Security Performance Analysis for Best Relay Selection in Energy-Harvesting Cooperative Communication Networks

GUANGNA ZHANG¹, YUANYUAN GAO¹, (Member, IEEE), HYDONG LUO¹, SHIJE WANG², MINGXI GUO¹, AND NAN SHA¹
¹College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
²61660 Troops, Beijing 100089, China
Corresponding author: Yuanyuan Gao (njyygao@sina.com)

ABSTRACT In this paper, we investigate an energy-harvesting cooperative communication network, which comprises of a source, a destination, and multiple decode-and-forward (DF) relays in the presence of multiple passive eavesdropper (Es). Es attempt to intercept confidential information transmissions from the source to destination via DF relays. In this network, all the DF relays harvest energy from radio-frequency (RF) signals of a source through time-switching receivers. In order to improve the physical layer security of energy-harvesting cooperative communication networks, we propose a best relay selection (BRS) scheme, where the “best” relay is chosen to assist the source-destination transmission. For the purpose of comparison, we consider the classic direct transmission (DT) and equal relay selection (ERS) as benchmark schemes. We derive the exact closed-form expressions of outage probability (OP) and intercept probability (IP) for the ERS and BRS schemes over Rayleigh fading channels. Besides, the security-reliability tradeoff (SRT) is analyzed as a metric to evaluate the tradeoff performance of the proposed BRS scheme. Numerical results show that the SRT of the BRS scheme consistently outperforms that of the ERS scheme, which demonstrates the advantage of our proposed scheme against eavesdroppers. Besides, it is verified that total error rate (TER) defined as the sum of OP and IP can be minimized for both the ERS and BRS schemes through changing the time allocation factor between information transmission and energy harvesting phases. Moreover, there is a best energy conversion efficiency to obtain a maximal SRT value of the ERS and BRS schemes. In addition, as the number of DF relays increases, the SRT of BRS scheme improves notably, while that of ERS scheme remains unchanged. And as the number of Es increases, the SRT of both the ERS and BRS schemes become worse.

INDEX TERMS Cooperative communication, physical layer security, best relay selection (BRS), outage probability (OP), intercept probability (IP), security-reliability tradeoff (SRT).

I. INTRODUCTION Nowadays, energy harvesting (EH) emerges as a promising technique to deal with the scarcity of energy resources and prolong the lifetime of wireless networks, especially in hazardous environments where replacing or recharging batteries is infeasible or costly for sensors embedded inside the human body or in building structures, as well as wireless mobile devices that are not easily accessible [1]–[4]. Differing from the conventional EH from solar, wind, vibration and thermoelectric effects [5], [6], a new emerging technique called Simultaneous Wireless Information and Power Transfer (SWIPT) makes use of ambient radio-frequency (RF) signals to carry energy and information at the same time, which ensures energy-constrained nodes harvest energy and process information simultaneously [7]–[9]. Time-switching (TS) protocol and power-splitting (PS) protocol are two protocols for SWIPT [10], [11]. To be specific, the TS receiver harvests energy at the beginning of the transmission and processes information in the remaining time [9], [12]. While the PS receiver divides the arrived RF signals into two parts, which are employed for energy harvesting and information processing, respectively [9], [12], [13].
Because of the broadcast nature of wireless communication, confidential information transmissions may be readily intercepted by malicious eavesdroppers. Thus, wireless communication security has become a significant issue [14], [15]. In recent years, physical layer security has been investigated to protect encrypted data against eavesdroppers [16], [17], which exploits the physical characteristics of wireless fading channels as metrics to evaluate the secrecy of data transmission. Therefore, physical layer security can avoid being cracked through exhaustive key search to guarantee wireless security perfectly. In [18], Wyner first examined physical layer security for a discrete memoryless wiretap channel model, and then extended to a Gaussian, broadcast, and wireless fading channels in [19]–[21]. Besides, Wyner has demonstrated that when the achievable data rate of the main channel was larger than that of the wiretap channel, secure data transmission could be ensured.

Recently, cooperation communication is exploited as an effective way to guarantee physical layer security of wireless communication [22]–[24]. In cooperative communication networks, relays act as intermediate wireless devices and adopt amplify-and-forward (AF) and decode-and-forward (DF) protocols to process received signals. Cooperative beamforming and cooperative jamming are two general means to take advantage of relay nodes. Although replacing or recharging batteries of relay nodes can avoid energy harvesting, it incurs a high cost and cannot be convenient or even hazardous, such as in toxic environments. Therefore, researchers begin to pay more attention on combining the energy harvesting and cooperation communication to prolong the lifetime of wireless networks and solve the scarcity of energy resources [25]–[38]. Literature [27] investigated the secrecy performance of a two-hop communication between a source and a destination using destination-assisted jamming, for the reason that the source used an AF wireless energy-harvesting untrusted relay to forward the confidential information to the legitimate destination. References [28]–[31] combined cooperative jamming and energy-harvesting relay to improve the physical layer security performance. Reference [28] proposed an energy-harvesting destination aided cooperative jamming framework to protect encrypted information from being intercepted by the untrusted relay. And a source-destination link with an energy-harvesting full-duplex relay and a jammer in the presence of an eavesdropper was investigated in [29]. In [30], source and EH relay could transmit message signal in addition to sending jamming signal simultaneously to degrade the capacity at eavesdropper. Besides, [31] researched an adaptive cooperative jamming (ACJ) scheme to adaptively adjust power allocation factor to maximize the secrecy rate in practical networks where there is no eavesdroppers’ channel state information (CSI). References [32] and [33] studied wireless-powered two-way relay network, where [32] selected a best relay at the destination in energy-harvesting amplify-and-forward (EH-AF) protocol and energy-harvesting decode-and-forward (EH-DF) protocol technologies to maximize the end-to-end achievable secrecy rates, [33] investigated the relay system with a cooperative jammer to maximize the minimum guaranteed secrecy capacity in the existence of multiple eavesdroppers. Multiple relays capable of harvesting energy from RF signals were employed in [25], [26], [34], where [25] proposed a centralized scheme and a distributed sub-optimal scheme in a game theoretic approach, and [26] focused on the performance analysis of energy-harvesting relay-aided cooperative network under slow fading channels from a perspective of outage behavior. Moreover, [34] investigated the AF and compress-and-forward (CF) relay networks with energy-harvesting untrusted relay nodes, and derived the achievable secrecy rate for two scenarios. To be more practical, [35]–[38] extended the researches to nonlinear EH model, where [35] considered the wirelessly powered two-way communication, and [36] analyzed the performance of wireless powered AF relaying over Nakagami-m fading channels. Besides, [37] designed the SWIPT protocol for massive multi-input multi-output (mMIMO) system in the beam-domain (BD), and [38] proposed a secure two-phase communication protocol with the help of a hybrid base station (HBS) in the wireless powered communication networks (WPCNs) employing the nonlinear EH model.

Motivated by the above research, we explore physical layer security for an EH cooperative communication network consisting of a source, a destination, and multiple decode-and-forward (DF) relays, which are capable of collecting the energy from RF signal of the source. Multiple passive eavesdroppers (Es) are assumed to tap the confidential information transmissions from the source to destination via relay nodes. A best relay selection (BRS) scheme is proposed to improve the physical layer security of the above network. Besides, we present the classic direct transmission (DT) and equal relay selection (ERS) schemes to compare with the BRS scheme.

Then we derive the exact closed-form expressions of outage probability (OP) and intercept probability (IP) for the aforementioned ERS and BRS schemes over Rayleigh fading channels, which are used to characterize wireless reliability and security respectively. Besides, we analyze the security-reliability tradeoff (SRT) to describe the tradeoff performance of the ERS and BRS schemes. For the reason that Nakagami-m distribution is equal to Rayleigh distribution, Rician distribution and unilateral Gaussian distribution respectively when it chooses different shape parameter, which can better fit with the actual channel fading. Therefore, it is more practical to study other performance metrics such as achievable secrecy rate, optimal power allocation, secrecy throughout under Nakagami-m fading channels [22], [36], [39]. The numerical results show as follows: Firstly, the SRT of the BRS scheme always performs better than that of ERS scheme. Secondly, adjusting the time allocation factor between information transmission and energy harvesting phases can minimize the total error rate (TER) for both the ERS and BRS schemes. Thirdly, a best energy conversation efficiency exists...
II. SYSTEM MODEL

Fig.1 presents a system model of the energy-harvesting cooperative communication network consisting of a source (S), a destination (D), $N_r$ DF relays equipped with energy harvesters, and $N_e$ passive eavesdroppers which may overhear encrypted data transmissions from S to D via relay nodes independently. Besides, each node in Fig.1 is equipped with one antenna and operates in time division duplex mode. The solid and dash lines represent the main links and wiretap links, respectively. We assume that there exists no direct links between S and D/E due to the deep shadowing [23], [24]. Moreover, we suppose that the distances between relays are much smaller compared with the distances between each relay and S/D/E due to the deep shadowing [23], [24].

The system model in this paper is applicable to a scenario where shared electrical vehicles equipped with energy harvesters may be charged by RF signals of other surrounding environments or a potential application include a wireless sensor network for structure monitoring by embedding sensors in buildings, bridges, roads, and so on [3], [25], [40].

to maximize SRT value of the above two schemes. Finally, with the number of relays increasing, the SRT of BRS scheme becomes better, while that of ERS scheme remains all the same. And with the number of Es increasing, the SRT of both the ERS and BRS schemes become worse.

The remainder of this paper is summarized as follows. In section II, system model of the energy-harvesting cooperative communication network is presented. In section III, we propose a BRS scheme to combat eavesdropping attacks. And the OP and IP as well as SRT of ERS and BRS schemes are carried out. Next, numerical results and discussions are presented in section IV. Finally, we conclude our work in section V.

FIGURE 1. System model of energy-harvesting cooperative communication network.

Here, the channel gain coefficients of S-$R_i$, $R_i$-$D$, $R_i$-$E_i$ are denoted as $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{il}|^2$, respectively. Noting that all channels are modeled as quasi-static Rayleigh fading channels throughout this paper, therefore $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{il}|^2$ are independently exponentially distributed random variables with zero means and respective variances $\sigma_{si}^2$, $\sigma_{id}^2$ and $\sigma_{il}^2$, that is

$$f_{|h_{pq}|^2}(x) = \frac{1}{\sigma_{pq}^2} \exp \left(-\frac{x}{\sigma_{pq}^2}\right) \quad (1)$$

where $(p, q)$ includes $(s, i)$, $(i, d)$ and $(i, l)$, $i \in 1, 2, \cdots, N_r$, $l \in 1, 2, \cdots, N_e$. Noting that only the instantaneous CSI of main channels S-$R_i$, $R_i$-$D$ are considered to be available, while that of the wiretap channels $R_i$-$E_i$ are unavailable because all Es are passive.

In this paper, we adopt TS protocol to harvest energy and process information, which is shown in Fig.2. In Fig.2, $T$ is the duration of EH and information transmission from S to D, and $\alpha$ is the time allocation ratio for relays harvesting energy from the source signal ($0 \leq \alpha \leq 1$). Here, the same $\alpha$ is employed for all relays. However, different value of $\alpha$ will affect the network security performance. Therefore, it is our future work to explore the case that different relays have different $\alpha$. To be specific, relays harvest energy from RF signals of S for a duration of $\alpha T$. All the energy harvested is consumed by the relays to assist in information transmission. Then the remaining $(1-\alpha)T$ is used for information transmission. Because two time slots are required to transmit source signal from S to D via $R_i$, such that $(1-\alpha)T/2$ is used to transmit information from S to $R_i$, and the remaining $(1-\alpha)T/2$ is used to transmit information from $R_i$ to D. Here, we assume that each relay will use up all of the energy they have harvested and will harvest it again in the next $T$ duration just as they have done in the previous $T$ duration.

The energy harvested at $R_i$ is expressed as

$$E_h = \eta \alpha T P_s |h_{si}|^2 \quad (2)$$

where $P_s$ is the transmit power of S, $\eta$ is the energy conversion efficiency, $0 \leq \eta \leq 1$. Therefore, the transmit power of $R_i$ is

$$P_i = \frac{2\eta \alpha P_s |h_{si}|^2}{1-\alpha} \quad (3)$$

FIGURE 2. Illustration of the TS energy harvesting model.
Then in the first phase of information transmission, the received signal at $R_i$ from $S$ is written as

$$y_{si} = \sqrt{P_i} h_{si} x_s + n_i$$  \hspace{1cm} (4)$$

where $x_s$ is the source signal, $n_i$ is the additive white Gaussian noise (AWGN) with zero mean and variance $N_0$ at $R_i$. Then, the channel capacity of $S-R_i$ is obtained using the theory of Shannon capacity

$$C_{si} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{|h_{si}|^2 P_s}{N_0} \right)$$  \hspace{1cm} (5)$$

Learning from Shannon’s coding theorem, when $C_{si} > R_i$, the relay $R_i$ is equipped to decode the received signal in success, where $R$ is the data rate; Otherwise, $R_i$ cannot recover the signal successfully. There are $2^N$ possible subsets, denoted as $\lambda_i$, in which all the relays can successfully decode $x_s$. The sample space of $\lambda$ is described as

$$\Omega = \{ \emptyset, \lambda_1, \lambda_2, \ldots, \lambda_m, \ldots, \lambda_{2^N-1} \}$$  \hspace{1cm} (6)$$

where $\emptyset$ represents no relay can decode $x_s$ successfully; $\lambda_n$ denotes the $n$th nonempty subset of the $N_r$ relay nodes, and all relays in $\lambda_n$ can decode $x_s$.

Hence, the event $\lambda = \emptyset$ can be written as

$$C_{si} < R_i, \quad i = 1, 2, \ldots, N_r$$  \hspace{1cm} (7)$$

Meanwhile, the event $\lambda = \lambda_n$ is expressed as

$$\begin{cases} C_{si} > R_i, & R_i \in \lambda_n \\ C_{sj} < R_j, & R_j \in \lambda_n \end{cases}$$  \hspace{1cm} (8)$$

where $\lambda_n$ represents the complementary set of $\lambda_n$.

In the second phase, one relay $R_i$ is selected from $\lambda_n$ to forward $x_s$ to $D$. The received signal at $D$ is written as

$$y_d = \sqrt{P_d} h_{id} x_s + n_d$$  \hspace{1cm} (9)$$

where $n_d$ is the AWGN with zero mean and variance $N_0$ at $D$. In this paper, we just consider the scenario that only single relay rather than multiple relays is selected to help information transmission, for the reason that complex symbol-level synchronization among all the relays is required in multiple relays selected scheme to avoid inter-symbol interference. Besides, each relay in multiple relays selected scheme must finish the wireless communication processes of them. Therefore, higher complexity is induced in multiple relays selected scheme, and it is of interest to investigate employing multiple relays to assist in transmitting signal in our future work.

The channel capacity of $R_i-D$ is acquired from Eq.(9)

$$C_{id} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{|h_{id}|^2 P_i}{N_0} \right)$$  \hspace{1cm} (10)$$

Meanwhile, Es attempt to intercept the decoded signal $x_s$, and the received signal at $E_l$ is expressed as

$$y_{el} = \sqrt{P_l} h_{il} x_s + n_l$$  \hspace{1cm} (11)$$

where $n_l$ is the AWGN with zero mean and variance $N_0$ at $E_l$. Similar to Eq.(10), the channel capacity of $R_i-E_l$ can be written as

$$C_{ie_l} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{|h_{il}|^2 P_i}{N_0} \right)$$  \hspace{1cm} (12)$$

For the reason that all eavesdroppers tap encrypted information independently with each other, if the strongest $E$ has successfully tapped the information from $R_i$, then secure data transmission would not be guaranteed. Hence, we denote the overall channel capacity of $R_i-E_l$ as

$$C_{ie} = \max_{l \in \xi} C_{ie_l} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{\max_{l \in \xi} |h_{il}|^2 P_i}{N_0} \right)$$  \hspace{1cm} (13)$$

where $\xi$ is the set of Es.

Substitute Eq.(3) into Eq.(10) and Eq.(13) respectively to obtain

$$C_{id} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{2\eta\alpha P_s |h_{id}|^2}{(1 - \alpha) N_0} \right)$$  \hspace{1cm} (14)$$

$$C_{ie} = \frac{(1 - \alpha) T}{2} \log_2 \left( 1 + \frac{2\eta\alpha P_s |h_{il}|^2 \max_{l \in \xi} |h_{il}|^2}{(1 - \alpha) N_0} \right)$$  \hspace{1cm} (15)$$

Two significant metrics, that is OP and IP, are discussed in [41], [42] to characterize network reliability and security, respectively, which are defined as

$$P_{out} = \Pr(C_d < R)$$  \hspace{1cm} (16)$$

$$P_{int} = \Pr(C_e > R)$$  \hspace{1cm} (17)$$

Additionally, SRT is employed to evaluate network tradeoff performance [22]

$$SRT = (1 - P_{out}) \cdot (1 - P_{int})$$  \hspace{1cm} (18)$$

which shows that the greater of SRT, the better of the system tradeoff performance; and the smaller of SRT, the worse of the system tradeoff performance.

III. SECURITY PERFORMANCE ANALYSIS OF THE ERS SCHEME AND THE BRS SCHEME

In this section, we analyze the OP and IP as well as the SRT of the ERS scheme and BRS scheme.

A. ERS SCHEME

In this scheme, each relay that can decode $x_s$ in success has the equal chance to be selected to assist in signal transmission. Thus one relay is selected randomly among $\lambda_n$.

Based on the law of total probability, we can acquire the OP of the ERS scheme as

$$P_{out}^{ERS} = \Pr(C_{id} < R, \lambda = \emptyset)$$

$$+ \sum_{n=1}^{2^N-1} \Pr(C_{id} < R, \lambda = \lambda_n)$$  \hspace{1cm} (19)$$
For the event $\hat{\mathcal{A}} = \emptyset$, no relay can be chosen, so that $C_{id} = 0$. Thus, $C_{id} < R$ always sets up. According to this result and employing Eq.(7) and Eq.(8), Eq.(19) is simplified as

$$P_{out}^{ERS} = Pr(\hat{\mathcal{A}} = \emptyset) + \sum_{n=1}^{2N-1} Pr(\hat{\mathcal{A}} = \mathcal{A}_n) Pr(C_{id} < R)$$

$$= \prod_{i=1}^{N} Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right) + \sum_{n=1}^{2N-1} \prod_{i=\mathcal{A}_n}^{N} Pr\left(|h_{id}|^2 > \frac{\Delta}{\gamma}\right)$$

$$ \times \prod_{R_j \in \mathcal{A}_n} \prod_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right) \times Pr(C_{id} < R)$$  

(20)

where $\Delta = 2^{\frac{\gamma}{2(1-\eta)}} - 1, \gamma = P_s/N_0$. Noting that $|h_{id}|^2$, $|h_{id}|^2$ and $|h_{id}|^2$ are independently exponentially distributed random variables with zero means and respective variances $\sigma^2_{li}$, $\sigma^2_{li}$ and $\sigma^2_{li}$, we can obtain

$$Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right) = 1 - e^{-\frac{\Delta}{\sigma^2_{li}}}$$  

(21)

Then we can acquire the closed-form expressions of $Pr\left(|h_{id}|^2 > \frac{\Delta}{\gamma}\right)$ and $Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right)$ using Eq.(21).

According to Eq.(14), $Pr(C_{id} < R)$ is written as

$$Pr(C_{id} < R) = \frac{1}{|\mathcal{A}_n|} \sum_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 |hd| < \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma}\right)$$  

(22)

where $|\mathcal{A}_n|$ is the cardinality of the set $\mathcal{A}_n$. We denote $X_i = |h_{id}|^2$, $Y_i = |h_{id}|^2$, so the joint probability density function (PDF) of $(X_i, Y_i)$ can be given as

$$f_{X_i, Y_i}(x_i, y_i) = \frac{1}{\sigma^2_{li}} e^{-\frac{x_i^2 + y_i^2}{2\sigma^2_{li}}}$$  

(23)

Let us denote $q_{id} = Pr\left(|h_{id}|^2 |hd| < \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma}\right)$. Hence, we can further obtain the expression of $q_{id}$ as

$$q_{id} = Pr\left(X_i < \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma}\right) = \int_{0}^{\infty} f_{X_i, Y_i}(x_i, y_i)dx_i dy_i$$  

(24)

where $\tau = \left\{(x_i, y_i) | x_i y_i < \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma}\right\}$. Employ the PDF of $(X_i, Y_i)$ to rewrite $q_{id}$ as

$$q_{id} = \int_{0}^{\infty} \frac{1}{\sigma^2_{li}} e^{-\frac{\Delta}{\sigma^2_{li}}} dx_i \int_{0}^{\infty} \frac{1}{\sigma^2_{li}} e^{-\frac{\Delta}{\sigma^2_{li}}} dy_i$$

$$= \int_{0}^{\infty} \frac{1}{\sigma^2_{li}} e^{-\frac{\Delta}{\sigma^2_{li}}} \left(1 - e^{-2\eta \alpha \gamma \sigma^2_{li}}\right) dx_i$$

$$= 1 - \frac{1}{\sigma^2_{li}} \sqrt{\frac{2\Delta (1 - \alpha) \sigma^2_{li}}{\eta \alpha \gamma \sigma^2_{si}}} k_1\left(\sqrt{\frac{2\Delta (1 - \alpha) \sigma^2_{li}}{\eta \alpha \gamma \sigma^2_{si}}} k_1\right)$$  

(25)

Meanwhile, the IP of the ERS scheme is expressed as

$$P_{int}^{ERS} = Pr(C_{ie} > R, \hat{\mathcal{A}} = \emptyset) + \sum_{n=1}^{2N-1} Pr(C_{ie} > R, \hat{\mathcal{A}} = \mathcal{A}_n)$$

(26)

When $\hat{\mathcal{A}} = \emptyset$, $C_{ie} > R$ cannot establish. Similar to Eq.(20), we rewrite Eq.(26) as

$$P_{int}^{ERS} = \sum_{n=1}^{2N-1} \prod_{R_j \in \mathcal{A}_n} \prod_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 > \frac{\Delta}{\gamma}\right)$$

$$\times \prod_{R_j \in \mathcal{A}_n} \prod_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right) \times Pr(C_{ie} > R)$$  

(27)

where $Pr\left(|h_{id}|^2 > \frac{\Delta}{\gamma}\right)$ and $Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right)$ have been obtained before. The closed-form expression of $Pr(C_{ie} > R)$ is given in Appendix A.

Moreover, the expression of SRT for the ERS scheme is written as

$$SRT = \left(1 - P_{out}^{ERS}\right) \cdot \left(1 - P_{int}^{ERS}\right)$$  

(28)

**B. BRS SCHEME**

In this subsection, we analyze the OP and IP as well as SRT of the BRS scheme. For the reason that only the instantaneous CSI of main channels are available, the best relay selection criteria is expressed as

$$R_{bd} = \arg\max_{R_j \in \mathcal{A}_n} \left|h_{bd}\right|^2$$  

(29)

Similar to Eq.(20), the OP of the BRS scheme is written as

$$P_{out}^{BRS} = Pr(\hat{\mathcal{A}} = \emptyset) + \sum_{n=1}^{2N-1} Pr(\hat{\mathcal{A}} = \mathcal{A}_n) Pr(C_{bd} < R)$$

$$= \prod_{i=1}^{N} Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right)$$

$$+ \sum_{n=1}^{2N-1} \prod_{R_j \in \mathcal{A}_n} \prod_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 > \frac{\Delta}{\gamma}\right)$$

$$\times \prod_{R_j \in \mathcal{A}_n} \prod_{R_j \in \mathcal{A}_n} Pr\left(|h_{id}|^2 < \frac{\Delta}{\gamma}\right) \times Pr(C_{bd} < R)$$  

(30)

The main work to obtain $P_{out}^{BRS}$ is to derive the closed-form expression of $Pr(C_{bd} < R)$, which is shown in Appendix B.
Meanwhile, the IP of the BRS scheme is obtained based on Eq. (27)

\[ P_{\text{BRS int}} = \sum_{n=1}^{2N_r - 1} \prod_{R_i \in A_n} \Pr \left( |h_{si}|^2 > \frac{\Delta}{\gamma} \right) \]

\[ \times \prod_{R_j \in A_n} \Pr \left( |h_{sj}|^2 < \frac{\Delta}{\gamma} \right) \times \Pr (C_{be} > R) \]

(31)

We demonstrate the derivation of the closed-form expression of \( \Pr (C_{be} > R) \) in Appendix C.

Therefore, the expression of SRT for the BRS scheme is expressed as

\[ SRT = \left( 1 - P_{\text{BRS out}} \right) \cdot \left( 1 - P_{\text{BRS int}} \right) \]

(32)

IV. NUMERICAL RESULTS AND DISCUSSIONS

This section presents the numerical results of the OP and IP as well as SRT for the ERS scheme and BRS scheme under the Rayleigh fading channels. And the simulation results are also demonstrated to validate our theoretical analysis.

For benchmarking purpose, we suppose data rate \( R = 0.8 \text{bit/s/Hz} \), \( T = 1s \), \( \sigma_{ii}^2 = \sigma_{jj}^2 = 0.6 \), \( \sigma_{id}^2 = \sigma_{kd}^2 = 1 \), \( \sigma_{il}^2 = 0.2 \). And the number of relays \( N_r = 4 \), the number of eavesdroppers \( N_e = 3 \). Moreover, the time allocation ratio \( \alpha = 0.4 \) and energy conversion efficiency \( \eta = 0.4 \) are assumed. In addition, we employ the term ‘s’ represents the simulation results, while the term ‘t’ denotes our theoretical results.

Fig. 3 shows OP and IP versus transmit power \( \gamma \) of the ERS scheme and BRS scheme as well as the direct transmission. Simulation results match well with the theoretical results. From Fig.3, we can know that the OP of these three schemes decrease with an increasing value of \( \gamma \), while the corresponding IP of them increase. This result illustrates that there exists an SRT between the OP and IP in the wireless communication network in the presence of Es. Therefore, we analyze the SRT of the ERS and BRS schemes in the following Fig. 7 and Fig. 8. Besides, we observe that the OP of the BRS scheme is always better than that of the ERS scheme when \( \gamma \) is more than 6dB, whereas the IP of the BRS is consistently same as that of the ERS scheme. The reason for this result is that only the CSI of main links are considered to be available in both ERS and BRS schemes without knowing the CSI of the wiretap channels. In addition, the OP of the ERS and BRS schemes are consistently worse than that of DT, while the above two schemes are better than that of DT in terms of their IP.

We define the sum of OP and IP as the TER of the wireless communication network. In this part, the TER regarding to time allocation ratio \( \alpha \) is discussed. Fig. 4 demonstrates that the TER of BRS scheme is always lower than that of ERS scheme when \( \alpha \) is less than 0.8. Moreover, one can easily observe that TER of both the ERS and BRS schemes can be minimized by changing the value of \( \alpha \) between information transmission and EH phases at relays.

In Fig. 5, the OP and IP versus \( \eta \) of the ERS and BRS schemes are illustrated. It is obvious that the OP of ERS and BRS schemes decrease as \( \eta \) increases from zero to one.
while the corresponding IP of them increase accordingly. Because more energy can be employed to forward information at relays with an increasing value of $\eta$, then the signal strength received at destination as well as the eavesdroppers are enhanced giving rise to a decreasing OP and an increasing IP. Besides, the relationship of OP or IP for the BRS and ERS schemes are consistent with the results in Fig.1.

It is meaningful to further explore the SRT of two schemes in order to have a more intuitive understanding of the impact of $\eta$ on network tradeoff performance, which is given in Fig.6. We can see from Fig.6 that the SRT of the BRS scheme is consistently better than that of the ERS scheme. Besides, the SRT of both the ERS and BRS schemes can arrive at the maximum by adjusting the value of $\eta$, which means that both the above schemes can realize optimum tradeoff performance. Moreover, the BRS scheme can achieve the best tradeoff performance when $\eta$ is 0.4 (defined as $\eta_{\text{best}}$), which is lower than that of ERS scheme. For both the ERS and BRS schemes, when $\eta$ is lower or more than $\eta_{\text{best}}$, the OP or IP of them become larger resulting in a smaller SRT, respectively.

Similar to Fig.7, Fig. 8 describes the SRT versus $\gamma$ of the ERS and BRS schemes when $N_e$ = 4, 6, 10. It is known from Fig.8 that the SRT of ERS scheme is inferior to that of BRS scheme with the same $N_e$. Additionally, with an increasing number of $N_e$, the SRT of both schemes degrade accordingly. It is concluded that more confidential information will be overheard when the number of Es increases in the wireless network, which leads to the destruction of network security performance. Similarly, when the value of $N_e$ for both schemes is the same, the ERS scheme needs more transmit power to arrive at the best SRT than BRS scheme.

V. CONCLUSION

In this paper, we have studied security performance of two relay selection schemes-ERS and BRS schemes in an energy-harvesting cooperative communication network, which may be attacked by multiple uncooperative Es. Moreover, all the DF relays using time-switching receivers can collect energy from RF signals of a source. The exact closed-form expressions of OP and IP for the BRS and ERS schemes are derived over Rayleigh fading channels to describe wireless reliability and security respectively. Moreover, the SRT of them are also
analyzed to evaluate the network tradeoff performance. It is proved that the SRT of BRS scheme always performs better than that of the ERS scheme with the same $N_f$ and $N_e$, which demonstrates the advantage of our proposed BRS scheme against vicious attackers. Therefore, it is superb to employ the BRS scheme to enhance the security and reliability of wireless communication networks. Besides, the SRT of the BRS scheme can be improved by adjusting energy conversation efficiency $\eta$ or increasing the number of relays. Moreover, changing the time allocation factor $\alpha$ between information transmission and energy harvesting phases will minimize the TER of the cooperative communication network. It is noted that the same $\alpha$ is employed for all relays in this paper, which may be a restriction in practical application. Therefore, it is valuable to explore the case that different relays have different $\alpha$ in our future work, so as to achieve an optimal security-reliability tradeoff performance of the EH cooperative communication network.

**APPENDIXES**

**APPENDIX A**

**DERIVATION OF Pr(C_{ie} > R) IN EQ.(27)**

According to Eq.(15), $\Pr(C_{ie} > R)$ is written as

$$\Pr(C_{ie} > R) = \frac{1}{|\mathbb{N}_{\eta}|} \sum_{R_i \in \mathbb{N}_{\eta}} \Pr\left(|h_i|^2 \max_{l \in \xi} |h_l|^2 > \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma} \right)$$

Denoting $Z = \max_{l \in \xi} |h_l|^2$, we get the cumulative distribution function (CDF) of $Z$ as

$$F_Z(z) = \Pr\left(\max_{l \in \xi} |h_l|^2 < z\right) = 1 + \sum_{n=1}^{2N_e-1} (-1)^{P_n} 1 - \sum_{l \in \mathbb{N}_{\eta}} z_{il}$$

where $P_n$ is the $n$th nonempty subset of $\xi$. Then differentiate $Z$ to get the PDF of $Z$ as

$$f_Z(z) = \sum_{n=1}^{2N_e-1} (-1)^{P_n+1} \frac{1}{\sigma_d^2} e^{-\frac{z}{\sigma_d^2}}$$

Let us denote $\psi_1 = \Pr\left(|h_i|^2 \max_{l \in \xi} |h_l|^2 > \frac{\Delta (1 - \alpha)}{2\eta \alpha \gamma}\right)$, we obtain the expression of $\psi_1$ as

$$\psi_1 = \int_0^\infty f_Z(z) dz$$

where $C_n$ is the $n$th nonempty subset of $\mathbb{N}_{\eta} - R_i$. The expression of $\varphi_1$ is expressed in Eq.(25). Additionally, the
expression of $\psi_{II}$ is derived as following

$$
\psi_{II} = \sum_{n=1}^{2^{-a_{n_1}-1}-1} (-1)^C_{n_1} \int_{\tau} e^{-\sum_{R_k \in C_n} \frac{n_1}{\sigma_{id}} f_{X_i, Y_i} (x_i, y_i) dx_i dy_i
$$

$$
= \sum_{n=1}^{2^{-a_{n_1}-1}-1} (-1)^C_{n_1} \cdot \int_{0}^{\infty} \frac{1}{\sigma_{id}} e^{-\sum_{R_k \in C_n} \frac{n_1}{\sigma_{id}} dx_i} \int_{0}^{\Delta(1-a)} \frac{1}{\eta \varphi \sigma_{id}^2} \left( \sum_{R_k \in C_n} \frac{1}{\sigma_{id}} \right)^2 \cdot \varphi \Delta(1-a) \sigma_{id}^2 d\eta
$$

$$
= \sum_{n=1}^{2^{-a_{n_1}-1}-1} (-1)^C_{n_1} \cdot \frac{1}{\sigma_{id}} \cdot \left( \frac{1}{\sigma_{id}} \right)^2 \cdot \frac{2 \Delta(1-a)}{\eta \varphi \sigma_{id}^2} \left( \sum_{R_k \in C_n} \frac{1}{\sigma_{id}} \right)^2

\text{(40)}
$$

APPENDIX C

DERIVATION OF $\Pr(C_{be} > R)$ IN EQ.(31)

According to Eq.(15), $\Pr(C_{be} > R)$ is written as

$$
\Pr(C_{be} > R) = \Pr \left( \left| h_{bd} \right|^2 > \frac{\Delta (1-a)}{2 \eta \varphi \sigma_{id}^2} \right)
$$

$$
= \sum_{R_k \in \alpha_{d}} \Pr \left( \left| h_{bd} \right|^2 > \frac{\Delta (1-a)}{2 \eta \varphi \max \left| h_{id} \right|^2} \right)
$$

$$
= \sum_{R_k \in \alpha_{d}} \Pr \left( \left| h_{bd} \right|^2 > \frac{\Delta (1-a)}{2 \eta \varphi \max \left| h_{id} \right|^2} \right)
$$

$$
\cdot \Pr \left( \max_{R_k \in \alpha_{d} - R_k} \left| h_{id} \right|^2 < \left| h_{id} \right|^2 \right)
$$

$$
= \sum_{R_k \in \alpha_{d}} \psi_1 \psi_{II}

\text{(41)}
$$

The closed-form expression of $\psi_1$ has been obtained in Eq.(36). Then we pay our attention on deriving the expression of $\psi_{II}$. Denoting $X = \left| h_{id} \right|^2$, the PDF of $X$ can be given as

$$
f_X (x) = \frac{1}{\sigma_{id}} e^{-\frac{x}{\sigma_{id}^2}}. \text{ Then we acquire } \psi_{II} as

\psi_{II} = \Pr \left( \max_{R_k \in \alpha_{d} - R_k} \left| h_{id} \right|^2 < \left| h_{id} \right|^2 \right)
$$

$$
= \int_{0}^{\infty} \prod_{R_k \in \alpha_{d} - R_k} \Pr \left( \left| h_{id} \right|^2 < x \right) f_X (x) dx
$$

$$
= \int_{0}^{\infty} \left( 1 + \sum_{n=1}^{2^{-a_{n_1}-1}-1} (-1)^C_{n_1} e^{-\sum_{R_k \in C_n} \frac{n_1}{\sigma_{id}} \varphi} \right) f_X (x) dx
$$

$$
= \int_{0}^{\infty} \left( 1 + \sum_{n=1}^{2^{-a_{n_1}-1}-1} (-1)^C_{n_1} e^{-\sum_{R_k \in C_n} \frac{n_1}{\sigma_{id}} \varphi} \right) f_X (x) dx
$$

$$
= \int_{0}^{\infty} \left( 1 + \sum_{n=1}^{2^{-a_{n_1}-1}-1} \frac{\sigma_{id}^2}{\sigma_{id}^2} \right) f_X (x) dx
$$

$$
= \int_{0}^{\infty} \left( 1 + \sum_{n=1}^{2^{-a_{n_1}-1}-1} \frac{\sigma_{id}^2}{\sigma_{id}^2} \right) f_X (x) dx
$$

REFERENCES


GUANGNA ZHANG received the B.S. degree in measurement and control technology from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2014, and the M.S. degrees in communications engineering from the College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2017. She is currently pursuing the Ph.D. degree with PLA Army Engineering University. Her research interests include wireless communication, physical layer security, and cooperative communications.

YUANYUAN GAO received the B.S., M.S., and Ph.D. degrees in communications engineering from the College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 1990, 1994, and 2005, respectively. She is currently a Professor and the Dean of the Wireless Communications Department, CCE, PLA Army Engineering University. Her research topics span a large spectrum, including space-time coding, MIMO, cooperative communications, and anti-jamming communications.

HUADONG LUO received the B.S. degree from the PLA University of Science and Technology (PLAUST), Nanjing, China, in 2011. He is currently pursuing the M.S. degree with PLA Army Engineering University. His research interests include military equipment science and unmanned air vehicle technique.

SHIJIE WANG received the B.S. and M.S. degrees in communications engineering from the College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with PLA Army Engineering University. His research topics include wireless communication, physical layer security, and stochastic geometry.
MINGXI GUO received the B.S. and M.S. degrees in communication engineering and the Ph.D. degree in communications and information system from the PLA University of Science and Technology, Nanjing, China, in 2001, 2004, and 2010, respectively. He is currently an Associate Professor with the College of Communications Engineering, PLA Army Engineering University. His research interests include MIMO communication systems, signal processing for wireless communications, and cooperative communications.

NAN SHA received the B.S., M.S., and Ph.D. degrees in communications engineering from the College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2003, 2006, and 2014, respectively. His research interests include physical-layer network coding and cooperative communications.

***