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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

Wireless-Powered Two-Way Relaying Protocols for Optimizing Physical Layer Security

Kisong Lee, *Member, IEEE*, Jun-Pyo Hong, *Member, IEEE*, Hyun-Ho Choi, *Member, IEEE*, and Tony Q. S. Quek, *Fellow, IEEE*,

***Abstract*—This paper considers a two-way relay network, in which two sources exchange data through a relay and a cooperative jammer transmits an artificial noise (AN) while a number of nearby eavesdroppers overhear to recover data from both sources. The relay harvests energy from the two source signals and the AN, and then, uses this harvested energy to forward the received signals to the two sources. Each source eliminates its own signal from the relaying signal by self-cancellation and then decodes the data signal received from the other source. For this wireless-powered two-way relay system, we propose two secure relay protocols based on power splitting and time switching techniques. The two protocols are power splitting-based two-way relaying (PS-TWR) and time switching-based two-way relaying (TS-TWR), in which the relay respectively controls the power splitting ratio (ρ) and time switching ratio (α), in order to achieve a balance between the data receiving and the energy harvesting. The optimal values of ρ and α for each protocol are found analytically to maximize the minimum guaranteed secrecy capacity ($C_S^{\min}$) considering multiple eavesdroppers in high signal-to-noise ratio environments. Numerical results show that both the PS-TWR and TS-TWR protocols using the optimized values of ρ and α achieve the near-optimal $C_S^{\min}$ no matter how many eavesdroppers exist anywhere. Comparisons of the two protocols in various scenarios also show that PS-TWR achieves better $C_S^{\min}$ than TS-TWR because PS-TWR inherently has a shorter vulnerable time for eavesdropping than TS-TWR.**

***Index Terms*—Energy harvesting, physical layer security, secrecy capacity, two-way relay, power splitting, time switching**

I. Introduction

The demand for high-speed mobile communications continues to increase rapidly with recent emphasis on the emergence of real-time multimedia services. According to a recent report [1], mobile data traffic is expected to grow at a compound annual growth rate (CAGR) of 46% between 2016 and 2021 and global video traffic is predicted to account for 82% of total Internet traffic by 2021. As a result, improved spectral efficiency is currently considered one of the main objectives for future mobile systems.

There has been extensive investigation of relay networks to meet the performance requirements of next-generation wireless systems. Typically, these are based on one-way relaying, in which the relay can forward a single message at a time. However, with recent advances in self-interference cancellation techniques, two-way relaying has begun to attract considerable attention, as a means of improving the spectral efficiency of one-way relay networks [2]–[4]. A two-way relay forwards received signals from each of two transceivers at the same time, and each transceiver is able to recover the desired message from the relaying signal via self-interference cancellation. Given that two independent messages are transferred at a time, a two-way relay network approximately provides a two-fold increase in spectral efficiency compared with conventional one-way relaying.

Wireless communication security is also one of main issues in the development of the Internet of things (IoT) because wireless channels are inherently vulnerable to eavesdropping; this problem likely to become more severe as the number of wireless devices increases. As one of the more promising techniques enabling secure wireless communication, physical layer security has been widely investigated [5]–[8]. Considering the fact that relays are more susceptible to eavesdropping than any other node, physical layer security techniques in two-way relay networks were recently considered in [9]–[14]. Relays can be classified into two different types; in the first, trusted relays are authorized to facilitate secure communications between sources [9]–[11]. In the second, untrusted relays are not permitted to decode confidential information even though they are required to forward source signals [12]–[14]. In [9], a joint trusted relay and jammer selection was proposed under the constraint of secrecy rate in two-way cooperative networks with multiple intermediate nodes. Moreover, in two-way trusted relay networks in which all nodes are equipped with multi-antennas, the impact of three different antenna selection schemes on the trade-off between secrecy and system complexity was analysed [10], and precoding designs for user signal and jamming signals were proposed for secure communication [11]. In two-way untrusted relay networks, the effect of external friendly jammers on physical layer security was studied [12], and a joint transmit design and relay selection was investigated [13]. In [14], secure beamforming designs, together with an asymptotic analysis of secrecy sum

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(MSIT) (No. 2018R1C1B6003297). *(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 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, Hankyong National University, Anseong 17579, Korea (e-mail: hhchoi@hknu.ac.kr).

T. Q. S. Quek is with the Singapore University of Technology and Design, Singapore 487372, and also with the Department of Electronics Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, South Korea (e-mail: tonyquek@sutd.edu.sg).

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

rate, were provided for two-way untrusted relay networks with multi-antennas.

The additional power consumed in relaying signals makes it hard for the relay to keep operating, and energy deficiency is thus considered another main challenge in the realization of relay networks. One approach for mitigating this problem involves energy harvesting (EH) from radio frequency (RF) signals; this has seen extensive investigation in various wireless networks, based on the technique of simultaneous wireless information and power transfer (SWIPT) [15]–[18]. In [15], [16], two mode switching techniques were proposed, namely *opportunistic time switching* and *dynamic power splitting*, to perform information receiving and EH on the receiver side. In [17], [18], two relaying protocols based on time switching and power splitting were suggested to enable both information processing and EH at the relay.

Furthermore, in some recent works, EH has been considered in two-way relay networks to deal with the energy scarcity of the relay, providing assistance with the transmission of sources [19]–[23]. In [19], the performances of two-way relaying protocol for SWIPT were analysed with respect to the outage probability, the ergodic capacity, and the finite-SNR diversity multiplexing trade-off. In [20], a hybrid relaying scheme that alters the relaying strategy depending on instantaneous transmit powers was proposed to maximize sum throughput with causal energy arrival, while in [21], a transceiver and relay design for SWIPT with distributed energy beamforming was studied in a two-way relay channel. An optimal power splitting at wireless-powered relay was derived in [22] to maximize the end-to-end transmission rate in two-way relay networks, while [23] contained an investigation of the performances of analog network coding, in terms of system outage, ergodic sum-rate, and sum symbol error rate, in two-way relay networks, where the sources had multiple antennas and the wireless-powered relay had a single antenna.

Despite these advances, however, there is still a need for research on both physical layer security and EH in relay networks, to satisfy the requirements of future wireless networks in terms of spectral efficiency, security, and energy efficiency. With this in mind, we consider secure two-way relay networks using EH in the presence of multiple eavesdroppers. Specifically, two sources try to exchange data with each other via a wireless-powered two-way relay using a cooperative jammer, without any information leakage to eavesdroppers. The relay harvests energy from some portion of the received signals and utilizes this harvested energy to forward the received signals to the sources without consuming the relay's own energy. Each source then decodes the signal transmitted by the other source from the relaying signal using the self-interference cancellation technique. In this system, we attempt to optimize the amount of harvested energy at the relay in order to maximize the secrecy capacity, defined as the difference between the capacity of the legitimate link and that of the wiretap link [6]. To the best of our knowledge, wireless-powered two-way relaying strategies for maximizing secrecy capacity have not previously been investigated, although several authors have considered physical layer security [9]–[14] or EH [19]–[23] in two-way relay networks. Our main contributions can be summarized as follows.

- We present a wireless-powered two-way relay model for secure communication in the presence of multiple eavesdroppers and solve the problem of how to maximize the minimum guaranteed secrecy capacity ($C_S^{\min}$).
- We propose two secure relaying protocols: *power splitting-based two-way relaying* (PS-TWR) and *time switching-based two-way relaying* (TS-TWR). These adaptively control the amount of energy harvested from the received signals by means of power splitting and time switching, respectively, taking account of information leakage to eavesdroppers.
- In high signal-to-noise ratio (SNR) environments, we first prove the concavity of the secrecy capacity for each source with respect to the power splitting ratio (ρ) and time switching ratio (α), and then derive analytically the optimal ρ^* for PS-TWR and the optimal α^* for TS-TWR to maximize $C_S^{\min}$.
- Our asymptotic analysis corresponds to the results obtained from exhaustive search even in a reasonable SNR regime, and provides insightful information for understanding the behaviours of the proposed relaying strategies. Specifically, both PS-TWR and TS-TWR can achieve a near-optimal performance in terms of $C_S^{\min}$ regardless of the locations and number of eavesdroppers. Furthermore, the comparison of PS-TWR and TS-TWR shows that PS-TWR is better protected from eavesdropping than TS-TWR.

The remainder of this paper is organized as follows. In Section II, we describe the system model of the wireless-powered two-way relay network. In Sections III and IV, we describe the proposed PS-TWR and TS-TWR protocols and derive their optimal ratios, ρ^* and α^* respectively, to maximize their minimum guaranteed secrecy capacities. In Section V, we compare PS-TWR with TS-TWR and discuss their behaviours in various different scenarios. We provide our conclusions in Section VI.

II. System Model

Fig. 1 shows the system model of the wireless-powered two-way relaying networks considered here, in which there are two sources (S_1 and S_2), a relay (R), a jammer (Z), and K eavesdroppers (E_k for $k \in \{1, \cdots, K\}$). The wireless-powered relay harvests energy from external RF signals, before forwarding the combined received source signals to both sources. The K eavesdroppers are randomly located near the relay to overhear the relaying signal. The channels for S_1-to-R, S_2-to-R, Z-to-R, S_1-to-E_k, S_2-to-E_k, Z-to-E_k, and R-to-E_k are denoted h_{1r}, h_{2r}, h_{zr}, g_{1k}, g_{2k}, g_{zk}, and g_{rk}, respectively, and the channel between two nodes is assumed to be reciprocal, e.g., $h_{ij} = h_{ji}$ [19], [20], [22], [23]. Moreover, we suppose a quasi-static channel fading with a frequency non-selective parameter, which means that the channel remains constant over one coherence interval and changes independently in different coherence intervals [9], [12]. The noises for S_1, S_2, R, and E_k are denoted $n_{s,1}$, $n_{s,2}$, n_r, and n_k, respectively, and are all assumed to follow an

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

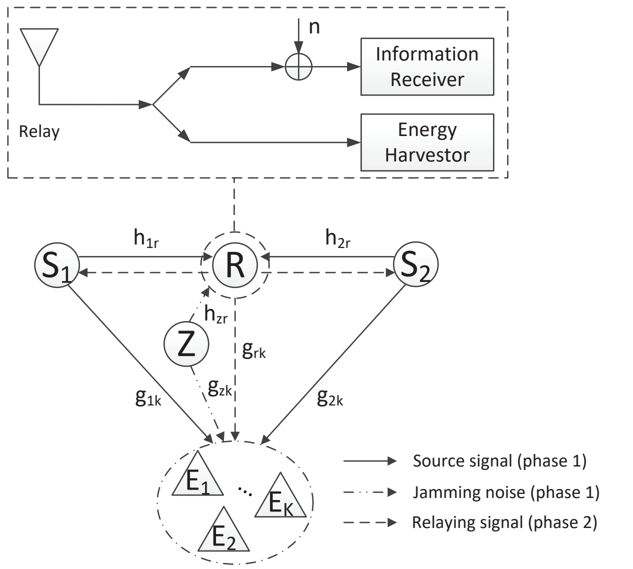


Fig. 1. System model of wireless-powered two-way relay networks with multiple eavesdroppers

additive white Gaussian noise (AWGN) with zero-mean and variance σ^2, i.e., $n_{s,1} = n_{s,2} = n_r = n_k \sim \mathcal{CN}\left(0, \sigma^2\right)$.

The considered system operates in two phases. During the first phase, the two sources transmit their data signals, s_1 and s_2, to the relay at the same time. When the jammer detects the transmission of sources, it transmits artificial noise (AN) z which is generated with a Gaussian pseudo-random generator to hinder the eavesdroppers from decoding source signals. The relay is assumed to have no power source and harvest energy from both its received signal that is a superposition of source signals and the AN [17], [19]–[23]. In addition, the AN generator and its seed table are assumed to be shared beforehand between the jammer and the relay, so that the relay is able to cancel out the AN from the received signal [24]–[27].

In the first phase, the relay is able to adopt a power splitting technique [16] or a time switching technique [15] to balance the energy harvesting and the information processing. It is assumed that all the harvested energy is used to forward the signal in the following phase [16], [17]. On the one hand, since the eavesdroppers have no information on the AN, the AN plays a role of additional noise for degrading the signal reception at the eavesdroppers [28].

In the second phase, the relay cancels out the AN from the received signal and forwards it to each source with the harvested energy. Based on the received signal from the relay, each source tries to recover the information signal of the other source by using the self-interference cancellation. Here, we assume the perfect interference cancellation [9]–[14]. On the other hand, the eavesdroppers attempt to overhear the relaying signal, but the decoding of each signal is hindered by the other source's signal. In other words, the information signal of each source plays a role of the AN in the recovery of the other source's information signal. Although each source is able to remove its information signal from the received signal with the self-interference cancellation, the eavesdroppers have no priori information on the source signal and cannot do interference cancellation [9]–[11].

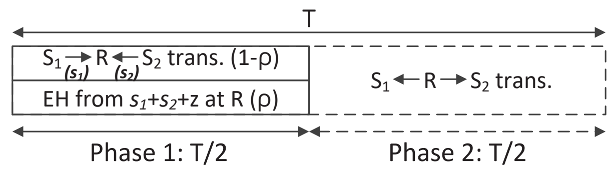


Fig. 2. Power splitting-based two-way relaying protocol

III. Power Splitting-based Two-Way Relaying Protocol

A. Protocol Description

Fig. 2 shows the PS-TWR protocol, in which the block time, T, is divided into two phases of equal length [16], [17]. During the first phase of length $\frac{T}{2}$, the relay adopts a power splitting technique to harvest energy and receive information simultaneously from the received source signals, s_1 and s_2 [16]. Specifically, the received RF signals at the relay are split into two portions: a portion ρ used for harvesting energy and a portion $1-\rho$ used for receiving information, subject to $0 \leq \rho \leq 1$. Then, the received signal at the relay, y_r, is given by

$$\begin{aligned} y_r = &\sqrt{(1-\rho)P_1}h_{1r}s_1 + \sqrt{(1-\rho)P_2}h_{2r}s_2 \\ &+ \underbrace{\sqrt{(1-\rho)P_z}h_{zr}z}_{\text{cancel out}} + n_r \end{aligned} \tag{1}$$

where P_1, P_2, and P_z are the transmission powers at S_1, S_2, and Z, respectively, and s_1, s_2, and z have a normalized power, such that $\mathbb{E}[|s_1|^2] = \mathbb{E}[|s_2|^2] = \mathbb{E}[|z|^2] = 1$. In addition, the relay can remove the AN from y_r because it shares the information on z with the jammer. The harvested energy at the relay, E_h, is represented by

$$E_h = \frac{T\eta\rho(P_1|h_{1r}|^2 + P_2|h_{2r}|^2 + P_z|h_{zr}|^2)}{2} = \frac{T\eta\rho E_r}{2} \tag{2}$$

where η is an energy conversion efficiency within the range $0 < \eta \leq 1$ and E_r is defined as $P_1|h_{1r}|^2 + P_2|h_{2r}|^2 + P_z|h_{zr}|^2$.

On the other hand, the source signals, s_1 and s_2, are wiretapped by eavesdroppers, so the received signal at the eavesdropper E_k during the first phase, $y_k^{[1]}$, is expressed as

$$y_k^{[1]} = \sqrt{P_1}g_{1k}s_1 + \sqrt{P_2}g_{2k}s_2 + \sqrt{P_z}g_{zk}z + n_k. \tag{3}$$

Then, the SNR at E_k for detecting s_j destined for S_i during the first phase, $\Gamma_{k,i}^{[1]}$, is obtained as

$$\Gamma_{k,i}^{[1]} = \frac{P_j|g_{jk}|^2}{P_i|g_{ik}|^2 + P_z|g_{zk}|^2 + \sigma^2}. \tag{4}$$

Note that the AN from Z as well as the signal from S_i hinder the eavesdropper k from decoding source signal s_j. The achievable rate at E_k during the first phase is found as $R_{k,i}^{[1]} = \frac{T}{2}\log_2(1 + \Gamma_{k,i}^{[1]})$.

During the second phase with the remaining $\frac{T}{2}$ duration, the relay amplifies and forwards the received signal to the sources

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

using the harvested energy, E_h. Thus, the transmitted signal from the relay, x_r, is expressed as

$$x_r = \frac{\sqrt{P_r} y_r}{\sqrt{(1-\rho)(P_1|h_{1r}|^2 + P_2|h_{2r}|^2 + P_z|h_{zr}|^2) + \sigma^2}} = \frac{\sqrt{P_r} y_r}{\sqrt{(1-\rho)E_r + \sigma^2}} \tag{5}$$

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

$$P_r = \frac{E_h}{T/2} = \eta\rho E_r. \tag{6}$$

Then, the received signal at S_1, $y_{s,1}$, is found as

$$\begin{aligned} y_{s,1} &= h_{1r}x_r + n_{s,1} \\ &= \frac{\sqrt{(1-\rho)P_2 P_r} h_{1r} h_{2r} s_2 + \sqrt{P_r} h_{1r} n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + \underbrace{\frac{\sqrt{(1-\rho)P_1 P_r} h_{1r}^2 s_1}{\sqrt{(1-\rho)E_r + \sigma^2}}}_{\text{self-cancellation}} + n_{s,1} \\ &= \frac{\sqrt{(1-\rho)P_2 P_r} h_{1r} h_{2r} s_2 + \sqrt{P_r} h_{1r} n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + n_{s,1}. \end{aligned} \tag{7}$$

Similarly, the received signal at S_2, $y_{s,2}$, is obtained as

$$\begin{aligned} y_{s,2} &= h_{2r}x_r + n_{s,2} \\ &= \frac{\sqrt{(1-\rho)P_1 P_r} h_{1r} h_{2r} s_1 + \sqrt{P_r} h_{2r} n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + \underbrace{\frac{\sqrt{(1-\rho)P_2 P_r} h_{2r}^2 s_2}{\sqrt{(1-\rho)E_r + \sigma^2}}}_{\text{self-cancellation}} + n_{s,2} \\ &= \frac{\sqrt{(1-\rho)P_1 P_r} h_{1r} h_{2r} s_1 + \sqrt{P_r} h_{2r} n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + n_{s,2}. \end{aligned} \tag{8}$$

In (7) and (8), each source can eliminate the part related to its own signal, e.g., $\frac{\sqrt{(1-\rho)P_1 P_r} h_{1r}^2 s_1}{\sqrt{(1-\rho)E_r+\sigma^2}}$ and $\frac{\sqrt{(1-\rho)P_2 P_r} h_{2r}^2 s_2}{\sqrt{(1-\rho)E_r+\sigma^2}}$, by the self-interference cancellation. On the other hand, the received signal at the eavesdropper E_k during the second phase, $y_k^{[2]}$, is expressed as

$$\begin{aligned} y_k^{[2]} &= g_{rk}x_r + n_k \\ &= \frac{\sqrt{(1-\rho)P_1 P_r} h_{1r} g_{rk} s_1 + \sqrt{(1-\rho)P_2 P_r} h_{2r} g_{rk} s_2}{\sqrt{(1-\rho)E_r + \sigma^2}} + \frac{\sqrt{P_r} g_{rk} n_r}{\sqrt{(1-\rho)E_r + \sigma^2}} + n_k. \end{aligned} \tag{9}$$

From (7) and (8), SNR at S_i for receiving s_j for $i, j \in \{1,2\}$ and $i \neq j$, Γ_i, is represented by

$$\Gamma_i = \frac{\frac{(1-\rho)P_j P_r |h_{ir}|^2 |h_{jr}|^2}{(1-\rho)E_r + \sigma^2}}{\frac{P_r |h_{ir}|^2 \sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} = \frac{\eta\rho(1-\rho)E_r P_j |h_{ir}|^2 |h_{jr}|^2}{\eta\rho E_r |h_{ir}|^2 \sigma^2 + \sigma^2((1-\rho)E_r + \sigma^2)}. \tag{10}$$

Then, the achievable rate at S_i is given by $R_i = \frac{T}{2}\log_2(1+\Gamma_i)$. On the other hand, from (9), the SNR at E_k for detecting s_j destined for S_i during the second phase, $\Gamma_{k,i}^{[2]}$, is calculated as

$$\Gamma_{k,i}^{[2]} = \frac{\frac{(1-\rho)P_j P_r |h_{jr}|^2 |g_{rk}|^2}{(1-\rho)E_r + \sigma^2}}{\frac{(1-\rho)P_i P_r |h_{ir}|^2 |g_{rk}|^2}{(1-\rho)E_r + \sigma^2} + \frac{P_r |g_{rk}|^2 \sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} = \frac{\eta\rho(1-\rho)E_r P_j |h_{jr}|^2 |g_{rk}|^2}{\eta\rho E_r |g_{rk}|^2((1-\rho)P_i |h_{ir}|^2 + \sigma^2) + \sigma^2((1-\rho)E_r + \sigma^2)}. \tag{11}$$

The achievable rate at E_k during the second phase is found as $R_{k,i}^{[2]} = \frac{T}{2}\log_2(1+\Gamma_{k,i}^{[2]})$. Then, the achievable rate at E_k is calculated as the summation of $R_{k,i}^{[1]}$ and $R_{k,i}^{[2]}$, such as $R_{k,i} = R_{k,i}^{[1]} + R_{k,i}^{[2]}$ for $i \in \{1,2\}$ and $k \in \{1,2,\cdots,K\}$.

B. Optimal Power Splitting Ratio

The secrecy capacity at S_i when E_k overhears s_j destined for S_i, $C_{S,i}^k$, is expressed as

$$C_{S,i}^k \triangleq [R_i - R_{k,i}]^+, \; i \in \{1,2\}, \; k \in \{1,2,\cdots,K\} \tag{12}$$

where $[\cdot]^+ = \max(0,\cdot)$. Considering the fact that there are k wiretap links for each source, the minimum guaranteed secrecy capacity for S_i is represented by

$$C_{S,i} \triangleq \min_k \left\{C_{S,i}^k\right\}. \tag{13}$$

Finally, the minimum guaranteed secrecy capacity for both sources is defined as follows [7], [8].

$$\begin{aligned} C_S^{\min} &\triangleq \min_i \{C_{S,i}\} \\ &= \min_i \min_k \left\{C_{S,i}^k\right\} \\ &= \min_i \min_k \left\{[R_i - R_{k,i}]^+\right\} \\ &= \min_i \left\{\left[R_i - \max_k\{R_{k,i}\}\right]^+\right\} \\ &= \min_i \left\{[R_i - R_{k_i^*,i}]^+\right\} \\ &= \min_i \left\{\left[\frac{T}{2}\log_2\left(\frac{1+\Gamma_i}{(1+\Gamma_{k_i^*,i}^{[1]})(1+\Gamma_{k_i^*,i}^{[2]})}\right)\right]^+\right\} \end{aligned} \tag{14}$$

where $R_{k_i^*,i} \triangleq \max_k\{R_{k,i}\}$ and $k_i^* \triangleq \arg\max_k\{R_{k,i}\}$ for $i \in \{1,2\}$ and $k \in \{1,2,\cdots,K\}$. In other words, the eavesdropper k_i^* is the one with the largest achievable rate for wiretapping s_j destined for S_i. Under the assumption of high SNR, $C_S^{\min}$ can be approximated as

$$C_S^{\min} \approx \min_i \left\{\left[\frac{T}{2}\log_2\left(\frac{\Gamma_i}{(1+\Gamma_{k_i^*,i}^{[1]})\Gamma_{k_i^*,i}^{[2]}}\right)\right]^+\right\}, \; i \in \{1,2\}. \tag{15}$$

This assumption is reasonable because EH technology is commonly applicable in high SNR environments due to the low sensitivity of RF EH [29]. We discuss the influence of this

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

approximation on performance in some detail in subsection V-A.

Our objective is to find the optimal power splitting ratio ρ^* that maximizes the minimum guaranteed secrecy capacity under the assumption of high SNR. The optimal ρ^* is expressed as

$$\rho^* = \arg\max_{\rho} \left\{ \min_{i} \left\{ \left[\frac{T}{2} \log_2 \left(\frac{\Gamma_i}{(1+\Gamma^{[1]}_{k_i^*,i})\Gamma^{[2]}_{k_i^*,i}} \right) \right]^+ \right\} \right\} \tag{16}$$

where $i \in \{1,2\}$. In addition, $\Gamma^{[1]}_{k_i^*,i}$ is not a function of ρ, so the problem is equivalent to

$$\rho^* = \arg\max_{\rho} \left\{ \min_{i} \left\{ \frac{\Gamma_i}{\Gamma^{[2]}_{k_i^*,i}} \right\} \right\}, \ i \in \{1,2\}. \tag{17}$$

Thus, we define

$$\begin{aligned}\Gamma_{s,i} &\triangleq \frac{\Gamma_i}{\Gamma^{[2]}_{k_i^*,i}} \\ &= \frac{|h_{ir}|^2\{\eta\rho E_r|g_{rk_i^*}|^2((1-\rho)P_i|h_{ir}|^2+\sigma^2)+\sigma^2((1-\rho)E_r+\sigma^2)\}}{|g_{rk_i^*}|^2\{\eta\rho E_r|h_{ir}|^2\sigma^2+\sigma^2((1-\rho)E_r+\sigma^2)\}} \\ &= \frac{|h_{ir}|^2\{-\rho^2\mathcal{A}_i+\rho(\mathcal{A}_i+\mathcal{B}_i)+\mathcal{D}\}}{|g_{rk_i^*}|^2\{\rho\mathcal{C}_i+\mathcal{D}\}}\end{aligned} \tag{18}$$

where

$$\mathcal{A}_i = \eta E_r P_i |g_{rk_i^*}|^2 |h_{ir}|^2, \tag{19}$$
$$\mathcal{B}_i = E_r(\eta|g_{rk_i^*}|^2-1)\sigma^2, \tag{20}$$
$$\mathcal{C}_i = E_r(\eta|h_{ir}|^2-1)\sigma^2, \tag{21}$$
$$\mathcal{D} = \sigma^2(E_r+\sigma^2). \tag{22}$$

To find the solution of ρ_i for maximizing each $\Gamma_{s,i}$, we first show the concavity of $\Gamma_{s,i}$.

Lemma 1. $\Gamma_{s,i}$ *is concave with respect to (w.r.t.)* ρ_i *subject to* $0 \le \rho_i \le 1$.

Proof: The second derivative of $\Gamma_{s,i}$ w.r.t. ρ_i is

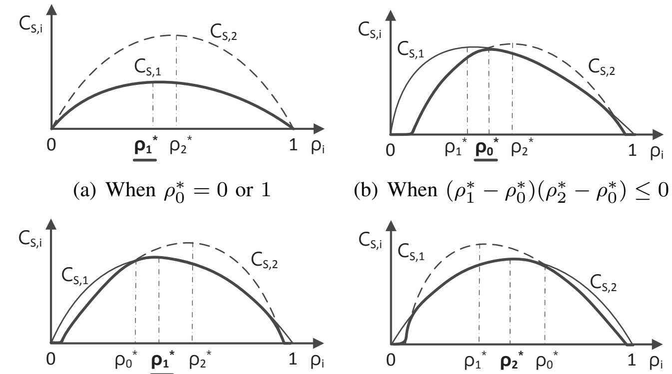
$$\frac{\partial^2\Gamma_{s,i}}{\partial\rho_i^2} = -\frac{2|h_{ir}|^2\mathcal{D}\{\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})+\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)\}}{|g_{rk_i^*}|^2(\rho_i\mathcal{C}_i+\mathcal{D})^3}. \tag{23}$$

It is clear that $\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})$ and $(\rho_i\mathcal{C}_i+\mathcal{D})$ are positive. In addition, $\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})+\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i) > 0$ regardless of the sign of $\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)$ because $\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})$ has order σ^2 while $\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)$ has order σ^4. As a result, $\frac{\partial^2\Gamma_{s,i}}{\partial\rho_i^2} < 0$ and $\Gamma_{s,i}$ is concave w.r.t. ρ_i. ■

From Lemma 1, we propose the following.

Proposition 1. *The optimal power splitting ratio* (ρ_i^*) *for maximizing* $\Gamma_{s,i}$ *for* $i \in \{1,2\}$ *is given by*

$$\rho_i^* = \frac{-\mathcal{A}_i\mathcal{D}+\sqrt{\mathcal{A}_i\mathcal{D}\{\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})+\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)\}}}{\mathcal{A}_i\mathcal{C}_i}, \ i \in \{1,2\}. \tag{24}$$



(a) When $\rho_0^* = 0$ or 1

(b) When $(\rho_1^*-\rho_0^*)(\rho_2^*-\rho_0^*) \le 0$

(c) When $(\rho_1^*-\rho_0^*)(\rho_2^*-\rho_0^*) > 0$ and $C_{S,1}^* \le C_{S,2}^*$

(d) When $(\rho_1^*-\rho_0^*)(\rho_2^*-\rho_0^*) > 0$ and $C_{S,1}^* > C_{S,2}^*$

Fig. 3. Illustration of possible cases for determining ρ^*

Proof: We can find ρ_i for maximizing $\Gamma_{s,i}$ from the following condition.

$$\frac{\partial\Gamma_{s,i}}{\partial\rho_i} = -\frac{|h_{ir}|^2\{\mathcal{A}_i\mathcal{C}_i\rho_i^2+2\mathcal{A}_i\mathcal{D}\rho_i-(\mathcal{A}_i+\mathcal{B}_i-\mathcal{C}_i)\mathcal{D}\}}{|g_{rk_i^*}|^2(\rho_i\mathcal{C}_i+\mathcal{D})^2} = 0. \tag{25}$$

Using the quadratic formula, the solutions of (25) can be found as

$$\rho_{i,\pm} = \frac{-\mathcal{A}_i\mathcal{D}\pm\sqrt{\mathcal{A}_i\mathcal{D}\{\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})+\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)\}}}{\mathcal{A}_i\mathcal{C}_i}. \tag{26}$$

In (26), $\mathcal{C}_i < 0$ because $\eta|h_{ir}|^2 < 1$ in $\mathcal{C}_i$. Therefore, the inequality, $\mathcal{A}_i(\mathcal{C}_i+\mathcal{D}) < \mathcal{A}_i\mathcal{D}$, holds. In addition, $\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})$ is larger than $|\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)|$ as discussed in (23). This indicates that $\sqrt{\mathcal{A}_i\mathcal{D}\{\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})+\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)\}}$ takes a value between 0 and $\mathcal{A}_i\mathcal{D}$. Moreover, $\rho_{i,-} > 1$ because $|\mathcal{D}| > |\mathcal{C}_i|$ and $\mathcal{C}_i < 0$, while $0 < \rho_{i,+} < 1$. As a result, $\rho_{i,+}$ can be determined as ρ_i^*. ■

In the high SNR regime, the equations with order σ^4 can be eliminated so that $\mathcal{C}_i(\mathcal{B}_i-\mathcal{C}_i)$ goes to zero and $\mathcal{D} \approx \sigma^2 E_r$. Then, ρ_i^* in (24) is approximated as

$$\begin{aligned}\rho_i^* &\approx \frac{-\mathcal{A}_i\mathcal{D}+\sqrt{\mathcal{A}_i\mathcal{D}\{\mathcal{A}_i(\mathcal{C}_i+\mathcal{D})\}}}{\mathcal{A}_i\mathcal{C}_i} \\ &= \frac{-\mathcal{D}+\sqrt{\mathcal{D}(\mathcal{C}_i+\mathcal{D})}}{\mathcal{C}_i} \\ &\approx \frac{-\sigma^2E_r+\sqrt{\sigma^2E_r(E_r(\eta|h_{ir}|^2-1)\sigma^2+\sigma^2E_r)}}{E_r(\eta|h_{ir}|^2-1)\sigma^2} \\ &= \frac{1}{1+\sqrt{\eta|h_{ir}|^2}}.\end{aligned} \tag{27}$$

This result means that PS-TWR can be optimized for each source by only the channel information of h_{ir} for $i \in \{1,2\}$ in a high SNR regime without any knowledge about channel information to the eavesdroppers (i.e., g_{rk} and g_{ik}). This property makes PS-TWR more practical because the location of eavesdroppers is unknown in real environments.

From the result of Proposition 1, we need to determine the optimal ρ^* for maximizing $\min\{C_{S,1}, C_{S,2}\}$ for high SNR. Note that $C_{S,i}$ is derived directly from $\Gamma_{s,i}$ for high SNR.

There exists ρ_0^* that satisfies $\Gamma_{s,1} = \Gamma_{s,2}$ such that we should consider ρ_i^* and ρ_0^* jointly. Fig. 3 illustrates possible cases for determining ρ^*; a) If there is no crossover point that satisfies $C_{S,1} = C_{S,2}$ (i.e., $\rho_0^* = 0$ or 1), ρ_i^* that achieves smaller $C_{S,i}$ is chosen as ρ^*. b) When ρ_0^* lies between ρ_1^* and ρ_2^* (i.e., $(\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) \leq 0$), ρ_0^* is chosen as ρ^*. c) and d) When ρ_0^* is smaller or larger than both ρ_1^* and ρ_2^* (i.e., $(\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) > 0$), ρ_i^* that accomplishes a smaller $C_{S,i}$ is chosen as ρ^*.

Then, ρ_0^* can be derived as follows. It is obvious that $\mathcal{C}_i \approx -E_r\sigma^2$ since $\eta|h_{ir}|^2 \ll 1$ in $\mathcal{C}_i$. Therefore, the denominator of $\Gamma_{s,i}$ can be approximated as $|g_{rk_i^*}|^2\{\rho\mathcal{C}_i + \mathcal{D}\} \approx |g_{rk_i^*}|^2(1-\rho)E_r\sigma^2$. Then, we can build (28) from $\Gamma_{s,1} = \Gamma_{s,2}$. Using the quadratic formula, the solution of (28) can be found as

$$\rho_{\pm} = \min\left[\max\left[\frac{1}{2} \pm \sqrt{\frac{1}{4} - \frac{\left(\frac{|h_{1r}|^2}{|g_{rk_1^*}|^2} - \frac{|h_{2r}|^2}{|g_{rk_2^*}|^2}\right)\sigma^2}{\eta(P_2|h_{2r}|^4 - P_1|h_{1r}|^4)}}, 0\right], 1\right]. \tag{29}$$

Note that $\rho_\pm$ represents the crossover point where $\Gamma_{s,1} = \Gamma_{s,2} = \Gamma_s$, in other words, $C_{S,1} = C_{S,2} = C_S$ in the high SNR regime. Comparing C_S at ρ_+ with that at ρ_-, ρ_0^* is chosen to have a larger C_S, as follows.

$$\rho_0^* = \begin{cases} \rho_+ & \text{if} \quad C_S(\rho_+) \geq C_S(\rho_-), \\ \rho_- & \text{if} \quad C_S(\rho_+) < C_S(\rho_-). \end{cases} \tag{30}$$

In consideration of ρ_i^* and ρ_0^*, the optimal power splitting ratio for maximizing $\min\{C_{S,1}, C_{S,2}\}$ is finally determined as

$$\rho^* = \begin{cases} \rho_0^* & \text{if} \ (\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) \leq 0, \\ \rho_1^* & \text{if} \ (\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) > 0 \text{ and } C_{S,1}(\rho_1^*) \leq C_{S,2}(\rho_2^*), \\ \rho_2^* & \text{if} \ (\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) > 0 \text{ and } C_{S,1}(\rho_1^*) > C_{S,2}(\rho_2^*). \end{cases} \tag{31}$$

C. Evaluation of Optimality

For the purpose of verifying the optimality of the proposed ρ^*, we assume $T = 1$, $P_1 = P_2 = P_z = 1$, $\sigma^2 = 10^{-5}$, $K = 10$, and $\eta = 0.5$ [30]. For wireless channels, we generate $|h_{1r}|^2$, $|h_{2r}|^2$, $|h_{zr}|^2$, and $|g_{zk}|^2$ with an exponential random variable with mean $\lambda = 1$. Similarly, we generate $|g_{rk}|^2$ and $|g_{2k}|^2$ with an exponential random variable with mean λ_e, but λ_e varies from 1 to 3 to show the effects of eavesdropping channels on the performances. On the other hand, $|g_{1k}|^2$ is simply set to be with $\frac{1}{\lambda_e}$ to reflect an inverse proportional relationship between $|g_{1k}|^2$ and $|g_{2k}|^2$.

Fig. 4 shows the minimum guaranteed secrecy capacity ($C_S^{\min}$) versus the power splitting ratio (ρ) for different λ_e. Note that the optimal ρ^* is the solution obtained by exhaustive search to maximize (14) without the high SNR approximation, while the proposed ρ^* is the analytical result obtained from (31) under the high SNR assumption. It is obvious that $C_S^{\min}$ is concave w.r.t. ρ so that the optimal ρ^* for maximizing $C_S^{\min}$ exists. The performance of $C_S^{\min}$ decreases as λ_e increases because the increase in λ_e enhances the rate of the eavesdroppers. It is clearly shown that the proposed ρ^* are in good agreement with the optimal ρ^* for each λ_e.

Fig. 5 shows the optimal ρ^* and the minimum guaranteed secrecy capacity versus the transmit SNR ($\frac{P}{\sigma^2}$), respectively. It is observed that ρ^* slightly increases as SNR increases, which means that in the PS-TWR protocol it is beneficial for the relay to use a larger portion of the received power for harvesting energy in higher SNR. As shown in Fig. 5(a), the proposed ρ^* is in good agreement with the optimal ρ^* for all SNR regimes in spite of the high SNR approximation. Accordingly, there is little difference in $C_S^{\min}$ between the proposed ρ^* and the optimal ρ^* in Fig. 5(b). As λ_e changes, ρ^* does not change much. Especially, the higher the SNR, the less the difference according to λ_e. This phenomenon is consistent with the result of (27), that is, the optimal ρ^* is not affected by the channels to eavesdroppers (i.e., g_{rk} and g_{ik}) in the high SNR regime.[1] In addition, the difference in $C_S^{\min}$ according to λ_e is further reduced, as shown in Fig. 5(b). This is because the change of $C_S^{\min}$ around the optimal ρ^* is small, as shown in Fig. 4. Therefore, the proposed ρ^* achieves the near-optimal $C_S^{\min}$ regardless of λ_e.

IV. Time Switching-based Two-Way Relaying Protocol

A. Protocol Description

Fig. 6 illustrates the TS-TWR protocol where the block time is divided into two phases depending on the functionality of reception and transmission at the relay. The first phase for reception consists of two subphases. The first subphase is used for harvesting energy and its duration is allocated αT. The second subphase is used for receiving information from the source signals. On the other hand, the second phase is used for the relay to transmit the received signal to the sources using the harvested energy [17]. The time durations for receiving and transmitting information are allocated the same duration $\frac{(1-\alpha)T}{2}$.

During the first subphase, the harvested energy at the relay, E_h, is given by

$$E_h = T\eta\alpha(P_1|h_{1r}|^2 + P_2|h_{2r}|^2 + P_z|h_{zr}|^2) = T\eta\alpha E_r \tag{32}$$

where E_r is defined as $P_1|h_{1r}|^2 + P_2|h_{2r}|^2 + P_z|h_{zr}|^2$. During the second subphase, the received signal at the relay, y_r, is expressed as

$$y_r = \sqrt{P_1}h_{1r}s_1 + \sqrt{P_2}h_{2r}s_2 + \underbrace{\sqrt{P_z}h_{zr}z}_{\text{cancel out}} + n_r. \tag{33}$$

Here, the part related to z can be cancelled at the relay. On the other hand, the received signal at the eavesdropper E_k during the first phase, $y_k^{[1]}$, and the SNR at E_k for detecting s_j destined for S_i during the first phase, $\Gamma_{k,i}^{[1]}$, are the same as (3) and (4), respectively. However, the achievable rate at E_k during the first phase is different due to the different overhearing time and is given by $R_{k,i}^{[1]} = \frac{(1+\alpha)T}{2}\log_2(1+\Gamma_{k,i}^{[1]})$.

[1]From (31), ρ^* is determined depending on the relationship between ρ_i^* and ρ_0^*. In most cases in our simulations, the condition $(\rho_1^* - \rho_0^*)(\rho_2^* - \rho_0^*) > 0$ is satisfied, so ρ_i^* rather than ρ_0^* is chosen as ρ^*.

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

$$
\begin{aligned}
0 &= (|g_{rk_1^*}|^2|h_{2r}|^2\mathcal{A}_2-|g_{rk_2^*}|^2|h_{1r}|^2\mathcal{A}_1)\rho^2+(|g_{rk_2^*}|^2|h_{1r}|^2(\mathcal{A}_1+\mathcal{B}_1)-|g_{rk_1^*}|^2|h_{2r}|^2(\mathcal{A}_2+\mathcal{B}_2))\rho+\mathcal{D}(|g_{rk_2^*}|^2|h_{1r}|^2-|g_{rk_1^*}|^2|h_{2r}|^2)\\
&\approx (|g_{rk_1^*}|^2|h_{2r}|^2\mathcal{A}_2-|g_{rk_2^*}|^2|h_{1r}|^2\mathcal{A}_1)\rho^2+(|g_{rk_2^*}|^2|h_{1r}|^2\mathcal{A}_1-|g_{rk_1^*}|^2|h_{2r}|^2\mathcal{A}_2)\rho+\mathcal{D}(|g_{rk_2^*}|^2|h_{1r}|^2-|g_{rk_1^*}|^2|h_{2r}|^2). \qquad (28)
\end{aligned}
$$

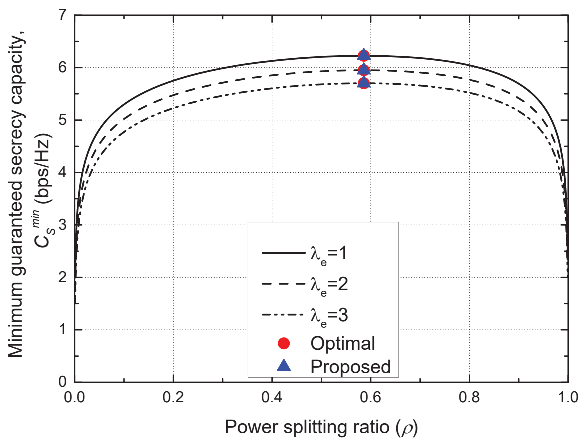
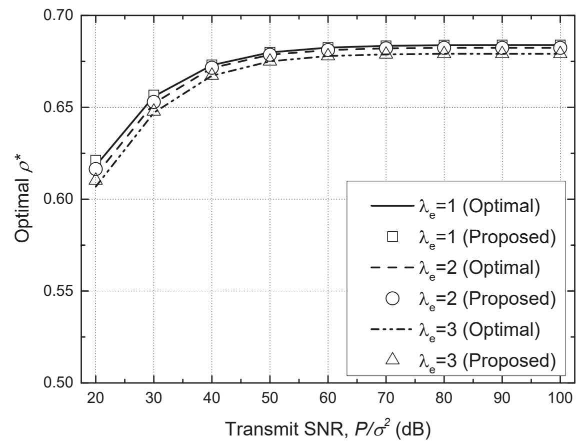
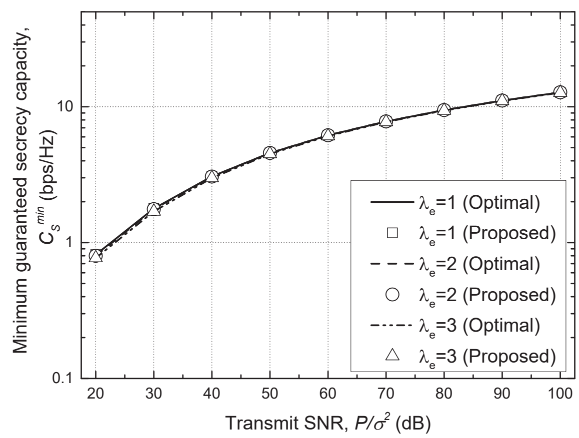


Fig. 4. Minimum guaranteed secrecy capacity vs. power splitting ratio



(a) Optimal power splitting ratio vs. transmit SNR



(b) Minimum guaranteed secrecy capacity vs. transmit SNR

Fig. 5. Performances against transmit SNR

During the second phase, the transmitted signal from the relay, x_r, using E_h is represented by

$$
\begin{aligned}
x_r &= \frac{\sqrt{P_r}y_r}{\sqrt{P_1|h_{1r}|^2+P_2|h_{2r}|^2+P_z|h_{zr}|^2+\sigma^2}}\\
&= \frac{\sqrt{P_r}y_r}{\sqrt{E_r+\sigma^2}} \qquad (34)
\end{aligned}
$$

where the denominator $\sqrt{E_r+\sigma^2}$ is the power constraint factor at the relay. In addition, the transmission power at the relay, P_r, is given by

$$
P_r = \frac{E_h}{(1-\alpha)T/2} = \frac{2\eta\alpha E_r}{1-\alpha}. \qquad (35)
$$

Then, the received signal at S_1, y_1, is expressed as

$$
\begin{aligned}
y_{s,1} &= h_{1r}x_r + n_{s,1}\\
&= \frac{\sqrt{P_2P_r}h_{1r}h_{2r}s_2+\sqrt{P_r}h_{1r}n_r}{\sqrt{E_r+\sigma^2}} + \underbrace{\frac{\sqrt{P_1P_r}h_{1r}^2s_1}{\sqrt{E_r+\sigma^2}}}_{\text{self}-\text{cancellation}} + n_{s,1}\\
&= \frac{\sqrt{P_2P_r}h_{1r}h_{2r}s_2+\sqrt{P_r}h_{1r}n_r}{\sqrt{E_r+\sigma^2}} + n_{s,1}. \qquad (36)
\end{aligned}
$$

In addition, the received signal at S_2, y_2, is obtained as

$$
\begin{aligned}
y_{s,2} &= h_{2r}x_r + n_{s,2}\\
&= \frac{\sqrt{P_1P_r}h_{1r}h_{2r}s_1+\sqrt{P_r}h_{2r}n_r}{\sqrt{E_r+\sigma^2}} + \underbrace{\frac{\sqrt{P_2P_r}h_{2r}^2s_2}{\sqrt{E_r+\sigma^2}}}_{\text{self}-\text{cancellation}} + n_{s,2}\\
&= \frac{\sqrt{P_1P_r}h_{1r}h_{2r}s_1+\sqrt{P_r}h_{2r}n_r}{\sqrt{E_r+\sigma^2}} + n_{s,2}. \qquad (37)
\end{aligned}
$$

Similar to the PS-TWR protocol, each source can remove its own signal, e.g., $\frac{\sqrt{P_1P_r}h_{1r}^2s_1}{\sqrt{E_r+\sigma^2}}$ and $\frac{\sqrt{P_2P_r}h_{2r}^2s_2}{\sqrt{E_r+\sigma^2}}$, by the self-interference cancellation. On the other hand, the received

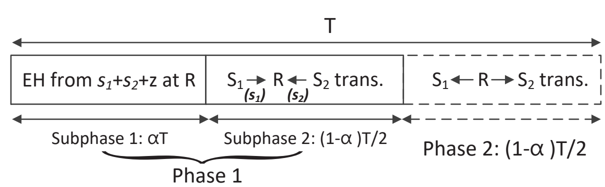


Fig. 6. Time switching-based two-way relaying protocol

signal at the eavesdropper E_k during the second phase, $y_k^{[2]}$, is given by

$$
\begin{aligned}
y_k^{[2]} &= g_{rk}x_r + n_k\\
&= \frac{\sqrt{P_1P_r}h_{1r}g_{rk}s_1+\sqrt{P_2P_r}h_{2r}g_{rk}s_2}{\sqrt{E_r+\sigma^2}} + \frac{\sqrt{P_r}g_{rk}n_r}{\sqrt{E_r+\sigma^2}} + n_k. \qquad (38)
\end{aligned}
$$

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

From (36) and (37), the SNR at S_i for receiving s_j, Γ_i, is found as

$$\Gamma_i = \frac{\frac{2\eta\alpha E_r P_j |h_{ir}|^2 |h_{jr}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r |h_{ir}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)} + \sigma^2} = \frac{2\eta\alpha E_r P_j |h_{ir}|^2 |h_{jr}|^2}{2\eta\alpha E_r |h_{ir}|^2 \sigma^2 + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (39)$$

Then, the achievable rate at S_i is obtained as $R_i = \frac{(1-\alpha)T}{2}\log_2(1+\Gamma_i)$ for $i \in \{1,2\}$. On the other hand, from (38), the SNR at E_k for detecting s_j transmitted to S_i during the second phase, $\Gamma_{k,i}^{[2]}$, is represented by

$$\Gamma_{k,i}^{[2]} = \frac{\frac{2\eta\alpha E_r P_j |h_{jr}|^2 |g_{rk}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r P_i |h_{ir}|^2 |g_{rk}|^2}{(1-\alpha)(E_r+\sigma^2)} + \frac{2\eta\alpha E_r |g_{rk}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)} + \sigma^2} = \frac{2\eta\alpha E_r P_j |h_{jr}|^2 |g_{rk}|^2}{2\eta\alpha E_r |g_{rk}|^2 (P_i |h_{ir}|^2 + \sigma^2) + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (40)$$

The achievable rate at E_k during the second phase is given by $R_{k,i}^{[2]} = \frac{(1-\alpha)T}{2}\log_2(1+\Gamma_{k,i}^{[2]})$. Then, the achievable rate at E_k is obtained as the summation of $R_{k,i}^{[1]}$ and $R_{k,i}^{[2]}$, such as $R_{k,i} = R_{k,i}^{[1]} + R_{k,i}^{[2]}$ for $i \in \{1,2\}$ and $k \in \{1,2,\cdots,K\}$.

B. Optimal Time Switching Ratio

Similar to the PS-TWR protocol, the minimum guaranteed secrecy capacity is formulated as

$$\begin{aligned} C_S^{\min} &\triangleq \min_i \{C_{S,i}\} \\ &= \min_i \min_k \{C_{S,i}^k\} \\ &= \min_i \min_k \left\{ [R_i - R_{k,i}]^+ \right\} \\ &= \min_i \left\{ \left[R_i - \max_k \{R_{k,i}\} \right]^+ \right\} \\ &= \min_i \left\{ [R_i - R_{k_i^*,i}]^+ \right\} \\ &= \min_i \left\{ \left[\frac{(1-\alpha)T}{2} \log_2 \left(\frac{1+\Gamma_i}{1+\Gamma_{k_i^*,i}^{[2]}} \right) - \frac{(1+\alpha)T}{2} \log_2(1+\Gamma_{k_i^*,i}^{[1]}) \right]^+ \right\} \quad (41) \\ &\approx \min_i \left\{ \left[\frac{(1-\alpha)T}{2} \log_2 \frac{\Gamma_i}{\Gamma_{k_i^*,i}^{[2]}} - \frac{(1+\alpha)T}{2} \log_2(1+\Gamma_{k_i^*,i}^{[1]}) \right]^+ \right\} \quad (42) \end{aligned}$$

where $R_{k_i^*,i} \triangleq \max_k \{R_{k,i}\}$ and $k_i^* \triangleq \arg\max_k \{R_{k,i}\}$ for $i \in \{1,2\}$ and $k \in \{1,2,\cdots,K\}$. The approximation from (41) to (42) is obtained by assuming high SNR.

Our objective is to find the optimal time switching ratio α^* that maximizes this minimum guaranteed secrecy capacity. Under the assumption of high SNR, we try to find an optimal α^* that maximizes (42), which is expressed as

$$\alpha^* = \arg\max_\alpha \left\{ \min_i \left\{ \left[\frac{(1-\alpha)T}{2} \log_2 \frac{\Gamma_i}{\Gamma_{k_i^*,i}^{[2]}} - \frac{(1+\alpha)T}{2} \log_2(1+\Gamma_{k_i^*,i}^{[1]}) \right]^+ \right\} \right\}, \ i \in \{1,2\} \quad (43)$$

Here, we define $\Gamma_{s,i}$ as

$$\begin{aligned} \Gamma_{s,i} &\triangleq \frac{\Gamma_i}{\Gamma_{k_i^*,i}^{[2]}} \\ &= \frac{|h_{ir}|^2 \{2\eta\alpha E_r |g_{rk_i^*}|^2 (P_i |h_{ir}|^2 + \sigma^2) + \sigma^2(1-\alpha)(E_r+\sigma^2)\}}{|g_{rk_i^*}|^2 \{2\eta\alpha E_r |h_{ir}|^2 \sigma^2 + \sigma^2(1-\alpha)(E_r+\sigma^2)\}} \\ &= \frac{|h_{ir}|^2((\mathcal{F}_i - \mathcal{D})\alpha + \mathcal{D})}{|g_{rk_i^*}|^2((\mathcal{G}_i - \mathcal{D})\alpha + \mathcal{D})} \end{aligned} \quad (44)$$

where

$$\mathcal{F}_i = 2\eta E_r |g_{rk_i^*}|^2 (P_i |h_{ir}|^2 + \sigma^2), \quad (45)$$

$$\mathcal{G}_i = 2\eta E_r |h_{ir}|^2 \sigma^2, \quad (46)$$

$$\mathcal{D} = \sigma^2(E_r + \sigma^2). \quad (47)$$

Now, we show the concavity of $C_{S,i}$ w.r.t. α_i to find the solution of α_i for maximizing each $C_{S,i}$.

Lemma 2. *$C_{S,i}$ is concave w.r.t. α_i subject to $0 \le \alpha_i \le 1$ in the high SNR regime.*

Proof: We define $h_i(\alpha_i) \triangleq f(\alpha_i) r_i(\alpha_i) - q_i(\alpha_i)$, where $h_i(\alpha_i) \triangleq C_{S,i}$, $f(\alpha_i) \triangleq \frac{(1-\alpha_i)T}{2}$, $r_i(\alpha_i) \triangleq \log_2(\Gamma_{s,i})$, and $q_i(\alpha_i) \triangleq \frac{(1+\alpha)T}{2}\log_2(1+\Gamma_{k_i^*,i}^{[1]})$. Then, the second derivative of $h_i(\alpha_i)$ w.r.t. α_i can be derived as

$$\begin{aligned} h_i^{''}(\alpha_i) &= f^{''}(\alpha_i) r_i(\alpha_i) + 2f^{'}(\alpha_i) r_i^{'}(\alpha_i) + f(\alpha_i) r_i^{''}(\alpha_i) \\ &= 2f^{'}(\alpha_i) r_i^{'}(\alpha_i) + f(\alpha_i) r_i^{''}(\alpha_i). \quad (\because f^{''}(\alpha_i) = 0) \end{aligned} \quad (48)$$

Here, $f^{'}(\alpha_i)$, $r_i^{'}(\alpha_i)$, and $r_i^{''}(\alpha_i)$ are calculated as

$$\begin{aligned} f^{'}(\alpha_i) &= -\frac{T}{2}, \\ r_i^{'}(\alpha_i) &= \frac{\mathcal{D}(\mathcal{F}_i - \mathcal{G}_i)}{\ln 2 X_i Y_i}, \\ r_i^{''}(\alpha_i) &= \frac{-\mathcal{D}(\mathcal{F}_i - \mathcal{G}_i)\{(\mathcal{G}_i - \mathcal{D})X_i + (\mathcal{F}_i - \mathcal{D})Y_i\}}{\ln 2 X_i^2 Y_i^2}, \end{aligned} \quad (49)$$

where $X_i = (\mathcal{F}_i - \mathcal{D})\alpha_i + \mathcal{D}$ and $Y_i = (\mathcal{G}_i - \mathcal{D})\alpha_i + \mathcal{D}$. Therefore, $h_i^{''}(\alpha_i)$ is represented by

$$h_i^{''}(\alpha_i) = \frac{-T\mathcal{D}(\mathcal{F}_i - \mathcal{G}_i)\left\{\left(\left(\frac{1+\alpha_i}{2}\right)\mathcal{G}_i + \left(\frac{1-\alpha_i}{2}\right)\mathcal{D}\right) X_i + \frac{1-\alpha_i}{2}(\mathcal{F}_i - \mathcal{D})Y_i\right\}}{\ln 2 X_i^2 Y_i^2}. \quad (50)$$

Since $\mathcal{F}_i > \mathcal{G}_i$ and $\mathcal{F}_i > \mathcal{D}$ hold in the high SNR regime, we can conclude that $h''(\alpha_i) < 0$ and $C_{S,i}$ is concave w.r.t. α_i for $0 \le \alpha_i \le 1$. ■

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

From Lemma 2, we can obtain the following proposition.

Proposition 2. *In the high SNR regime, the optimal time splitting ratio (α_i^*) for maximizing $C_{S,i}$ for $i \in \{1,2\}$ is given by*

$$\alpha_i^* = \frac{1}{\mathbb{W}\left(\frac{2\eta|h_{ir}|^2(P_i|h_{ir}|^2+\sigma^2)(1+\Gamma^{[1]}_{k_i^*,i})}{\sigma^2\cdot e}\right)+1} \tag{51}$$

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

Proof: Based on Lemma 2, we can find the optimal α_i^* for maximizing $C_{S,i}$ from the following condition.

$$\frac{\partial C_{S,i}}{\partial \alpha_i} = \frac{T}{2\ln 2}\Bigg(\frac{\mathcal{F}_i}{(\mathcal{F}_i-\mathcal{D})\alpha_i+\mathcal{D}} - \frac{\mathcal{G}_i}{(\mathcal{G}_i-\mathcal{D})\alpha_i+\mathcal{D}} - \ln\frac{|h_{ir}|^2}{|g_{rk_i^*}|^2} - \ln((\mathcal{F}_i-\mathcal{D})\alpha_i+\mathcal{D}) + \ln((\mathcal{G}_i-\mathcal{D})\alpha_i+\mathcal{D}) - \ln(1+\Gamma^{[1]}_{k_i^*,i})\Bigg) = 0. \tag{52}$$

With the assumption of high SNR, the conditions, $\mathcal{F}_i \gg \mathcal{D}$, $\mathcal{F}_i \gg \mathcal{G}_i$, and $\mathcal{D} \gg \mathcal{G}_i$, can hold. Thus, (52) is transformed to

$$\frac{\partial C_{S,i}}{\partial \alpha_i} = \frac{1}{\alpha_i} + \ln\frac{1-\alpha_i}{\alpha_i} - \ln\frac{\mathcal{F}_i|h_{ir}|^2(1+\Gamma^{[1]}_{k_i^*,i})}{\mathcal{D}|g_{rk_i^*}|^2} = 0. \tag{53}$$

By solving (53), the optimal α_i^* is obtained as

$$\begin{aligned}\alpha_i^* &= \frac{1}{\mathbb{W}\left(\frac{\mathcal{F}_i|h_{ir}|^2(1+\Gamma^{[1]}_{k_i^*,i})}{\mathcal{D}|g_{rk_i^*}|^2\cdot e}\right)+1} \\ &= \frac{1}{\mathbb{W}\left(\frac{2\eta E_r|g_{rk_i^*}|^2(P_i|h_{ir}|^2+\sigma^2)|h_{ir}|^2(1+\Gamma^{[1]}_{k_i^*,i})}{\sigma^2(E_r+\sigma^2)|g_{rk_i^*}|^2\cdot e}\right)+1} \quad (54) \\ &\approx \frac{1}{\mathbb{W}\left(\frac{2\eta|h_{ir}|^2(P_i|h_{ir}|^2+\sigma^2)(1+\Gamma^{[1]}_{k_i^*,i})}{\sigma^2\cdot e}\right)+1}. \quad (55)\end{aligned}$$

■

Now we can find α_0^* that satisfies the condition $C_{S,1} = C_{S,2}$ without difficulty by using a binary search method in the range between α_1^* and α_2^*. In the same way as the PS-TWR protocol, considering α_i^* and α_0^*, the optimal time switching ratio for maximizing $\min\{C_{S,1}, C_{S,2}\}$ is finally determined as

$$\alpha^* = \begin{cases}\alpha_0^* & \text{if } (\alpha_1^*-\alpha_0^*)(\alpha_2^*-\alpha_0^*) \le 0, \\ \alpha_1^* & \text{if } (\alpha_1^*-\alpha_0^*)(\alpha_2^*-\alpha_0^*) > 0 \text{ and } C_{S,1}(\alpha_1^*) \le C_{S,2}(\alpha_2^*), \\ \alpha_2^* & \text{if } (\alpha_1^*-\alpha_0^*)(\alpha_2^*-\alpha_0^*) > 0 \text{ and } C_{S,1}(\alpha_1^*) > C_{S,2}(\alpha_2^*).\end{cases} \tag{56}$$

C. Evaluation of Optimality

To evaluate the optimality of the proposed α, we utilize the same parameters used in Section III-C. Fig. 7 shows the minimum guaranteed secrecy capacity ($C_S^{\min}$) versus the time switching ratio (α) for different λ_e. Here, the optimal α^* is the solution found by exhaustive search to maximize (41) while the proposed α^* is obtained from (56). As proved, $C_S^{\min}$ shows the concave shape with respect to α and there is an optimal α^* to maximize $C_S^{\min}$. Similar to the PS-TWR protocol, the proposed α^* is in concordance with the optimal α^* for each λ_e.

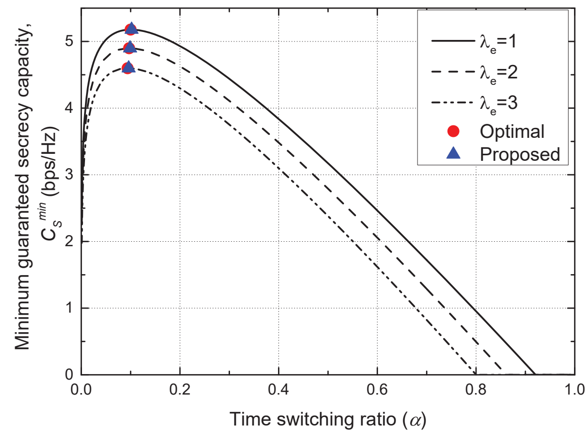
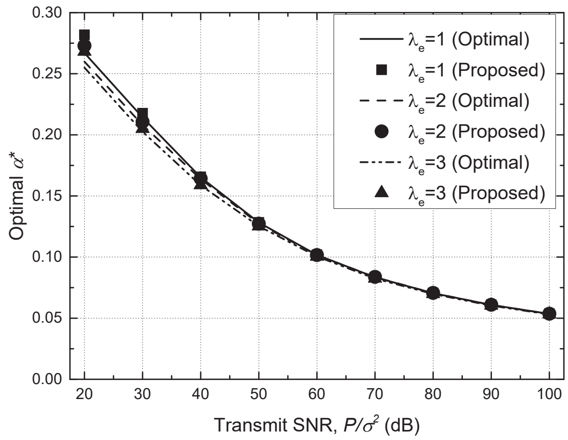


Fig. 7. Minimum guaranteed secrecy capacity vs. time switching ratio

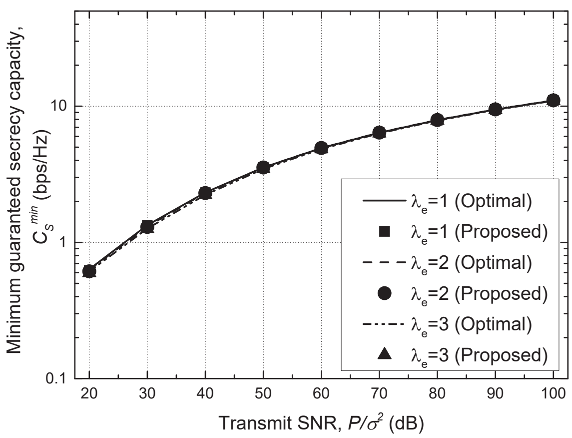
Fig. 8 shows the optimal α^* and the minimum guaranteed secrecy capacity versus the transmit SNR ($\frac{P}{\sigma^2}$), respectively. Unlike the optimal ρ^* in the PS-TWR protocol, the optimal α^* decreases as SNR increases. This means that it is advantageous for the relay to spend more time on information processing rather than EH in order to improve $C_S^{\min}$ with high SNR. As shown in Fig. 8(a), the proposed α^* is in good agreement with the optimal α^* in most SNR regions, but there is a little difference between them when $\frac{P}{\sigma^2} \le 30$ dB due to the high SNR approximation. Nevertheless, the performance difference in terms of $C_S^{\min}$ is negligible over all SNR regions, as shown in Fig. 8(b). In addition, it is observed that both α^* and $C_S^{\min}$ are almost unaffected by λ_e, similar to the results of PS-TWR. This means that in practice we can obtain the optimal α^* without considering the channel information about the eavesdroppers (i.e., g_{rk} and g_{ik}) and this α^* achieves the near-optimal $C_S^{\min}$ in the TS-TWR protocol.

V. Comparison of PS-TWR and TS-TWR Protocols

To understand the advantages and disadvantages of PS-TWR and TS-TWR protocols, we compare the two proposed protocols in various realistic environments. We consider the network environment as symmetric and asymmetric cases according to the changes of wireless channel and transmit power. To confirm the performance gain with the conventional schemes, we also consider the PS-static and TS-static protocols that utilize the static value of 0.5 for ρ and α, respectively. We set the default parameters as follows: $T = 1$ [18], $\eta = 0.5$ [30], $K = 10$, $P_1 = P_2 = P_z = P = 43$ dBm [18], and $\sigma^2 = -97$ dBm [18]. For the generation of wireless channels, we define the channel between any node i and j as $h_{ij} = \frac{f_{ij}}{d_{ij}^m}$, where d_{ij} is the physical distance between two nodes, m is a path-loss exponent, and f_{ij} is a fading coefficient. Here,

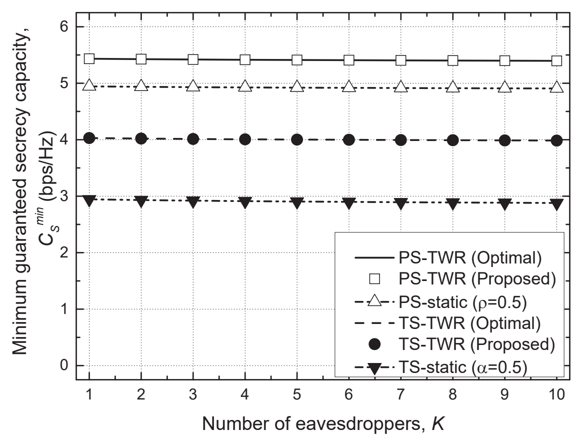


(a) Optimal time switching ratio vs. transmit SNR

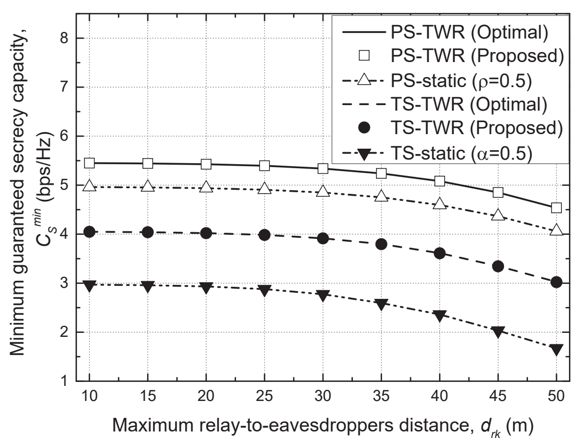


(b) Minimum guaranteed secrecy capacity vs. transmit SNR

Fig. 8. Performances against transmit SNR



(a) $C_S^{\min}$ vs. number of eavesdroppers (K)



(b) $C_S^{\min}$ vs. maximum relay-to-eavesdroppers distance (d_{rk})

Fig. 9. Effects of eavesdropping channels on the minimum guaranteed secrecy capacity ($C_S^{\min}$)

f_{ij} is an exponential random variable with mean λ_{ij}. We set $\lambda_{ij} = 1$ [15]–[17] for all wireless channels and $m = 2.7$ assuming an urban cellular network environment [31]. The minimum power level for harvesting energy at the relay is set as -10 dBm [29], [30]. In addition, the cooperative jammer is randomly generated at a distance within 5 m from the relay while eavesdroppers are randomly distributed at a distance between 5 and 25 m from the relay.

A. Symmetric Case

Symmetric case assumes that the distance between source 1 and source 2 (d_{12}) is fixed at 100 m, the two sources use the same transmit power, and the relay is always placed at the mid-point of d_{12}.

Fig. 9 shows the effects of eavesdropping channels on the minimum guaranteed secrecy capacity ($C_S^{\min}$) according to (a) the number of eavesdroppers (K) and (b) the maximum relay-to-eavesdroppers distance (d_{rk}). As K and d_{rk} increase, the eavesdroppers can be closer to any source and thus have more opportunities to overhear the source signal. As a result, the $C_S^{\min}$ of all schemes slightly decreases. It is shown that in both PS-TWR and TS-TWR, the optimal and proposed performances match well each other over all ranges of K and d_{rk}. Thus, we can confirm that the proposed TWR protocols ensure information security regardless of the number and locations of eavesdroppers.

Fig. 10 shows the minimum guaranteed secrecy capacity versus the transmission power of the two sources (P). As P increases, the relay can harvest more energy from the AN as well as the source signals and both sources can receive a stronger signal from the other source, but the eavesdroppers are still interrupted by stronger source signals and AN. In consequence, the $C_S^{\min}$ of both protocols improves with increasing P.

Fig. 11 shows the minimum guaranteed secrecy capacity versus the S_1-to-S_2 distance (d_{12}). As d_{12} increases, the signal attenuation between S_1 and S_2 increases, and thus the $C_S^{\min}$ of the two protocols decreases.

From Figs. 9-11, it is shown that PS-TWR achieves a better $C_S^{\min}$ than TS-TWR. This is because TS-TWR basically has a longer vulnerable time for eavesdropping than PS-TWR. That is, the eavesdroppers can overhear s_1 and s_2 from the sources during the first phase with the length of $\frac{T}{2}$ in PS-TWR,

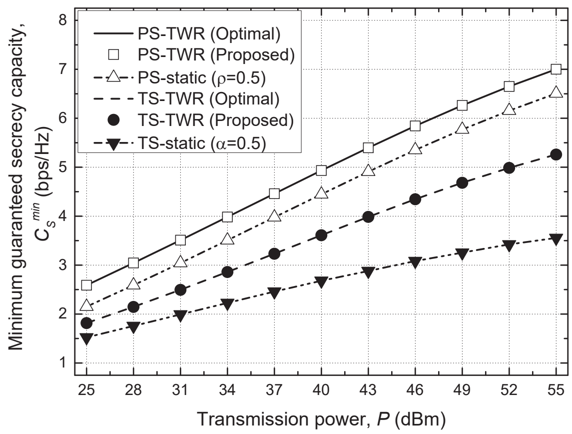


Fig. 10. Minimum guaranteed secrecy capacity vs. transmission power (P)

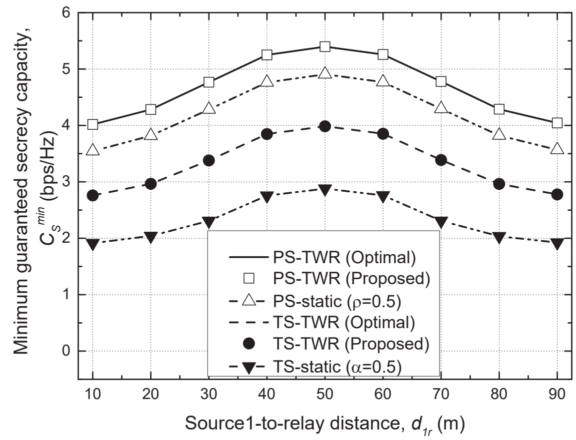


Fig. 12. Minimum guaranteed secrecy capacity vs. S_1-to-R distance (d_{1r}) when $d_{12} = 100$ m

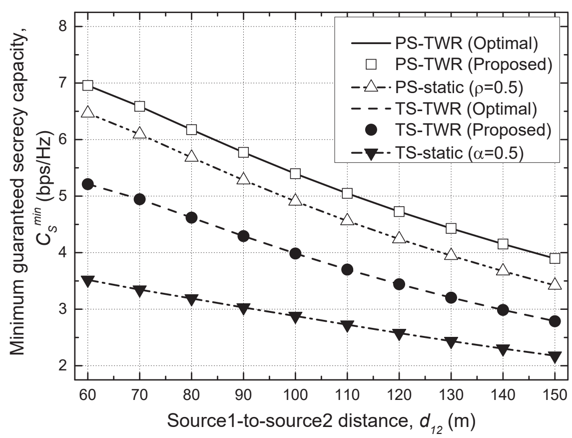


Fig. 11. Minimum guaranteed secrecy capacity vs. S_1-to-S_2 distance (d_{12})

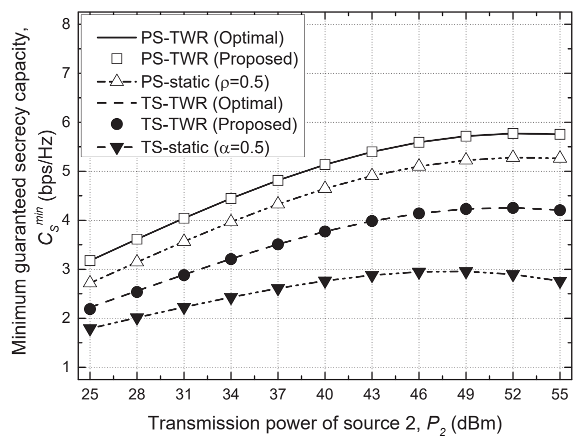


Fig. 13. Minimum guaranteed secrecy capacity vs. transmission power of source 2 (P_2) when $P_1 = 43$ dBm

but $\frac{(1+\alpha)T}{2}$ in TS-TWR. Moreover, PS-TWR and TS-PWR outperforms PS-static and TS-static, respectively, because they adapt ρ and α optimally according to the environmental change. Namely, they achieve the near-optimal $C_S^{\min}$ for all realizations of wireless channels.

B. Asymmetric Case

We consider the asymmetric case by changing the location of relay and the transmit power of source 2.

Fig. 12 shows the minimum guaranteed secrecy capacity versus the S_1-to-R distance (d_{1r}) when d_{12} is fixed at 100 m. As shown in Fig. 12, $C_S^{\min}$ deteriorates as relay is closer to one of the sources because this causes a serious imbalance between $C_{S,1}$ and $C_{S,2}$. Therefore, both protocols maximize $C_S^{\min}$ when the relay is placed at the mid-point of d_{12}.

Fig. 13 shows the minimum guaranteed secrecy capacity versus the transmission power of source 2 (P_2) when P_1 is fixed as 43 dBm. Unlike the case of symmetric transmission power as shown in Fig. 10, as P_2 increases, not only S_1 receives a strong signal from S_2, but the eavesdroppers are also more likely to overhear the signal from S_2. As a result, the $C_S^{\min}$ of all schemes degrades when P_2 is greater than 49 dBm.

VI. Conclusions

We investigated a wireless-powered two-way relay system with a cooperative jammer to maximize the minimum guaranteed secrecy capacity in the existence of multiple eavesdroppers. We proposed PS-TWR and TS-TWR protocols that adaptively control the power splitting ratio (ρ) and time switching ratio (α), respectively, according to the network condition. We proved the concavity of the secrecy capacity for each source with respect to ρ and α under the assumption of high SNR and derived optimal values of ρ and α to maximize the minimum guaranteed secrecy capacity ($C_S^{\min}$). Analysis and simulation results showed that the proposed PS-TWR and TS-TWR protocols using the derived ρ^* and α^* achieve the near-optimal $C_S^{\min}$ in various network environments no matter how many eavesdroppers exist anywhere. In addition, the comparison of PS-TWR and TS-TWR revealed that PS-TWR is well protected against the eavesdropping than TS-TWR. We expect the proposed wireless-powered two-way re-

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/TIFS.2018.2847452, IEEE Transactions on Information Forensics and Security

laying protocols to show promise as alternatives for resolving not just energy deficiency but also information security in energy-limited wireless networks. To extend this study, we can consider the cooperation among multiple eavesdroppers to decode the received signal together and we leave this issue for further study.

References

[1] Cisco visual networking index: Forecast and methodology, 2016-2021, June 6, 2017 [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

[2] R. H. Y. Louie, Y. Li, B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison," *IEEE Trans. Wireless Commun.,* vol. 9, no. 2, pp. 764-777, Feb. 2010.

[3] M. Zhou, Q. Cui, R. Jantti, X. Tao, "Energy-efficient relay selection and power allocation for two-way relay channel with analog network coding," *IEEE Commun. Lett.,* vol. 16, no. 6, pp. 816-819, June 2012

[4] H.-M. Wang, Q. Yin, Z.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.,* vol. 60, no. 7, pp. 3532-3545, July 2012.

[5] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347-376, First Quart 2017.

[6] 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.

[7] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076-6085, Dec. 2013.

[8] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35-38, Jan. 2013.

[9] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans Inf. Forensics Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[10] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189-2203, Apr. 2014.

[11] H. Long, W. Xiang, and Y. Li, "Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Trans Inf. Forensics Security*, vol. 12, no. 6, pp. 1309-1318, June 2017.

[12] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[13] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Nov. 2013, pp. 1555-1559.

[14] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185-2199, May 2014.

[15] 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.

[16] 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.

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

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

[19] Z. Chen, B. Xia, and H. Liu, "Wireless information and power transfer in two-way amplify-and-forward relaying channels," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2014, pp. 168-172.

[20] K. Tutuncuoglu, B. Varan, and A. Yener, "Throughput maximization for two-way relay channels with energy harvesting nodes: The impact of relaying strategies," *IEEE Trans. Commun.*, vol. 63, no.6, pp. 2081-2093, June 2015.

[21] Z. Fang, X. Yuan, and X. Wang, "Distributed energy beamforming for simultaneous wireless information and power transfer in the two-way relay channel," *IEEE Signal Process. Lett.*, vol. 22, no. 6, pp. 656-660, June 2015.

[22] M. Ju, J. H. Oh, and K.-S. Hwang, "PSR-based ANC protocol in energy harvesting bidirectional networks," in *Proc. International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2016, pp. 187-191.

[23] S. Modem and S. Prakriya, "Performance of analog network coding based two-way EH relay with beamforming," *IEEE Trans. Commun.*, vol. 65, no.4, pp. 1518-1535, Apr. 2017.

[24] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO beamforming for simultaneous wireless information and power transfer," *IEEE Trans. Signal Process.,* vol. 62, no. 18, pp. 4798-4810, Sep. 2014.

[25] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.,* vol. 15, no. 4, pp. 3085-3096, Apr. 2016.

[26] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.,* vol. 65, no. 1, pp. 180-190, Jan. 2016.

[27] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure OFDM system," *IEEE Trans. Veh. Technol.,* vol. 67, no. 2, pp. 1331-1346, Feb. 2018.

[28] F. Jameel, S. Wyne, and Z. Ding, "Secure communications in three-step two-way energy harvesting DF relaying," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1-1, 2017.

[29] 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.

[30] 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.

[31] 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.

Kisong Lee [S'10-M'14] received the B.S. degree in the Department of Electrical Engineering from Information and Communications University (ICU), Korea, in 2007 and the M.S. and Ph.D. degrees in the Department of Electrical Engineering from the Korea Advanced Institute of Science and Technology (KAIST), Korea, in 2009 and 2013, respectively. He was a researcher in the Electronics and Telecommunications Research Institute (ETRI) from September 2013 to February 2015. From March 2015 to August 2017, he was an assistant professor in the Department of Information and Telecommunication Engineering at Kunsan National University. He is currently an assistant professor in the School of Information and Communication Engineering, Chungbuk National University, Cheongju, South Korea. His research interests include self-organizing networks, radio resource management, magnetic induction communication, wireless power transfer, and energy harvesting networks.

Jun-Pyo Hong [S'08-M'14] received the B.Sc. degree from the Information and Communications University, Daejeon, Korea, in 2008 and the M.S. and Ph.D. degrees from the Korea Advance Institute of Science and Technology (KAIST), Daejeon, Korea, in 2010 and 2014, respectively, all in electrical engineering. In 2015, he was a researcher at Electronics and Telecommunications Research Institute (ETRI), where he worked on RAN architecture for mobile communication systems. He is currently an Assistant Professor with Department of Information and Communications Engineering, Pukyoung National University, Busan, Korea.

Hyun-Ho Choi [S'02-M'07] received his B.S., M.S. and Ph.D. degrees all in the Department of Electrical Engineering from Korea Advanced Institute of Science and Technology (KAIST), Korea, in 2001, 2003, and 2007, respectively. From Feb. 2007 to Feb. 2011, he was a senior engineer at the Communication Lab. In Samsung Advanced Institute of Technology (SAIT), Korea. Since March 2011, he has been a professor in the Department of Electrical, Electronic, and Control Engineering, and the Institute for Information Technology Convergence, Hankyong National University, Korea. His current research interests include bio-inspired algorithms, distributed optimization, machine learning, wireless energy harvesting, mobile ad hoc networks, and next-generation wireless communication. He was a co-recipient of the SAIT patent award (2010) and the paper award at Samsung conference (2010), and also received the excellent paper award at ICUFN 2012, the best paper award at ICN 2014, and the best paper award at Qshine 2016. He is a member of IEEE, IEICE, KICS and KIICE.

Tony Q.S. Quek [S'98-M'08-SM'12-F'18] received the B.E. and M.E. degrees in Electrical and Electronics Engineering from Tokyo Institute of Technology, respectively. At MIT, he earned the Ph.D. in Electrical Engineering and Computer Science. Currently, he is a tenured Associate Professor with the Singapore University of Technology and Design (SUTD). He also serves as the Acting Head of ISTD Pillar and the Deputy Director of the SUTD-ZJU IDEA. His current research topics include wireless communications and networking, internet-of-things, network intelligence, wireless security, and big data processing.

Dr. Quek has been actively involved in organizing and chairing sessions, and has served as a member of the Technical Program Committee as well as symposium chairs in a number of international conferences. He is currently an elected member of IEEE Signal Processing Society SPCOM Technical Committee. He was an Executive Editorial Committee Member for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, and an Editor for the IEEE WIRELESS COMMUNICATIONS LETTERS. He is a co-author of the book "Small Cell Networks: Deployment, PHY Techniques, and Resource Allocation" published by Cambridge University Press in 2013 and the book "Cloud Radio Access Networks: Principles, Technologies, and Applications" by Cambridge University Press in 2017.

Dr. Quek was honored with the 2008 Philip Yeo Prize for Outstanding Achievement in Research, the IEEE Globecom 2010 Best Paper Award, the 2012 IEEE William R. Bennett Prize, the 2015 SUTD Outstanding Education Awards – Excellence in Research, the 2016 IEEE Signal Processing Society Young Author Best Paper Award, the 2017 CTTC Early Achievement Award, the 2017 IEEE ComSoc AP Outstanding Paper Award, and the 2017 Clarivate Analytics Highly Cited Researcher. He is a Distinguished Lecturer of the IEEE Communications Society and a Fellow of IEEE.