Wireless Pers Commun (2017) 96:6425–6457
DOI 10.1007/s11277-017-4485-8

Improving Secrecy Outage and Throughput Performance in Two-Way Energy-Constraint Relaying Networks Under Physical Layer Security

Sang Quang Nguyen[1] · **Hyung Yun Kong**[2]

Published online: 30 May 2017

Abstract In this paper, we propose three secrecy cooperative transmission protocols for a two-way energy-constrained relaying network in which two sources wish to exchange information with the help of multiple intermediate relays being subjected to wiretapping by multiple eavesdroppers. In the secure two-way communication (STW protocol), an energy-constrained relay is preselected via one of three investigated relay-selection strategies, which harvest the energy from the radio-frequency signals of one source and decode-and-forward the signals to another source. In secure two-way communication with network coding (STWNC protocol), the network coding technique is applied at a relay preselected via one of two investigated relay-selection strategies. In secure two-way communication with cooperative jamming and network coding (STWJNC protocol), under cooperative jamming, the network coding technique is applied at two sources and a preselected relay where a jammer-relay pair is preselected via one of two investigated selection strategies. The power-splitting receiver is applied at the energy-constrained relay for all proposed protocols. To evaluate performance, we derive new closed-form expressions for the secrecy outage probability and the throughput performance of the three protocols with the different relay and jammer-selection strategies. Our analysis is verified using Monte Carlo simulations.

Keywords Energy harvesting · Two-way communication · Physical layer security · Relay selection · Network coding · Cooperative jamming

✉ Sang Quang Nguyen
sangnqdv05@gmail.com

Hyung Yun Kong
hkong@mail.ulsan.ac.kr

[1] Duy Tan University, Da Nang, Vietnam

[2] University of Ulsan, Ulsan, Republic of Korea

1 Introduction

Energy harvesting is a promising solution to increase the life cycles of wireless devices and maintain network connectivity [1–4]. Conventionally, wireless devices harvest energy from external natural resources, such as wind, solar, or vibration, which is random and unsteady. Consequently, reliable communication is not ensured [5]. To cope with this limitation, energy harvesting from radio frequency (RF; or wireless power transfer) is an interesting approach [6–10]. The authors in [10] worked on an ideal receiver that can simultaneously decode the information and harvest the energy from a signal. In [5, 9], two practical receiver architectures were proposed: power splitting (PS), where the receiver splits the received signal into two parts (one for energy harvesting and one for information decoding), and time switching, where the receiver switches the received signal between information-decoding and energy-harvesting processes. Many researchers have subsequently investigated PS and TS in different system models and aspects [4, 11–14]. The authors in [4] investigated the symbol error rate of RF energy harvesting in a cooperative relaying network, where an energy-limited relay harvested the energy to assist in relaying the source information to the destination. In [11], co-channel interference was shown to be a potential energy source for a relay node in an opportunistic EH network. The authors in [12, 13] studied the throughput performance using both PS and TS in an amplify-and-forward (AF) relaying network [12], and they analyzed adaptive time-switching [13]. In [13], the power allocation strategy for a decode-and-forward (DF) relaying network was studied. In [15], the authors studied the throughput of three proposed wireless power transfer policies using a TS structure in an AF two-way relaying network. The authors in [16] study three different relay selection schemes of the DF energy-harvesting base power splitting relaying network.

Because the wireless medium has broadcasting nature, security issues for wireless communication has received considerable attention from researchers. Conventionally, security is addressed at higher layers using cryptographic methods [17]. However, due to the greater number of potential attacks when security is implemented at higher layers, many studies have been conducted on physical layer security (PLS). Security is evaluated in terms of the achievable secrecy rate (ASR), first defined by Aaron Wyner as the maximum rate of reliable information sent from the source to the desired destination in the presence of eavesdroppers [18]. Wyner showed that communication between the source and the destination is secure if the ASR of the source-eavesdropper link is smaller than that of the source-destination link. Following this finding, the authors in [19] studied physical layer security in wire-tap channels, and extended it to broadcast channels [20] and fading channels [21]. The application of PLS in cooperative communication to improve the secrecy performance of a wireless relaying network was investigated in [22]. In [23], the authors investigated physical layer security in a two-way relay network with friendly jammers under attack by an unauthenticated relay. In [24], the ergodic secrecy capacity metric was studied in distrusted AF relay networks. In [25], cooperative single-carrier systems affected by multiple eavesdroppers were evaluated in terms of the exact and asymptotic ergodic secrecy rate. Some relay-selection schemes [26] as well as assistance from a cooperative friendly jammer [27] have been shown to enhance the secrecy outage performance in cooperative cognitive radio networks. In [28], the authors analyze achievable secrecy rates with total and individual relay power constraints as well as design relay beamforming weights to enhance the secrecy rate for the cooperative multiple DF relay networks. The eavesdroppers are interfered with by jamming signals sent from a node

acting as a jammer, which is selected from a number of relays [29]. In [30], while the source transmits an encoded signal, relays transmit a jamming signal to confound eavesdroppers.

The source message can be encrypted using network coding for two binary jamming messages, i.e., XOR the original binary stream of the source and the binary jamming stream. The attack of the eavesdropper can be perfectly avoided when the jamming message is securely transmitted in the cooperative jamming phase. Thus, to increase the secrecy obtained by transmitting the jamming message, the jamming message should be transmitted by the best jammer, which is selected from multiple available ones.

To the best of our knowledge, no published literature has investigated a cooperative jammer combined with network coding to improve the secrecy performance of the energy-constrained two-way DF relaying network in the presence of multiple eavesdroppers. In the current work, we propose three transmission protocols with various relay/jammer-selection strategies. These strategies each select a cooperative relay before the source transmits the signal [31]. The STW protocol does not use network coding or cooperative jamming, so the secrecy in the two-way transmission of this protocol is achieved via conventional operation with four time slots (TSs). The STWJNC protocol applies network coding at a preselected relay, which reduces the number of TSs to three. Finally, the STWJNC protocol employs cooperative jamming and uses network coding at both the source node and the selected relay. We compare these three protocols as follows. We analyze three relay-selection strategies for the STW protocol, two relay-selection strategies for the STWNC protocol, and two jammerrelay-selection strategies for the STWJNC protocol. The preselected relay harvests the energy from the two source nodes in the STW and STWNC protocols, whereas it harvests energy from the preselected jammer in the STWJNC protocol. For performance evaluation, the secrecy outage probability (SOP) and secrecy throughput performance (STP) are derived as closed-form expressions with high SNR regions for the STW and STWNC protocols, and as exact closed-form expressions for the STWJNC protocol. Our derivations are validated using Monte Carlo Simulation.

The rest of this paper is organized as follows. Section 2 describes three transmission protocols for a two-way energy-constrained DF relaying network. The transmission operation and performance analysis of the STW, STWNC, and STWJNC protocols are given in Sects. 3, 4, and 5, respectively. Section 6 presents the numerical results, and various design insights are discussed. Finally, Sect. 7 summarizes our conclusions.

Notation The notation $\mathcal{CN}(0, N_0)$ denotes a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance N_0. $\mathcal{E}\{.\}$ denotes mathematical expectation. The functions $f_X(.)$ and $F_X(.)$ present the probability density function (PDF) and cumulative distribution function (CDF) of RV X. The function $K_1(x)$ denotes a first-order modified Bessel function of the second kind [32], and $\Gamma(x, y)$ is an incomplete Gamma function [32, Eq. (8.310.1)] . $C_b^a = \frac{b!}{a!(b-a)!}$. Notation Pr[.] returns the probability. Notation $[x]^+$ returns x if $x \geq 0$ and 0 if $x < 0$. The sign $\oplus$ indicates the XOR operator. The function ${}_2F_1(.)$ represents Gausss hypergeometric function [32].

2 System Model

As shown in Fig. 1, we consider three transmission protocols for a wireless network consisting of two source nodes $S1$ and $S2$ (that want to exchange data), M energy-constrained relay nodes R_m, $m \in \{1, 2, \ldots, M\}$, N jammer nodes J_n, $n \in \{1, 2, \ldots, N\}$, and L malicious

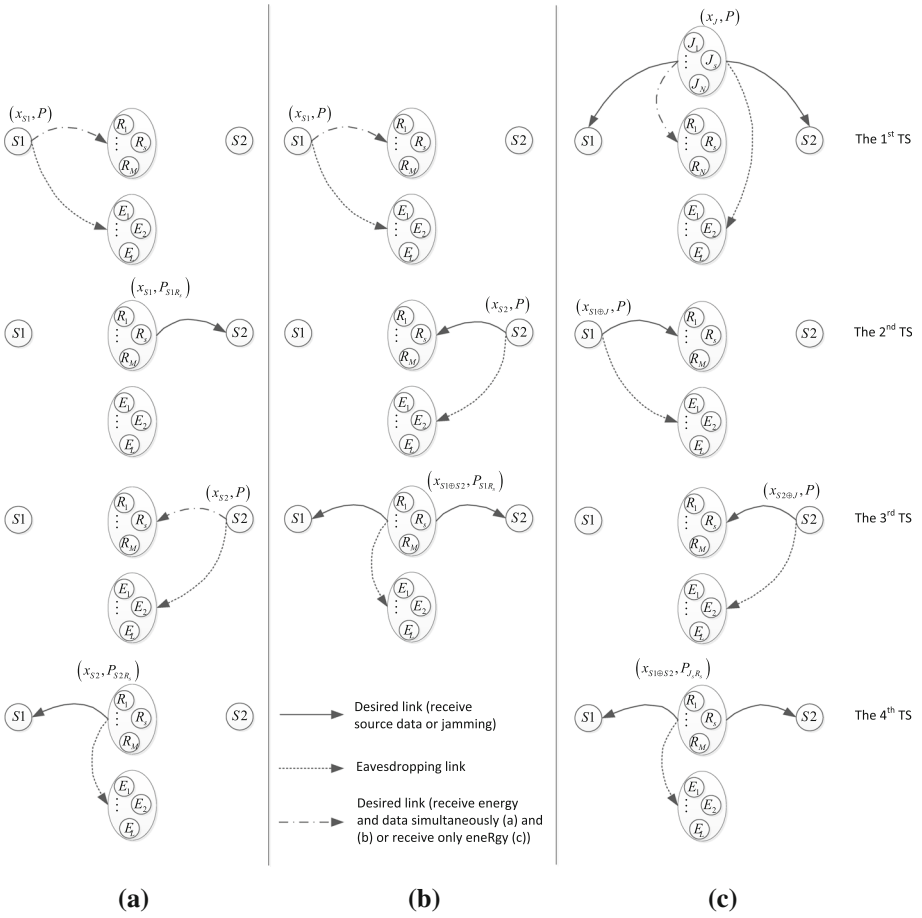

Fig. 1 Three transmission protocols of the two-way energy-constrained DF relaying network under a physical layer security: **a** No jammers and no network coding at relay, **b** without jammers and with network coding at relay, and **c** with the help of both jammers and network coding at relay

eavesdroppers E_l, $l \in \{1, 2, \ldots, L\}$. It is assumed that the direct link between the two source nodes is omitted due to deep shadowing [31]. Thus, communication between the two sources can be carried out through the best proactive DF relay, denoted R_s, that is selected from M available relay nodes by a particular selection strategy. It is worth noting that all L eavesdropper nodes can capture the information transmitted in the network. To enhance the secrecy of the communication, a jammer node J_s is selected to broadcast a random binary jamming message to the two source nodes $S1$ and $S2$ in the presence of L eavesdropper nodes. We assume each node is equipped with a single antenna operating in half-duplex mode, and the global channel state information (CSI) is available [22] at each node. Therefore, R_s and J_s can be selected before transmitting the jamming and data. The selection schemes used in this paper for each protocol are described in the next sections.

We use (h_{AB}, d_{AB}) to denote the Rayleigh channel coefficient over the distance for the link between two nodes A and B, where $A \in \{S1, S2, J_n, R_s\}$, $B \in \{S1, S2, R_s, E_l\}$, $A \neq B$ and where R_s, J_s, and E_l denote the mth relay node in cluster-R, the nth jammer node in

cluster-J, and the lth eavesdropper node in cluster-E, respectively. Thus, the corresponding channel gain $g_{AB} \triangleq |h_{AB}|^2$ is an exponential RV with parameters $\lambda_{AB} = (d_{AB})^{\beta}$, where β denotes the path-loss exponent.

In this paper, M relay nodes, N jammer nodes, and L eavesdropper nodes are located in cluster-R, cluster-J, and cluster-E, respectively [16]. Thus, the distance between two nodes in a cluster is insignificant compared to the distance between a node inside and a node outside a cluster, and the data links are independent and identically distributed (i.i.d) [31]. We obtain the corresponding cumulative distribution function (CDF) and probability density function (PDF) as $F_{g_{AB}}(x) = 1 - e^{-\lambda_{AB}x}$ and $f_{g_{A,B}}(x) = \lambda_{AB}e^{-\lambda_{AB}x}$, respectively.

We consider the energy harvesting technique as a power-splitting architecture with a power splitting ratio $\rho \in (0, 1)$ for energy harvesting and $(1 - \rho)$ for decoding the source signal [12, Fig. 3]. We assume that the fading coefficient h_{AB} does not vary during one block time of completing the exchange of one packet between two source nodes, and that it is independent of and identical to the next block time [16]. For convenient demonstration, let P denote the transmit power of all transmitters, i.e., the two sources, the selected relay R_s, and the selected jammer J_s; let $n_B(t) \sim CN(0, N_0)$ indicate the zero-mean and variance N_0 of the additive white Gaussian noise (AWGN) at the receiver B, $B \in \{S1, S2, R_s, E_l\}$; and let $n_{B,c}(k) \sim CN(0, \mu N_0)$ denote the zero-mean and variance of the noise that arises from converting a signal from the RF band to a baseband signal at all the receivers [16].

The next three sections present the operation and performance analysis of the three investigated transmission protocols. The performance of each protocol with the various relay/jammer selection strategies is evaluated using two performance metrics: SOP and STP.

3 Secure Two-Way Energy-Constrained Relaying Communication (STW)

3.1 Transmission Operation

The STW protocol takes four time slots (TSs) for the complete exchange of data between two source nodes $S1$ and $S2$ (see Fig. 1a) during a block time. In the first TS, $S1$ sends its signal x_{S1}, $\mathcal{E}\left\{|x_{S1}|^2 = 1\right\}$, to the preselected energy-constrained relay R_s in the presence of L eavesdropper nodes E_l, $l \in \{1, 2, \ldots, L\}$. The received signals at R_s and E_l are expressed respectively by

$$y_{S1R_s}(t) = \sqrt{P}h_{S1R_s}x_{S1}(t) + n_{R_s}(t) \tag{1}$$

$$y_{S1E_l}(t) = \sqrt{P}h_{S1E_l}x_{S1}(t) + n_{E_l}(t) \tag{2}$$

The received RF signal at the selected relay R_s, $y_{S1R_s}(t)$, is processed for energy harvesting (3) and information decoding (4), as follows:

$$y_{S1R_s,\mathrm{h}}(t) = \sqrt{\rho}y_{S1R_s}(t) = \sqrt{\rho P}h_{S1R_s}x_{S1}(t) + \sqrt{\rho}n_{R_s}(t) \tag{3}$$

$$y_{S1R_s,\mathrm{d}}(t) = \sqrt{1-\rho}\,y_{S1R_s}(t) = \sqrt{(1-\rho)P}h_{S1R_s}x_{S1}(t) + \sqrt{(1-\rho)}n_{R_s}(t) \tag{4}$$

The sampled baseband signals at E_l and R_s, e.g., $y_{S1E_l}(k)$ and $y_{S1R_s,d}(k)$, are obtained by down conversion of the signals $y_{S1R_s,d}(t)$ and $y_{S1E_l}(t)$ in (2) and (4), respectively [12, 16], as follows

$$y_{S1E_l}(k) = \sqrt{P}h_{S1E_l}x_{S1}(k) + n_{E_l}(k) + n_{E_l,c}(k) \tag{5}$$

$$y_{S1R_s,d}(k) = \sqrt{(1-\rho)P}h_{S1R_s}x_{S1}(k) + \sqrt{(1-\rho)}n_{R_s}(k) + n_{R_s,c}(k) \tag{6}$$

The received SNRs of the links $S1 \rightarrow E_l$ and $S1 \rightarrow R_s$ and the achievable secrecy rate (ASR) from $S1$ to R_s can be attained from (5) and (6), respectively, as follows:

$$\psi_{S1E_l} = \frac{P|h_{S1E_l}|^2}{(1+\mu)N_0} = \omega_1\psi g_{S1E_l} \tag{7}$$

$$\psi_{S1R_s} = \frac{(1-\rho)P|h_{S1R_s}|^2}{(1-\rho+\mu)N_0} = \omega_2\psi g_{S1R_s} \tag{8}$$

$$C_{S1R_s}^{\mathrm{STW}} \triangleq \left[\frac{1}{4}\log_2\left(\frac{1+\omega_2\psi g_{S1R_s}}{1+\omega_1\psi \max\limits_{l=1,2,\ldots,L} g_{S1E_l}}\right)\right]^+ = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_2\psi g_{S1R_s}}{1+\omega_1\psi g_{S1E\max}}\right)\right]^+ \tag{9}$$

where $\psi \triangleq \frac{P}{N_0}$, $\omega_1 \triangleq \frac{1}{1+\mu}$, $\omega_2 \triangleq \frac{1-\rho}{1-\rho+\mu}$, $g_{S1E\max} \triangleq \max_{l=1,2,\ldots,L} g_{S1E_l}$; the pre-log 1 / 4 indicates that there are four TSs for completing the transmission of the STW protocol.

From (3), the harvested energy at R_s is given by

$$E_{S1R_s} = \eta\rho P g_{S1R_s} T \tag{10}$$

where $0 \le \eta \le 1$ is the harvesting efficiency, and T is the transmission time of one TS.

R_s uses the power P_{S1R_s} in (11) to forward the data of $S1$ to $S2$ under eavesdropping by E_l in the second TS during the time interval T. The transmitted power from R_s and the received sampled baseband signals at $S2$ and E_l are expressed respectively by

$$P_{S1R_s} = E_{S1R_s}/T = \eta\rho P g_{S1R_s} \tag{11}$$

$$y_{R_sS2}(k) = \sqrt{P_{S1R_s}}h_{R_sS2}x_{S1}(k) + n_{S2}(k) + n_{S2,c}(k) \tag{12}$$

$$y_{R_sE_l}(k) = \sqrt{P_{S1R_s}}h_{R_sE_l}x_{S1}(k) + n_{E_l}(k) + n_{E_l,c}(k) \tag{13}$$

The received SNRs of the links $R_s \rightarrow S2$ and $R_s \rightarrow E_l$, and the ASR from R_s to $S2$, are respectively given by

$$\psi_{R_sS2} = \frac{P_{S1R_s}|h_{R_sS2}|^2}{(1+\mu)N_0} = \omega_3\psi g_{S1R_s} g_{R_sS2} \tag{14}$$

$$\psi_{R_sE_l} = \frac{P_{S1R_s}|h_{R_sE_l}|^2}{(1+\mu)N_0} = \omega_3\psi g_{S1R_s} g_{R_sE_l} \tag{15}$$

$$\begin{aligned} C_{R_sS2}^{\mathrm{STW}} &= \left[\frac{1}{4}\log_2\left(\frac{1+\omega_3\psi g_{S1R_s} g_{R_sS2}}{1+\omega_3\psi g_{S1R_s} \max\limits_{l=1,2,\ldots,L} g_{R_sE_l}}\right)\right]^+ \\ &= \left[\frac{1}{4}\log_2\left(\frac{1+\omega_3\psi g_{S1R_s} g_{R_sS2}}{1+\omega_3\psi g_{S1R_s} g_{R_sE\max}}\right)\right]^+ \end{aligned} \tag{16}$$

where $\omega_3 \triangleq \frac{\eta\rho}{1+\mu}$.

In the third and fourth TSs, the transmission of the links $S2 \rightarrow R_s$ and $R_s \rightarrow S1$ under eavesdropping by E_l are the same as those of links $S1 \rightarrow R_s$ and $R_s \rightarrow S2$, respectively, due to the symmetric particularity. Thus, similarly to (9) and (16), we obtain the ASRs from $S2$ to R_s and from R_s to $S1$, respectively, as follows:

$$C_{S2R_s}^{\mathrm{STW}} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_2\psi g_{S2R_s}}{1+\omega_1\psi g_{S2E\max}}\right)\right]^+ \tag{17}$$

$$C_{R_sS1}^{\mathrm{STW}} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_3\psi g_{S2R_s}g_{R_sS1}}{1+\omega_3\psi g_{S2R_s}g_{R_sE\max}}\right)\right]^+ \tag{18}$$

For this protocol, we consider three relay-selection schemes for choosing the relay R_s. In the first, we note that any eavesdropping of the selected relay R_s occurs in the second and fourth TSs, so R_s is selected based on the minimum eavesdropping channel (called MIRE), as represented in (19a). In the second, R_s is selected based on the maximum channel gain of the link $S1 - R$ (MAS1R), as formulated in (19b). In the third scheme, R_s is selected randomly from the M available nodes (RAN) (19c).

$$R_s = \arg\min_{m=1,2,\ldots,M}(g_{R_mE\max}) \tag{19a}$$

$$R_s = \arg\max_{m=1,2,\ldots,M}(g_{S1R_m}) \tag{19b}$$

$$R_s = \mathrm{random}(R_1, R_2, \ldots, R_M) \tag{19c}$$

3.2 Performance Analysis

3.2.1 Secrecy Outage Probability

The probability of a successful exchange of data between two source nodes is the probability that all four ASRs are above the target, $C_t > 0$. This can be formulated as follows:

$$P_{non-out}^{\mathrm{STW}} = \Pr\left[C_{S1R_s}^{\mathrm{STW}} \geq C_t, C_{R_sS2}^{\mathrm{STW}} \geq C_t, C_{S2R_s}^{\mathrm{STW}} \geq C_t, C_{R_sS1}^{\mathrm{STW}} \geq C_t\right] \tag{20}$$

The system experiences an outage if at least one of the four ASRs is less than C_t. In other words, the SOP of the STW protocol can be given by

$$\begin{aligned} P_{out}^{\mathrm{STW}} &= 1 - P_{non-out}^{\mathrm{STW}} \\ &= 1 - \Pr\left[C_{S1R_s}^{\mathrm{STW}} \geq C_t, C_{R_sS2}^{\mathrm{STW}} \geq C_t, C_{S2R_s}^{\mathrm{STW}} \geq C_t, C_{R_sS1}^{\mathrm{STW}} \geq C_t\right] \end{aligned} \tag{21}$$

By substituting the expressions of $C_{S1R_s}^{\mathrm{STW}}$, $C_{R_sS2}^{\mathrm{STW}}$, $C_{S2R_s}^{\mathrm{STW}}$, and $C_{R_sS1}^{\mathrm{STW}}$ from Eqs. (9), (16), (17), and (18), respectively, into (21), we obtain

$$
\begin{aligned}
P_{out}^{\mathrm{STW}} &= 1-\Pr\left[\begin{array}{l} g_{S1R_s} \geq \dfrac{\varphi-1}{\omega_2\psi}+\dfrac{\varphi\omega_1 g_{S1E\max}}{\omega_2}, \\ g_{R_sS2} \geq \dfrac{\varphi-1}{\omega_3\psi g_{S1R_s}}+\varphi g_{R_sE\max}, \\ g_{S2R_s} \geq \dfrac{\varphi-1}{\omega_2\psi}+\dfrac{\varphi\omega_1 g_{S2E\max}}{\omega_2}, \\ g_{R_sS1} \geq \dfrac{\varphi-1}{\omega_3\psi g_{S2R_s}}+\varphi g_{R_sE\max} \end{array}\right] \\
&= 1-\int_0^\infty f_{g_{S1E\max}}(x_1)\int_0^\infty f_{g_{S2E\max}}(x_2)\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty f_{g_{S1R_s}}(x_3) \\
&\quad\times\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty f_{g_{S2R_s}}(x_4)\int_0^\infty f_{g_{R_sE\max}}(x_5)\int_{\frac{\varphi-1}{\omega_3\psi x_4}+\varphi x_5}^\infty f_{g_{R_sS1}}(x_6) \\
&\quad\times\int_{\frac{\varphi-1}{\omega_3\psi x_3}+\varphi x_5}^\infty f_{g_{R_sS2}}(x_7)dx_7dx_6dx_5dx_4dx_3dx_2dx_1
\end{aligned}
\tag{22}
$$

where $\varphi \triangleq 2^{4C_t}$.

Depending on which of the three relay selection strategies is used, from (19a), (19b), and (19c), we obtain three expressions of SOP, $P_{out,\mathrm{MIRE}}^{\mathrm{STW}}$, $P_{out,\mathrm{MAS1R}}^{\mathrm{STW}}$, and $P_{out,\mathrm{RAN}}^{\mathrm{STW}}$, respectively, as follows

$$
\begin{aligned}
P_{out,\mathrm{MIRE}}^{\mathrm{STW}} &= 1-\Omega_1(M,L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE}) \\
&\quad\times\int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\
&\quad\times\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1}C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2} \\
&\quad\times\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty \lambda_{S1R}e^{-\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}} \\
&\quad\times\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}e^{-\lambda_{S2R}x_4}e^{\frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4}}dx_4dx_3dx_2dx_1
\end{aligned}
\tag{23a}
$$

$$
\begin{aligned}
P_{out,\mathrm{MAS1R}}^{\mathrm{STW}} &= 1-\Omega_2(L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE}) \\
&\quad\times\int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\
&\quad\times\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1}C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2} \\
&\quad\times\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty M\lambda_{S1R}\sum_{k=0}^{M-1}C_{M-1}^k(-1)^k e^{-(1+k)\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}} \\
&\quad\times\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}e^{-\lambda_{S2R}x_4}e^{\frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4}}dx_4dx_3dx_2dx_1
\end{aligned}
\tag{23b}
$$

$$
\begin{aligned}
P_{out,\mathrm{RAN}}^{\mathrm{STW}} &= 1-\Omega_2(L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE}) \\
&\times \int_0^{\infty} L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\
&\times \int_0^{\infty} L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^{w}(-1)^w e^{-(1+w)\lambda_{S2E}x_2} \\
&\times \int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^{\infty} \lambda_{S1R}e^{-\lambda_{S1R}x_3} e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}} \\
&\times \int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^{\infty} \lambda_{S2R}e^{-\lambda_{S2R}x_4} e^{\frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4}} dx_4 dx_3 dx_2 dx_1
\end{aligned}
\tag{23c}
$$

where (23a) is obtained from (22) by applying the PDFs of RVs $g_{S1E\max}$, $g_{S2E\max}$, g_{S1R_s}, g_{S2R_s}, $g_{R_sE\max}$, g_{R_sS1}, and g_{R_sS2} as follows: $f_{g_{S1E\max}}(x_1) = L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t e^{-(1+t)\lambda_{S1E}x_1}$ (see Appendix 1), $f_{g_{S2E\max}}(x_2) = L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^{w}(-1)^w e^{-(1+w)\lambda_{S2E}x_2}$ (see Appendix 1), $f_{g_{S1R_s}}(x_3) = \lambda_{S1R}e^{-\lambda_{S1R}x_3}$, $f_{g_{S2R_s}}(x_4) = \lambda_{S2R}e^{-\lambda_{S2R}x_4}$, $f_{g_{R_sE\max}}(x_5) = ML\lambda_{RE}\sum_{k=0}^{L-1} C_{L-1}^{k}(-1)^k \sum_{u=0}^{M-1} C_{M-1}^{u}(-1)^u \sum_{v=0}^{Lu} C_{Lu}^{v}(-1)^v e^{-(1+k+v)\lambda_{RE}x_5}$ (see Appendix 1), $f_{g_{R_sS1}}(x_6) = \lambda_{RS1}e^{-\lambda_{RS1}x_6}$, and $f_{g_{R_sS2}}(x_7) = \lambda_{RS2}e^{-\lambda_{RS2}x_7}$, respectively, and denoted $\Omega_1(L,M,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE}) \triangleq LM\lambda_E\sum_{k=0}^{L-1} C_{L-1}^{k}(-1)^k \sum_{u=0}^{M-1} C_{M-1}^{u}(-1)^u \sum_{v=0}^{Lu} \frac{C_{Lu}^{v}(-1)^v}{(1+k+v)\lambda_{RE}+\varphi(\lambda_{RS1}+\lambda_{RS2})}$; (23b) is obtained from (22) by applying $f_{g_{S1E\max}}(x_1) = L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t e^{-(1+t)\lambda_{S1E}x_1}$, $f_{g_{S2E\max}}(x_2) = L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^{w}(-1)^w e^{-(1+w)\lambda_{S2E}x_2}$, $f_{g_{S1R_s}}(x_3) = M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^{k}(-1)^k e^{-(1+k)\lambda_{S1R}x_3}$, $f_{g_{S2R_s}}(x_4) = \lambda_{S2R}e^{-\lambda_{S2R}x_4}$, $f_{g_{R_sE\max}}(x_5) = L\lambda_{RE}\sum_{u=0}^{L-1} C_{L-1}^{u}(-1)^u e^{-(1+u)\lambda_{RE}x_5}$, $f_{g_{R_sS1}}(x_6) = \lambda_{RS1}e^{-\lambda_{RS1}x_6}$, $f_{g_{R_sS2}}(x_7) = \lambda_{RS2}e^{-\lambda_{RS2}x_7}$, and denoted $\Omega_2(L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE}) \triangleq L\lambda_{RE}\sum_{u=0}^{L-1} \frac{C_{L-1}^{u}(-1)^u}{(1+u)\lambda_{RE}+\varphi(\lambda_{RS1}+\lambda_{RS2})}$; (23c) is obtained in the same way as (23b) with $M=1$. We have the asymptotic expansion of the exponential function as follows

$$
e^{x} \overset{x\to 0}{=} 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + O\left(x^4\right) \tag{24}
$$

Note that $\frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4} \to 0$ when ψ is high. We obtain the following approximate expression:

$$
e^{\frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4}} = 1 - \frac{(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4} + O\left(\left[\frac{\lambda_{RS1}(\varphi-1)}{\omega_3\psi x_4}\right]^2\right) \approx 1 - \frac{(\varphi-1)\lambda_{RS1}}{\omega_3\psi x_4} \tag{25}
$$

Then, the SOP of the STW protocol with each of the three relay-selection strategies can be expressed when ψ is high, as follows:

$$
P_{out,\mathrm{MIRE}}^{\mathrm{STW}} = 1 - \Omega_1(L,M,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE})\left(I_{1,\mathrm{MIRE}} + I_{2,\mathrm{MIRE}}\right) \tag{26a}
$$

$$
P_{out,\mathrm{MAS1R}}^{\mathrm{STW}} = 1 - \Omega_2(L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE})\left(I_{1,\mathrm{MAS1R}} + I_{2,\mathrm{MAS1R}}\right) \tag{26b}
$$

$$
P_{out,\mathrm{RAN}}^{\mathrm{STW}} = 1 - \Omega_2(L,\varphi,\lambda_{RS1},\lambda_{RS2},\lambda_{RE})\left(I_{1,\mathrm{RAN}} + I_{2,\mathrm{RAN}}\right) \tag{26c}
$$

where

$$I_{1,\mathrm{MIRE}} = I_{1,\mathrm{RAN}} \triangleq \int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1}$$
$$\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2}\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty \lambda_{S1R}e^{-\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}$$
$$\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}e^{-\lambda_{S2R}x_4}dx_4dx_3dx_2dx_1,$$

$$I_{2,\mathrm{MIRE}} = I_{2,\mathrm{RAN}} \triangleq \frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi}$$
$$\int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1}\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2}$$
$$\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty \lambda_{S1R}e^{-\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}\frac{e^{-\lambda_{S2R}x_4}}{x_4}dx_4dx_3dx_2dx_1,$$

$$I_{1,\mathrm{MAS1R}} \triangleq \int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1}\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^w(-1)^w$$
$$e^{-(1+w)\lambda_{S2E}x_2}\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^k(-1)^k e^{-(1+k)\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}$$
$$\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}e^{-\lambda_{S2R}x_4}dx_4dx_3dx_2dx_1,$$

$$I_{2,\mathrm{MAS1R}} \triangleq \frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi}\int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1}\int_0^\infty L\lambda_{S2E}\sum_{w=0}^{L-1}$$
$$C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2}\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^k(-1)^k e^{-(1+k)\lambda_{S1R}x_3}$$
$$e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_2}{\omega_2}}^\infty \lambda_{S2R}\frac{e^{-\lambda_{S2R}x_4}}{x_4}dx_4dx_3dx_2dx_1.$$

Lemma 1 *The following expression is valid for the integral* $I_{1,\mathrm{MAS1R}}$

$$I_{1,\mathrm{MAS1R}} = e^{\frac{-(\varphi-1)\lambda_{S2R}}{\omega_2\psi}}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E})\left[\begin{array}{l}\Omega_4(L,M,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E})\\ +\dfrac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_5(L,M,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E})\end{array}\right] \tag{27}$$

where $\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \triangleq L\lambda_{S2E}\sum_{w=0}^{L-1}\frac{C_{L-1}^w(-1)^w\omega_2}{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}}$, $\Omega_4(L,M,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E}) \triangleq LM\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t\sum_{k=0}^{M-1}\frac{C_{M-1}^k(-1)^k\omega_2 e^{\frac{-(1+k)(\varphi-1)\lambda_{S1R}}{\omega_2\psi}}}{(1+k)[(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R}]}$, $\Omega_5(L,M,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E}) \triangleq LM\lambda_{S1E}\lambda_{S1R}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t\sum_{k=0}^{M-1} C_{M-1}^k(-1)^k\frac{\omega_2}{(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R}2}$ $F_1\left(1,1;2;\frac{(1+t)\omega_2\lambda_{S1E}}{(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R}}\right)$.

Proof Given in Appendix 2. □

From that, the integrals $I_{1,\mathrm{MIRE}}$ and $I_{1,\mathrm{RAN}}$ can be obtained as

$$I_{1,\mathrm{MIRE}} = I_{1,\mathrm{RAN}} = I_{1,\mathrm{MAS1R}}\big|_{M=1} = e^{\frac{-(\varphi-1)\lambda_{S2R}}{\omega_2\psi}}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \left[\begin{array}{l}\Omega_4(L,1,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E}) \\ +\dfrac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_5(L,1,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E})\end{array}\right] \tag{28}$$

Lemma 2 *The following expression is valid for the integral* $I_{2,\mathrm{MAS1R}}$

$$I_{2,\mathrm{MAS1R}} = \frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi}\Omega_5(L,1,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \left[\begin{array}{l}\Omega_4(L,M,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E}) \\ +\dfrac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_5(L,M,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E})\end{array}\right] \tag{29}$$

Proof Given in Appendix 3. □

The integrals $I_{2,\mathrm{MIRE}}$ and $I_{2,\mathrm{RAN}}$ are then given by

$$I_{2,\mathrm{MIRE}} = I_{2,\mathrm{RAN}} = I_{2,\mathrm{MAS1R}}\big|_{M=1} = \frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi}\Omega_5(L,1,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \left[\begin{array}{l}\Omega_4(L,1,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E}) \\ +\dfrac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_5(L,1,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E})\end{array}\right] \tag{30}$$

Finally, we can obtain expressions for $P^{\mathrm{STW}}_{out,\mathrm{MIRE}}$, $P^{\mathrm{STW}}_{out,\mathrm{MAS1R}}$, and $P^{\mathrm{STW}}_{out,\mathrm{RAN}}$ by substituting (27–30) into (26a–26c).

3.2.2 Secrecy Throughput Performance

In this subsection, we derive the STP of the STW protocol, which is defined as the effective time for the transmissions by the two sources $S1$ and $S2$ at the secrecy target rate C_t bits/sec/Hz. In the STW protocol, the total number of time slots is $4T$, and the effective communication time for a transmission from $S1$ to R_s and from $S2$ to R_s is $2T$ (the first and third TSs). The throughput of the STW protocol with one of the three relay-selection strategies is given by

$$\tau^{\mathrm{STW}}_{\mathrm{MIRE/MAS1R/RAN}} = \left(1 - P^{\mathrm{STW}}_{out,\mathrm{MIRE/MAS1R/RAN}}\right)\frac{C_t}{2} \tag{31}$$

where $\tau^{\mathrm{STW}}_{\mathrm{MIRE/MAS1R/RAN}}$ and $P^{\mathrm{STW}}_{out,\mathrm{MIRE/MAS1R/RAN}}$ are STP and SOP, respectively.

4 Secure Two-Way Energy-Constrained Relaying Communication with Network Coding (STWNC)

4.1 Transmission Operation

In the STWNC protocol, to reduce transmission time, we shorten the transmission period to $3T$ by applying the digital network coding technique at the preselected relay R_s. Thus, the STWNC protocol uses three time slots for a complete data-exchange period, as shown in Fig. 1b. In the first TS, the binary message m_{S1} of the source $S1$ is presented by the signal x_{S1}, $\mathcal{E}\left\{|x_{S1}|^2 = 1\right\}$, which is transmitted to the preselected energy-constrained relay R_s in the presence of L eavesdropper nodes E_l, $l \in \{1, 2, \ldots, L\}$. The ASR from $S1$ to R_s with this protocol is similar to that with the STW protocol, replacing the pre-log 1 / 4 with 1 / 3, as follows:

$$C_{S1R_s}^{\text{STWNC}} = \left[\frac{1}{3}\log_2\left(\frac{1+\omega_2\psi g_{S1R_s}}{1+\omega_1\psi g_{S1E\max}}\right)\right]^+ \tag{32}$$

In this protocol, the preselected relay R_s only harvested the energy from the received signal transmitted by $S1$ in the first TS. The harvested energy is the same as in (10):

$$E_{S1R_s} = \eta\rho P g_{S1R_s} T \tag{33}$$

The source $S2$ sends its message m_{S2}, presented as signal x_{S2}, to R_s under eavesdropping by E_l; thus, the ASR from $S2$ to R_s is expressed as

$$C_{S2R_s}^{\text{STWNC}} = \left[\frac{1}{3}\log_2\left(\frac{1+\omega_1\psi g_{S2R_s}}{1+\omega_1\psi g_{S2E\max}}\right)\right]^+ \tag{34}$$

After successfully and safely decoding the two binary messages, m_{S1} and m_{S2}, during the first two TSs, R_s combines them by applying the digital network coding and generates a new message, $m_{S1\oplus S2}$, where $m_{S1\oplus S2} = m_{S1} \oplus m_{S2}$. The message $m_{S1\oplus S2}$ is presented by the signal $x_{S1\oplus S2}$, and it is broadcasted back to both source nodes $S1$ and $S2$ by R_s during the third TS with the transmitted power $P_{S1R_s} = E_{S1R_s}/T = \eta\rho P g_{S1R_s}$. The received baseband signals at $S1$, $S2$, and E_l can be respectively given by

$$y_{R_sS1}(k) = \sqrt{P_{R_s}} h_{R_sS1} x_{S1\oplus S2}(k) + n_{S1}(k) + n_{S1,c}(k) \tag{35}$$

$$y_{R_sS2}(k) = \sqrt{P_{R_s}} h_{R_sS2} x_{S1\oplus S2}(k) + n_{S2}(k) + n_{S2,c}(k) \tag{36}$$

$$y_{R_sE_l}(k) = \sqrt{P_{R_s}} h_{R_sE_l} x_{S1\oplus S2}(k) + n_{E_l}(k) + n_{E_l,c}(k) \tag{37}$$

Note that, during the third TS, the transmitted message $m_{S1\oplus S2}$ is coded; thus, the eavesdroppers E_l cannot obtain the messages from the two sources, m_{S1} and m_{S2}. In other words, the eavesdroppers E_l, $l \in \{1, 2, \ldots, L\}$, do not impact the ASRs of the two links $R_s \to S1$ and $R_s \to S2$. Consequently, the achievable secrecy capacities of the links $R_s - S1$ and $R_s - S2$ are respectively expressed as

$$C_{R_sS1}^{\text{STWNC}} = \left[\frac{1}{3}\log_2(1+\omega_3\psi g_{S1R_s} g_{R_sS1})\right]^+ \tag{38}$$

$$C_{R_sS2}^{\text{STWNC}} = \left[\frac{1}{3}\log_2(1+\omega_3\psi g_{S1R_s}g_{R_sS2})\right]^+ \tag{39}$$

In the STWNC protocol, we do not consider the relay-selection scheme based on the minimum channel gain from the selected relay R_s to eavesdroppers because there is no impact of eavesdroppers on the transmission of R_s in the third TS. Thus, we analyze the performance with the two other considered relay-selection strategies, in (19b) and (19c), for this protocol.

4.2 Performance Analysis

4.2.1 Secrecy Outage Probability

The SOP with the STWNC protocol is expressed the same way as that with the STW protocol:

$$P_{out}^{\text{STWNC}} = 1 - \Pr\left[\begin{matrix} C_{S1R_s}^{\text{STWNC}} \geq C_t, C_{S2R_s}^{\text{STWNC}} \geq C_t, \\ C_{R_sS1}^{\text{STWNC}} \geq C_t, C_{R_sS2}^{\text{STWNC}} \geq C_t \end{matrix}\right] \tag{40}$$

By substituting the expressions for $C_{S1R_s}^{\text{STWNC}}$, $C_{S2R_s}^{\text{STWNC}}$, $C_{R_sS1}^{\text{STWNC}}$, and $C_{R_sS2}^{\text{STWNC}}$ from Eqs. (32), (34), (38), and (39), respectively, into (40), we obtain

$$\begin{aligned} P_{out}^{\text{STWNC}} &= 1 - \Pr\left[\begin{matrix} g_{S1R_s} \geq \dfrac{\phi-1}{\omega_2\psi} + \dfrac{\phi\omega_1 g_{S1E\max}}{\omega_2}, g_{S2R_s} \geq \dfrac{\phi-1}{\omega_1\psi} + \phi g_{S2E\max}, \\ g_{R_sS1} \geq \dfrac{\phi-1}{\omega_3\psi g_{S1R_s}}, g_{R_sS2} \geq \dfrac{\phi-1}{\omega_3\psi g_{S1R_s}} \end{matrix}\right] \\ &= 1 - \int_0^\infty f_{g_{S1E\max}}(x_1)\int_0^\infty f_{g_{S2E\max}}(x_2)\int_{\frac{\phi-1}{\omega_2\psi}+\frac{\phi\omega_1 x_1}{\omega_2}}^\infty f_{g_{S1R_s}}(x_3) \\ &\quad \times \int_{\frac{\phi-1}{\omega_2\psi}+\phi x_2}^\infty f_{g_{S2R_s}}(x_4)\int_{\frac{\phi-1}{\omega_3\psi x_3}}^\infty f_{g_{R_sS1}}(x_5)\int_{\frac{\phi-1}{\omega_3\psi x_3}}^\infty f_{g_{R_sS2}}(x_6)dx_6dx_5dx_4dx_3dx_2dx_1 \end{aligned} \tag{41}$$

where $\phi \triangleq 2^{3C_t}$. By applying the relay selection strategy in (19b) (MAS1R) to this protocol, and approximating $e^{\frac{-(\phi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_3\psi x_3}} \approx 1 + \frac{-(\phi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_3\psi x_3}$, we attain the SOP for $P_{out,\text{MAS1R}}^{\text{STWNC}}$ as follows:

$$P_{out,\text{MAS1R}}^{\text{STWNC}} = 1 - e^{\frac{-(\phi-1)\lambda_{S2R}}{\omega_2\psi}}(I_7 + I_8) \tag{42}$$

where

$$
\begin{aligned}
I_7 &\triangleq \int_0^{\infty} L\lambda_{S1E} \sum_{t=0}^{L-1} C_{L-1}^{t} (-1)^t e^{-(1+t)\lambda_{S1E} x_1} \\
&\quad \times \int_0^{\infty} L\lambda_{S2E} \sum_{w=0}^{L-1} C_{L-1}^{w} (-1)^w e^{-(1+w)\lambda_{S2E} x_2} e^{-\phi\lambda_{S2R} x_2} \\
&\quad \times \int_{\frac{\phi-1}{\omega_2\psi}+\frac{\phi\omega_1 x_1}{\omega_2}}^{\infty} M\lambda_{S1R} \sum_{k=0}^{M-1} C_{M-1}^{k} (-1)^k e^{-(1+k)\lambda_{S1R} x_3} dx_3 dx_2 dx_1 \\
&= \Omega_4(L, M, \varphi, \omega_1, \omega_2, \psi, \lambda_{S1R}, \lambda_{S1E}) \Omega_2(L, \phi, 0, \lambda_{S2R}, \lambda_{S2E}), \\
I_8 &\triangleq \frac{-(\phi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_3\psi} \int_0^{\infty} L\lambda_{S1E} \sum_{t=0}^{L-1} C_{L-1}^{t} (-1)^t e^{-(1+t)\lambda_{S1E} x_1} \\
&\quad \times \int_0^{\infty} L\lambda_{S2E} \sum_{w=0}^{L-1} C_{L-1}^{w} (-1)^w e^{-(1+w)\lambda_{S2E} x_2} e^{-\phi\lambda_{S2R} x_2} \\
&\quad \times \int_{\frac{\phi-1}{\omega_2\psi}+\frac{\phi\omega_1 x_1}{\omega_2}}^{\infty} M\lambda_{S1R} \sum_{k=0}^{M-1} C_{M-1}^{k} (-1)^k \frac{e^{-(1+k)\lambda_{S1R} x_3}}{x_3} dx_3 dx_2 dx_1 \\
&= \frac{-(\phi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_3\psi} \Omega_2(L, \phi, 0, \lambda_{S2R}, \lambda_{S2E}) \\
&\quad \Omega_5(L, M, \varphi, \omega_1, \omega_2, \lambda_{S1R}, \lambda_{S1E})
\end{aligned}
$$

With the relay selection strategy in (19c) (RAN), the SOP can be obtained as

$$
\begin{aligned}
P_{out,\mathrm{RAN}}^{\mathrm{STWNC}} = P_{out,\mathrm{MAS1R}}^{\mathrm{STWNC}}\Big|_{M=1} &= 1 - e^{\frac{-(\phi-1)\lambda_{S2R}}{\omega_2\psi}} \Omega_2(L, \phi, 0, \lambda_{S2R}, \lambda_{S2E}) \\
&\left(\begin{array}{l} \Omega_4(L, 1, \phi, \omega_1, \omega_2, \psi, \lambda_{S1R}, \lambda_{S1E}) \\ + \dfrac{-(\phi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_3\psi} \Omega_5(L, 1, \phi, \omega_1, \omega_2, \lambda_{S1R}, \lambda_{S1E}) \end{array} \right).
\end{aligned} \tag{43}
$$

4.2.2 Secrecy Throughput Performance

With the STWNC protocol, the effective transmission time of the two sources $S1$ and $S2$ at the secrecy target rate C_t bits/sec/Hz is $2T$ / $3T$. The throughput of this protocol with one of the two relay-selection strategies MAS1R or RAN is

$$
\tau_{\mathrm{MAS1R/RAN}}^{\mathrm{STWNC}} = \left(1 - P_{out,\mathrm{MAS1R/RAN}}^{\mathrm{STWNC}}\right) \frac{2C_t}{3}. \tag{44}
$$

5 Secure Two-Way Energy-Constrained Relaying Communication with Cooperative Jamming and Network Coding (STWJNC)

5.1 Transmission Operation

In the STWJNC protocol, there are four TSs for completing the exchange of data between two source nodes, as shown in Fig. 1c. In this protocol, the preselected jammer node J_s has

two functions that (1) help the two sources code their messages by XORing them with the jamming message, and (2) transmit the energy to the R_s. In the first TS, J_s broadcasts the jamming message m_J (presented by signal x_J) to the two sources and the preselected relay R_s in the presence of L eavesdroppers. The ASRs from J_s to the two sources $S1$ and $S1$ are respectively given as

$$C_{J_sS1}^{\text{STWJNC}} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_1\psi g_{J_sS1}}{1+\omega_1\psi g_{J_sE\max}}\right)\right]^+ \tag{45}$$

$$C_{J_sS2}^{\text{STWJNC}} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_1\psi g_{J_sS2}}{1+\omega_1\psi g_{J_sE\max}}\right)\right]^+ \tag{46}$$

In this protocol, R_s uses the received RF signal transmitted from J_s for only harvesting the energy. Thus, the harvested power at R_s is given by

$$P_{J_sR_s} = \eta P g_{J_sR_s} \tag{47}$$

We consider whether $S1$ and $S2$ can successfully and safely decode the jamming message in the first time slot, that is, $S1$ and $S2$ can successfully decode the jamming message, but the eavesdroppers cannot.

5.1.1 *Consider the Case When the Two Source Nodes Can Successfully and Safely Decode the Jamming Message During the First Time Slot; i.e.,* $C_{J_sS1}^{\text{STWJNC}} \geq C_t$ *and* $C_{J_sS2}^{\text{STWJNC}} \geq C_t$

We propose the optimal jammer-relay pair (J_s, R_s) (called OPT) selection strategy (48a), described as follows: among the K jammers $(1 \leq K \leq N)$ that can successfully and safely transmit the jamming message, an optimal jammer-relay pair is selected for which J_s has the highest channel gain with R_s. For comparison, we analyze one more jammerrelay pair using a random (RAN) selection strategy, as formulated in (48b) below.

$$J_s, R_s = \arg \max_{\substack{k=1,2,\ldots,K \\ m=1,2,\ldots,M}} (g_{J_kR_m}) \tag{48a}$$

$$\begin{cases} R_s = \text{random}\,(R_1, R_2, \ldots, R_M) \\ J_s = \text{random}\,(J_1, J_2, \ldots, J_K) \end{cases} \tag{48b}$$

During the second TS, the source node $S1$ generates the coded message $m_{S1\oplus J_s}$ (by $m_{S1\oplus J_s} \triangleq m_{S1} \oplus m_{J_s}$), and sends it to R_s. Note that the eavesdroppers cannot obtain the source message m_{S1} in this case. The ASR of the link $S1 - R_s$ is expressed as

$$C_{S1R_s}^{\text{STWJNC},1} = \left[\frac{1}{4}\log_2(1+\omega_1\psi g_{S1R_s})\right]^+ \tag{49}$$

where the index 1 in $C_{S1R_s}^{\text{STWJNC},1}$ indicates that we are analyzing the STWJNC protocol of this case, e.g., $C_{J_sS1}^{\text{STWJNC}} \geq C_t$ and $C_{J_sS2}^{\text{STWJNC}} \geq C_t$.

Similarly, $S2$ transmits the coded message $m_{S2\oplus J_s}$ (presented by the signal $x_{S2\oplus J_s}$) to R_s during the third TS, and the ASR is obtained as follows

$$C_{S2R_s}^{\mathrm{STWJNC},1} = \left[\frac{1}{4}\log_2(1+\omega_1\psi g_{S2R_s})\right]^+ \tag{50}$$

After successfully decoding the received messages $m_{S1\oplus J_s}$ and $m_{S2\oplus J_s}$ during the second and third TSs, the relay R_s uses digital network coding to create a new message $m_{S1\oplus S2}$ by XORing $m_{S1\oplus J_s}$ and $m_{S2\oplus J_s}$; i.e., $m_{S1\oplus J_s} \oplus m_{S2\oplus J_s} = m_{S1} \oplus m_{J_s} \oplus m_{S2} \oplus m_{J_s} = m_{S1} \oplus m_{S2} \triangleq m_{S1\oplus S2}$. It then broadcasts the new message to the two source nodes during the fourth TS. If the two sources successfully decode the message $m_{S1\oplus S2}$, they can safely extract the desired message by XORing it with their own messages. The ASRs of the two links $R_s - S1$ and $R_s - S2$ during the fourth TS are given respectively by

$$C_{R_sS1}^{\mathrm{STWJNC},1} = \left[\frac{1}{4}\log_2(1+\omega_4\psi g_{J_sR_s}g_{R_sS1})\right]^+ \tag{51}$$

$$C_{R_sS2}^{\mathrm{STWJNC},1} = \left[\frac{1}{4}\log_2(1+\omega_4\psi g_{J_sR_s}g_{R_sS2})\right]^+ \tag{52}$$

where $\omega_4 \triangleq \frac{\eta}{1+\mu}$.

5.1.2 Consider the Case When the Two Source Nodes do not Successfully and Safely Decode the Jamming Message During the First Time Slot; i.e., One of Source Nodes S1 and S2 does not Successfully Decode the Jamming Message or Atleast One Eavesdropper Gets the Jamming Message: $C_{J_sS1}^{\mathrm{STWJNC}} < 0$ *and/or* $C_{J_sS2}^{\mathrm{STWJNC}} < 0$

In this case, there is no jammer that can successfully and safely transmit the jamming message to the two sources ($K = 0$). In other words, the jammers are unhelpful for coding the two sources messages; thus, the jammer J_s is selected from the N jammer nodes to transmit the energy to R_s. The two jammer-relay pair selection strategies (48a) and (48b) can be rewritten as follows:

$$J_s, R_s = \arg \max_{\substack{n=1,2,\ldots,N \\ m=1,2,\ldots,M}} (g_{J_nR_m}) \tag{53a}$$

$$\begin{cases} R_s = \mathrm{random}(R_1, R_2, \ldots, R_M) \\ J_s = \mathrm{random}(J_1, J_2, \ldots, J_N) \end{cases} \tag{53b}$$

The eavesdroppers can impact the transmission of the two links $S1 \leftrightarrow R_s$ and $S2 \leftrightarrow R_s$; therefore, the ASRs from $S1$ to R_s during the second TS, from $S2$ to R_s during the third TS, and from R_s to $S1$ and $S2$ during the fourth TS can be given respectively by

$$C_{S1R_s}^{\mathrm{STWJNC},2} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_1\psi g_{S1R_s}}{1+\omega_1\psi g_{S1E\max}}\right)\right]^+ \tag{54}$$

$$C_{S2R_s}^{\mathrm{STWJNC},2} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_1\psi g_{S2R_s}}{1+\omega_1\psi g_{S2E\max}}\right)\right]^+ \tag{55}$$

$$C_{R_sS1}^{\mathrm{STWJNC},2} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_4\psi g_{J_sR_s}g_{R_sS1}}{1+\omega_4\psi g_{J_sR_s}g_{R_sE\max}}\right)\right]^+ \tag{56}$$

$$C_{R_sS2}^{\mathrm{STWJNC},2} = \left[\frac{1}{4}\log_2\left(\frac{1+\omega_4\psi g_{J_sR_s}g_{R_sS2}}{1+\omega_4\psi g_{J_sR_s}g_{R_sE\max}}\right)\right]^+. \tag{57}$$

5.2 Performance Analysis

5.2.1 Secrecy Outage Probability of the STWJNC Protocol

Addressing the optimal jammerrelay-pair-selection strategy first, the SOP of the STWJNC protocol, $P_{out,\mathrm{OPT}}^{\mathrm{STWJNC}}$, can be expressed as

$$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC}} = \Pr[K,N]P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1} + \Pr[0,N]P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},2} \tag{58}$$

where $\Pr[K,N]$ denotes the probability that there are K jammers and $\Pr[0,N]$ denotes the probability that there is no jammer that can successfully and safely transmit the jamming message to the two sources. These probabilities can be expressed as (59) and (60) as follows. We note that (59.2) is obtained from (59.1) by applying the result in Appendix 4

$$\begin{aligned}
&\Pr(K,N)\\
&\quad\triangleq \sum_{K=1}^{N} C_N^K \Pr\begin{bmatrix}\min(C_{J_1S1},C_{J_1S2})\geq C_t, \min(C_{J_2S1},C_{J_2S2})\geq C_t,\ldots,\\ \min(C_{J_KS1},C_{J_KS2})\geq C_t, \min\left(C_{J_{K+1}S1},C_{J_{K+1}S2}\right)<C_t,\\ \min\left(C_{J_{K+2}S1},C_{J_{K+2}S2}\right)<C_t,\ldots,\min(C_{J_NS1},C_{J_NS2})<C_t\end{bmatrix}\\
&\quad\overset{(59.1)}{=} \sum_{K=1}^{N} C_N^K\left\{\Pr[\min(C_{J_1S1},C_{J_1S2})\geq C_t]\right\}^K\left\{\Pr\left[\min\left(C_{J_{K+1}S1},C_{J_{K+1}S2}\right)<C_t\right]\right\}^{N-K} \qquad (59)\\
&\quad\overset{(59.2)}{=} \sum_{K=1}^{N} C_N^K\left\{e^{\frac{-(\varphi-1)\left(\lambda_{JS1}+\lambda_{JS2}\right)}{\omega_1\psi}}\Omega_2(L,\varphi,\lambda_{JS1},\lambda_{JS2},\lambda_{JE})\right\}^K\\
&\qquad\left\{1-e^{\frac{-(\varphi-1)\left(\lambda_{JS1}+\lambda_{JS2}\right)}{\omega_1\psi}}\Omega_2(L,\varphi,\lambda_{JS1},\lambda_{JS2},\lambda_{JE})\right\}^{N-K}
\end{aligned}$$

$$\begin{aligned}
\Pr(0,N) &\triangleq \Pr\begin{bmatrix}\min(C_{J_1S1},C_{J_1S2})<C_t, \min(C_{J_2S1},C_{J_2S2})<C_t,\\ \ldots,\min(C_{J_NS1},C_{J_NS2})<C_t\end{bmatrix}\\
&= \left\{\Pr\left[\min\left(C_{J_{K+1}S1},C_{J_1S2}\right)<C_t\right]\right\}^N \qquad (60)\\
&= \left\{1-e^{\frac{-(\varphi-1)\left(\lambda_{JS1}+\lambda_{JS2}\right)}{\omega_1\psi}}\Omega_2(L,\varphi,\lambda_{JS1},\lambda_{JS2},\lambda_{JE})\right\}^N
\end{aligned}$$

$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1}$ and $P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},2}$ are expressed by (61) and (62), respectively, below:

$$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1} = 1-\Pr\begin{bmatrix}C_{S1R_s}^{\mathrm{STWJNC},1}\geq C_t, C_{S2R_s}^{\mathrm{STWJNC},1}\geq C_t,\\ C_{R_sS1}^{\mathrm{STWJNC},1}\geq C_t, C_{R_sS2}^{\mathrm{STWJNC},1}\geq C_t\end{bmatrix} \tag{61}$$

$$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},2} = 1 - \Pr\left[\begin{array}{l} C_{S1R_s}^{\mathrm{STWJNC},2} \geq C_t, C_{S2R_s}^{\mathrm{STWJNC},2} \geq C_t, \\ C_{R_sS1}^{\mathrm{STWJNC},2} \geq C_t, C_{R_sS2}^{\mathrm{STWJNC},2} \geq C_t \end{array}\right] \tag{62}$$

Lemma 3 *The following expression is valid for* $P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1}$

$$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1} = 1 - e^{\frac{-(\varphi-1)(\lambda_{S1R}+\lambda_{S2R})}{\omega_1\psi}} \Omega_6(K, M, \varphi, \omega_4, \psi, \lambda_{JR}, \lambda_{RS1}, \lambda_{RS2}) \tag{63}$$

where

$$\Omega_6(K, M, \varphi, \omega_4, \psi, \lambda_{JR}, \lambda_{RS1}, \lambda_{RS2}) \triangleq KM\lambda_{JR} \sum_{k=0}^{KM-1} C_{KM-1}^{k}(-1)^k \sqrt{\frac{4(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})}{(1+k)\omega_4\psi\lambda_{JR}}} K_1\left(\sqrt{\frac{4(1+k)(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})\lambda_{JR}}{\omega_4\psi}}\right)$$

Proof See Appendix 5. □

Lemma 4 *The following expression is valid for* $P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},2}$

$$P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},2} = 1 - e^{\frac{-(\varphi-1)(\lambda_{S1R}+\lambda_{S2R})}{\omega_1\psi}} \Omega_2(L, \varphi, \lambda_{S1R}, 0, \lambda_{S1E}) \Omega_2(L, \varphi, \lambda_{S2R}, 0, \lambda_{S2E}) \Omega_2(L, \varphi, \lambda_{RS1}, \lambda_{RS2}, \lambda_{RE}) \Omega_6(N, M, \varphi, \omega_4, \psi, \lambda_{JR}, \lambda_{RS1}, \lambda_{RS2}) \tag{64}$$

Proof See Appendix 6. □

Combining (58), (59), (60), (63), and (64), we obtain the SOP for the STWJNC protocol with the optimal jammerrelay-pair-selection strategy. And when the random jammerrelay-pair-selection strategy is applied, the SOP of the STWJNC protocol can be derived by $P_{out,\mathrm{RAN}}^{\mathrm{STWJNC}} = P_{out,\mathrm{OPT}}^{\mathrm{STWJNC}}\Big|_{N=K=M=1}$.

5.2.2 Secrecy Throughput Performance of the STWNC Protocol

In the STWJNC protocol, the rate of the effective transmission time of the two sources $S1$ and $S2$ with respect to the total time is $2T$ / $4T$. Thus, the throughput of this protocol with each of the two relay-selection strategies can be expressed as follows:

$$\tau_{\mathrm{OPT/RAN}}^{\mathrm{STWJNC}} = \left(1 - P_{\mathrm{OPT/RAN}}^{\mathrm{STWJNC}}\right)\frac{C_t}{2}. \tag{65}$$

6 Numerical Results and Discussion

This section discusses the theoretical derivations and the Monte-Carlo simulations conducted to validate the analysis for the STW, STWNC, and STWJNC protocols described in the previous three sections. The simulations were conducted to verify the theoretical derivations as well as to determine the performance of the three proposed protocols. In a

two-dimensional plan, the coordinates are $(0,0)$, $(1,1)$, $(x_R,0)$, (x_E,y_E), and (x_J,y_J), respectively, for the two source nodes $S1$ and $S2$, the relay-nodes-cluster-based R_m with $m \in \{1,2,\ldots,M\}$, the eavesdropper-nodes-cluster-based E_l with $l \in \{1,2,\ldots,L\}$, and (appearing only in the STWJNC protocol) the jammer-nodes-cluster-based J_n with $n \in \{1,2,\ldots,N\}$. Thus, the distances of the links $S1-R_m$, $S2-R_m$, $S1-E_l$, $S2-E_l$, R_m-E_l, J_n-S1, J_n-S2, J_n-R_m, and J_n-E_l are $d_{S1R}=|x_R|$, $d_{S2R}=|1-x_R|$, $d_{S1E}=\sqrt{(x_E)^2+(y_E)^2}$, $d_{S2E}=\sqrt{(1-x_E)^2+(1-y_E)^2}$, $d_{RE}=\sqrt{(x_R-x_E)^2+(y_E)^2}$, $d_{JS1}=\sqrt{(x_J)^2+(y_J)^2}$, $d_{JS2}=\sqrt{(1-x_J)^2+(1-y_J)^2}$, $d_{JR}=\sqrt{(x_R-x_J)^2+(y_J)^2}$, and $d_{JE}=\sqrt{(x_J-x_E)^2+(y_J-y_E)^2}$, respectively. In all the simulation scenarios, the following parameters were used: $\mu=1$, $\beta=3$, and $C_t=0.5$. For simple presentation, the acronym $\mathrm{U}-\mathrm{V}$ indicates that we are considering the protocol U ($\mathrm{U} \in \{\mathrm{STW},\mathrm{STWNC},\mathrm{STWJNC}\}$) with the relay- or jammerrelay-pair-selection strategy V ($\mathrm{V} \in \{\mathrm{MIRE},\mathrm{MAS1R},\mathrm{RAN},\mathrm{OPT}\}$). In addition, we set $\rho=0.5$ and $\eta=0.8$ for the cases shown in Figs. 2, 3, 4 and 5.

Figure 2 shows an evaluation and comparison of the performance of the three protocols with their different relay selection strategies. The performance is based on the secrecy outage probability as a function of ψ, M, L, or N, as shown in Fig. 2a–d. The positions of the cluster-based relays, eavesdroppers, and jammers are set at $(0.5,0)$, $(0.5,-1)$, and $(0.5,0.5)$, respectively. The SOPs of STW-MIRE, STW-MAS1R, STW-RAN, STWNC-MAS1R, and STWNC-RAN are approximately derived when is high, in Eqs. (26a), (26b), (26c), (43) and (44), respectively. Thus, the theoretical results curves are not exactly the same as the simulation curves (however, their differences are very small) when ψ is low, e.g., $\psi<10$ dB, as shown in Fig. 2a. In contrast, STWJNC-OPT and STWJNC-RAN are

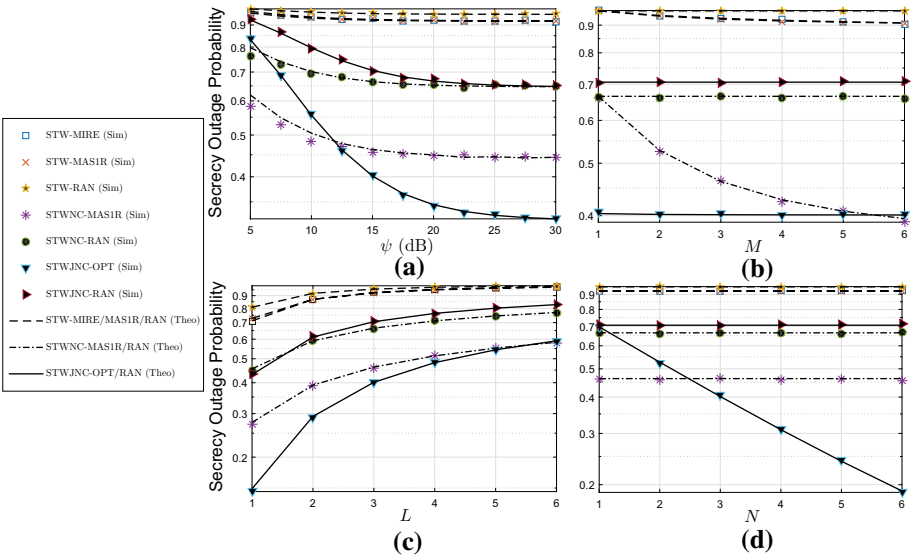

Fig. 2 Secrecy outage probability as a function of **a** *psi* when $M=L=N=3$, **b** M when $L=N=3$ and $\psi=15$ dB, **c** L when $M=N=3$ and $\psi=15$ dB, and **d** N when $M=L=3$ and $\psi=15$ dB

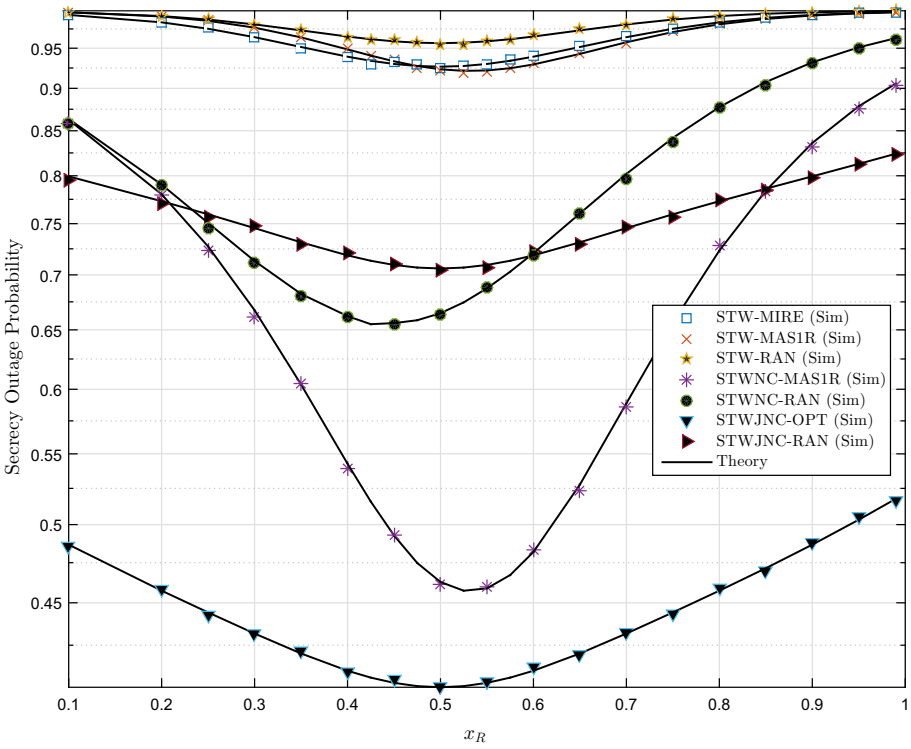

Fig. 3 Secrecy outage probability as a function of x_R when $(x_E = 0.5, y_E = -1)$, $(x_J = 0.5, y_J = 0.5)$, $M = L = N = 3$, and $\psi = 15$

exactly derived, so the theoretical results match very well with the simulation results for all values of ψ , as shown in Fig. 2a. When ψ is fixed at a high value, e.g., $\psi = 15$ dB, the simulation and theoretical results are in excellent agreement for STW-MIRE, STW-MAS1R, STW-RAN, STWNC-MAS1R and STWNC-RAN, as shown in Fig. 2b–d.

We can observe in Fig. 2a that all the protocols improve the secrecy outage performance for high values of ψ. The SOPs of the STW protocol with its three relay-selection strategies (STW-MIRE, STW-MAS1R, and STW-RAN) are not decreased much because, when ψ increases, the eavesdropping channel gain also increases. Motivated to reduce the impact of eavesdroppers on the transmissions from the two source nodes by using a selected relay, we additionally use network coding with the STWNC protocol, and a combination of network coding and cooperative jamming with the STWJNC protocol. The results show that STWNC-MAS1R, STWNC-RAN, STWJNC-OPT, and STWJNC-RAN achieve higher performance than the STW protocol.

Next, we compare the performance between the STWNC and STWJNC protocols. Using the random selection scheme, STWJNC-RAN attains lower performance than STWCN-RAN because, when the jammer is chosen randomly, it is difficult for the STWJNC-RAN protocol to transmit the jamming message successfully and safely to the two source nodes during the first TS. Second, comparing the MAS1R strategy with the STWCN protocol and the OPT strategy with the STWJNC protocol, for low ψ (below about 12 dB), STWNC again outperforms STWJNC. This occurs because the two sources

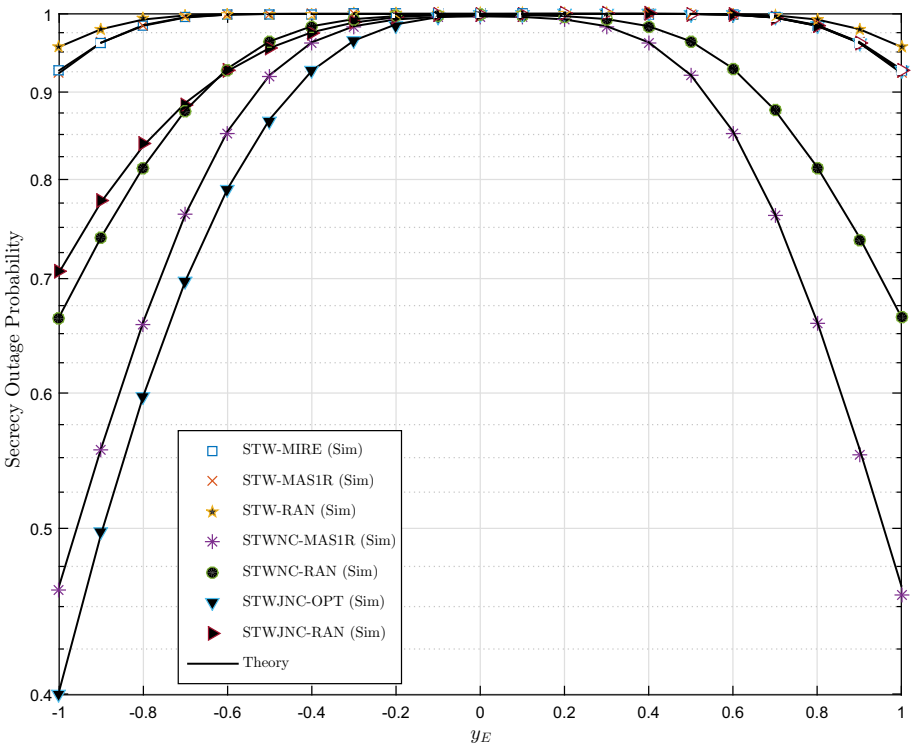

Fig. 4 Secrecy outage probability as a function of y_E when $x_E = 0.5$, $x_R = 0.5$, $(x_J = 0.5, y_J = 0.5)$, $M = L = N = 3$, and $\psi = 15$

nodes may be unable to decode the jamming message transmitted from the selected jammer J_s and because the relay may not harvest enough energy from the selected jammer to forward the information during the fourth TS. However, STWJNC-OPT achieves much higher performance than STWNC-MAS1R when ψ is high. The reason is that, with STWJNC-OPT, the selected relay R_s uses the energy harvested from J_s for transmission, whereas with STWNC-MAS1R, R_s has to harvest the energy from the received RF signal transmitted from $S1$, which causes the decoding performance for the link $S1 - R_s$ to be less with STWNC-MAS1R than with STWJNC-OPT.

STW-RAN, STWNC-RAN, and STWJNC-RAN maintain their SOPs as the number of relay nodes (M) increases, as shown in Fig. 2b, because a random relay is selected with each protocol. STW-MAS1R and STWNC-MAS1R have improved performance when the number of relays increases. This is because more energy can be harvested from $S1$, which improves the decoding process for the two links $S1 - R_s$ and $R_s - S2$. In contrast, the performance of STWJNC-OPT is improved lightly when M increases. The performance of all protocols is reduced when the number of eavesdroppers (L) increases, as shown in Fig. 2c. This is because, when L increases, the impact of eavesdroppers on the system is greater. When the number of jammer nodes (N) increases, only the STWJNC-OPT protocol improves the performance because a change of N value only affects this protocol (Fig. 2d). Moreover, STWJNC-OPT still has lower performance than STWNC-MAS1R when $N =$

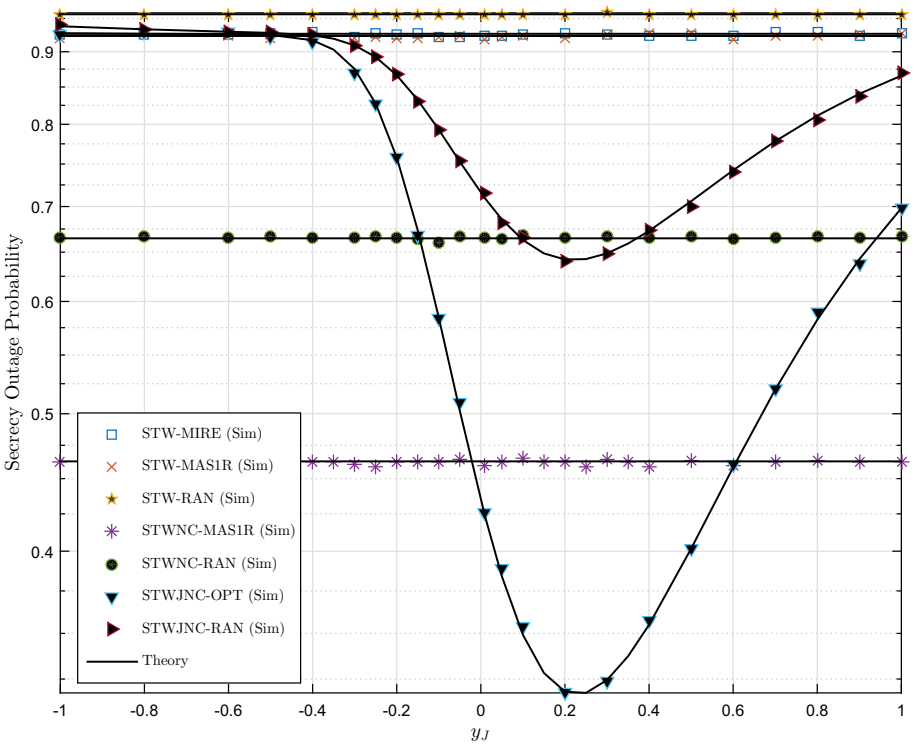

Fig. 5 Secrecy outage probability as a function of y_J when $x_J = 0.5$, $x_R = 0.5$, $(x_E = 0.5, y_E = -1)$, $M = L = N = 3$, and $\psi = 15$

1, 2 because, with small values of N, STWJNC-OPT is unable to select a J_s that can transmit successfully and safely to the two sources during the first TS. Finally, as shown in Fig. 2a–d, the performances of the STW-MIRE and STW- MAS1R protocols are very similar. With its lack of network coding, the STW protocol has the lowest performance with all relay-selection strategies and parameters. STWNC-RAN outperforms STWJNC-RAN in all Fig. 2a–d because, in this scenario, (1) network coding helps to improve performance by reducing the impact of eavesdroppers, and (2) STWNC-RAN uses three TSs, which is more effective than the four TSs of STWJNC-RAN. However, when the values of ψ and N are large enough, e.g., $\psi \geq 15$ dB and $N \geq 3$, with the optimal jammer-relay selection strategy (J_s is preselected), the impact of eavesdroppers can be greatly reduced, and thus, STWJNC-OPT outperforms STWNC-MAS1R.

Figure 3 shows the impact of the position of the relay cluster on the secrecy performance of the protocols, as x_R is shifted from 0.1 to 0.99. This figure shows that each protocol achieves its best performance when the relay is located around the midpoint between the two source nodes, i.e., $x_R \in (0.45, 0.55)$ because a relay at this position can balance the efficiency of the decoding processes between the two links $S1 \leftrightarrow R$ and $S12 \leftrightarrow R$. The performance of STWJNC-RAN is higher than that of STWNC-RAN when the relays are located near $S1$, e.g., $x_R \in (0.1, 0.22)$, or near $S2$, e.g., $x_R \in (0.6, 1)$. This is because, for relays near $S1$, the distance between $S2$ and R is long, making it difficult in the STWNC-RAN protocol for the relay to harvest the energy and still achieve a high decoding performance for the received

signal transmitted by $S2$. In contrast, the relay in STWJNC-RAN harvests the energy from the jammer, so the decoding efficiency of the link $S2 \rightarrow R$ is improved.

The impact of the position of the eavesdroppers with respect to the relays and jammers is presented in Fig. 4. When the eavesdroppers are very far from the relays and jammers ($y_E = -1$), all protocols achieve their best performance because the eavesdroppers have the lowest impact. When the eavesdroppers are near the relays and far from the jammers ($y_E \in (-0.6, 0)$), STWJNC-RAN achieves higher performance than STWNC-RAN. This is because, when $y_E \in (-0.6, 0)$, the eavesdroppers have a strong impact on the data transmitted by the two sources and relays, which reduces the performance of STWNC-RAN. In contrast, with STWJNC-RAN, this impact is reduced by coding the jamming message transmitted by the jammer. STWNC-RAN outperforms STWJNC-RAN in the other regions of y_E, i.e., $y_E \in (-1, -0.6)$ and $y_E \in (0, 1)$. This is because, (1) when $y_E \in (-1, -0.6)$, the eavesdroppers have little impact, and STWNC-RAN is more effective because it uses fewer time slots than STWJNC-RAN, and (2) when $y_E \in (0, 1)$, the jammers unable to transmit successfully and safely the jamming message to two source nodes during the first TS of STWJNC-RAN because the eavesdroppers are very near the jammers. Moreover, STWJNC-OPT also has very bad performance (similar to the performances of the STWJNC-RAN and STW protocols) when the eavesdroppers are near the jammers, i.e., $y_E \in (0, 1)$.

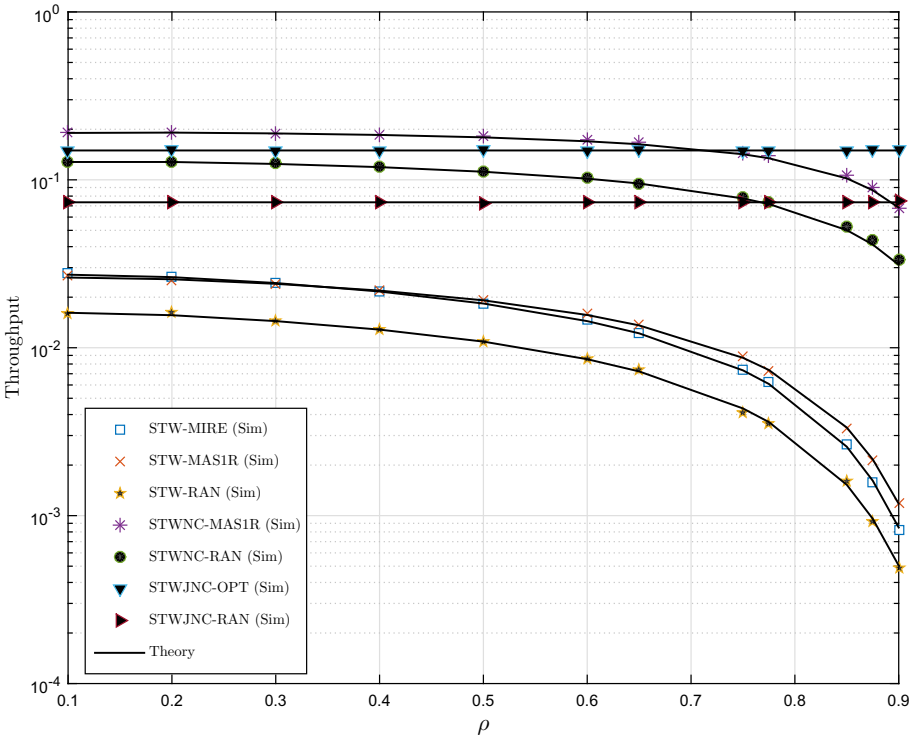

Fig. 6 Secrecy throughput performance as a function of ρ when $x_R = 0.5$, $x_J = y_J = 0.5$, $(x_E = 0.5, y_E = -1)$, $M = L = N = 3$, $\psi = 15$, and $\eta = 0.8$

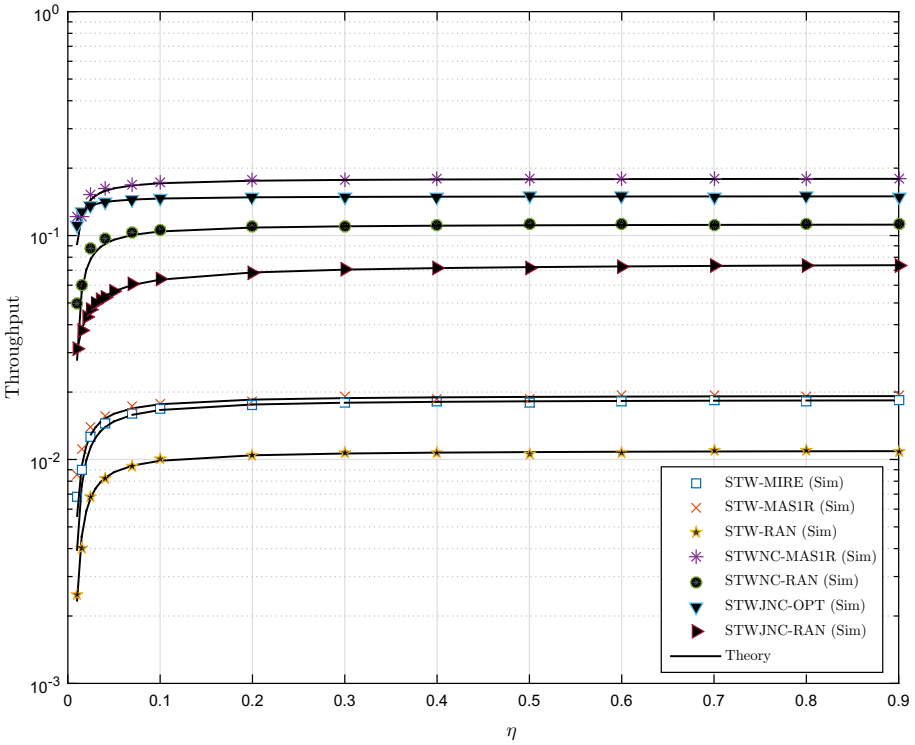

Fig. 7 Secrecy throughput performance as a function of η when $x_R = 0.5$, $x_J = y_J = 0.5$, $(x_E = 0.5, y_E = -1)$, $M = L = N = 3$, $\psi = 15$, and $\rho = 0.5$

In Fig. 5, we present the SOP as a function of y_J. As expected, only STWJNC-RANs and STWJNC-OPTs performances change, achieving their highest levels when $y_J \approx 0.2$. This can be explained by the fact that the position $J(x_J = 0.5, y_J \simeq 0.2)$ is the optimal point such that (1) the two source nodes can receive the jamming message successfully and safely, and (2) the relay R_s receives high energy from the RF signal transmitted by J_s.

In Fig. 6, we investigate the effect of ρ on the STP of the protocols. We can observe in Fig. 6 that the throughput performances of the STW and STWNC protocols are reduced when ρ increases because, at high ρ values, the quality of the decoding process at the relay is degraded. In contrast, when ρ is low, the decoding processes for the links $S1 \rightarrow R_s$ and $S2 \rightarrow R_s$ are guaranteed because R_s does not harvest much energy from the RF signals transmitted from $S1$ and $S2$. In addition, the STW protocol with any of its relay selection schemes (MIRE, MAS1R, and RAN) has the lowest throughput performance. Finally, the STWNC protocol obtains higher secrecy throughput performance than the STWJNC protocol when ρ is not too large $(\rho \leq 0.7)$.

Figure 7 illustrates the secrecy throughput performance (STP) as a function of the energy harvesting efficiency η. For very small values of η $(0 < \eta < 0.2)$, the STP of each protocol is low due to insufficient energy for the relay R_s to transmit the data. When η increases, R_s can harvest more energy, which improves the forwarding performance of R_s;

Table 1 Result summary

Figures	Result
2a	The performances of all protocols is improved when ψ increases
	STWNC and STWJNC achieve higher performance than STW
	STWJNC-RAN attains lower performance than STWNC-RAN for all values of ψ
	STWNC-MAS1R outperforms STWJNC-OPT for low ψ ($\psi < 12dB$) SI is high
	STWJNC-OPT achieves much higher performance than STWNC when ψ is high
2b	STW-MAS1R and STWNC-MAS1R have improved performance when M increaes
2c	The performance of all protocols is reduced when L increases
2d	Only STWJNC-OPT improves the performance when N increases
	STWJNC-OPT has lower performance than STWNC-MAS1R when $N = 1, 2$
2a–2d	The performances of STW-MIRE and STW-MAS1 are very similarly
3	Each protocol achieves its best performance when relays are located around the midpoint of two source nodes
	The performance of STWJNC-RAN is higher than that of STWNC-RAN relays are located near $S1$ or near $S2$.
4	All protocols achieve their best performance when eavesdroppers are very far from the relays and jammers
	STWJNC-RAN achieves higher performance than STWNC-RAN when the eavesdroppers are near the relays and far from the jammers
	STWJNC-OPT has very bad performance (similar to the performances of the STWJNC-RAN and STW protocols) when the eavesdroppers are the jammers
5	Only STWJNC-RAN and STWJNC-OPT change the performance, and achieve their highest levels when $y_J = 0.2$
6	Throughput performances of STW and STWNC protocols are reduced when ρ increases
	STW protocol with any of its relay selection schemes (MIRE, MAS1R, and RAN) has the lowest throughput performance
	STWNC protocols obtains higher throughput performance than the STWJNC protocol when ρ is not too large ($\rho \leq 0.7$)
7	Each protocol has low thrgoughput performance when η is small
	STWNC-MAS1R obtains the best throughput performance among the seven considered schemes

however, the eavesdroppers can also more easily overhear the data. Thus, the STP keeps increasing very slightly as η increases, $0.1 < \eta < 0.9$. STWNC-MAS1R obtains the best STP among the seven considered schemes (Table 1).

7 Conclusions

In this paper, we first considered the conventional secured two-way energy-constrained relaying network along with three different relay selection strategies. Second, to improve performance, we applied a digital network coding technique at a preselected relay R_s to

reduce the number of time slots used as well as the impact of eavesdroppers on the forwarding process of R_s during the third time slot. Third, we proposed another protocol that employs jammer nodes and combines cooperative jamming and network coding along with two different jammerrelay-pair-selection strategies. We derived closed-form expressions for secrecy outage probability and throughput performance for each scheme. We used Monte Carlo simulations to verify our analysis. The simulation and theoretical results showed the following. (1) The performances of all protocols improve with increasing ψ, η or decreasing L, ρ. (2) The outage performance of STWJNC-OPT is higher than that of STWNC-MAS1R when ψ and N are high enough; however, STWNC-MAS1R achieves better throughput performance than STWJNC-OPT. (3) The outage performance of STWJNC-RAN is only higher than that of STWNC-RAN when the relays are located near one of the two source nodes or eavesdroppers, but STWNC-RAN has higher throughput performance at all values, compared to STWJNC-RAN. (4) In all the scenarios, the outage and throughput performances of the STW protocol are the lowest. (5) The performances of STW-MIRE and STW-MAS1R are nearly the same. (6) The theoretical results match the simulation results well.

Appendix 1: The PDF of RVs $g_{R_sE\max}$, $g_{S2E\max}$, and $g_{S1E\max}$ When Using the Relay Selection Strategy in (19a)

The CDFs of RVs $g_{R_sE\max}$, $g_{S2E\max}$, and $g_{S1E\max}$ can be given respectively as

$$\begin{aligned} F_{g_{R_sE\max}}(x) &= \Pr\left[\min_{m=1,2,\ldots,M}\left(\max_{l=1,2,\ldots,L} g_{R_mE_l}\right)<x\right] \\ &= 1-\prod_{m=1}^{M}\left\{1-\prod_{l=1}^{L}\Pr[g_{R_mE_l}<x]\right\} = 1-\left[1-\left(1-e^{-\lambda_{RE}x}\right)^{L}\right]^{M} \end{aligned} \tag{66}$$

$$F_{g_{S2E\max}}(x) = \Pr\left[\max_{m=1,2,\ldots,L} g_{S2Em}<x\right] = \left(1-e^{-\lambda_{S2E}x}\right)^{L} \tag{67}$$

$$F_{g_{S1E\max}}(x) = \Pr[g_{S1E\max}<x] = \left(1-e^{-\lambda_{S1E}x}\right)^{L} \tag{68}$$

Then, by differentiating (66), (67), and (68), we obtain the PDFs of RVs $g_{R_sE\max}$, $g_{S2E\max}$, and $g_{S1E\max}$, respectively, as follows:

$$\begin{aligned} f_{g_{R_sE\max}}(x) &= ML\lambda_{RE}e^{-\lambda_{RE}x}\left(1-e^{-\lambda_{RE}x}\right)^{L-1}\left[1-\left(1-e^{-\lambda_{RE}x}\right)^{L}\right]^{M-1} \\ &= ML\lambda_{RE}\sum_{k=0}^{L-1}C_{L-1}^{k}(-1)^{k}\sum_{u=0}^{M-1}C_{M-1}^{u}(-1)^{u}\sum_{v=0}^{Lu}C_{Lu}^{v}(-1)^{v}e^{-(1+k+v)\lambda_{RE}x} \end{aligned} \tag{69}$$

$$\begin{aligned} f_{g_{S2E\max}}(x) &= L\lambda_{S2E}e^{-\lambda_{S2E}x}\left(1-e^{-\lambda_{S2E}x}\right)^{L-1} \\ &= L\lambda_{S2E}\sum_{w=0}^{L-1}C_{L-1}^{w}(-1)^{w}e^{-(1+k)\lambda_{S2E}x} \end{aligned} \tag{70}$$

$$
\begin{aligned}
f_{g_{S1E\max}}(x) &= L\lambda_{S1E}e^{-\lambda_{S1E}x}\left(1-e^{-\lambda_{S1E}x}\right)^{L-1} \\
&= L\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^{t}(-1)^{t}e^{-(1+t)\lambda_{S1E}x}.
\end{aligned} \tag{71}
$$

Appendix 2: Proof of Lemma 1

At first, the integral $I_{1,\mathrm{MAS1R}}$ can be expressed as

$$
\begin{aligned}
I_{1,\mathrm{MAS1R}} &\overset{(72.1)}{=} e^{\frac{-(\varphi-1)\lambda_{S2R}}{\omega_2\psi}}\int_0^{\infty}L\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^{t}(-1)^{t}e^{-(1+t)\lambda_{S1E}x_1} \\
&\int_0^{\infty}L\lambda_{S2E}\sum_{w=0}^{L-1}C_{L-1}^{w}(-1)^{w}e^{-\left[\frac{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}}{\omega_2}\right]x_2} \\
&\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1x_1}{\omega_2}}^{\infty}M\lambda_{S1R}\sum_{k=0}^{M-1}C_{M-1}^{k}(-1)^{k}e^{-(1+k)\lambda_{S1R}x_3}e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}dx_3dx_2dx_1 \\
&\overset{(72.2)}{\approx} e^{\frac{-(\varphi-1)\lambda_{S2R}}{\omega_2\psi}}(I_3+I_4)
\end{aligned} \tag{72}
$$

where (72.2) is obtained by approximating $e^{\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}}\approx 1+\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3}$.

The term I_3 and I_4 in (72) are denoted and derived as in (73) and (74) as follows

$$
\begin{aligned}
I_3 &\triangleq \int_0^{\infty}L\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^{t}(-1)^{t}e^{-(1+t)\lambda_{S1E}x_1} \\
&\int_0^{\infty}L\lambda_{S2E}\sum_{w=0}^{L-1}C_{L-1}^{w}(-1)^{w}e^{-\left[\frac{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}}{\omega_2}\right]x_2} \\
&\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1x_1}{\omega_2}}^{\infty}M\lambda_{S1R}\sum_{k=0}^{M-1}C_{M-1}^{k}(-1)^{k}e^{-(1+k)\lambda_{S1R}x_3}dx_3dx_2dx_1 \\
&= L\lambda_{S2E}\sum_{w=0}^{L-1}\frac{C_{L-1}^{w}(-1)^{w}\omega_2}{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}} \\
&\quad LM\lambda_{S1E}\sum_{t=0}^{L-1}C_{L-1}^{t}(-1)^{t}\sum_{k=0}^{M-1}\frac{C_{M-1}^{k}(-1)^{k}\omega_2e^{\frac{-(1+k)(\varphi-1)\lambda_{S1R}}{\omega_2\psi}}}{(1+k)[(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R}]} \\
&\triangleq \Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E})\Omega_4(L,M,\varphi,\omega_1,\omega_2,\psi,\lambda_{S1R},\lambda_{S1E})
\end{aligned} \tag{73}
$$

$$
\begin{aligned}
I_4 &\triangleq \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\int_0^{\infty} L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\
&\quad \int_0^{\infty} L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^{w}(-1)^w e^{-\left[\frac{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}}{\omega_2}\right]x_2} \\
&\quad \int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^{\infty} M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^{k}(-1)^k \frac{e^{-(1+k)\lambda_{S1R}x_3}}{x_3} dx_3 dx_2 dx_1 \\
&\overset{(74.1)}{=} \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \\
&\quad \int_0^{\infty} L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\
&\quad M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^{k}(-1)^k \Gamma\left[0,(1+k)\lambda_{S1R}\left(\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}\right)\right] dx_1 \\
&\overset{(74.2)}{\approx} \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \\
&\quad \int_0^{\infty} LM\lambda_{S1E}\lambda_{S1R}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t \sum_{k=0}^{M-1} C_{M-1}^{k}(-1)^k e^{-(1+t)\lambda_{S1E}x_1} \\
&\quad \Gamma\left[0,\frac{(1+k)\varphi\omega_1\lambda_{S1R}x_1}{\omega_2}\right] dx_1 \\
&\overset{(74.3)}{=} \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \\
&\quad LM\lambda_{S1E}\lambda_{S1R}\sum_{t=0}^{L-1} C_{L-1}^{t}(-1)^t \sum_{k=0}^{M-1} C_{M-1}^{k}(-1)^k \\
&\quad \frac{\omega_2}{(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R_2}} F_1\left(1,1;2;\frac{(1+t)\omega_2\lambda_{S1E}}{(1+t)\omega_2\lambda_{S1E}+(1+k)\varphi\omega_1\lambda_{S1R}}\right) \\
&\triangleq \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E}) \\
&\quad \Omega_5(L,M,\varphi,\omega_1,\omega_2,\lambda_{S1R},\lambda_{S1E})
\end{aligned}
\tag{74}
$$

where (74.1) is obtained from by using $\int_0^{\infty} L\lambda_{S2E}\sum_{w=0}^{L-1} C_{L-1}^{w}(-1)^w e^{-\left[\frac{(1+w)\omega_2\lambda_{S2E}+\varphi\omega_1\lambda_{S2R}}{\omega_2}\right]x_2} = \Omega_3(L,\varphi,\omega_1,\omega_2,\lambda_{S2R},\lambda_{S2E})$ and $\int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^{\infty}\frac{e^{-(1+k)\lambda_{S1R}x_3}}{x_3}dx_3 = \Gamma\left[0,(1+k)\lambda_{S1R}\left(\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}\right)\right]$ (see [32, Eq. (3.381.3)]); (74.2) is obtained from (74.1) by approximating $\frac{\varphi-1}{\omega_2\psi}\overset{\text{high }\psi}{\approx} 0$; (73.3) is obtained from (74.2) by using the Eq. (6.455.1) of [32] in the case of $\mu=1$ and $v=0$, as $\int_0^{\infty} e^{-\beta x}\Gamma(0,\alpha x)dx = \frac{1}{\alpha+\beta_2}F_1\left(1,\,1\,;\,2\,;\frac{\beta}{\alpha+\beta}\right)$.

We finish the proof by combining (72), (73), and (74).

Appendix 3: Proof of Lemma 2

The integral $I_{2,\mathrm{MAS1R}}$ can be obtained after some steps with using [32, Eq. (3.381.3)] and approximating $\frac{\varphi-1}{\omega_2\psi} \approx 0$, and $\frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi x_3} \approx 0$ when ψ is high, as follows

$$I_{2,maS1R} \approx \frac{-(\varphi-1)\lambda_{RS1}}{\omega_3\psi}(I_5 + I_6) \tag{75}$$

where I_5 and I_6 are denoted and derived as in (76) and (77), respectively

$$\begin{aligned} I_5 &\triangleq \int_0^\infty L\lambda_{S1E}\sum_{u=0}^{L-1} C_{L-1}^u(-1)^u e^{-(1+u)\lambda_{S1E}x_1} \\ &\quad \int_0^\infty L\lambda_{S2E}\lambda_{S2R}\sum_{k=0}^{L-1} C_{L-1}^k(-1)^k e^{-(1+k)\lambda_{S2E}x_2}\Gamma\left[0, \frac{\varphi\omega_1\lambda_{S2R}x_2}{\omega_2}\right] \\ &\quad \int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty \lambda_{S1R}e^{-\lambda_{S1R}x_3}dx_3dx_2dx_1 \\ &= \Omega_4(L, M, \varphi, \omega_1, \omega_2, \psi, \lambda_{S1R}, \lambda_{S1E})\Omega_5(L, 1, \varphi, \omega_1, \omega_2, \lambda_{S2R}, \lambda_{S2E}) \end{aligned} \tag{76}$$

$$\begin{aligned} I_6 &\triangleq \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\int_0^\infty L\lambda_{S1E}\sum_{t=0}^{L-1} C_{L-1}^t(-1)^t e^{-(1+t)\lambda_{S1E}x_1} \\ &\quad \int_0^\infty L\lambda_{S2E}\lambda_{S2R}\sum_{w=0}^{L-1} C_{L-1}^w(-1)^w e^{-(1+w)\lambda_{S2E}x_2}\Gamma\left[0, \frac{\varphi\omega_1\lambda_{S2R}x_2}{\omega_2}\right] \\ &\quad \int_{\frac{\varphi-1}{\omega_2\psi}+\frac{\varphi\omega_1 x_1}{\omega_2}}^\infty M\lambda_{S1R}\sum_{k=0}^{M-1} C_{M-1}^k(-1)^k\frac{e^{-(1+k)\lambda_{S1R}x_3}}{x_3}dx_3dx_2dx_1 \\ &= \frac{-(\varphi-1)\lambda_{RS2}}{\omega_3\psi}\Omega_5(L, M, \varphi, \omega_1, \omega_2, \lambda_{S1R}, \lambda_{S1E}) \\ &\quad \Omega_5(L, 1, \varphi, \omega_1, \omega_2, \lambda_{S2R}, \lambda_{S2E}) \end{aligned} \tag{77}$$

We finish the proof by combining (75), (76), and (77).

Appendix 4: Proof of Equation (59.2)

The expression for the probability term $\Pr[\min(C_{J_1S1}, C_{J_1S2}) \geq C_t]$ can be obtained as follows:

$$\begin{aligned} &\Pr[\min(C_{J_sS1}, C_{J_sS2}) \geq C_t] \\ &= \Pr\left[g_{J_sS1} \geq \frac{\varphi-1}{\omega_1\psi} + \varphi g_{J_sE\max}\right]\Pr\left[g_{J_sS2} \geq \frac{\varphi-1}{\omega_1\psi} + \varphi g_{J_sE\max}\right] \\ &= e^{\frac{-(\varphi-1)(\lambda_{JS1}+\lambda_{JS2})}{\omega_1\psi}}L\lambda_{JE}\sum_{k=0}^{L-1}\frac{C_{L-1}^k(-1)^k}{(1+k)(\lambda_{JE}+\lambda_{JE})+\varphi(\lambda_{JS1}+\lambda_{JS2})} \\ &= e^{\frac{-(\varphi-1)(\lambda_{JS1}+\lambda_{JS2})}{\omega_1\psi}}\Omega_2(L, \varphi, \lambda_{JS1}, \lambda_{JS2}, \lambda_{JE}) \end{aligned} \tag{78}$$

By substituting (78) into (59.1), we finish the proof.

Appendix 5: Proof of Lemma 3

By substituting (49), (50), (51), and (5) into (61), we obtain

$$\begin{aligned} P_{out,\mathrm{OPT}}^{\mathrm{STWJNC},1} &= 1-\Pr\left[\begin{array}{l} g_{S1R_s}\geq\dfrac{\varphi-1}{\omega_1\psi}, g_{S2R_s}\geq\dfrac{\varphi-1}{\omega_1\psi}, \\ g_{R_sS1}\geq\dfrac{\varphi-1}{\omega_4\psi g_{J_sR_s}}, g_{R_sS2}\geq\dfrac{\varphi-1}{\omega_4\psi g_{J_sR_s}}\end{array}\right] \\ &= 1-\int_{\frac{\varphi-1}{\omega_1\psi}}^{\infty} f_{g_{S1R_s}}(x_1)\int_{\frac{\varphi-1}{\omega_1\psi}}^{\infty} f_{g_{S2R_s}}(x_2)\int_0^{\infty} f_{g_{J_sR_s}}(x_3) \\ &\quad \int_{\frac{\varphi-1}{\omega_4\psi x_3}}^{\infty} f_{g_{R_sS1}}(x_4)\int_{\frac{\varphi-1}{\omega_4\psi x_3}}^{\infty} f_{g_{R_sS2}}(x_5)dx_5dx_4dx_3dx_2dx_1 \end{aligned} \tag{79}$$

From the optimal jammer and relay selection strategy, in (48a), the CDF of RV $g_{J_sR_s}$ is expressed as

$$F_{g_{J_sR_s}}(x_3)=\Pr\left[\max_{\substack{k=1,2,\ldots,K\\ m=1,2,\ldots,M}}(g_{J_kR_m})<x_3\right]=\left(1-e^{-\lambda_{JR}x_3}\right)^{KM} \tag{80}$$

By substituting (80), $f_{g_{S1R_s}}(x_1)=\lambda_{S1R}e^{-\lambda_{S1R}x_1}$, $f_{g_{S2R_s}}(x_2)=\lambda_{S2R}e^{-\lambda_{S2R}x_2}$, $f_{g_{J_sR_s}}(x_3)=KM\lambda_{JR}\sum_{k=0}^{KM-1}C_{KM-1}^{k}(-1)^k e^{-(1+k)\lambda_{JR}x_3}$, $f_{g_{R_sS1}}(x_4)=\lambda_{RS1}e^{-\lambda_{RS1}x_4}$, and $f_{g_{R_sS2}}(x_5)=\lambda_{RS2}e^{-\lambda_{RS2}x_5}$ into (79), we can obtain

$$\begin{aligned} P_{out,\mathrm{opt}}^{\mathrm{STWJNC},1} &= 1-e^{\frac{-(\varphi-1)(\lambda_{S1R}+\lambda_{S2R})}{\omega_1\psi}} \\ &\quad \int_0^{\infty} KM\lambda_{JR}\sum_{k=0}^{KM-1}C_{KM-1}^{k}(-1)^k e^{-(1+k)\lambda_{JR}x_3}e^{\frac{-(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_4\psi x_3}}dx_3 \end{aligned} \tag{81}$$

From [32, Eq. (3.381.1)], $\int_0^{\infty}e^{-\beta/4x-\gamma x}dx=\sqrt{\beta/\gamma}K_1\left(\sqrt{\beta\gamma}\right)$, we obtain

$$\begin{aligned} &\int_0^{\infty} e^{-(1+k)\lambda_{JR}x_3}e^{\frac{-(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})}{\omega_4\psi x_3}}dx_3=\sqrt{\frac{4(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})}{(1+k)\omega_4\psi\lambda_{JR}}} \\ &K_1\left(\sqrt{\frac{4(1+k)(\varphi-1)(\lambda_{RS1}+\lambda_{RS2})\lambda_{JR}}{\omega_4\psi}}\right) \end{aligned} \tag{82}$$

By substituting (82) into (81), we complete the proof.

Appendix 6: Proof of Lemma 4

By substituting (54), (55), (56), and (57) into (62), we obtain

$$P_{out,\mathrm{opt}}^{\mathrm{STWJNC},2} = 1 - \Pr\left[\begin{array}{l} g_{S1R_s} \geq \dfrac{\varphi-1}{\omega_1\psi} + \varphi g_{S1E\max}, g_{S2R_s} \geq \dfrac{\varphi-1}{\omega_1\psi} + \varphi g_{S2E\max}, \\ g_{R_sS1} \geq \dfrac{\varphi-1}{\omega_4\psi g_{J_sR_s}} + \varphi g_{R_sE\max}, g_{R_sS2} \geq \dfrac{\varphi-1}{\omega_4\psi g_{J_sR_s}} + \varphi g_{R_sE\max} \end{array}\right]$$

$$= 1 - \int_0^\infty f_{g_{S1E\max}}(x_1) \int_0^\infty f_{g_{S2E\max}}(x_2) \int_{\frac{\varphi-1}{\omega_1\psi}+\varphi x_1}^\infty f_{g_{S1R_s}}(x_3) \int_{\frac{\varphi-1}{\omega_1\psi}+\varphi x_2}^\infty f_{g_{S2R_s}}(x_4) \quad (83)$$

$$\int_0^\infty f_{g_{J_sR_s}}(x_5) \int_0^\infty f_{g_{R_sE\max}}(x_6) \int_{\frac{\varphi-1}{\omega_4\psi x_5}+\varphi x_6}^\infty f_{g_{R_sS1}}(x_7) \int_{\frac{\varphi-1}{\omega_4\psi x_5}+\varphi x_6}^\infty f_{g_{R_sS2}}(x_8)$$

$$dx_8 dx_7 dx_6 dx_5 dx_4 dx_3 dx_2 dx_1$$

By substituting the PDFs of the eight RVs $g_{S1E\max}$, $S2E\max$, $S1R_s$, $S2R_s$, $g_{J_sR_s}$, $g_{R_sE\max}$, g_{R_sS1}, and g_{R_sS2}, into (83) and after some manipulations of (83), the Eq. (64) in Lemma 4 is obtained. This completes the proof.

References

1. Raghunathan, V., Ganeriwal, S., & Srivastava, M. (2006). Emerging techniques for long lived wireless sensor networks. *IEEE Communications Magazine*, *44*(4), 108–114.
2. Paradiso, J. A., & Starner, T. (2005). Energy scavenging for mobile and wireless electronics. *IEEE Pervasive Computing*, *4*(1), 18–27.
3. Ulukus, S., Yener, A., Erkip, E., Simeone, O., Zorzi, M., Grover, P., et al. (2015). Energy harvesting wireless communications: A review of recent advances. *IEEE Journal on Selected Areas in Communications*, *33*(3), 360–381.
4. Medepally, B., & Mehta, N. B. (2010). Voluntary energy harvesting relays and selection in cooperative wireless networks. *IEEE Transactions on Wireless Communications*, *8*(11), 3543–3553.
5. Zhou, X., Zhang, R., & Ho, C. K. (2013). Wireless information and power transfer: Architecture design and rate-energy tradeoff. *IEEE Transactions on communications*, *61*(11), 4754–4767.
6. Lumpkins, W. (2014). Nikola Teslas dream realized: Wireless power energy harvesting. *IEEE Consumer Electronics Magazine*, *3*(1), 39–42.
7. Pinuela, M., Mitcheson, P. D., & Lucyszyn, S. (2013). Ambient RF energy harvesting in urban and semi-urban environments. *IEEE Transactions on Microwave Theory and Techniques*, *61*(7), 2715–2726.
8. Grover, P., & Sahai, A. (2010). Shannon meet Tesla: Wireless information and power transfer. In *IEEE international symposium on information theory proceedings (ISIT)*, pp. 2363–2367.
9. Zhang, R., & Ho, C. K. (2013). MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Transactions on Wireless Communications*, *12*(5), 1989–2001.
10. Varshney, L. R. (2008). Transporting information and energy simultaneously. In IEEE international symposium on information theory (ISIT), pp. 1612–1616.
11. Liu, L., Zhang, R., & Chua, K. C. (2013). Wireless information transfer with opportunistic energy harvesting. *IEEE Transactions on Wireless Communications*, *12*(1), 288–300.
12. Nasir, A. A., Xiangyun, Z., Durrani, S., & Kennedy, R. A. (2013). Relaying protocols for wireless energy harvesting and information processing. *IEEE Transactions on Wireless Communications*, *12*(7), 3622–3636.
13. Nasir, A. A., Zhou, X., Durrani, S., & Kennedy, R. A. (2015). Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis. *IEEE Transactions on Communications*, *63*(5), 1607–1622.
14. Ding, Z., Perlaza, S. M., Esnaola, I., & Poor, H. V. (2014). Power allocation strategies in energy harvesting wireless cooperative networks. *IEEE Transactions on Wireless Communications*, *13*(2), 846–860.
15. Liu, Y., Wang, L., Elkashlan, M., & Duong, T. Q. (2014). Two-way relaying networks with wireless power transfer: Policies design and throughput analysis. In *IEEE global communications conference (GLOBECOM)*, pp. 4030–4035.

16. Son, P. N., & Kong, H. Y. (2015). Energy-harvesting relay selection schemes for decode-and-forward dual-hop networks. *IEICE Transactions on Communications, E98-B*(4), 661–672.
17. Stallings, W. (2003). *Cryptography and network security principles and practices* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.
18. Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal*, *54*(8), 1355–1387.
19. Leung-Yan-Cheong, S., & Hellman, M. E. (1978). The Gaussian wire-tap channel. *IEEE Transaction on Information Theory*, *24*(4), 451–456.
20. Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348.
21. Liang, Y., Poor, H. V., & Shamai, S. (2008). Secure communication over fading channels. *IEEE Transactions on Information Theory*, *54*(6), 2470–2492.
22. Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, *58*(3), 1875–1888.
23. Zang, R., Song, L., Han, Z., Jiao, B., & Debbah, M. (2010). Physical layer security for for two way relay communications with friendly jammers. In: *IEEE global telecommunications conference (GLOBECOM)*, pp. 1–6.
24. Wang, L., Elkashlan, M., Huang, J., Tran, N. H., & Duong, T. Q. (2014). Secure transmission with optimal power allocation in untrusted relay networks. *IEEE Wireless Communications Letters*, *3*(3), 289–292.
25. Wang, L., Kim, K. J., Duong, T. Q., Elkashlan, M., & Poor, H. V. (2014). On the security of cooperative single carrier systems. In *IEEE global telecommunications conference (GLOBECOM)*, Austin, TX, pp. 1596–1601.
26. Duong, T. Q., Duy, T. T., Elkashlan, M., Tran, N. H., & Dobre, O. A. (2014). Secured cooperative cognitive radio networks with relay selection. In *IEEE global telecommunications conference (GLOBECOM)*, Austin, TX, pp. 3074–3079.
27. Liu, Y., Wang, L., Duy, T. T., Elkashlan, M., & Duong, T. Q. (2015). Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communication Letters*, *4*(1), 46–49.
28. Jong-Ho, L. (2015). Cooperative relaying protocol for improving physical layer security in wireless decode-and-forward relaying networks. *Wireless Personal Communications*, *83*(4), 3033–3044.
29. Krikidis, I., Thompson, J. S., & Mclaughlin, S. (2009). Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, *8*(10), 50035011.
30. Long, H., Xiang, W., Wang, J., Zhang, Y., & Wang, W. (2014). Cooperative jamming and power allocation with untrusty two-way relay nodes. *IET Communications*, *8*(13), 2290–2297.
31. Duy, T. T., Duong, T. Q., Benevides da Costa, D., Bao, V. N. Q., & Elkashlan, M. (2015). Proactive relay selection with joint impact of hardware impairment and co-channel interference. *IEEE Transaction on Communications*, *64*(5), 1594–1606.
32. Gradshteyn, I. S., Ryzhik, I. M., Jeffrey, A., & Zwillinger, D. (2007). *Table of integral, series and products* (7th ed.). London: Academic Press.

Sang Quang Nguyen received the B.E. degree (2010) and M.E. degree (2013) in Ho Chi Minh City University of Transport and Ho Chi Minh City University of Technology, Vietnam, respectively. In 2017, he received Ph.D. degree in Electrical Engineering from University of Ulsan, South Korea. He is currently a member of Research Center of New Technology (NewTech) of the Faculty of Electrical & Electronics Engineering (FEEE) of Duy Tan University (DTU), Vietnam. His major interests are: cooperative communications, cognitive radio, physical layer security, and energy harvesting.

Hyung Yun Kong He received the M.E. and Ph.D. degrees in electrical engineering from Polytechnic University, Brooklyn, New York, USA, in 1991 and 1996, respectively. He also received a BE in electrical engineering from New York Institute of Technology, New York, in 1989. From 1996 to 1998, he was with LG electronics Co., Ltd., as a member of the multimedia research lab developing PCS mobile phone systems. In 1997, he was promoted to the LG chairman's office planning future satellite communication systems. From 1998 until now, he is a Professor in School of Electrical Engineering at the University of Ulsan, Korea. His research area includes channel coding, detection and estimation, cooperative communications, cognitive radio and wireless sensor networks. He is a member of IEEK, KICS, KIPS, IEEE, and IEICE.