Multidisciplinary : Rapid Review : Open Access Journal

Received September 12, 2020, accepted October 6, 2020, date of publication October 13, 2020, date of current version October 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3030794

Security and Reliability Analysis of a Two-Way Half-Duplex Wireless Relaying Network Using Partial Relay Selection and Hybrid TPSR Energy Harvesting at Relay Nodes

DUY-HUNG HA[1], TAN N. NGUYEN[2], (Member, IEEE), MINH H. Q. TRAN[3], XINGWANG LI[4], (Senior Member, IEEE), PHUONG T. TRAN[2], (Senior Member, IEEE), AND MIROSLAV VOZNAK[1], (Senior Member, IEEE)

[1]VSB, Technical University of Ostrava, 708 00 Ostrava, Czech Republic
[2]Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 729000, Vietnam
[3]Optoelectronics Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 729000, Vietnam
[4]School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454003, China

Corresponding author: Tan N. Nguyen (nguyennhattan@tdtu.edu.vn)

This work was supported by the VSB, Technical University of Ostrava, Czech Republic, under Grant SGS SP2020/65.

ABSTRACT In recent years, physical layer security has been considered as an effective method to enhance the information security beside the cryptographic techniques that are used in upper layers. In this paper, we provide the security analysis for a two-way relay network, where the two sources can only communicate through the intermediate relay nodes. In particular, we consider the scenario that there is an eavesdropper in the vicinity of one source node. Both reliability and security aspects are taken into consideration in our work. To enhance the reliability of communication, the intermediate relays are supplied with the energy harvested from the sources' radio frequency (RF) signals using hybrid time-switching and power splitting (TPSR) protocol. Also, we apply the relay selection technique to select the best relay for the information exchange between two sources. Regarding security, the secrecy of information is improved with the help of friendly jammers nearby the eavesdropper. We provide the in-dept reliability and security analysis in terms of the closed-form expressions of the outage probability (OP) at the source nodes, the intercept probability (IP) at the eavesdropper, the secrecy outage probability (SOP), and the average secrecy capacity (ASC) of the system. Finally, the Monte Carlo simulations are also conducted to verify the correctness of our analysis and the effectiveness of the proposed scheme. Numerical results confirms that with the appropriate and feasible choices of involved parameters, both outage OP and IP can be kept at small values to guarantee the reliable and secure communication of the system.

INDEX TERMS Half-duplex, energy harvesting, decode-and-forward, two-way relay channel, physical layer security, intercept probability, secrecy outage probability, average secrecy capacity.

I. INTRODUCTION

Secrecy is always a critical issue in wireless communications because of the information leakage resulting from the broadcast nature of the wireless medium. It leaves unprotected information vulnerable. Besides conventional cryptographic techniques to improve the security, the pioneering work by Wyner [1] on the wiretap channel and subsequent works [2], [3] show that the secrecy can also be guaranteed along with reliability by introducing randomness in coding or signaling to confuse the eavesdropper at the physical layer. This is known as physical layer security (PLS). During the last decade, PLS has experienced a resurgence of interest from a lot of scientists [4] due to its potential to enhance the quality of communication to satisfy the vast demand of mobile users. PLS has been applied in relay networks [5], cellular networks [6], [7], cognitive radio networks [8], IoT networks [9], and massive multiple-input multiple-output (MIMO) networks [10]. In multi-user networks, physical layer security can be improved by node cooperation.

The associate editor coordinating the review of this manuscript and approving it for publication was Marco Martalo.

Relay nodes can actively relay the source signal - cooperative relay (CR) or passively jam the eavesdropper - cooperative jamming (CJ).

In CR scheme, relay not only listens and forwards messages from the source to the destination, but also prevent the information from leaking to eavesdroppers [5], [11]–[13]. For example, in [5], the authors proposed a generalized multi-relay selection scheme to improve the security in a cooperative relay network. They derived a semi-closed-form expression of the secrecy outage probability (SOP) and jointly optimize the power allocation factor and the number of relay to minimize the SOP. On the other hand, relays in the CJ scheme do not only forward the messages from the source to the destinations, but also generate signals to interfere with the eavesdroppers. CJ scheme includes artificial-noise (AN) and noise forwarding (NF) schemes. In AN scheme, the cooperative jammers generate Gaussian AN to interfere with the eavesdropper such as in [14]–[17]. In [15], the authors conceived an AN aided two-way opportunistic relay selection scheme for enhancing the security of a two-way multiple-relay network. For NF scheme, the helpers can send dummy codewords which are independent of the source messages and can be decoded reliably at the destination. However, dummy codewords introduce extra randomness at the observation of the eavesdropper, and the information security is improved. This technique was introduced in [11], [18]. Later, Chiang and Lehnert [19] jointly designed the optimal co-variance matrices of the multiple-antenna signals at the source and helper to maximize the secrecy rate of the NF scheme. Recently, Lee and Khisti [20] exploited a NF scheme to establish the secure degrees of-freedom of the Gaussian diamond-wiretap channel with rate-limited relay cooperation, where the eavesdropper not only listens the relay transmission but also wiretaps some of communication links among relays.

The concept of energy harvesting (EH), that represents the direct using of available energy in the surroundings through energy conversion from a given physical domain into electricity, has been raised a decade ago and is now an intensive research and application field [21]. In fact, the main focus for wireless networks has been shifted from spectral efficiency and quality of service (QoS) constraints to energy efficiency and green communication [22], especially in the fifth generation (5G) and sixth generation (6G) networks to reduce the power consumption [23]. Green and inexhaustible energy resources such as solar, wind, thermal and mechanical vibrations are currently considered for improving the energy efficiency of energy-constrained networks such as wireless sensor networks. Unfortunately, the collection of these energy sources depends heavily on the environment. Different from those above solutions, EH from RF signals has emerged as a promising solution and attracted a lot of attention in recent years, especially because RF signals can be utilized for both energy and information transmission simultaneously. This idea was first raised in the seminal paper of Varshney in 2008 [24]. Since then, RF energy harvesting has been developed mainly in three forms: wireless power transfer (WPT) [25], wireless powered communication network (WPCN) [26], and simultaneous wireless information and power transfer (SWIPT) [27]. Nasir [28], [29] has significantly contributed to the development of RF energy harvesting. He introduced two practical protocol for RF energy harvesting in relay networks, namely time-switching relaying (TSR) and power splitting relaying protocols (PSR) and derived the analytical expression for key performance factor such as outage probability, throughput, and ergodic capacity for these protocols. In TSR technique, receiving node switches in time between information processing and EH, whereas, in PSR method, it splits the received power for information processing and EH. Later, the hybrid time-switching and power-splitting (TPSR) protocol was introduced and its performance was evaluated in [30]. In recent years, the performance of RF EH in various kind of wireless networks and various communication schemes have been analyzed, for instance, wireless sensor network [31], multi-hop relay network [32], multiple-antenna network [33], cognitive radio network [34], bidirectional relay network [35], mobile networks [36], and non-orthogonal multiple access (NOMA) scheme [37]. Especially, in 2020, Hoang *et al.* [38] analyzed a two-hop single-relay networks using hybrid TPSR EH protocol in the presence of an eavesdropper near the relay. The authors have derived the closed-form expressions of outage probability and intercept probability in their model.

Two-way relay channel (TWRC), in which two users exchange their messages with each other, has long been a typical model to study the performance of novel communication methods, protocols, or algorithms, including the wireless energy harvesting technique, for several decades. The classical two-way communication channel was first presented in the seminal paper of Shannon [39] in 1961. During the first decade of this century, research on TWRC has been resurged by the paper of [40] and since then has drawn much research attention again. In 2006, Katti *et al.* [41] proposed the digital network coding scheme for TWRC, in which the relay decodes the packets from different sources separately and broadcasts the XOR-ed version of them to both sources and saves one transmission time slot. Then in 2007, Katti *et al.* [42] again presented and analog network coding, in which the relays can receives signals from both source simultaneously and then broadcasts the sum of two signals back to the sources. This method even improves the throughput of TWRC compared to digital network coding by saving one more time slot of the communication. These two network coding techniques have been the main focus of TWRC for last decade. With the advance research of TWRC, the PLS in spectrally-efficient TWR networks has been extensively researched in the literature [6], [7], [14]–[16], [43]. In particular, Shukla [7] and Pandey and Yadav [6] investigated the secrecy outage performance of a full-duplex cellular multiuser two-way amplify-and-forward relay network, where a multiantenna base station using transmit antennas selection communicates with one of the several users by the assistance of a relay in the presence of a passive eavesdropper that employs maximal ratio combining.

Naturally, the application of wireless EH via RF signals in TWCN have been well studied. In 2015, the authors in [44] proposed and analyzed the EH transmission strategies for TWRC to maximize the sum-throughput of the system. In [45], the authors analyzed the performance of a wireless-powered communication network, in which a multiple-antenna two-way AF relay transfers power to multi-pair of single antenna users and then helps the users exchange their data. Zhou and Li [46] provided a jointly optimal design of relay precoding matrices and power splitting ration to maximize the energy efficiency for SWIPT in MIMO two-way amplify-and-forward relay networks, where the relay harvests energy from both sources to forward sources messages. An adaptive EH protocol for two-way AF relay network over the Rician fading environment was also introduced in [47]. On the other hand, partial relay selection (PRS) has been selected as a simple but effective method to enhance the reliability of data transmission at the cooperative phase in EH-based two-way relay networks, such as in [48].

To the best of our knowledge, the study of physical layer security in RF EH-based networks have not been investigated much in literature. The most recent results of PLS in EH-based networks [38], which was published in early 2020, only considered a simple relay network with single relay. Motivated by these above facts, in this paper we provide a thorough analysis on the reliability and security performance of a two-way relay networks using the hybrid TPSR EH protocol and PRS in the presence of an eavesdropper near one of the source nodes. The main contributions of this paper are summarized as follows:

– We derive the closed-form and semi-closed form expressions of key performance factors for our proposed model, including the outage probability (OP) of the legitimate communications, the intercept probability of the eavesdropper (IP), the secrecy outage probability of the system (SOP), and the average secrecy capacity (ASC). In fact, this is a challenging problem because the probability analysis involves a lot of random variables, which makes the derivation more complicated.

– This work also provides an insightful analysis of the effect of various system parameters on the reliability and security performance. It is worth to notice that there should be optimal values of the EH parameters like time-switching factor and power splitting factor for each relay and jammer configuration. It's also concluded from the analysis that increasing the number of available relay nodes can improve the overall performance better than increasing the number of jammers, except for very high values of transmit power.

– The correctness of our analysis is validated by Monte Carlo simulations. From numerical results, we provide the recommendation on selecting the configurations and appropriate values of system parameters to obtain the reliable and secure transmission without paying too much for the complexity of the system.

The rest of this paper is organized as follows. Section II describes the proposed two-way relay networks with hybrid TPSR EH protocol and PRS. Then, the derivation of key performance metrics, including OP, IP, SOP, and ASC of the proposed model is presented in Section III. Section IV shows the numerical results obtained from both analysis and Monte Carlo simulations. Finally, some conclusions are given in Section V.

II. SYSTEM MODEL

A. ENERGY HARVESTING AND SCHEDULING PROTOCOLS

Our proposed system model is illustrated by Fig. 1. Here, we consider a multiple-relay (M relay nodes) two-way relay networks, in which the relay nodes are equipped with RF energy harvesting capability and help two sources A and B exchange their information. The relay nodes are assumed to be located in a cluster, that means the distances from every available relay node to a source node are approximately the same. This assumption is reasonable in practice, especially for IoT device networks or wireless sensor networks. Partial relay selection is applied in our model, where only the relay with best channel to the source (without loss of generality, we consider the best channel gain to the source A)

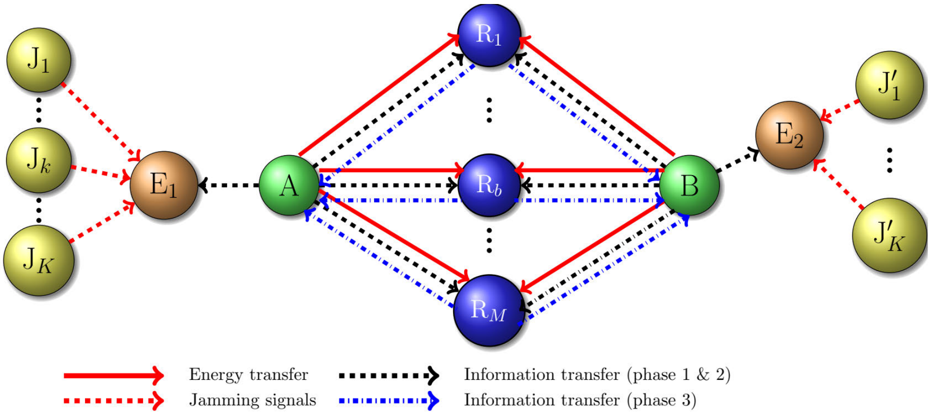

FIGURE 1. System model of the proposed energy harvesting scheme.

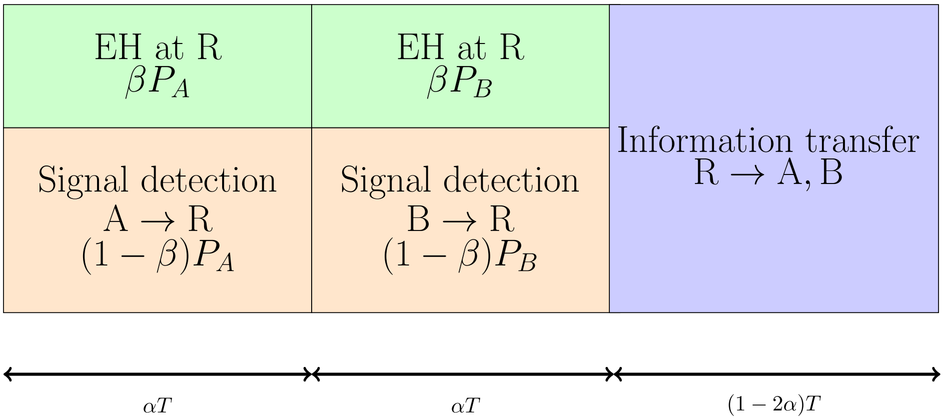
EH at R βP_A
EH at R βP_B
Signal detection A → R $(1-\beta)P_A$
Signal detection B → R $(1-\beta)P_B$
Information transfer R → A, B
αT
αT
$(1-2\alpha)T$

FIGURE 2. **Energy harvesting and scheduling protocol for the proposed model.**

is selected. All nodes in this model are single-antenna devices and operates on half-duplex mode. For EH protocol, we apply the hybrid time-switching and power-splitting (TPSR) protocol (see Fig. 2), which has been introduced in [49] and [50]. In this protocol, the information exchange between two source nodes is accomplished after three distinct phases using DF relaying strategy. For the first two phases, the sources A and B take turns to broadcast their messages, say x_1 and x_2, respectively, to the relay and the other source. Then in the final phase, the relay combines two message (using XOR operator) and broadcasts this XOR-ed message $x_{\oplus} = x_1 \oplus x_2$ to both sources. Now, each source, with knowledge about its own message, can retrieve the desired message sent to it. In this paper, we assume that the direct link between two sources is not available for communicating due to long distance and obstacles in surroundings such as buildings or mountains. It's worth noting that in this model, two phases are enough for transmitting the data if we apply physical-layer network coding (PNC) scheme [51], in which two sources can transmit signal to the relay simultaneously to save one time slot. However, for DF relaying, PNC requires that the network coding message must be decoded from the superimposed signals in the first phase. So, the relay must either have multi-user detection capability [52], or the source nodes must use special coding so that the relay can decode a linear combination of codewords from two source nodes [52], [53], and this makes the system more complicated to implement. Hence, we select the digital network coding scheme with three time slots in this work.

Fig. 2 explains more details on the hybrid TPSR protocol. We exploit the first and second phases to supply the relay with required energy from both A and B to help the relay exchange data later. To do this, the relay node uses a power divider to split the received signal in each source into two portions: the first portion is used to extracted the energy and stored at the relay, whereas the second portion of the signal is used for decoding the information message. We denote β, with $0 < \beta < 1$, as the power splitting factor, i.e. the proportion of the received power at the relay node that is used for EH. For simplicity but without loss of practicality, the power splitting factors for both sources' signals are set to be equal to each other. In addition, the durations of Phase 1 and Phase 2 of communication process are assumed to be the same, which is equal to αT, where T is the total duration of a single transmission block and $0 < \alpha < 0.5$ is the called the time-switching factor. That means the duration of the final phase is equal to $(1 - 2\alpha)T$.

Regarding the eavesdropping strategy, we intend to adopt a single eavesdropper near each source to retrieve the information transmited by that source, i.e. an eavedropper E_1 in the vicinity of the source A and an eavesdropper E_2 in the vicinity of the source B. In fact, eavesdropping strategy may involve multiple eavesdroppers, however, more eavesdroppers require higher cost and higher probability of being detected. For two-way communications, many recent works have considered single eavesdropper case, such as in [16], [43]. Regarding the position of eavesdropper, many scenarios may be employed in practice: near the source(s) [54] or in the middle of the communication link [16]. For two-way communications, the analysis in [43] confirmed that the eavesdropper has a better chance to eavesdrop the message when it is close to one of the transmitters. Furthermore, in practical applications such as in military or IoT sensor networks, the relay node is not fixed, but can be changed among available nodes between source and destination. Therefore, locating the eavesdropper near one relay node may not be reasonable. To conclude, our eavesdropping strategy are totally applicable in practice, especially in military communications, where the eavesdropper is usually put near each command center.

The eavesdropper E_1 tries to retrieves the information sent from A to any other node. Because E_1 is close to A, it is assumed that the direct link from the source B to E_1 is not available either. Therefore, even if it can receive the signal from a relay node, it cannot remove the message sent by B from the received signal. That means the signal received from the relay node is not useful for the eavesdropper.

Similarly, the eavesdropper E_2 tries to retrieves the information sent by B. Without loss of generality, we only consider E_1 (from now on we denote as E for simplicity. To enhance the security of communications, many friendly jammers are used to suppress the received signal at the eavesdropper. In particulars, when A broadcasts its message, the jammers also transmit the artificial noise to the eavesdropper. This artificial noise is known by the relay nodes, so we can ignore any negative effect caused by this signal to the relay nodes.

Assume that the channels between two arbitrary nodes are block Rayleigh fading, where channel coefficients remain constant during one transmission block and change independently across different transmission blocks. Let us denote $h_{X,Y}$, for $X, Y \in \{\mathrm{A}, \mathrm{B}, \mathrm{E}, \mathrm{R}_1, \mathrm{R}_2, \ldots, \mathrm{R}_M, \mathrm{J}_1, \mathrm{J}_2, \ldots, \mathrm{J}_K\}$ as the channel gain of the link from node X to node Y (here, node R_i is the i^{th} relay node and M is the number of available relay nodes, J_k is the k^{th} jamming node and K is the number of jammers). In this paper, we assume that the channels are reciprocal. Because the channels are Rayleigh fading, the squared amplitudes of the channel gains such as $|h_{A,R_i}|^2$, $|h_{B,R_i}|^2$, $|h_{AE}|^2$, etc. are exponential random variables (RVs) whose cumulative distribution function (CDF) and probability density function (PDF) have the following forms, respectively:

$$F_X(x) = 1 - e^{-\lambda x} \tag{1}$$

$$f_X(x) = \begin{cases} \lambda e^{-\lambda x} & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases} \tag{2}$$

where λ is the mean of the exponential random variable X.

Now we are going through the mathematical representation for the entire process. As mentioned above, the source A uses the first time slot to send its packet to both relay and the second source B. The received signal at the relay R can be expressed as

$$y_{A,R_i} = h_{A,R_i} x_A + n_{R_i}^{(1)}, \tag{3}$$

where $E\{|x_A|^2\} = P_A$ (P_A represents the average transmit power at A), $E\{\cdot\}$ denotes the expectation operator; $n_{R_i}^{(1)}$ denotes the zero-mean additive white Gaussian noise (AWGN) with variances N_0.

Using the power splitting technique, the energy that the relay R can harvest from the RF signal of A is given by

$$E_{R_i} = \eta\beta\alpha T P_A \left|h_{AR_i}\right|^2, \tag{4}$$

where $0 < \eta \leq 1$ is the effective energy conversion efficiency (which takes into account the energy loss by harvesting circuits and also by decoding and processing circuits).

In the second time slot, B transmits x_2 to the relay nodes R_i. Therefore, the received signals at the relay R_i can be expressed as

$$y_{B,R_i} = h_{B,R_i} x_B + n_{R_i}^{(2)}, \tag{5}$$

where $E\{|x_B|^2\} = P_B$ is the average transmit power at the B, $n_{R_i}^{(2)}$ is zero-mean additive white Gaussian noise (AWGN) with variance N_0.

Adding to the received energy in the first phase, the total harvested energy at the relay node R can be obtained as

$$E_{R_i} = \eta\beta\alpha T \left(P_A \left|h_{AR_i}\right|^2 + P_B \left|h_{BR_i}\right|^2\right). \tag{6}$$

For simplicity, we assume that the average transmit powers from sources A and B are both equal to P. So, the equation (7) can be rewritten as

$$E_{R_i} = \eta\beta\alpha TP \left(\left|h_{AR_i}\right|^2 + \left|h_{BR_i}\right|^2\right). \tag{7}$$

In this work, we assume that the power consumption for joint decoding and processing at relay is negligible as compared to the power used for signal transmission as in [26]–[29], [36], [37]. This assumption is justifiable because power consumption for joint decoding and processing can be estimated and budgeted while the energy required for RF transmission increases with the transmission distance. Furthermore, the deduction amount of harvested energy (to use for decoding) can be counted as the reduction of the effective energy efficiency η, so our analysis does not change if power consumption for decoding and processing is considered. As a result, the average transmit power of the relay node during the third time slot can be given as

$$\begin{aligned} P_{R_i} &= \frac{E_R}{T(1-2\alpha)} = \frac{\eta\beta\alpha TP \left(\left|h_{AR_i}\right|^2 + \left|h_{BR_i}\right|^2\right)}{T(1-2\alpha)} \\ &= \kappa P \left(\left|h_{AR_i}\right|^2 + \left|h_{BR_i}\right|^2\right), \end{aligned} \tag{8}$$

where $\kappa \triangleq \frac{\eta\beta\alpha}{1-2\alpha}$.

The signals received at R_i from A and B will be decoded and re-encoded by using the network coding scheme [55]. Let $\hat{x}_A$ and $\hat{x}_B$ denote the decoded messages from A and B, respectively. Then during the third time slot, the relay uses its power P_{R_i} to broadcast the exclusive-OR of the decoded message $x_{R_i} = \hat{x}_A \oplus \hat{x}_B$ to both sources A and B. The received signals at A and B can be expressed, respectively, as

$$\begin{aligned} y_A &= h_{R_iA} x_{R_i} + n_A, \\ y_B &= h_{R_iB} x_{R_i} + n_B, \end{aligned} \tag{9}$$

where $E\left\{\left|x_{R_i}\right|^2\right\} = P_{R_i}$; n_A and n_B are i.i.d. AWGN noise terms, which have zero mean and variance of N_0.

From (3) and (5), the received SNRs at the relay for decoding the messages x_A and x_B can be obtained respectively as

$$\gamma_{AR_i} = \frac{(1-\beta)\left|h_{AR_i}\right|^2 P}{N_0} = (1-\beta)\left|h_{AR_i}\right|^2 \Psi, \tag{10}$$

$$\gamma_{BR_i} = \frac{(1-\beta)\left|h_{BR_i}\right|^2 P}{N_0} = (1-\beta)\left|h_{BR_i}\right|^2 \Psi. \tag{11}$$

where $\Psi \triangleq \frac{P}{N_0}$ is the transmit-signal-power-to-noise-ratio. In this paper, we assume that the channels are reciprocal, so $h_{BR_i} = h_{R_iB}$ and $h_{AR_i} = h_{R_iA}$.

During the third phase, the source nodes A and B need to decode successfully the received signal from the relay R_i, then with the knowledge on its transmitted message, it can recover the message sent by the other source. Without loss of generality, we can only consider the decoding performance at the source B. The signal-to-noise-ratio at this node during the third time-slot can be calculated as

$$\gamma_{R_iB} = \frac{\left|h_{R_iB}\right|^2 P_R}{N_0} = \frac{\kappa P\left(\left|h_{AR_i}\right|^2 + \left|h_{BR_i}\right|^2\right)\left|h_{R_iB}\right|^2}{N_0} = \kappa\Psi\left(\left|h_{AR_i}\right|^2 + \left|h_{BR_i}\right|^2\right)\left|h_{R_iB}\right|^2. \quad (12)$$

For the DF relaying strategy at the relay, there is a minor modification from the traditional protocol because digital network coding is used in this case. Specifically, the transmit message from the relay node during the third phase of transmission block should depend on the decoding results of x_1 and x_2 in the previous two phases. There are three possible situations as follows.

(1) The relay successfully decodes both x_1 and x_2 in the first two phases, then it will broadcast the message $x_1 \oplus x_2$ during the third phase;

(2) The relay decodes x_2 successfully but not x_1. In this case, it only broadcasts x_1 during the third phase without applying XOR operation;

(3) The relay cannot decode neither x_1 nor x_2, then no message is broadcasted in the third phase and the communication fails.

For both cases (1) and (2), both links from A to R and from R to B must be good to ensure the communication by the relayed path. Therefore, the equivalent signal-to-noise ratio (SNR) computed at the source B can be obtained as

$$\gamma_{DF} = \min\left\{\gamma_{AR_i}, \gamma_{R_iB}\right\} = \Psi\min\left\{(1-\beta)\left|h_{AR_i}\right|^2, \kappa\left(\left|h_{AR_i}\right|^2+\left|h_{BR_i}\right|^2\right)\left|h_{R_iB}\right|^2\right\}. \quad (13)$$

Now, let's consider the received signal at the eavesdroppers. For simplicity, we only consider the eavesdropper at A because of two reasons: (1) two eavesdroppers at A and B cannot communicate together due to the long distance, so their operations are independent; (2) the roles of these two eavesdroppers are similar, so the intercept probability analysis for one eavesdropper can be found by exchanging A and B in the analysis for the other. The eavesdropper E_1 tries to overhear the signals transmitted by A during the first phase of our communication protocol. However, during this phase, it also receives the artificial noises from the K jammers (J_k, for $k = 1, 2, \ldots, K$). It should be noted that we don't consider the overhearing of signal from the relay during the broadcasting phase (third time slot) because the message sent by the relay is a combination of messages from A and B. Without knowledge of the message from B (it's too far to eavesdrop from B), the information from relay is just useless to the eavesdropper (the signal from the relay nodes during phase 3 is only useful for retrieving the message from B, but for that purpose, the eavesdropper near B, i.e. E_2, should do better). As a result, the eavesdropper must rely on the received signal during phase 1, which can be expressed as

$$y_E = h_{AE}x_s + \sum_{k=1}^{K} h_{J_kE}x_k + n_E, \quad (14)$$

where x_s is the message transmitted by A; x_k is the artificial noise transmitted by the jammer J_k, which satisfies $E(|x_k|^2) = P_J$ is the transmit power of each jammer; and n_E is the AWGN noise at E, which has zero mean and variance of N_0.

From (14), it is easy to derive the received signal-to-interference-and-noise ratio SINR at the eavesdropper:

$$\gamma_E = \frac{P_s|h_{AE}|^2}{\sum_{k=0}^{K}\left|h_{J_kE}\right|^2 P_J + N_0} = \frac{\Psi|h_{AE}|^2}{\sum_{k=1}^{K}\left|h_{J_kE}\right|^2\Psi_J + 1}, \quad (15)$$

where $\Psi_J \triangleq \frac{P_J}{N_0}$.

Assume that the channels between two arbitrary nodes are block Rayleigh fading [28], [29], [36], [45], where channel coefficients remain constant during one transmission block and change independently across different transmission blocks. Therefore, the channel power gains $X_i = \left|h_{AR_i}\right|^2 = \left|h_{R_iA}\right|^2$, $Y_i = \left|h_{BR_i}\right|^2 = \left|h_{R_iB}\right|^2$, $Z = |h_{AE}|^2$, and $T = \left|h_{J_kE}\right|^2$ are independent exponential random variables (RVs) whose cumulative density functions (CDFs) has the following form:

$$F_U(u) = 1 - e^{-\lambda_u u}, \quad (16)$$

where $U \in \{X_i, Y_i, Z, T\}$ and $\lambda_u \in \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$, correspondingly. To take path-loss into account, we can model these parameters as $\lambda_1 = d_1^{\chi}$, $\lambda_2 = d_2^{\chi}$, $\lambda_3 = d_3^{\chi}$, and $\lambda_4 = d_4^{\chi}$. Here, d_1, d_2, d_3 and d_4 are the link distances of the A $\rightarrow$ R_i, B $\rightarrow$ R_i, A $\rightarrow$ E and E $\rightarrow$ J_k, respectively, and χ is the path-loss exponent whose value may range from 2 to 6. For simplicity, we assume that all jammers are at approximately equal distance to the eavesdropper. Similarly, all relay nodes belong to a cluster such that the distances from each source to all relay nodes are approximately the same.

B. PARTIAL RELAY SELECTION

In our system, we apply the partial relay selection (PRS) method[1] to enhance the quality of communication. It means that the cooperative relay can be selected among M relay nodes by the following criterion:

$$R_b = \arg\max_{\{R_i:i=\overline{1,M}\}} \left|h_{AR_i}\right|^2. \quad (17)$$

In other words, the relay which provides the highest channel gain between itself and A in the third time slot is selected for the cooperative communications.

[1] Another selection method is optimal relay selection (ORS), in which the relay that maximizes the secrecy capacity is selected. ORS can provide better performance, but we consider PRS here because its simplicity to implement

Remark 1: In PRS protocol, it will require the channel sate information (CSI) between A and the relay nodes. In practice, A can estimate CSI via local control message and hence it can be easily determine the best candidate as in (17). Moreover, it is worth noting that without loss of generality, we assume the relay is close to B than to A, so the relay selection should be performed based on the quality of the first-hop links to enhance the overall performance.

According to the result from the paper [56], the CDF and PDF (probability density function) of $X = |h_{AR_b}|^2$ can be given by

$$F_X(x) = \sum_{j=0}^{M} (-1)^j \binom{M}{j} e^{-j\lambda_1 x} \tag{18}$$

and

$$f_X(x) = \lambda_1 \sum_{j=0}^{M-1} (-1)^j \binom{M-1}{j} e^{-(j+1)\lambda_1 x}. \tag{19}$$

III. PERFORMANCE ANALYSIS

In this section, we derive the key performance factors of our proposed system, including outage probability (OP), intercept probability (IP), secrecy outage probability (SOP) and the average secrecy capacity (ASC)of the system.

A. OUTAGE PROBABILITY

First, we have the achievable data rate of the legitimate communication link A → B and the eavesdropper link given respectively as

$$C_B = (1-\alpha)\log_2\left(1+\gamma_{DF}\right), \tag{20}$$

$$C_E = (1-\alpha)\log_2\left(1+\gamma_{E}\right), \tag{21}$$

where γ_{DF} is given by (13).

Assume that the relay node R_b is selected for the cooperative communications and let $X = |h_{AR_b}|^2$, $Y = |h_{BR_i}|^2$, then we can rewrite the equivalent SNR at the receiver B as

$$\gamma_{DF} = \min\left\{(1-\beta)X\Psi, \kappa\Psi\left(X+Y\right)Y\right\}. \tag{22}$$

The outage probability occurs when the data rate of the system exceeds the achievable data rate of the link, i.e. $C_B < R$, where R is the data transmission rate. Therefore, it can be expressed as

$$\begin{aligned} OP &= \Pr\left\{C_B < R\right\} \\ &= \Pr\left\{\min\left\{(1-\beta)\Psi X, \kappa\Psi\left(X+Y\right)Y\right\} < \gamma_{th}\right\} \end{aligned} \tag{23}$$

where $\gamma_{th} \triangleq 2^{\frac{R}{(1-\alpha)}} - 1$ is the SNR threshold of B, which is the solution of the equation $C_B = R$.

Now we can state the Theorem 1 on the outage probability of our proposed system as follows.

Theorem 1: The OP of the proposed two-way relay networks with partial relay selection and power-splitting energy harvesting at relay nodes can be found as

$$\begin{aligned} OP = 1 &+ \sum_{j=1}^{M} (-1)^j \binom{M}{j} e^{-j\lambda_1 \frac{\gamma_{th}}{(1-\beta)\Psi} - \lambda_2\xi} \\ &+ \sum_{n=0}^{\infty}\sum_{j=1}^{M} \frac{(-1)^j (j\lambda_1-\lambda_2)^n (j\lambda_1\gamma_{th})^{n+1}\lambda_2}{n!\,(\kappa\Psi)^{n+1}} \binom{M}{j} \\ &\times \Gamma\left(-n-1, \frac{j\lambda_1\gamma_{th}}{\kappa\Psi\xi}\right). \end{aligned} \tag{24}$$

where M is the number of available relay nodes, γ_{th} is the SNR threshold of receiver, $\kappa \triangleq \frac{\eta\beta\alpha}{1-2\alpha}$, $\Psi \triangleq \frac{P}{N_0}$, $\xi = \frac{1}{2}\left[\sqrt{\frac{\gamma_{th}^2}{(1-\beta)^2\Psi^2} + \frac{4\gamma_{th}}{\kappa\Psi}} - \frac{\gamma_{th}}{(1-\beta)\Psi}\right]$, and $\Gamma(s,x) \triangleq \int\limits_x^\infty t^{s-1}e^(-t)dt$ is the incomplete Gamma function.

Proof: We can rewrite the equation (23) as

$$\begin{aligned} OP &= \Pr\left\{\min\left\{(1-\beta)\Psi X, \kappa\Psi\left(X+Y\right)Y\right\} < \gamma_{th}\right\} \\ &= 1 - \Pr\left\{(1-\beta)\Psi X \ge \gamma_{th}, \kappa\Psi\left(X+Y\right)Y \ge \gamma_{th}\right\} \\ &= 1 - \Pr\left\{X \ge \frac{\gamma_{th}}{(1-\beta)\Psi}, X \ge \frac{\gamma_{th}}{\kappa\Psi Y} - Y\right\} \\ &= 1 - \underbrace{\Pr\left(\frac{\gamma_{th}}{\kappa\Psi Y} - Y \ge \tilde{\gamma}_{th}, X \ge \frac{\gamma_{th}}{\kappa\Psi Y} - Y\right)}_{P_1} \\ &\quad - \underbrace{\Pr\left(\frac{\gamma_{th}}{\kappa\Psi Y} - Y \le \tilde{\gamma}_{th}, X \ge \tilde{\gamma}_{th}\right)}_{P_2}. \end{aligned} \tag{25}$$

where $\tilde{\gamma}_{th} \triangleq \frac{\gamma_{th}}{(1-\beta)\Psi}$.

Let $\xi = \frac{1}{2}\left(\sqrt{(\tilde{\gamma}_{th})^2 + \frac{4\gamma_{th}}{\kappa\Psi}} - \tilde{\gamma}_{th}\right)$ be the positive solution of the equation $\frac{\gamma_{th}}{\kappa\Psi y} - y = \tilde{\gamma}_{th}$, the probability terms in (25) can be rewritten as

$$\begin{aligned} P_1 &= \int\limits_0^\xi \Pr\left(X \ge \frac{\gamma_{th}}{\kappa\Psi y} - y\right) f_Y(y)dy \\ &= \int\limits_0^\xi \left[1 - F_X\left(\frac{\gamma_{th}}{\kappa\Psi y} - y\right)\right] f_Y(y)dy \\ &= -\int\limits_0^\xi \left\{\sum_{j=1}^{M} (-1)^j \binom{M}{j} e^{-j\lambda_1\left(\frac{\gamma_{th}}{\kappa\Psi y} - y\right)}\right\} f_Y(y)dy \\ &= -\sum_{j=1}^{M} (-1)^j \binom{M}{j} \lambda_2 \int\limits_0^\xi e^{y(j\lambda_1-\lambda_2)} e^{-\frac{j\lambda_1\gamma_{th}}{\kappa\Psi y}} dy, \end{aligned} \tag{26}$$

$$\begin{aligned} P_2 &= \int\limits_\xi^\infty \Pr\left(X \ge \tilde{\gamma}_{th}\right) f_Y(y)dy = \int\limits_\xi^\infty \left[1 - F_X\left(\tilde{\gamma}_{th}\right)\right] f_Y(y)dy \\ &= \sum_{j=1}^{M} (-1)^{j+1} \binom{M}{j} \cdot e^{-j\lambda_1\tilde{\gamma}_{th}} \int\limits_\xi^\infty f_Y(y)dy \\ &= \sum_{j=1}^{M} (-1)^{j+1} \binom{M}{j} e^{-j\lambda_1\tilde{\gamma}_{th} - \lambda_2\xi}. \end{aligned} \tag{27}$$

The integral in P_1 can be solved by changing variable $t = 1/y$ and applying Taylor's series expansion $e^x = \sum\limits_{n=0}^{\infty} \frac{x^n}{n!}$ for $x = \frac{j\lambda_1 - \lambda_2}{t}$:

$$\begin{aligned}
P_1 &= -\sum_{j=1}^{M} (-1)^j \binom{M}{j} \lambda_2 \int\limits_{1/\xi}^{\infty} t^{-2} e^{\frac{(j\lambda_1-\lambda_2)}{t}} e^{-j\frac{\lambda_1 \gamma_{th} t}{\kappa\Psi}} dt \\
&= -\sum_{n=0}^{\infty}\sum_{j=1}^{M} \frac{(-1)^j (j\lambda_1 - \lambda_2)^n \lambda_2}{n!} \binom{M}{j} \int\limits_{1/\xi}^{\infty} \frac{e^{-j\lambda_1\gamma_{th} t}}{\kappa\Psi t^{n+2}} dt \\
&= \sum_{n=0}^{\infty}\sum_{j=1}^{M} \frac{(-1)^{j+1} (j\lambda_1 - \lambda_2)^n (j\lambda_1\gamma_{th})^{n+1} \lambda_2}{n!(\kappa\Psi)^{n+1}} \binom{M}{j} \\
&\quad \times \Gamma\left(-n-1, \frac{j\lambda_1\gamma_{th}}{\kappa\Psi\xi}\right). \qquad (28)
\end{aligned}$$

where the last equality comes from [57, 3.462.16].

By substituting (19), (27) and (28) into (25), we finally get (24). ■

B. INTERCEPT PROBABILITY

The intercept probability at the eavesdropper E is defined as the probability that capacity of the legitimate link falls below the wiretap link's capacity, i.e. $C_E > C_B$. By using the result of the outage probability analysis, we obtain the Theorem 2.

Theorem 2: The intercept probability at the eavesdropper E in the proposed two-way relay networks with jamming by artificial noise is given by (29), as shown at the bottom of the page, where K is the number of jammers, $\Psi \triangleq \frac{P}{N_0}$, and $\Psi_J \triangleq \frac{P_J}{N_0}$, and $\tilde{\xi}_x = \frac{1}{2}\left[\sqrt{\frac{x^2}{(1-\beta)^2} + \frac{4x}{\kappa}} - \frac{x}{(1-\beta)}\right]$.

Proof: By definition and using (13) and (15), the intercept probability by the eavesdropper E can be found as

$$\begin{aligned}
\text{IP} &= \Pr(C_E \geq C_B) = \Pr(\gamma_E \geq \gamma_{DF}) \\
&= \Pr\left(\frac{Z}{\Psi_J T + 1} \geq \min\{(1-\beta)X, \kappa(X+Y)Y\}\right). \qquad (30)
\end{aligned}$$

where $\Psi_J \triangleq P_J/N_0$, $Z = |h_{AE}|^2$, $T = \sum\limits_{k=1}^{K} |h_{J_k E}|^2$.

Let's denote $V = \min\{(1-\beta)X, \kappa(X+Y)Y\}$ and $U = \frac{Z}{\Psi_J T + 1}$. Then (30) can be rewritten as

$$\begin{aligned}
\text{IP} &= \Pr(U \geq V) \\
&= \int\limits_0^{\infty} f_U(u) du \int\limits_0^{u} f_V(v) dv = \int\limits_0^{\infty} f_U(u).F_V(u) du. \qquad (31)
\end{aligned}$$

By using (15), the CDF of U can be written as

$$\begin{aligned}
F_U(u) &= \Pr\{U \leq u\} = \Pr\left\{\frac{Z}{\Psi_J T + 1} \leq u\right\} \\
&= \Pr\{Z < u(T\Psi_J + 1)\} \\
&= \int\limits_0^{\infty} F_Z(u(t\Psi_J + 1)) f_T(t) dt, \qquad (32)
\end{aligned}$$

where $F_Z(\cdot)$ and $f_T(\cdot)$ are the CDF of Z and PDF of T, respectively.

As mentioned in the previous section, Z is an exponential random variable with parameter λ_3, while T is the sum of K i.i.d. exponential random variable with parameter λ_4. As a result, the CDF of Z is given by (16) and T is a gamma random variable with the parameters K and λ_4, whose PDF is given by [58]:

$$f_T(t) = \frac{\lambda_4^K}{(K-1)!} t^{K-1} e^{-\lambda_4 t}. \qquad (33)$$

By substituting (16) and (37) into (32), we can rewrite $F_U(u)$ as

$$\begin{aligned}
F_U(u) &= \int\limits_0^{\infty} F_Z(u(t\Psi_J + 1)) f_T(t) dt \\
&= \int\limits_0^{\infty} f_T(t) dt - \frac{\lambda_4^K e^{-\lambda_3 u}}{(K-1)!} \int\limits_0^{\infty} t^{K-1} e^{-t(\lambda_4 + \lambda_3 u \Psi_J)} dt \\
&= 1 - \frac{\lambda_4^K \Gamma(K) e^{-\lambda_3 u}}{(K-1)!(\lambda_4 + \lambda_3 u \Psi_J)^K} \\
&= 1 - \frac{\lambda_4^K e^{-\lambda_3 u}}{(\lambda_4 + \lambda_3 u \Psi_J)^K}, \qquad (34)
\end{aligned}$$

where the second last equality is obtained by using [57, 3.381.4] and the last equality is obtained by replacing $\Gamma(K) = (K-1)!$.

$$\begin{aligned}
\text{IP} = 1 &+ \int\limits_0^{\infty} \left\{\sum_{n=0}^{\infty}\sum_{j=1}^{M} \frac{(-1)^j (j\lambda_1 - \lambda_2)^n [j\lambda_1 x]^{n+1} \lambda_2}{n!(\kappa)^{n+1}} \binom{M}{j} \Gamma\left(-n-1, \frac{j\lambda_1 x}{\kappa\tilde{\xi}_x}\right)\right\} \\
&\times \frac{e^{-\lambda_3 x}\left[(\lambda_3)^2 \frac{\Psi_J}{\lambda_4} x + \lambda_3 + \frac{\lambda_3 \Psi_J K}{\lambda_4}\right]}{\left(1 + \frac{\lambda_3 \Psi_J x}{\lambda_4}\right)^{K+1}} dx \\
&+ \int\limits_0^{\infty} \left\{\sum_{j=1}^{M} (-1)^j \binom{M}{j} e^{-\frac{j\lambda_1(x)}{(1-\beta)} - \lambda_2 \tilde{\xi}_x}\right\} \frac{e^{-\lambda_3 x}\left[(\lambda_3)^2 \frac{\Psi_J}{\lambda_4} x + \lambda_3 + \frac{\lambda_3 \Psi_J K}{\lambda_4}\right]}{\left(1 + \frac{\lambda_3 \Psi_J x}{\lambda_4}\right)^{K+1}} dx. \qquad (29)
\end{aligned}$$

By taking the derivative of (38), we obtain the PDF of U as

$$f_U(u) = \frac{e^{-\lambda_3 u}\left[(\lambda_3)^2 \frac{\Psi_J}{\lambda_4} u + \lambda_3 + \frac{\lambda_3 \Psi_J K}{\lambda_4}\right]}{\left(1 + \frac{\lambda_3 u \Psi_J}{\lambda_4}\right)^{K+1}}. \tag{35}$$

On the other hand, the CDF of V is obtained by using the result of Theorem 1 (substituting γ_{th} by $v\Psi$ in (24))

$$\begin{aligned} F_V(v) &= \Pr(V \le v) = \Pr\left(\frac{\gamma_{DF}}{\Psi} \le v\right) \\ &= 1 + \sum_{j=1}^{M} (-1)^j \binom{M}{j} e^{-\frac{j\lambda_1 v}{(1-\beta)} - \lambda_2 \tilde{\xi}_v} \\ &\quad + \sum_{n=0}^{\infty}\sum_{j=1}^{M} \frac{(-1)^j (j\lambda_1 - \lambda_2)^n (j\lambda_1 v)^{n+1} \lambda_2}{n!\,(\kappa)^{n+1}} \binom{M}{j} \\ &\quad \times \Gamma\left(-n-1, \frac{j\lambda_1 v}{\kappa \tilde{\xi}_v}\right). \end{aligned} \tag{36}$$

where $\tilde{\xi}_v = \frac{1}{2}\left[\sqrt{\frac{v^2}{(1-\beta)^2} + \frac{4v}{\kappa}} - \frac{v}{(1-\beta)}\right]$.

By substituting (35) and (36) into (31), we obtain (29). The proof is complete. ■

Remark 2: It can be seen from (29) that the intercept probability does not depend on Ψ.

Remark 3: It is worth noting that our analytical results in this paper can be easily extended to the general case when there exist hardware noise terms at both relay and primary transmitters. In fact, each SINR formula for the hardware imperfection case is a one-to-one mapping of the corresponding SINR for perfect hardware case presented above. For example, the received signal at relay and its corresponding SINR in hardware imperfection case can be rewritten respectively as

$$\begin{aligned} y_{A,R_i} &= h_{A,R_i}(x_A + \eta_A^{\mathrm{t}}) + \eta_{\mathrm{R}_i}^{\mathrm{r}} + n_{r_i}^{(1)}, \\ \gamma_{AR_i}^{HI} &= \frac{(1-\beta)\left|h_{AR_i}\right|^2 P}{|h_{\mathrm{AR_i}}|^2\, k_{\mathrm{AR_i}}^2\, P + N_0} = \frac{(1-\beta)}{k_{\mathrm{AR_i}}^2 + \frac{1}{\left|h_{AR_i}\right|^2 \Psi}} \\ &= \frac{1}{\frac{k_{\mathrm{AR_i}}^2}{1-\beta} + \frac{1}{\gamma_{AR_i}}}. \end{aligned}$$

where $\eta_A^{\mathrm{t}} \sim \mathcal{CN}(0, (k_{\mathrm{A}}^{\mathrm{t}})^2\, P)$ and $\eta_{R_i}^{\mathrm{r}} \sim \mathcal{CN}(0, (k_{\mathrm{R_i}}^{\mathrm{r}})^2\, P_{R_i})$ are HI noise terms caused by the transmitter impairment at A and receiver impairment at $\mathrm{R_i}$, respectively; $k_{\mathrm{AR_i}}^2 = (k_{\mathrm{A}}^{\mathrm{t}})^2 + (k_{\mathrm{R_i}}^{\mathrm{r}})^2$ denotes the aggregated HI level at both transmitter A ($k_{\mathrm{A}}^{\mathrm{t}}$) and receiver $\mathrm{R_i}$ ($k_{\mathrm{R_i}}^{\mathrm{r}}$) [59].

Then, to derive $P(\gamma_{AR_i}^{HI} < \gamma_{th})$, we can use:

$$\begin{aligned} P(\gamma_{AR_i}^{HI} < \gamma_{th}) &= P\left(\frac{1}{\frac{k_{\mathrm{AR_i}}^2}{1-\beta} + \frac{1}{\gamma_{AR_i}}} < \gamma_{th}\right) \\ &= P\left(\gamma_{AR_i} < \frac{1-\beta-k_{\mathrm{AR_i}}^2}{(1-\beta)\gamma_{th}}\right) \end{aligned}$$

By replacing γ_{th} in our original analysis by $\frac{1-\beta-k_{\mathrm{AR_i}}^2}{(1-\beta)\gamma_{th}}$, we can obtain the result for hardware imperfection case.

C. SECRECY OUTAGE PROBABILITY

In the literature on physical layer security, such as [19], the researchers are interested in the possibility of conveying confidential messages at a positive rate, termed secrecy rate, between a source and a legitimate destination while keeping an eavesdropper ignorant if the source-destination channel is better than the source-eavesdropper channel. In addition, the larger the difference of the channel strengths between the two channels, the higher the achieved secrecy rate. This secrecy rate is defined as

$$C_{sec} = \max\{C_B - C_E, 0\}, \tag{37}$$

where $C_B = (1-\alpha)\log_2(1+\gamma_{DF})$ is the achievable data rate at the node B.

The secrecy rate must be maintained above certain threshold to guarantee the confidentiality of the message. An secrecy outage occurs if the achievable secrecy rate falls below the threshold:

$$\mathrm{SOP} = \Pr\{C_{\mathrm{sec}} < R\} = \Pr\left\{\frac{1+\gamma_{DF}}{1+\gamma_E} < \gamma_{sc,th}\right\}, \tag{38}$$

where R is the threshold of the secrecy rate, and $\gamma_{sc,th} \triangleq 2^{\frac{R}{(1-\alpha)}}$.

The closed-form expression of this SOP can be found in the following theorem.

Theorem 3: The secrecy outage probability (SOP) of the proposed two-way wireless relay networks with partial relay selection, energy harvesting at relay nodes, and friendly jammers is given by (39), as shown at the bottom of the next page, where $a = \frac{j\lambda_1 \gamma_{sc,th}}{(1-\beta)\Psi} + \frac{\lambda_3}{\Psi}$, $b = \frac{\lambda_3 \Psi_J}{\lambda_4 \Psi}$, $\tilde{\gamma} \triangleq 2^{\frac{R}{(1-\alpha)}} - 1$ is the SNR threshold at E, and $\Gamma(s,x) \triangleq \int_x^{\infty} t^{s-1} e^{-t} dt$ is the incomplete gamma function.

Proof: To begin, we can rewrite (38) as

$$\begin{aligned} \mathrm{SOP} &= \Pr\left\{\frac{1+\gamma_{DF}}{1+\gamma_E} < \gamma_{sc,th}\right\} \\ &= \Pr\left\{\gamma_{DF} < (1+\gamma_E)\gamma_{sc,th} - 1\right\} \\ &= \int_0^{\infty} F_{\gamma_{DF}}\left((1+x)\gamma_{sc,th} - 1\right) f_{\gamma_E}(x)dx \end{aligned} \tag{40}$$

where $F_{\gamma_{DF}}(\cdot)$ and $f_{\gamma_E}(\cdot)$ are the CDF of γ_{DF} and PDF of γ_E, respectively.

By applying the result of Theorem 2 (just substitute u by $\frac{x}{\Psi}$ in (38)), the CDF and the PDF of γ_E can be found by

$$F_{\gamma_E}(x) = \Pr\{\gamma_E < x\} = 1 - \frac{e^{\frac{-\lambda_3 x}{\Psi}}}{\left(1 + \frac{\lambda_3 \Psi_J x}{\Psi \lambda_4}\right)^K} \tag{41}$$

and

$$f_{\gamma_E}(x)=\frac{df_{\gamma_E}}{dx}=\frac{e^{-\frac{\lambda_3 x}{\Psi}}\left[\left(\frac{\lambda_3}{\Psi}\right)^2\frac{\Psi_J}{\lambda_4}x+\frac{\lambda_3}{\Psi}+\frac{\lambda_3\Psi_J K}{\Psi\lambda_4}\right]}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}. \quad (42)$$

On the other hand, the CDF of γ_{DF} is obtained by using the result of Theorem 1 (substituting γ_{th} by y in (24))

$$\begin{aligned}F_{\gamma_{DF}}(y) &= 1+\sum_{j=1}^{M}(-1)^j\binom{M}{j}e^{-j\lambda_1\frac{y}{(1-\beta)\Psi}-\lambda_2\xi}\\ &\quad+\sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n(j\lambda_1 y)^{n+1}\lambda_2}{n!\,(\kappa\Psi)^{n+1}}\binom{M}{j}\\ &\quad\times\Gamma\left(-n-1,\frac{j\lambda_1 y}{\kappa\Psi\xi_y}\right). \quad (43)\end{aligned}$$

where $\xi_y=\frac{1}{2}\left[\sqrt{\frac{y^2}{(1-\beta)^2\Psi^2}+\frac{4y}{\kappa\Psi}}-\frac{y}{(1-\beta)\Psi}\right]$.

Let's denote $\tilde{\gamma}\triangleq\gamma_{sc,th}-1$ and

$$\begin{aligned}\Xi_x &= \xi_{\gamma_{sc,th}(1+x)-1}\\ &= \sqrt{\frac{(x\gamma_{sc,th}+\tilde{\gamma})^2}{4(1-\beta)^2\Psi^2}+\frac{(x\gamma_{sc,th}+\tilde{\gamma})}{\kappa\Psi}}-\frac{(x\gamma_{sc,th}+\tilde{\gamma})}{2(1-\beta)\Psi}.\end{aligned}$$

Now, by substituting (43) with $y=x\gamma_{sc,th}+\tilde{\gamma}$ into (40), we have (44), as shown at the bottom of the page. Finally, by substituting (42) into (44), we get (39). ■

D. AVERAGE SECRECY CAPACITY

The secrecy capacity of the proposed system depends on the SNRs of the legitimate link and the wire-tap link, which are random variables. The average secrecy capacity is defined as the expected value of the secrecy capacity [60]:

$$\begin{aligned}C_{avg} &= E\left[C_{Sec}\right]\\ &= (1-\alpha)\iint\limits_{\substack{x,y>0\\ y\geq x}}\log_2\left(\frac{1+y}{1+x}\right)f_{\gamma_{DF}}(y)f_{\gamma_E}(x)dxdy\\ &= (1-\alpha)\int_0^{\infty}f_{\gamma_E}(x)dx\int_x^{\infty}\log_2\left(\frac{1+y}{1+x}\right)f_{\gamma_{DF}}(y)dy. \quad (45)\end{aligned}$$

where $f_{\gamma_E}(\cdot)$ and $f_{\gamma_{DF}}(\cdot)$ are the PDF of γ_E and γ_{DF}, respectively.

We now state the following theorem on the average secrecy capacity of the proposed system.

Theorem 4: The average secrecy capacity C_{avg} of the proposed two-way relay network with PRS, EH at relay nodes, and friendly jammers is given by (46), as shown at the bottom of the next page, where $\Lambda_x\triangleq\left(\frac{\lambda_3}{\Psi}\right)^2\frac{\Psi_J}{\lambda_4}x+\frac{\lambda_3}{\Psi}+\frac{\lambda_3\Psi_J K}{\Psi\lambda_4}$ and $\Upsilon_y\triangleq\frac{\frac{y}{\{(1-\beta)\Psi\}^2}+\frac{2}{\kappa\Psi}}{2\sqrt{\left(\frac{y}{(1-\beta)\Psi}\right)^2+\frac{4y}{\kappa\Psi}}}-\frac{1}{2(1-\beta)\Psi}$.

Proof: The CDF of γ_{DF} has been given in (43). By taking the derivative of (43), we get the PDF of γ_{DF} as (47), as shown at the bottom of the next page, where the last equality is obtained by using [61, 8.8.13], where $\Upsilon_y\triangleq\frac{\frac{y}{\{(1-\beta)\Psi\}^2}+\frac{2}{\kappa\Psi}}{2\sqrt{\left(\frac{y}{(1-\beta)\Psi}\right)^2+\frac{4y}{\kappa\Psi}}}-\frac{1}{2(1-\beta)\Psi}$.

By substituting (47) and (42) into (45) we obtain (46). ■

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, some Monte Carlo simulations are presented to validate the derived expressions of OP, IP, SOP, and ASC. Moreover, the effect of various system parameters, such as transmit-power-to-noise-ratio, time switching factor,

$$\begin{aligned}\mathrm{SOP} &= 1+\int_0^{\infty}\left\{\sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n\left[j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)\right]^{n+1}\lambda_2}{n!(\kappa\Psi)^{n+1}}\binom{M}{j}\Gamma\left(-n-1,\frac{j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)}{\kappa\Psi\Xi_x}\right)\right\}\\ &\quad\times\frac{e^{-\frac{\lambda_3 x}{\Psi}}\left[\left(\frac{\lambda_3}{\Psi}\right)^2\frac{\Psi_J}{\lambda_4}x+\frac{\lambda_3}{\Psi}+\frac{\lambda_3\Psi_J K}{\Psi\lambda_4}\right]}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}dx\\ &\quad+\int_0^{\infty}\left\{\sum_{j=1}^{M}(-1)^j\binom{M}{j}e^{-\frac{j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)}{(1-\beta)\Psi}-\lambda_2\Xi_x}\right\}\frac{e^{-\frac{\lambda_3 x}{\Psi}}\left[\left(\frac{\lambda_3}{\Psi}\right)^2\frac{\Psi_J}{\lambda_4}x+\frac{\lambda_3}{\Psi}+\frac{\lambda_3\Psi_J K}{\Psi\lambda_4}\right]}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}dx \quad (39)\end{aligned}$$

$$\begin{aligned}\mathrm{SOP} &= \int_0^{\infty}\left\{1+\sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n\left[j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)\right]^{n+1}\lambda_2}{n!(\kappa\Psi)^{n+1}}\binom{M}{j}\Gamma\left(-n-1,\frac{j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)}{\kappa\Psi\Xi_x}\right)\right\}f_{\gamma_E}(x)dx\\ &\quad+\int_0^{\infty}\left\{\sum_{j=1}^{M}(-1)^j\binom{M}{j}e^{-\frac{j\lambda_1(\tilde{\gamma}+\gamma_{sc,th}x)}{(1-\beta)\Psi}-\lambda_2\Xi_x}\right\}f_{\gamma_E}(x)dx \quad (44)\end{aligned}$$

power splitting factor, number of relay nodes, number of jammers, and spectrum efficiency, on the system performance is investigated through these simulation results. All Monte Carlo simulations are generated using 10^5 samples of each channel gain. The settings of simulation parameters are listed in Table 1. Regarding to the channel settings, we adopt a simplified path loss model, i.e., $\lambda_i = d_i^{\chi}$, for $i \in \{1, 2, 3, 4\}$, where d_1, d_2, d_3, d_4 are the distances between A and the relay cluster, between B and the relay cluster, between A and the eavesdropper, and between the eavesdropper and the jamming cluster, respectively; χ denotes the path loss exponent, respectively. For illustrative purpose, we set $d_{1i} = 0.85$, $d_2 = 0.5, d_3 = d_4 = 2$, and $\chi = 2$, which leads to the values of λ_i, $i \in \{1, 2, 3, 4\}$ as in Table 1.

Firstly, we examine the reliability and security performance of the proposed model in terms of outage probability and intercept probability. Fig. 3 and Fig. 4 plot OP and IP versus the ratio between transmission power of the source A and the noise power density N_0, which is denoted by Ψ, for four different cluster size of the relay cluster and jamming clusters. It can be seen from these figures that the analytical results and the simulation results exactly match together. As expected, OP decreases with Ψ, while the IP does not depend on Ψ as stated in the Remark 3. It can also be observed that the both reliability and security performance can be improved by increasing the number of relay nodes and jammer nodes. However, when the number of relay nodes is sufficient, adding more nodes to the relay cluster does not significantly improve the outage performance (we can see the gaps among the cases $M = 3$, $M = 5$, and $M = 7$ are small). This can be explained as follows. Because the relays are located in a cluster, they are closed to each other. With partial relay selection, the more relays added to the cluster, the less likely that the newly added relay has best channel gain. After a certain number of relays, keep increasing the number of relays does not improve much. So, it is recommended that we use a moderate number of relays, let's say $M = 3$, and use cooperative jammers, for example $K = 2$, to obtain a desired performance.

TABLE 1. Simulation parameters.

Symbol	Parameter name	Fixed value	Varying range
R	Spectrum efficiency	0.25 bps/Hz	0.1 to 1 (bps/Hz)
η	Energy harvesting efficiency	0.8	none
α	Time division factor	0.3	0 to 0.5
β	Power splitting factor	0.5	0 to 1
λ_1	Mean of $\lvert h_{AR_i}\rvert^2$	0.7225	none
λ_2	Mean of $\lvert h_{BR_i}\rvert^2$	0.258	none
λ_3	Mean of $\lvert h_{AE}\rvert^2$	4	none
λ_4	Mean of $\lvert h_{J_kE}\rvert^2$	4	none
Ψ	Transmit-power-to-noise-ratio	15 dB	0 to 30 (dB)
Ψ_J	Jammer-power-to-noise-ratio	15 dB	0 to 30 (dB)
M	No. of relay nodes	1; 3; 5; 7	none
K	No. of jamming nodes	1; 3; 5; 7	none

$$
\begin{aligned}
C_{avg} &= (1-\alpha)\sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n\lambda_2}{n!}\binom{M}{j}\int_0^{\infty}\frac{(n+1)e^{-\frac{\lambda_3 x}{\Psi}}\Lambda_x}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}dx\int_x^{\infty}\log_2\left(\frac{1+y}{1+x}\right)\\
&\quad\times\left[\frac{y^n(j\lambda_1)^{n+1}}{(\kappa\Psi)^{n+1}}\Gamma\left(-n-1,\frac{j\lambda_1 y}{\kappa\Psi\xi_y}\right)\right]dy\\
&\quad-(1-\alpha)\sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n\lambda_2}{n!}\binom{M}{j}\int_0^{\infty}\frac{e^{-\frac{\lambda_3 x}{\Psi}}\Lambda_x}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}dx\int_x^{\infty}\log_2\left(\frac{1+y}{1+x}\right)\left[e^{\frac{-j\lambda_1 y}{\kappa\Psi\xi_y}}\xi_y^{n+1}\left(\frac{1}{y}-\frac{\Upsilon_y}{\xi_y}\right)\right]dy\\
&\quad+(1-\alpha)\sum_{j=1}^{M}(-1)^{j+1}\binom{M}{j}\int_0^{\infty}\frac{e^{-\frac{\lambda_3 x}{\Psi}}\Lambda_x}{\left(1+\frac{\lambda_3\Psi_J x}{\Psi\lambda_4}\right)^{K+1}}dx\int_x^{\infty}\log_2\left(\frac{1+y}{1+x}\right)e^{-\left[\frac{j\lambda_1 y}{(1-\beta)\Psi}+\lambda_2\xi_y\right]}\left[\frac{j\lambda_1}{(1-\beta)\Psi}+\lambda_2\Upsilon_y\right]dy \qquad (46)
\end{aligned}
$$

$$
\begin{aligned}
f_{\gamma_{DF}}(y) &= \frac{\partial F_{\gamma_{DF}}(y)}{\partial y}\\
&= \sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n(j\lambda_1)^{n+1}\lambda_2}{n!(\kappa\Psi)^{n+1}}\binom{M}{j}\frac{\partial}{\partial y}\left[y^{n+1}\Gamma\left(-n-1,\frac{j\lambda_1 y}{\kappa\Psi\xi_y}\right)\right]+\sum_{j=1}^{M}(-1)^j\binom{M}{j}\frac{\partial}{\partial y}\left[e^{\frac{-j\lambda_1 y}{(1-\beta)\Psi}-\lambda_2\xi_y}\right]\\
&= \sum_{n=0}^{\infty}\sum_{j=1}^{M}\frac{(-1)^j(j\lambda_1-\lambda_2)^n\lambda_2}{n!}\binom{M}{j}\left[\frac{(n+1)y^n(j\lambda_1)^{n+1}}{(\kappa\Psi)^{n+1}}\Gamma\left(-n-1,\frac{j\lambda_1 y}{\kappa\Psi\xi_y}\right)-e^{\frac{-j\lambda_1 y}{\kappa\Psi\xi_y}}\xi_y^{n+1}\left(\frac{1}{y}-\frac{\Upsilon_y}{\xi_y}\right)\right]\\
&\quad+\sum_{j=1}^{M}(-1)^{j+1}\binom{M}{j}e^{-\left[\frac{j\lambda_1 y}{(1-\beta)\Psi}+\lambda_2\xi_y\right]}\left[\frac{j\lambda_1}{(1-\beta)\Psi}+\lambda_2\Upsilon_y\right]. \qquad (47)
\end{aligned}
$$

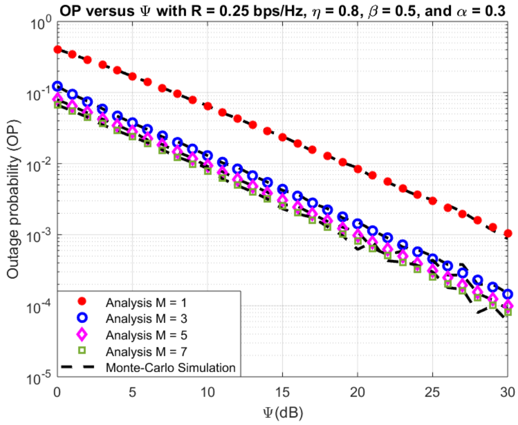

FIGURE 3. Outage probability of A → B link versus transmit-power-to-noise-ratio for different number of relays.

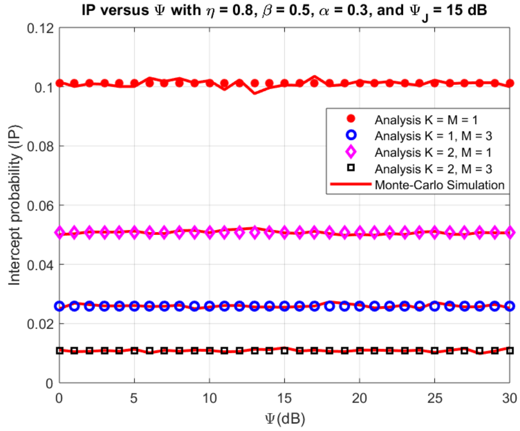

FIGURE 4. Intercept probability versus transmit-power-to-noise-ratio for different number of jammers and jammer power levels.

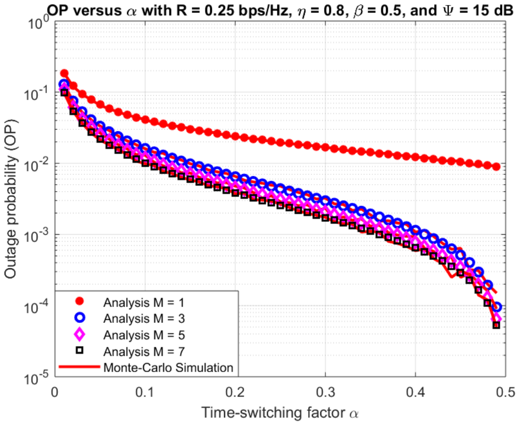

FIGURE 5. Outage probability of A → *B* link versus time-switching factor for different number of relays.

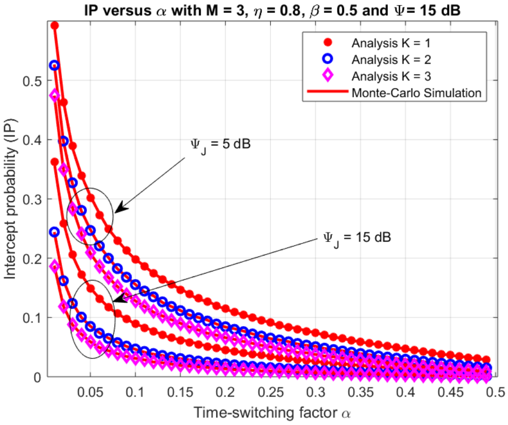

FIGURE 6. Intercept probability of A → *B* link versus time-switching factor for different number of jammers and jammer power levels.

The effect of the EH time-switching factor on the outage and security performance is shown in Fig. 5 and Fig. 6. We consider again four cluster sizes of the relay and jammer clusters, i.e., $M \in \{1, 3, 5, 7\}$, $K \in \{1, 2, 3\}$. As observed from Fig. 5, OP decreases with α. This can be explained as follows. For small α, the EH time is limited, so the relay nodes do not harvest much energy for their transmission. Therefore, increasing α would improve the quality of transmission. Again, it can be seen that increasing the number of relays $M \geq 3$ does not improve much on performance. On other aspect, Fig. 6 shows that IP decreases with α. It is obvious because increasing α means increasing the duration of energy harvesting time by the relay, which results in the better legitimate link condition, while the wire-tap link condition is not improved by increasing α. From these two figures, it is recommended that we choose α large enough and choose a proper number of jammers (for example, $K = 2$) and relays (for example, $M = 3$). Adding more jammers and relays after these certain numbers cannot bring significant benefit. In addition, the transmit power of jammer is not necessarily too large, with $\Psi_J = 5\ dB$ and with sufficient large α, we can achieve an acceptable performance.

Fig. 7 plots the OP versus the power-splitting factor β. There is a trade-off between the energy using to supply the

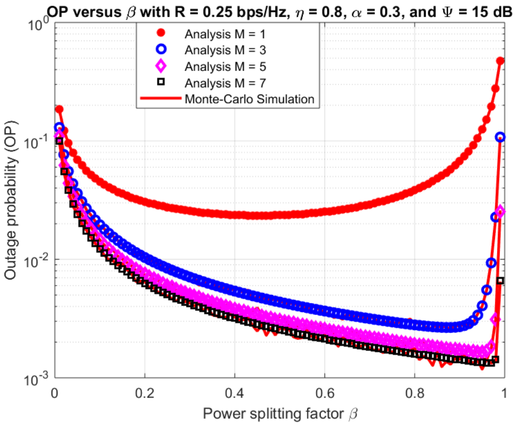

FIGURE 7. Outage probability of A → *B* link versus power-splitting factor for different number of relays.

relay nodes and to guarantee the transmission of the message from source A. That means there exists an optimal β to minimize the OP for each number of relay nodes. When the number of relay nodes is increased, the optimal value of β tend to approach 1 ($\beta = 0.46, 0.87, 0.95$, and 0.97 for $M = 1, 3, 5$, and 7, respectively). This is because when the number of relays increases, the quality of the link between A and the selected relay nodes is improved so that we do not worry much about the transmit power for message signal and can use more energy to supply the relay node.

The intercept probability is also affected by β as shown in Fig. 8. It is reasonable to see that there is also an optimal value of β that minimize the IP for each scenario. This is because the wiretap-link condition does not depend on β, while the OP of the main link from A $\rightarrow$ B get a single minimum at shown in Fig. 8. However, it is worth noting that the optimal value of β for minimizing IP is different from the one that minimizing OP. In fact, the optimal β in this case (minimizing IP should depend on the number of jammers, too, and also tend to increases when the number of jammers increases. In particular, the optimal values of β^* for $K = 1, 2, 3$ and Ψ_J =5 dB are 0.49, 0.53, and 0.56 respectively. For $\Psi_J = 15\ dB$, the optimal values β^* for $K = 1, 2, 3$ are 0.56, 0.66, and 0.73, respectively. Here, because α is not large enough, the IP is significantly impacted by Ψ_J.

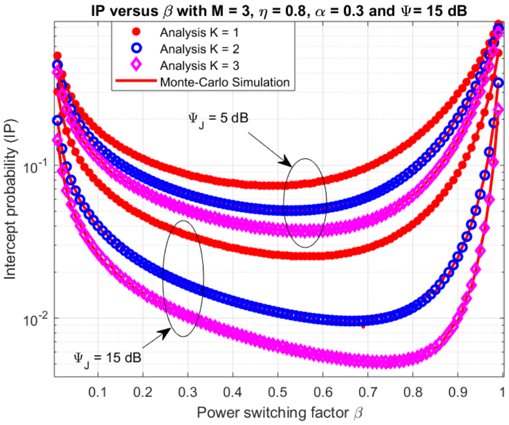

FIGURE 8. Intercept probability of A → *B* link versus spectrum efficiency for different number of jammers and jammer power levels.

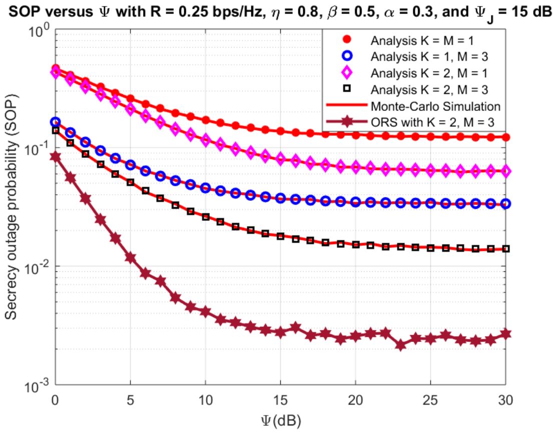

FIGURE 9. Secrecy outage probability of the proposed system versus transmit-power-to-noise-ratio for different configurations of relay and jammer nodes.

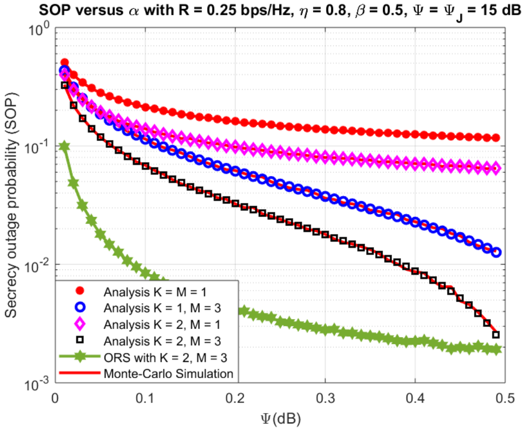

FIGURE 10. Secrecy outage probability of the proposed system versus time-switching factor for different configurations of relay and jammer nodes.

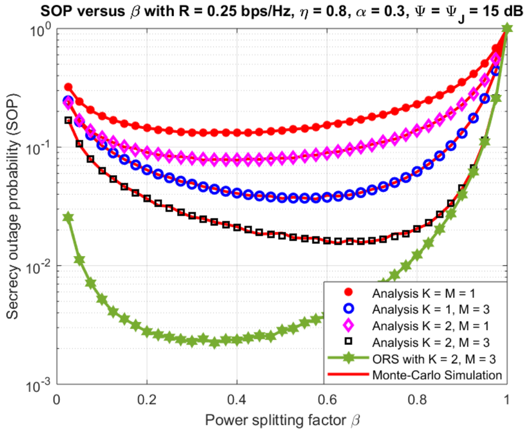

FIGURE 11. Secrecy outage probability of the proposed system versus power splitting factor for different configurations of relay and jammer nodes.

Figures 9, 10, and 11 depicts the impact of various parameters on the secrecy outage performance of our proposed systems. It's worth noting that in these three figures, all analytical curves match perfectly with the corresponding simulation curves, which validate the correctness of our analysis. In Fig. 9, we can observe that SOP decreases when Ψ increases, similar to OP in 3 but faster. It is interesting to note that there always exists an outage floor in each simulation case. That means when Ψ is large enough, the increasing of Ψ does not result in notably change in SOP. This floor is lower when more relay nodes and jammer nodes are considered for helping. In Fig. 9, Fig. 10, and Fig. 11, the SOP for optimal relay selection (ORS) is also given by simulation as a benchmark to compare with the partial relay selection (PRS) strategy. However, in this paper, we prefer PRS because its simplicity to implement.

Fig. 10 shows the effect of time-switching factor α on the secrecy performance. The SOP tends to decreases when α increases. Please note that the secrecy rate in this case is defined as difference in capacity between the source-relay link and the source-eavesdropper link. When α increases, the outage performance of source-relay link is slightly degraded because the SINR threshold increases, while the performance of relay-destination link is significantly improved due to higher harvested energy and smaller transmission time (so, transmit power becomes larger). On the other hand, increasing α does not improve the capacity of the source-eavesdropper link. That's why SOP decreases with α. It is shown in Fig. 10 that $K = 2, M = 3$ should be an appropriate choice for the numbers of relays and jammers, respectively.

As expected, there exists an optimal value of power splitting factor β that minimizes SOP, as shown in Fig. 11. This can be explained by the same argument as in Fig. 8. We can also observe that the optimal value of β increases from the scheme with less relays and jammers to the scheme with larger number of relays and jammers. Specifically, the optimal values of β for the cases $K = M = 1, K = 2, M = 1, K = 1, M = 3$, and $K = 2, M = 3$ are $0.375, 0.4, 0.55$, and 0.65 respectively. It's difficult to derive the closed-form formula for the optimal value of β, which is the solution of the equation $\frac{\partial(\mathrm{SOP})}{\partial\beta} = 0$ because the integral form of SOP. However, because the SOP is a single-minimum function with respect to β, it is easy to develop an iterative algorithm to find the optimal β numerically, for example, using Golden section search algorithm [62]. The 3-D plot of SOP function versus α and β for the case that $K = 2$ and $M = 3$ is shown in Fig. 12. We can find the global mimimum of SOP, which is equal to 0.00168, obtained as α approaches 0.5 and $\beta = 0.34$.[2]

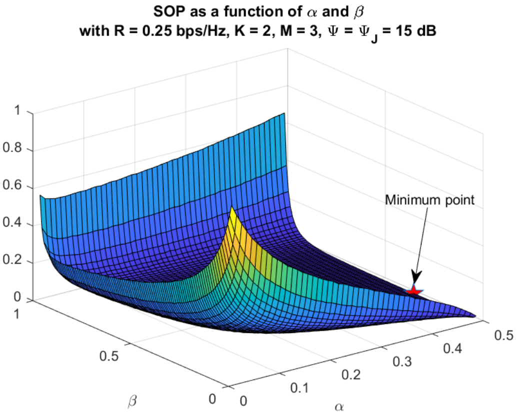

FIGURE 12. 3-D graph of SOP of A → B link versus α and β.

The average secrecy capacity (ASC) of the proposed system is illustrated in Figures 13, 14, and 15. First, we can see that ASC increases with the transmit-power-to-noise ratio

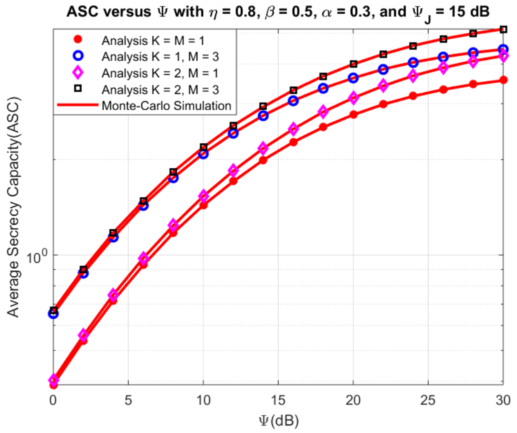

FIGURE 13. Average secrecy capacity of A versus transmit-power-to-noise-ratio for different configurations of relays and jammers.

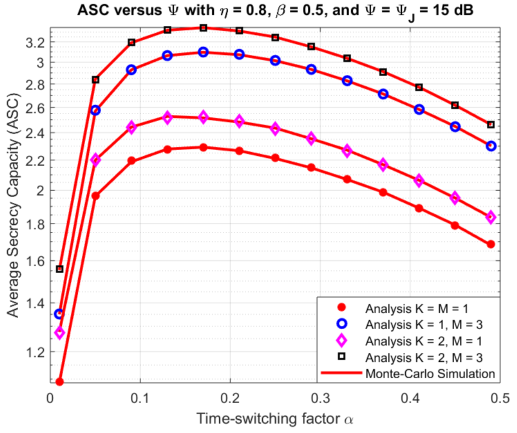

FIGURE 14. Average secrecy capacity of A versus time-switching factor α for different configurations of relays and jammers.

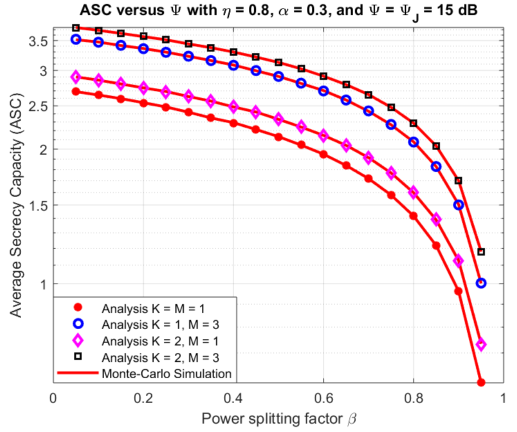

FIGURE 15. Average secrecy capacity of A versus power splitting factor β for different configurations of relays and jammers.

(SINR) in Fig. 13. It is obvious that the secrecy capacity is improved if we add more available-to-help relay nodes and more jammers. It seems that adding more available relay can bring more improvement that adding jammers, except for

[2] An adaptive TPSR protocol, in which α and β are regularly and optimally updated according to the channel states, can be implemented, with the tradeoff on complexity and cost.

sufficiently high SINR regime, which makes the source-relay communications good enough. Secondly, the ASC is a concave function with respect to the time-switching factor α, which can be explained as follows. For small α, the transmission duration is large enough, while the SOP decreases with α as we explained in Fig. 10, so the ASC increases with α. However, when α passed some certain threshold, the transmission time becomes smaller and has bad impact on the overall capacity. So the ASC starts to decrease. As seen from 14, the optimal α for 4 considered cases are very close together (around 0.17). Again, adding more available relays or adding more jammers can improve the ASC, where the former is better because here we have $\Psi = 15\ dB$. For the impact of power-splitting factor β, it is easily to see that larger β results in smaller ASC because in (46), increasing β leads to decreasing of the exponential terms and then the decreasing of ASC. By intuition, increasing β makes the chance of successful decoding the message at relay reduced, so the overall capacity is reduced. Fig. 15 confirms this argument, as we see that ASC falls to zero when β approaches 1. Again, the Monte Carlo simulations here confirms the analytical results.

V. CONCLUSION

In this paper, we propose a two-way half-duplex wireless relay networks in Rayleigh fading environment with partial relay selection and hybrid-TPSR-based EH at relay node, in which there is an eavesdropper in the vicinity of one source node. To enhance the security of the networks, some friendly jammers are employed to degrade the received signals at eavesdropper. We derive the closed-form expression of outage probability at the legitimate destination node, the intercept probability at eavesdropper, the secrecy outage probability, and the average secrecy capacity of the system. All analytical results are verified by Monte Carlo simulations. From the numerical results, we show that adding more available-to-help relay nodes or adding more jammers can improve the reliability and security performance of the system significantly, in which the former method can provide larger improvement in average-to-high SINR regime. For very high SINR, adding more jammers would be more beneficial. Secondly, there exists a unique optimal value for either time-switching or power splitting factor to minimize the outage probability, while the intercept probability increases with time-switching factor but does not depend on power splitting factor. For the secrecy outage probability, there may exist an outage floor if M and K is small. Therefore, it's recommended that we select α around 0.3 with $M = 3$ relay nodes and $K = 5$ or 7 jammers to obtain the desired performance but not to complicate the system. The results of this paper can find good applications in military communications as well as in IoT networks for smart cities, where the security of the messages is utmost important. For future work, we can extend the analysis to the case that multiple antennas are equipped at source nodes or eavesdroppers.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[5] W. Wang, K. C. Teh, and K. H. Li, "Generalized relay selection for improved security in cooperative DF relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28–31, Feb. 2016.

[6] A. Pandey and S. Yadav, "Physical-layer security for cellular multiuser two-way relaying networks with single and multiple decode-and-forward relays," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 12, p. e3639, Dec. 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3639

[7] M. K. Shukla, A. Pandey, S. Yadav, and N. Purohit, "Secrecy outage analysis of full duplex cellular multiuser two-way AF relay networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Mar. 2019, pp. 458–463.

[8] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[9] X. Li, M. Zhao, X.-C. Gao, L. Li, D.-T. Do, K. M. Rabie, and R. Kharel, "Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020.

[10] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[11] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[13] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[14] 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.

[15] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.

[16] M. K. Shukla, S. Yadav, and N. Purohit, "Secure transmission in cellular multiuser two-way amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11886–11899, Dec. 2018.

[17] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 971–975, May 2020.

[18] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[19] H.-T. Chiang and J. S. Lehnert, "Optimal jamming with codewords," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2012, pp. 1–6.

[20] S.-H. Lee and A. Khisti, "The Gaussian diamond-wiretap channel with rate-limited relay cooperation," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 338–341, Feb. 2017.

[21] A. A. Babayo, M. H. Anisi, and I. Ali, "A review on energy management schemes in energy harvesting wireless sensor networks," *Renew. Sustain. Energy Rev.*, vol. 76, pp. 1176–1184, Sep. 2017. Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032117304598

[22] I. Ahmed, M. M. Butt, C. Psomas, A. Mohamed, I. Krikidis, and M. Guizani, "Survey on energy harvesting wireless communications: Challenges and opportunities for radio resource allocation," *Comput. Netw.*, vol. 88, pp. 234–248, Sep. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615002029

[23] L. D. Nguyen, "Resource allocation for energy efficiency in 5G wireless networks," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 5, no. 14, Jun. 2018, Art. no. 154832.

[24] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.

[25] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, Feb. 2014.

[26] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[27] X. Li, M. Liu, C. Deng, D. Zhang, X.-C. Gao, K. M. Rabie, and R. Kharel, "Joint effects of residual hardware impairments and channel estimation errors on SWIPT assisted cooperative NOMA networks," *IEEE Access*, vol. 7, pp. 135499–135513, 2019.

[28] 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, Jul. 2013.

[29] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Throughput and ergodic capacity of wireless energy harvesting based DF relaying network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4066–4071.

[30] P. T. Tran, T. N. Nguyen, and M. Voznak, "Performance analysis of general hybrid TSR-PSR energy harvesting protocol for amplify-and-forward half-duplex relaying networks," *J. Adv. Eng. Comput.*, vol. 2, no. 2, pp. 121–130, Jun. 2018.

[31] W. Lu, Y. Gong, X. Liu, J. Wu, and H. Peng, "Collaborative energy and information transfer in green wireless sensor networks for smart cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1585–1593, Apr. 2018.

[32] P. Tin, P. M. Nam, T. T. Duy, P. Tran, and M. Voznak, "Secrecy performance of TAS/SC-based multi-hop Harvest-to-Transmit cognitive WSNs under joint constraint of interference and hardware imperfection," *Sensors*, vol. 19, no. 5, p. 1160, Mar. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1160

[33] X. Li, M. Huang, J. Li, Q. Yu, K. Rabie, and C. C. Cavalcante, "Secure analysis of multi-antenna cooperative networks with residual transceiver HIs and CEEs," *IET Commun.*, vol. 13, no. 17, pp. 2649–2659, Oct. 2019.

[34] S. K. Nobar, J. M. Niya, and B. M. Tazehkand, "Performance analysis of cognitive wireless powered communication networks under unsaturated traffic condition," *IEEE Trans. Green Commun. Netw.*, vol. 4, no. 3, pp. 819–831, Sep. 2020.

[35] T. N. Nguyen, P. T. Tran, and M. Vozňák, "Power splitting-based energy-harvesting protocol for wireless-powered communication networks with a bidirectional relay," *Int. J. Commun. Syst.*, vol. 31, no. 13, p. e3721, Sep. 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3721

[36] L. Irio, R. Oliveira, D. B. da Costa, and M.-S. Alouini, "Impact of wireless-powered communications in coexisting mobile networks," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1060–1064, Jul. 2020.

[37] X. Li, J. Li, and L. Li, "Performance analysis of impaired SWIPT NOMA relaying networks over imperfect weibull channels," *IEEE Syst. J.*, vol. 14, no. 1, pp. 669–672, Mar. 2020.

[38] N. Hoang An, M. Tran, T. N. Nguyen, and D.-H. Ha, "Physical layer security in a hybrid TPSR two-way half-duplex relaying network over a Rayleigh fading channel: Outage and intercept probability analysis," *Electronics*, vol. 9, no. 3, p. 428, Mar. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/3/428

[39] C. E. Shannon, "Two-way communication channels," in *Proc. 4th Berkeley Symp. Math., Statist., Probab.*, vol. 1, 1961, pp. 611–644.

[40] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 1668–1672.

[41] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 497–510, Jun. 2008.

[42] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 397–408, Oct. 2007, doi: 10.1145/1282427.1282425.

[43] S. Fu, T. Zhang, and M. Colef, "Secrecy in two-way relay systems," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Dec. 2010, pp. 1–5.

[44] 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, Jun. 2015.

[45] A. Salem and K. A. Hamdi, "Wireless power transfer in multi-pair two-way AF relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4578–4591, Nov. 2016.

[46] X. Zhou and Q. Li, "Energy efficiency for SWIPT in MIMO two-way amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4910–4924, Jun. 2018.

[47] T. N. Nguyen, T. H. Q. Minh, P. T. Tran, and M. Voznak, "Adaptive energy harvesting relaying protocol for two-way half-duplex system network over Rician fading channels," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–10, 2018.

[48] T. N. Nguyen, T. H. Quang Minh, P. T. Tran, M. Voznak, T. T. Duy, T.-L. Nguyen, and P. T. Tin, "Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods," *Ad Hoc Netw.*, vol. 84, pp. 178–187, Mar. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518301756

[49] P. N. Son and H. Y. Kong, "Improvement of the two-way decode-and-forward scheme by energy harvesting and digital network coding relay," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 3, p. e2960, Mar. 2017.

[50] T. N. Nguyen, P. T. Tran, and M. Voznak, "Wireless energy harvesting meets receiver diversity: A successful approach for two-way half-duplex relay networks over block Rayleigh fading channel," *Comput. Netw.*, vol. 172, May 2020, Art. no. 107176. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619314689

[51] S. C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond," *Phys. Commun.*, vol. 6, pp. 4–42, Mar. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490712000419

[52] P. Chen, Z. Xie, Y. Fang, Z. Chen, S. Mumtaz, and J. J. P. C. Rodrigues, "Physical-layer network coding: An efficient technique for wireless communications," *IEEE Netw.*, vol. 34, no. 2, pp. 270–276, Mar./Apr. 2020.

[53] S. Zhang and S. C. Liew, "Applying physical-layer network coding in wireless networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, pp. 1–12, Dec. 2010.

[54] Y. Ai, M. Cheffena, T. Ohtsuki, and H. Zhuang, "Secrecy performance analysis of wireless sensor networks," *IEEE Sensors Lett.*, vol. 3, no. 5, pp. 1–4, May 2019.

[55] B. Zhong and Z. Zhang, "Secure full-duplex two-way relaying networks with optimal relay selection," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1123–1126, May 2017.

[56] T. N. Nguyen, M. Tran, T.-L. Nguyen, D.-H. Ha, and M. Voznak, "Multi-source power splitting energy harvesting relaying network in half-duplex system over block Rayleigh fading channel: System performance analysis," *Electronics*, vol. 8, no. 1, p. 67, Jan. 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/1/67

[57] A. Jeffrey, D. Zwillinger, and I. S. Gradshteyn, "3-4—Definite integrals of elementary functions," in *Table of Integrals, Series, and Products*, 8th ed., D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, Eds. Boston, MA, USA: Academic, 2015, pp. 249–519. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780123849335000035

[58] T. T. Duy, T. L. Thanh, V. N. Q. Bao, and T. Q. Duong, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, Jul. 2015.

[59] B. C. Nguyen, T. Nguyen-Kieu, T. M. Hoang, P. T. Tran, and M. Vozň'ak, "Analysis of MRT/MRC diversity techniques to enhance the detection performance for MIMO signals in full-duplex wireless relay networks with transceiver hardware impairment," *Phys. Commun.*, vol. 42, Oct. 2020, Art. no. 101132. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490720302093

[60] X. Liu, "Average secrecy capacity of the weibull fading channel," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 841–844.

[61] F. W. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, *NIST Handbook of Mathematical Functions*, 1st ed. Cambridge, MA, USA: Cambridge Univ. Press, 2010.

[62] E. K. P. Chong and S. H. Zak, *An Introduction to Optimization*, 4th ed. Hoboken, NJ, USA: Wiley, 2013.

DUY-HUNG HA was born in Binh Dinh, Vietnam, in 1977. He received the B.S. degree in electronics and telecommunications engineering from the Institute of Post and Telecommunication, Viet Nam, in 2007, and the M.S. degree in electronics and telecommunications engineering from the University of Transport and Communications, Ha Noi, Viet Nam, in 2014. He is currently pursuing the Ph.D. degree in electrical engineering with the VSB, Technical University of Ostrava, Czech Republic. In 2017, he joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam, as a Lecturer. His major research interests include cooperative communications, cognitive radio, and physical-layer security.

TAN N. NGUYEN (Member, IEEE) was born in Nha Trang, Vietnam, in 1986. He received the B.S. and M.S. degrees in electronics and telecommunications engineering from the Ho Chi Minh University of Natural Sciences, a member of the Vietnam National University, Ho Chi Minh City, Vietnam, in 2008 and 2012, respectively, and the Ph.D. degree in electrical engineering from the VSB, Technical University of Ostrava, Czech Republic, in 2019. He got his Ph.D. degree in computer science, communication technology, and applied mathematics. In 2013, he joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam, where he has been working as a Lecturer. His major research interests include cooperative communications, cognitive radio, and physical-layer security.

MINH H. Q. TRAN received the Ph.D. thesis at Tomsk Polytechnic University, Tomsk, Russian Federation. He is currently working as a Lecturer with Faculty of Electrical and Electronic Engineering, Ton Duc Thang University, Ho Chi Minh, Vietnam. His research interests include study are high-voltage power systems, relay protections, optoelectronics, and telecommunication networks.

XINGWANG LI (Senior Member, IEEE) received the B.Sc. degree from Henan Polytechnic University, in 2007, the M.Sc. degree from the University of Electronic Science and Technology of China, in 2010, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2015.

From 2010 to 2012, he was working with Comba Telecom Ltd. In Guangzhou China, he works as an Engineer. He spent one year from 2017 to 2018 as a Visiting Scholar at Queen's University Belfast, Belfast, U.K. He is currently an Associated Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China. His research interests include MIMO communication, cooperative communication, hardware constrained communication, non-orthogonal multiple access, physical-layer security, unmanned aerial vehicles, the Internet-of-Things. He is currently an Editor on the Editorial Board of IEEE Access, *Computer Communications*, *Physical Communication*, and *KSII Transactions on Internet and Information Systems*. He is also a Lead Guest Editor of the Special Issue on Recent Advances in Physical Layer Technologies for 5G-Enabled Internet of Things; of Wireless Communications and Mobile Computing. He has served as many TPC/Co-Chair, such as IEEE Globecom, IEEE/CIC ICCC, IEEE WCNC, IEEE VTC, and IEEE/IET CSNDSP.

PHUONG T. TRAN (Senior Member, IEEE) was born in Ho Chi Minh, Vietnam, in 1979. He received the B.Eng. and M.Eng. degrees in electrical engineering from the Ho Chi Minh University of Technology, Ho Chi Minh, in 2002 and 2005, respectively, and the M.S. degree in mathematics and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2013. In 2007, he became a Vietnam Education Foundation Fellow at Purdue University. In 2013, he joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam. His major research interests include wireless communications and network information theory. He has serving as the Vice Dean of Faculty, since October 2014.

MIROSLAV VOZNAK (Senior Member, IEEE) was born in 1971. He received the Ph.D. degree in telecommunications from the VSB, Technical University of Ostrava, Czech Republic, in 2002. He is currently a Professor of electronics and communication technologies with the Department of Telecommunications, VSB, Technical University of Ostrava, and a Foreign Professor with Ton Duc Thang University, Ho Chi Minh City, Vietnam. He is a coauthor more than one hundred articles in journals indexed in the SCIE database. His research interests include IP telephony, wireless networks, network security, and big data analytics.