dBm to 55 dBm. In the case of identical transmission power, as P increases, the destination can receive a stronger source signal while the eavesdropper is interrupted by a stronger jamming noise. In consequence, the C_S of the two schemes improves with increasing P. In the case of non-identical transmission power, as P_s increases, not only the destination receives a strong signal from the source, but the eavesdropper is also more likely to overhear the signal from the source. As a result, the increasing rate of C_S is slow, compared to that in Fig.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2830880, IEEE Internet of Things Journal



(a) Case for identical transmission power ($P_s = P_z = P = 43$ dBm)



(b) Case for non-identical transmission power ($P_z = 43$ dBm)

Fig. 13. Secrecy capacity vs. transmission power (P)

13(a). In addition, PSR achieves a better performance of C_S than TSR when the transmission power is greater than 43 dBm for both cases.

In summary, PSR shows a better secrecy capacity than TSR when the channel condition is unfavourable to the eavesdropper for wiretapping (i.e, smaller m, higher η, and greater P). Moreover, the performance of proposed schemes generally coincides with that of exact schemes in real environments even though we derived optimal ρ and α with the assumption of high SNR.

VI. Conclusion

We investigated a wireless-powered relay system with destination-assisted jamming assuming the existence of an eavesdropper, in an attempt to maximize secrecy capacity. We proposed PSR and TSR schemes that adaptively control the power splitting ratio (ρ) and time switching ratio (α), respectively. We then proved the concavity of the secrecy capacity with respect to ρ and α under the assumption of high SNR and found closed-form optimal solutions of ρ and α to maximize secrecy capacity. Numerical results show that PSR and TSR schemes with ρ^* and α^* can achieve near-optimal secrecy capacity even if there is no CSI on the eavesdropper. Comparisons of PSR and TSR in various scenarios also revealed that the two schemes have complementary performances according to the network environments. PSR outperforms TSR in terms of secrecy capacity if the network deployment is unfavorable for the eavesdropper to wiretap the relay (i.e., smaller d_{sd}, larger d_{sr}, smaller m, higher η, and greater P). Therefore, the two proposed schemes can be used complementarily according to the network deployment. We expect the proposed relaying schemes to be applicable for resolving not only energy scarcity but also information security problems in future energy-limited wireless networks. For the further work, we will investigate the optimal policy of relay in consideration of the source-to-eavesdropper link.

References

[1] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia, and T. Watteyne, Understanding the limits of LoRaWAN. 2017. [Online]. Available: http://arxiv.org/abs/1607.08011

[2] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747-1761, Oct. 2015.

[3] X. Teng, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, Nov. 2014, pp. 417-423.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[5] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011.

[6] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39-42, Jan. 2013.

[7] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 682-694, Apr. 2013.

[8] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sep. 2013.

[9] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[10] X. Zhou, R. Zhang and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754-4767, Nov. 2013.

[11] L. Liu, R. Zhang, and K. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288-300, Jan. 2013.

[12] L. Liu, R. Zhang, and K. Chua, "Wireless information and power transfer: a dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990-4001, Sep. 2013.

[13] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying schemes for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, July 2013.

[14] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying schemes and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607-1622, May 2015.

[15] Z. Zhou, M. Peng, Z. Zhao, and Y. Li, "Joint power splitting and antenna selection in energy harvesting relay channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 823-827, July 2015.

[16] S. Atapattu and J. Evans, "Optimal energy harvesting schemes for wireless relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5789-5803, Aug. 2016.

[17] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401-415, Jan. 2016.

[18] H. Xing, K. K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616-6631, Dec. 2015.

[19] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538-1550, Dec. 2016.

[20] H. Xing, K. K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971-7984, Dec. 2016.

[21] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199-2213, Mar. 2017.

[22] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "Codesign of a cmos rectifier and small loop antenna for highly sensitive RF energy harvesters," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 3, pp. 622-634, Mar. 2014.

[23] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757-789, Second Quart. 2015.

[24] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1367, Oct. 1975.

[25] C. S. Patel and L. Stber, "Channel estimation for amplify and forward relay based cooperation diversity systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2348-2356, June 2007.

[26] F. Gao, T. Cui, and A. Nallanathan, "On channel estimation and optimal training design for amplify and forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1907-1916, May 2008.

[27] H. Meyr, M. Mseneclaey, and S. A. Fechtel, *Digital Communication Receivers, Synchronization, Channel Estimation, and Signal Processing*, J. G. Proakis, Ed. Wiley Series in Telecommunications and Signal Processing, 1998.