Physical Layer Security for Two-Way Relay NOMA Systems with Energy Harvesting

Hui Li[1], Yaping Chen[1], and Borong Zou[1*]
[1] School of Physics and Electronic Information Engineering, Henan Polytechnic University
Jiaozuo, People's Republic of China
[e-mail: li20022004@hpu.edu.cn, 211911010007@home.hpu.edu.cn, wdzbr296@hpu.edu.cn]
[*]Corresponding author: Borong Zou

Received September 23, 2021; revised March 4, 2022; accepted May 22, 2022; published June 30, 2022

Abstract

Due to the wide application of fifth generation communication, wireless sensor networks have become an indispensable part in our daily life. In this paper, we analyze physical layer security for two-way relay with energy harvesting (EH), where power splitter is considered at relay. And two kinds of combined methods, i.e., selection combining (SC) and maximum ratio combining (MRC) schemes, are employed at eavesdropper. What's more, the closed-form expressions for security performance are derived. For comparison purposes, this security behaviors for orthogonal multiple access (OMA) networks are also investigated. To gain deeper insights, the end-to-end throughput and approximate derivations of secrecy outage probability (SOP) under the high signal-to-noise ratio (SNR) regime are studied. Practical Monte-Carlo simulative results verify the numerical analysis and indicate that: i) The secure performance of SC scheme is superior to MRC scheme because of being applied on eavesdropper; ii) The secure behaviors can be affected by various parameters like power allocation coefficients, transmission rate, etc; iii) In the low and medium SNR region, the security and channel capacity are higher for cooperative non-orthogonal multiple access (NOMA) systems in contrast with OMA systems; iv) The systematic throughput can be improved by changing the energy conversion efficiency and power splitting factor. The purpose of this study is to provide theoretical direction and design of secure communication.

Keywords: Physical layer security, energy harvesting, two-way relay, non-orthogonal multiple access, wireless sensor networks.

The project was supported by Henan Provincial Science and Technology Research(Grant No. 222102210247).

1. Introduction

With the rapid development of science and technology, wireless sensor networks are widely applied in many fields, such as military, medical treatment, industry, commerce and so on. However, because of the resource limitations and broadcast nature of electromagnetic waves, legitimate information is inevitably at risk of being wiretapped. Although classical encryption algorithms can deal with this problem, its hardware requirements are high. Thus, an emerging technique (i.e., physical layer security) has been put forward to enhance the reliability and security by employing the random characteristics of wireless channels. At present, physical layer security has attracted the attention of many researchers [1, 2]. In [3], the authors proposed a novel layered physical layer security model and every layer had a hierarchical information security structure. The authors of [4] studied a transmission scheme based on the cooperative jammer, where the untrusted relay may wiretap the confidential information. The authors of [5] adopted the well-known statistical models over $\alpha-\eta-\kappa-\mu$ fading channels to analyze SOP and average secrecy capacity. In [6], the tradeoff between the physical layer security and end-to-end delay was studied employing the knowledge of queueing theory and stochastic geometry. A novel chaotic communication system to solve the security problem of data transmission was analyzed in the industrial Internet of Things [7].

Cooperative communication becomes an effective approach by expanding network coverage and furnishing greater diversity, and it solves these problems for the scarcity of spectrum resources and increase of communication blind zone [8, 9]. In a real scenario, the transmission of information must be supported by energy. However, some networks are hard to get a lot of energy from the remote devices. To solve this problem, relays with energy harvesting have great effect on the energy-constrained networks [10]. A comprehensive performance evaluation of unmanned aerial vehicles relay networks was provided. In addition, the relay was assumed to be wirelessly-powered and harvested energy from a nearby base station [11]. The application of the simultaneous wireless information and power transfer (SWIPT) strategy has a great influence on the maximization of lifetime for energy constrained relays [12]. Wireless information transfer and wireless power transfer are included in the SWIPT. The first one is the separation of two components as the receiver with two different functions. Another one is the combination of the two components as a unified receiver. The latter receiver architecture is more complex and researched extensively than the former [13, 14]. In small devices deployed in vehicle-to-everything communications, the authors of [15] proposed wireless power transfer that applied to roadside unit to improve spectrum efficiency. Utilizing energy-harvesting based spectrum sharing cooperation scheme, the authors of [16] studied the performance of an overlay cognitive NOMA system. Nowadays, many schemes for receiver architectures include time switching, power splitting are proposed. The authors of [17] studied the secrecy performance employing amplify-and-forward (AF) and decode-and-forward (DF) relaying equipped with a power splitting architecture with EH. Statistical results showed that the secrecy performance using DF relaying is better than AF relaying for the different power splitting parameters. In [18], the authors investigated a multiple-input multiple-output (MIMO) wireless system considering the wireless power transmission of electromagnetic or radio signals. Moreover, two actual designs including time switching and power splitting for the case of co-located receiver were studied. In [19], the downlink transmission was optimized for SWIPT in multi-cell large-scale MIMO systems, and average harvested energy under the restriction of large systems was analyzed. In [20], in order to serve better performance for user pairs, two-way transmission mode and linear energy harvesting in the downlink small-cell NOMA systems were investigated.

In contrast with the traditional one-way relay required four-step method, the two-way relay (TWR) operated in two steps or three steps improves channel capacity in a bidirectional transmission system [21]. The authors of [22] proposed a TWR-NOMA scheme supporting multi-pair of users that not only increased throughput related to power allocation factors and target rates, but also improved the spectral efficiency. In this connection, the SWIPT based on two-step or three-step two-way relay networks (TWRNs) has caught researchers' eye from academia and wireless industry [23, 24]. The two-way relay represents that two nodes exchange the information by sharing a single relay, which can relieve the constraint of spectral efficiency for only a relay on half-duplex mode. The TWR can be not only modeled as two steps (i.e., in the first step, two sensor nodes send messages to relay; in the second step, relay forwards to both nodes simultaneously), but also as three steps (i.e., relay receives information from two nodes in the first two steps, then forwards to both nodes in final step) [25]. In [26], the authors investigated three-step two-way DF relay systems with EH over independent $\kappa-\mu$ shadowed fading. The security beamforming designed for the two-way cognitive radio network with SWIPT was investigated [27]. Two kinds of secure relay protocols based power splitting and time switching algorithms were considered for these TWRNs. Meanwhile, the optimal values of power splitting and time switching ratio were analyzed with the purpose of maximizing the minimum secrecy capacity in high SNR environments [28]. Recently, combining TWR with NOMA, all kinds of performances are investigated by many academic researchers [29-31]. Specifically, the performances of the TWR-NOMA systems using two kinds of successive interference cancellation (SIC) schemes (i.e., imperfect SIC and perfect SIC) were studied in [29]. The authors in [30] analyzed the sum-rate of NOMA-TWRNs on AF and DF relaying modes, and the formulas for asymptotic and upper bound of sum-rate were analyzed. In [31], TWRNs based on NOMA including single eavesdropper and multiple eavesdroppers were developed. In addition, the relay not only forwarded confidential information to the legal nodes, but also emitted jamming signals all the time to improve secure performance.

Based on the previous discussion, two-step TWR-NOMA systems for wireless sensor networks are considered in this paper, where two legitimate sensor nodes interchange information by a half-duplex relay and there exists eavesdropping in every transmission. The main works of this paper are summarized as follows:

This paper describes a two-step TWR-NOMA system model, in which two sensor nodes transmit messages to relay in the first step, then relay forwards to both nodes in the second step, simultaneously. The radio-frequency signals received at relay is divided into two parts by power: one is applied to harvest energy, while another is used for information processing (IP). Moreover, the received signals from two different slots are processed employing two combined schemes at the eavesdropper, namely SC and MRC schemes.

The analytical SOP of this TWR-NOMA system is provided utilizing SC and MRC schemes over independent Rayleigh distribution. Besides, the SOPs for TWR-OMA system model and the scheme without power splitting are also studied as a contrast. Experimental results are consistent with the statistical results and confirm that SC scheme can get the better SOP due to smaller capacity of eavesdropping. The results also demonstrate that security performance of this system can be improved obviously by decreasing the value of target transmission rate and time allocation parameter.

To better understand secrecy performance, we derive the end-to-end throughput and approximate formulas of SOP for two different schemes in cooperative TWR-NOMA systems using the theorem of infinitesimal equivalence under high SNR regime. And the end-to-end throughput can be improved by changing the power splitting factor and energy conversion

efficiency. What's more, the results also show the TWR-NOMA systems acquire the lower SOP in the low and medium SNR environments and higher security capacity comparing with the TWR-OMA systems.

The particular arrangement of the paper is organized as below. In Section II, the model of two-step TWR-NOMA system is presented and the end-to-end SINRs are formulated. In Section III, new theoretical formulas of SOP for SC and MRC schemes are deduced. In Section IV, the accurate end-to-end throughput and asymptotical SOP in high SNR environments are provided. Numerical results and systematic performances are shown in Section V. Finally, Section VI summarizes the conclusions for this paper.

Notations: In this paper, $F_X(\cdot)$ and $f_X(\cdot)$ are the cumulative distribution function (CDF) and probability density function (PDF) for random variable X. $\mathcal{CN}(\mu,\sigma^2)$ symbolizes the complex Gaussian random variable with mean μ and variance σ^2. And $E(\cdot)$ and $\Pr(\cdot)$ represent the expectation and probability operation. For better understanding, other symbols are tabulated, as shown in **Table 1**.

Table 1. Parameters Notation [with $XY \in \{AR, AE, RB, RE, BR, BE, RA\}$, $i \in \{A, B\}$]

Parameter	Definition
h_{XY}	Transmission channel from *X* to *Y*
d_{XY}	Distance from *X* to *Y*
x_A , x_B	Transmission signals to nodes *A* and *B*
n_{XY}	Additive white Gaussian noise
P_i	Transmitted power from the node *i*
P_R	Transmitted power from the relay
a_{iR} , a_{Ri}	Corresponding power allocation coefficient
η	Energy conversion efficiency
β	Time allocation parameter
α	exponent for path loss
λ	power splitting parameter

2. System Model

As illustrated in **Fig. 1**, the system model for wireless sensor networks includes two legitimate sensor nodes (namely, the nearby node *A* and far node *B*), a two-way NOMA relay (*R*) and a single eavesdropper (*Eve*). It should be found that the direct link for nodes *A* and *B* is nonexistent because of fading deeply, so nodes *A* and *B* need to exchange their messages via relay, whereas the direct links for two nodes and *Eve* are considered. Thus, *Eve* is required to process the received messages using SC and MRC algorithms. All wireless channels are modeled as independent Rayleigh distribution and affected by the path loss and additive white Gaussian noise. Furthermore, all nodes are assumed to equip with an antenna and run in half-duplex mode. The whole process of communication is sub-divided into three stages: 1) During the first stage βT, the relay collects energy from nodes *A* and *B*; 2) In the second stage $(1-\beta)T/2$, nodes *A* and *B* send radio-frequency signals to relay, simultaneously; 3) In the third stage $(1-\beta)T/2$, the relay forwards messages to nodes *A* and *B* at the same time. The

leakage of information exists in latter two stages due to the transmission of information. In addition, what needs illustration is that g_{XY} denotes mean channel power gain [32] and n_{XY} symbolizes additive white Gaussian noise modeled as $\mathcal{CN}(0, N_0)$.

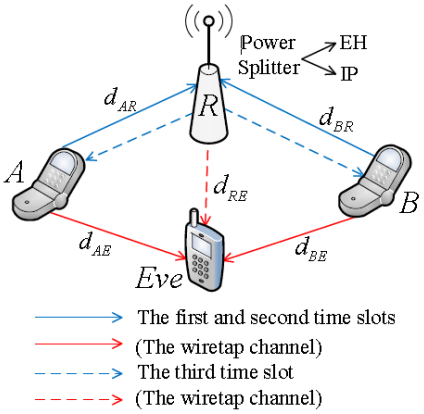

Fig. 1. System model

During the first and second stages, nodes *A* and *B* send the normalized signals x_A and x_B ($E\left(|x_A|^2\right) = E\left(|x_B|^2\right) = 1$) to the relay, simultaneously. The received superimposed signals at *R* from terminal node *i* is

$$y_{iR} = \sqrt{a_{AR} d_{AR}^{-\alpha} P_A} h_{AR} x_A + \sqrt{a_{BR} d_{BR}^{-\alpha} P_B} h_{BR} x_B + n_{iR} \tag{1}$$

where P_i denotes the transmitted power from the node *i*, $i \in \{A, B\}$, a_{iR} is the corresponding power allocation coefficient and meets the condition of $a_{AR} + a_{BR} = 1$, n_{iR} and n_{iE} are written as the superimposed Gaussian noise.

The received signals at relay *R* are divided to two parts by power splitting scheme: $\sqrt{\lambda} y_{iR}$ for EH and $\sqrt{1-\lambda} y_{iR}$ for IP. Therefore, the total harvested energy from both terminal nodes is given by

$$E_{total} = \lambda \eta \beta T \left(P_A a_{AR} d_{AR}^{-\alpha} |h_{AR}|^2 + P_B a_{BR} d_{BR}^{-\alpha} |h_{BR}|^2 \right) \tag{2}$$

where λ denotes power splitting ratio for sensor node *i*, and η is the energy conversion efficiency.

According to the SIC method of uplink NOMA, the information with a strong channel condition is decoded firstly and then eliminated [33]. If the user with poor channel quality is decoded first, it is necessary to allocate high transmitting power to ensure its receiving power, which will cause a waste of resources. The information x_A has the strong channel quality h_{AR}. Thus, signal x_A at *R* from node *A* to *R* is decoded primarily, the received signal-to-interference-plus-noise ratio (SINR) is written by

$$\gamma_{AR} = \frac{a_{AR} d_{AR}^{-\alpha} \rho_A (1-\lambda) |h_{AR}|^2}{a_{BR} d_{BR}^{-\alpha} \rho_B (1-\lambda) |h_{BR}|^2 + 1} \tag{3}$$

where $\rho_i = P_i / N_0$ is the SNR at node *i*.

Based on SIC method for uplink NOMA, the information x_A with the strong channel quality

should be detected and eliminated. Then, the received SNR to decode x_B at R is shown by

$$\gamma_{BR} = a_{BR} d_{BR}^{-\alpha} \rho_B (1-\lambda) |h_{BR}|^2 \tag{4}$$

At the same time, the signals wiretapped by the *Eve* can be expressed as

$$y_{iE} = \sqrt{a_{AR} d_{AE}^{-\alpha} P_A} h_{AE} x_A + \sqrt{a_{BR} d_{BE}^{-\alpha} P_B} h_{BE} x_B + n_{iE} \tag{5}$$

The SINRs at *Eve* to wiretap signals x_A and x_B can be represented as

$$\gamma_{AEA} = \frac{a_{AR} d_{AE}^{-\alpha} \rho_A (1-\lambda) |h_{AE}|^2}{a_{BR} d_{BE}^{-\alpha} \rho_B (1-\lambda) |h_{BE}|^2 + 1} \simeq \frac{a_{AR} d_{AE}^{-\alpha} |h_{AE}|^2}{a_{BR} d_{BE}^{-\alpha} |h_{BE}|^2} \tag{6}$$

and

$$\gamma_{BEB} = \frac{a_{BR} d_{BE}^{-\alpha} \rho_B (1-\lambda) |h_{BE}|^2}{a_{BR} d_{AE}^{-\alpha} \rho_A (1-\lambda) |h_{AE}|^2 + 1} \simeq \frac{a_{BR} d_{BE}^{-\alpha} |h_{BE}|^2}{a_{AR} d_{AE}^{-\alpha} |h_{AE}|^2} \tag{7}$$

respectively, where $\rho_A = \rho_B$ is assumed in this paper. What need to be explained is that the asymptotic operations used in the above expressions substantially approximate to the upper bound of SINRs (i.e., signal-to-interference ratios). This approximation is reasonable and has been widely used in the academic research when the performance analysis focuses on the case of limited interference, and the thermal noise can be negligible comparing to the aggravated interference from other equipment [34, 35].

After the first two stages, messages $\bar{x}_A$ and $\bar{x}_B$ denote decoded information of nodes *A* and *B*, respectively. During the third stage, *R* transmits the normalized composite messages $x_R = (\bar{x}_A + \bar{x}_B)/\sqrt{2}$ to node *i*. On account that nodes *i* knew its own message, it can reject own information to get other messages. Therefore, we assume that the instantaneous channel state information is practicable for all nodes. The received signals at node *i* are shown by

$$y_{RA} = \sqrt{a_{RA} d_{RA}^{-\alpha} P_R} h_{RA} \frac{\bar{x}_B}{\sqrt{2}} + n_{RA} \tag{8}$$

and

$$y_{RB} = \sqrt{a_{RB} d_{RB}^{-\alpha} P_R} h_{RB} \frac{\bar{x}_A}{\sqrt{2}} + n_{RB} \tag{9}$$

respectively, where $P_R = 2E_{total}/((1-\beta)T)$ is the transmit power at *R*, n_X is written as Gaussian noise $X \in \{RA, RB, RE\}$. a_{Ri} denotes the corresponding power allocation coefficient at *R* and satisfies the requirement of $a_{RA} + a_{RB} = 1$.

The corresponding SNRs from relay *R* to nodes *i* are expressed as

$$\gamma_{RA} = \frac{a_{RA} d_{RA}^{-\alpha} \rho_R |h_{RA}|^2}{2} \tag{10}$$

and

$$\gamma_{RB} = \frac{a_{RB} d_{RB}^{-\alpha} \rho_R |h_{RB}|^2}{2} \tag{11}$$

respectively, where $\rho_R = \frac{P_R}{N_0}$ is the SNR at node *R*.

During the exchange of information, the *Eve* wiretaps information x_A and x_B. At this phase,

the signals received at *Eve* can be shown as

$$y_{RE} = \left(\sqrt{a_{RA}} + \sqrt{a_{RB}}\right)\sqrt{d_{RE}^{-\alpha} P_R} h_{RE} x_R + n_{RE} \tag{12}$$

Therefore, the instantaneous SINRs at *Eve* that wiretaps the signals x_A and x_B are written by

$$\gamma_{REA} = \frac{a_{RB} d_{RE}^{-\alpha} \rho_R \left|h_{RE}\right|^2 / 2}{a_{RA} d_{RE}^{-\alpha} \rho_R \left|h_{RE}\right|^2 / 2 + 1} \simeq \frac{a_{RB}}{a_{RA}} \tag{13}$$

and

$$\gamma_{REB} = \frac{a_{RA} d_{RE}^{-\alpha} \rho_R \left|h_{RE}\right|^2 / 2}{a_{RB} d_{RE}^{-\alpha} \rho_R \left|h_{RE}\right|^2 / 2 + 1} \simeq \frac{a_{RA}}{a_{RB}} \tag{14}$$

It is obtained from (13) and (14) that the leakage of information in the third stage has no connection with the channel gain of h_{RE}. Thus, the channel gain of legitimate links plays a leading role.

Because the leakage of information occurs in two stages, the signals received need to be processed at *Eve*. Thus, SC and MRC schemes are employed in this system model. For the information received at *Eve*, the SC algorithm is discussed firstly. Then, according to (6), (7), (13) and (14), the SINRs of $\gamma_{AE}^{(SC)}$ and $\gamma_{BE}^{(SC)}$ are expressed as

$$\gamma_{AE}^{(SC)} \simeq \max\left(\gamma_{AEA}, \gamma_{REA}\right) \tag{15}$$

$$\gamma_{BE}^{(SC)} \simeq \max\left(\gamma_{BEB}, \gamma_{REB}\right) \tag{16}$$

Utilizing the MRC scheme, the instantaneous SINRs for wiretapping messages x_i are approximated as

$$\gamma_{AE}^{(MRC)} \simeq \gamma_{AEA} + \gamma_{REA} \tag{17}$$

$$\gamma_{BE}^{(MRC)} \simeq \gamma_{BEB} + \gamma_{REB} \tag{18}$$

According to the Shannon theorem, the channel capacities of legitimate channels C_i and wiretap channels C_{Ei} are shown as

$$C_i = \frac{1-\beta}{2} \log_2\left(1 + \gamma_i\right) \tag{19}$$

and

$$C_{Ei} = \frac{1-\beta}{2} \log_2\left(1 + \gamma_{iE}\right) \tag{20}$$

respectively, where the coefficient $(1-\beta)/2$ can be explained by the fact that this whole exchange of information takes place in two phases and all nodes run in half-duplex mode. On the grounds of DF protocol, the effective end-to-end SINRs can be obtained as $\gamma_A = \min\left(\gamma_{BR}, \gamma_{RA}\right)$ and $\gamma_B = \min\left(\gamma_{AR}, \gamma_{RB}\right)$. γ_{iE} includes $\gamma_{iE}^{(SC)}$ and $\gamma_{iE}^{(MRC)}$, which is discussed above.

3. Secrecy Performances Analysis

In this part, the secrecy performances of this two-way relay system for wireless sensor networks using SC and MRC schemes are studied.

The secrecy capacity of this system model for $A \to R \to B$ link or $B \to R \to A$ link can be defined as

$$C_{SEC}^{i} = \lceil C_i - C_{Ei} \rceil^{+} \tag{21}$$

where $\lceil X \rceil^{+} = \max(X, 0)$.

With regard to systematic secure performance, the SOP plays an indispensable part. We can formulate it as [36]

$$SOP(\gamma_{th}) = \Pr\left(\min\left(C_{SEC}^{A}, C_{SEC}^{B}\right) < R_{th}\right) = 1 - \left(1 - F_{\varphi_A}(\gamma_{th})\right)\left(1 - F_{\varphi_B}(\gamma_{th})\right) \tag{22}$$

where R_{th} is the threshold of secrecy transmission rate, F_{φ_A} and F_{φ_B} represent secrecy outage probabilities of the nearby node *A* and far node *B* respectively, $\gamma_{th} = 2^{2R_{th}/(1-\beta)}$ stands for the SNR threshold, $\varphi_i = (1+\gamma_i)/(1+\gamma_{Ei})$.

To get the secrecy outage probabilities for every node, the channel statistics for nodes *i* are discussed firstly. Combining with (4) and (10), the CDF of $\gamma_A(B \to R \to A)$ can be obtained as

$$F_{\gamma_A}(y) = \Pr\left(\min\left(\gamma_{BR}, \gamma_{RA}\right) < y\right) = 1 - \left(1 - F_{\gamma_{BR}}(y)\right)\left(1 - F_{\gamma_{RA}}(y)\right) = 1 - e^{-Ay} \tag{23}$$

where $A = \dfrac{2}{a_{RA} g_{RA} d_{RA}^{-\alpha} \rho_R} + \dfrac{1}{A_2 \rho_B (1-\lambda)}$.

In the same way, the effective CDF of $\gamma_B(A \to R \to B)$ can be shown as

$$F_{\gamma_B}(y) = \Pr\left(\min\left(\gamma_{AR}, \gamma_{RB}\right) < y\right) = 1 - \left(1 - F_{\gamma_{AR}}(y)\right)\left(1 - F_{\gamma_{RB}}(y)\right) = 1 - \frac{A_1}{A_1 + A_2 y} e^{-By} \tag{24}$$

where $A_1 = a_{AR} g_{AR} d_{AR}^{-\alpha}$, $A_2 = a_{BR} g_{BR} d_{BR}^{-\alpha}$, $B = \dfrac{2}{a_{RB} g_{RB} d_{RB}^{-\alpha} \rho_R} + \dfrac{1}{A_1 \rho_A (1-\lambda)}$.

3.1 SC Scheme

The closed-form formulas of SOP using SC algorithm at *Eve* can be expressed as

$$SOP^{(SC)}(\gamma_{th}) = 1 - \left(1 - F_{\varphi_A}^{(SC)}(\gamma_{th})\right)\left(1 - F_{\varphi_B}^{(SC)}(\gamma_{th})\right) \tag{25}$$

where the terms $F_{\varphi_A}^{(SC)}$ and $F_{\varphi_B}^{(SC)}$ represent secrecy outage probabilities of the nearby node *A* and far node *B* employing SC scheme, respectively.

To gain the expression of $SOP^{(SC)}$, $F_{\varphi_A}^{(SC)}$ will be derived firstly. The term $F_{\varphi_A}^{(SC)}$ in (25) can be calculated as

$$F_{\varphi_A}^{(SC)}(\gamma_{th}) = \int_0^{\infty} F_{\gamma_A}\left(\gamma_{th}(1+x) - 1\right) f_{\gamma_{BE}}^{(SC)}(x)\, dx \tag{26}$$

According to the above equation, $f_{\gamma_{BE}}^{(SC)}$ should be analyzed primarily. Employing SC scheme, the CDF of $\gamma_{BE}^{(SC)}$ can be evaluated as

$$\begin{aligned} F_{\gamma_{BE}}^{(SC)}(y) &= \Pr\left(\max\left(\gamma_{BEB},\gamma_{REB}\right)<y\right) \\ &= \Pr\left(\gamma_{BEB}<y,\gamma_{REB}<y\right) \\ &= \left(1-\frac{A_3}{A_3+A_4 y}\right)u\left(y-\frac{a_{RA}}{a_{RB}}\right) \end{aligned} \tag{27}$$

where $A_3 = a_{BR} g_{BE} d_{BE}^{-\alpha}$, $A_4 = a_{AR} g_{AE} d_{AE}^{-\alpha}$.

After calculation, the PDF of $\gamma_{BE}^{(SC)}$ can be obtained as

$$f_{\gamma_{BE}}^{(SC)}(y) = \delta\left(y-\frac{a_{RA}}{a_{RB}}\right) - \frac{A_3}{A_3+A_4 y}\delta\left(y-\frac{a_{RA}}{a_{RB}}\right) + \frac{A_3 A_4}{\left(A_3+A_4 y\right)^2}u\left(y-\frac{a_{RA}}{a_{RB}}\right) \tag{28}$$

Combining with (23), (28) and making full use of [37, eq. (3.351.4)], $F_{\varphi_A}^{(SC)}$ can be rewritten as

$$F_{\varphi_A}^{(SC)}(\gamma_{th}) = 1 - e^{-A(\gamma_{th}-1)}\left(e^{-\mu_1\gamma_{th}} - \mu_2 e^{-\mu_1\gamma_{th}} + \mu_3\gamma_{th}e^{\mu_3\gamma_{th}}\left(\frac{e^{-\mu_4\gamma_{th}}}{\mu_4\gamma_{th}} + Ei\left(-\mu_4\gamma_{th}\right)\right)\right) \tag{29}$$

where $\mu_1 = A a_{RA}/a_{RB}$, $\mu_2 = \frac{A_3 a_{RB}}{A_3 a_{RB} + A_4 a_{RA}}$, $\mu_3 = \frac{A A_3}{A_4}$, $\mu_4 = \mu_1 + \mu_3$, $Ei(q)$ symbolizes the exponential integral function represented as [38]

$$Ei(p) = \frac{(-p)^{i-1}}{(i-1)!}\left[-\ln p + \varphi(i)\right] - \sum_{m=0}^{\infty}\frac{(-p)^m}{(m-i+1)m!}$$

where $\begin{cases} \varphi(1) = -v, & i=1 \\ \varphi(i) = -v + \sum_{m=1}^{i-1}\frac{1}{m}, & i>1 \end{cases}$, and $v \approx 0.577$ denotes the Euler constant.

Theorem 1: For secrecy outage probability of the far node *B*, the closed-form expression of $F_{\varphi_B}^{(SC)}$ is given as

$$\begin{aligned} F_{\varphi_B}^{(SC)}(\gamma_{th}) = 1 - e^{-B(\gamma_{th}-1)}\Bigg[&\frac{A_1}{\varepsilon_1\gamma_{th}+\varepsilon_2}\left(1-\frac{A_4}{\varepsilon_3}\right)e^{-\frac{B\gamma_{th}a_{RB}}{a_{RA}}} - \frac{B_1}{A_2\gamma_{th}}e^{\varepsilon_4+B\gamma_{th}}Ei\left(-\varepsilon_4-\frac{B\gamma_{th}}{a_{RA}}\right) + \\ &\frac{e^{\frac{A_4 B\gamma_{th}}{A_3}}}{A_3^3}\left(\frac{\left(A_4B_2-A_3B_3\right)Be^{-\varepsilon_5\gamma_{th}}}{\varepsilon_5} + \left(\left(A_4B_2-A_3B_3\right)B\gamma_{th} + A_3B_2\right)Ei\left(-\varepsilon_5\gamma_{th}\right)\right)\Bigg] \end{aligned} \tag{30}$$

where $\varepsilon_1 = \frac{A_2}{a_{RA}}$, $\varepsilon_2 = A_1 - A_2$, $\varepsilon_3 = \frac{A_3 a_{RB}}{a_{RA}} + A_4$, $\varepsilon_4 = \frac{\varepsilon_2 B}{A_2}$, $\varepsilon_5 = \left(\frac{a_{RB}}{a_{RA}} + \frac{A_4}{A_3}\right)B$, $B_1 = \frac{A_2 B_2 \gamma_{th}}{A_3^2}$, $B_2 = \frac{A_1 A_2 A_3^3 A_4 \gamma_{th}}{\left[\left(A_3-A_4\right)A_2\gamma_{th} + \left(A_1-A_2\right)A_3\right]^2}$, $B_3 = \frac{A_2 A_4^2 B_2 \gamma_{th} - A_1 A_3^3 A_4}{\left(A_2\gamma_{th} - A_2 + A_1\right)A_3^2}$.

Proof: See Appendix A.

Eventually, replacing (25) with (29) and (30), the SOP utilizing SC scheme at *Eve* is obtained.

3.2 MRC Scheme

The closed-form formulas of SOP using MRC algorithm at *Eve* can be expressed as

$$SOP^{(MRC)}\left(\gamma_{th}\right)=1-\left(1-F_{\varphi_A}^{(MRC)}\left(\gamma_{th}\right)\right)\left(1-F_{\varphi_B}^{(MRC)}\left(\gamma_{th}\right)\right) \tag{31}$$

where the terms $F_{\varphi_A}^{(MRC)}$ and $F_{\varphi_B}^{(MRC)}$ represent secrecy outage probabilities of the nearby node *A* and far node *B* for MRC scheme, respectively.

To obtain the close-form expression of secrecy outage probability when MRC scheme is utilized at *Eve*, $F_{\varphi_A}^{(MRC)}$ will be derived firstly. The term $F_{\varphi_A}^{(MRC)}$ can be calculated as

$$F_{\varphi_A}^{(MRC)}\left(\gamma_{th}\right)=\int_0^{\infty}F_{\gamma_A}\left(\gamma_{th}\left(1+x\right)-1\right)f_{\gamma_{BE}}^{(MRC)}\left(x\right)dx \tag{32}$$

Then, taking advantage of MRC scheme at *Eve*, the PDF of $\gamma_{BE}^{(MRC)}$ can be expressed as

$$\begin{aligned}F_{\gamma_{BE}}^{(MRC)}\left(y\right)&=\Pr\left(\gamma_{BEB}+\gamma_{REB}<y\right)\\&=\int_0^{\infty}F_{|h_{BE}|^2}\left(\left(y-\frac{a_{RA}}{a_{RB}}\right)\frac{a_{AR}d_{AE}^{-\alpha}}{a_{BR}d_{BE}^{-\alpha}}x\right)f_{|h_{AE}|^2}\left(x\right)dx\\&=1-\frac{A_3a_{RB}}{A_3a_{RB}+A_4\left(a_{RB}y-a_{RA}\right)}\end{aligned} \tag{33}$$

The CDF of $\gamma_{BE}^{(MRC)}$ can be calculated as

$$f_{\gamma_{BE}}^{(MRC)}\left(y\right)=\frac{m_1}{\left(m_3+m_2\left(a_{RB}y-a_{RA}\right)\right)^2} \tag{34}$$

where $m_1=A_3A_4a_{RB}^2$, $m_2=A_4$, $m_3=A_3a_{RB}$.

According to (32), the $F_{\varphi_A}^{(MRC)}$ can be calculated as

$$\begin{aligned}F_{\varphi_A}^{(MRC)}\left(\gamma_{th}\right)&=\int_0^{\infty}\left(1-e^{-A\left(\gamma_{th}x+\gamma_{th}-1\right)}\right)\frac{m_1}{\left(m_3+m_2\left(a_{RB}x-a_{RA}\right)\right)^2}dx\\&=G_1\int_{\frac{a_{RA}}{a_{RB}}}^{\infty}\frac{1}{\left(1+H_1x\right)^2}dx-G_2\int_0^{\infty}\frac{e^{-\frac{A\gamma_{th}x}{a_{RB}}}}{\left(x+H_2\right)^2}dx\end{aligned} \tag{35}$$

where $G_1=\frac{m_1}{\left(m_3-m_2a_{RA}\right)^2}$, $G_2=\frac{m_1}{m_2^2a_{RB}}e^{-A\left(\frac{\gamma_{th}}{a_{RB}}-1\right)}$, $H_1=\frac{m_2a_{RB}}{m_3-m_2a_{RA}}$, $H_2=\frac{m_3}{m_2}$. Employing [37, eq. (3.353.3)] in (35), $F_{\varphi_A}^{(MRC)}$ can be obtained as

$$F_{\varphi_A}^{(MRC)}\left(\gamma_{th}\right)=\frac{G_1a_{RB}}{H_1a_{RB}+H_1^2a_{RA}}-\frac{AG_2\gamma_{th}}{a_{RB}}e^{\frac{AH_2\gamma_{th}}{a_{RB}}}Ei\left(-\frac{AH_2\gamma_{th}}{a_{RB}}\right)-\frac{G_2}{H_2} \tag{36}$$

Theorem 2: For secrecy outage probability of the far node *B* for MRC scheme, the closed-form expression of $F_{\varphi_B}^{(MRC)}$ is given as

$$F_{\varphi_B}^{(MRC)}(\gamma_{th}) = \frac{G_3 a_{RA}}{H_3 a_{RA} + H_3^2 a_{RB}} - G_4 \left[\frac{C_1}{n_2} \left(-e^{W_2} Ei\left(-(W_1+W_2)\right) \right) + \frac{C_2 W_3 e^{-W_1}}{n_4^2 (W_1+W_3)} + \frac{e^{W_3}\left(C_2(1+W_3) - C_3 B\gamma_{th}\right)}{n_4^2} Ei\left(-(W_1+W_3)\right) - \frac{a_{RA} C_3 e^{-W_1}}{n_4 (a_{RB} n_4 + a_{RA} n_3)} \right] \tag{37}$$

where $m_4 = A_3 A_4 a_{RA}^2$, $m_5 = A_3$, $m_6 = A_4 a_{RA}$, $G_3 = \frac{m_4}{(m_6 - m_5 a_{RB})^2}$, $G_4 = A_1 m_4 e^{-B(\gamma_{th}-1)}$,

$H_3 = \frac{m_5 a_{RA}}{m_6 - m_5 a_{RB}}$, $n_1 = A_2(\gamma_{th} - 1) + A_1$, $n_2 = A_2 \gamma_{th}$, $n_3 = m_6 - m_5 a_{RB}$, $n_4 = m_5 a_{RA}$,

$C_1 = \frac{n_2^2}{(n_2 n_3 - n_1 n_4)^2}$, $C_2 = \frac{n_2 n_4^2}{(n_2 n_3 - n_1 n_4)^2}$, $C_3 = \frac{n_4(2n_2 n_3 - n_1 n_4)}{(n_2 n_3 - n_1 n_4)^2}$, $W_1 = \frac{a_{RB} B\gamma_{th}}{a_{RA}}$,

$W_2 = \frac{n_1 B\gamma_{th}}{n_2}$, $W_3 = \frac{n_3 B\gamma_{th}}{n_4}$.

Proof: See Appendix B.

4. Throughput and Asymptotic SOPs Analysis

To better analyze this system, the end-to-end throughput for link $A \to R \to B$ and asymptotic secrecy outage probabilities are analyzed for wireless sensor networks. The end-to-end throughput is defined as

$$T_{E2E} = (1 - P_{outR})(1 - P_{outB}) R_{th} \beta \tag{38}$$

where P_{outR} and P_{outB} denote the secrecy outage probabilities of link $A \to R$ and link $R \to B$, respectively.

The channel statistics for γ_{AEA} and γ_{REA} are calculated firstly. The CDF and PDF of γ_{AEA} are given as

$$F_{\gamma_{AEA}}(y) = \Pr\left(\frac{a_{AR} d_{AE}^{-\alpha} |h_{AE}|^2}{a_{BR} d_{BE}^{-\alpha} |h_{BE}|^2} < y \right) = 1 - \frac{A_4}{A_3 y + A_4} \tag{39}$$

and

$$f_{\gamma_{AEA}}(y) = \frac{A_3 A_4}{(A_3 y + A_4)^2} \tag{40}$$

In the same way, the PDF of γ_{REA} is expressed as

$$f_{\gamma_{REA}}(y) = \sigma\left(y - \frac{a_{RB}}{a_{RA}} \right) \tag{41}$$

The CDFs of $F_{\gamma_{AR}}$ and $F_{\gamma_{RB}}$ are obtained easily as

$$F_{\gamma_{AR}}(y) = 1 - \frac{A_1}{A_1 + A_2 y} e^{-\frac{y}{A_1 \rho_A (1-\lambda)}} \tag{42}$$

and

$$F_{\gamma_{RB}}(y) = 1 - e^{-\frac{y}{a_{RB} g_{RB} d_{RB}^{-\alpha} \rho_R}} \tag{43}$$

The term P_{outR} in (38) can be obtained as

$$P_{outR}=\Pr\left(C_{AR}-C_{AEA}<R_{th}\right)=\Pr\left(\frac{1+\gamma_{AR}}{1+\gamma_{AEA}}<\gamma_{th}\right)=\int_0^{\infty}F_{\gamma_{AR}}\left(\gamma_{th}\left(1+x\right)-1\right)f_{\gamma_{AEA}}\left(x\right)dx \quad (44)$$

Substituting (40) and (42) into (44), P_{outR} can be rewritten as

$$\begin{aligned}P_{outR}=1-e^{-\frac{\gamma_{th}-1}{A_1\rho_A\left(1-\lambda\right)}}\Bigg[&-\frac{B_1e^{n_5}}{A_2\gamma_{th}}Ei\left(-n_5\right)+\frac{B_2e^{n_6}}{A_3^2}\left(\left(1+n_6\right)Ei\left(-n_6\right)+e^{-n_6}\right)\\&-\left(\frac{\gamma_{th}e^{n_6}Ei\left(-n_6\right)}{A_1\rho_A\left(1-\lambda\right)}+\frac{A_3}{A_4}\right)\frac{B_3}{A_3^2}\Bigg]\end{aligned} \quad (45)$$

where $n_5=\dfrac{n_1}{A_1A_2\rho_A\left(1-\lambda\right)}$, $n_6=\dfrac{A_4\gamma_{th}}{A_1A_3\rho_A\left(1-\lambda\right)}$.

Combining (41) and (43), the term P_{outB} in (38) can be calculated as

$$P_{outB}=\Pr\left(C_{RB}-C_{REA}<R_{th}\right)=\Pr\left(\frac{1+\gamma_{RB}}{1+\gamma_{REA}}<\gamma_{th}\right)=1-e^{-\frac{2\left(\gamma_{th}-a_{RA}\right)}{a_{RA}a_{RB}g_{RB}d_{RB}^{-\alpha}\rho_R}} \quad (46)$$

To further evaluate the network performance, the approximate SOPs of this two-step TWR-NOMA system over Rayleigh fading channel are derived under SC and MRC schemes. Because of the mathematical intractability, the asymptotic SOPs are difficult to figure out when $\rho\to\infty$. Therefore, the method of infinitesimal equivalence is applied to this paper. In high SNR region, the terms *A*, *B* are approximately 0. According to $\exp\left(x\right)\underset{x\to0}{\approx}1+x$ and $Ei\left(-x\right)\underset{x\to0}{\approx}\ln x$, the asymptotical SOPs for TWR-NOMA systems for SC scheme are shown as

$$\begin{aligned}F_{\varphi_A}^{Asy(SC)}=1-\left(1-A\left(\gamma_{th}-1\right)\right)\Big[&\left(1-\mu_2\right)\left(1-\mu_1\gamma_{th}\right)\\&+\left(1+\mu_3\gamma_{th}\right)\left(\left(1-\mu_4\gamma_{th}\right)\mu_2+\mu_3\gamma_{th}\ln\left(\mu_4\gamma_{th}\right)\right)\Big]\end{aligned} \quad (47)$$

$$\begin{aligned}F_{\varphi_B}^{Asy(SC)}=1-\left(1-B\left(\gamma_{th}-1\right)\right)\Bigg[&\frac{A_1}{\varepsilon_1\gamma_{th}+\varepsilon_2}\left(1-\frac{A_4}{\varepsilon_3}\right)\left(1-\frac{B\gamma_{th}a_{RB}}{a_{RA}}\right)-\frac{B_1}{A_2\gamma_{th}}\left(1+\varepsilon_4+B\gamma_{th}\right)\ln\left(\varepsilon_4+\frac{B\gamma_{th}}{a_{RA}}\right)+\\&\frac{\left(A_3+A_4B\gamma_{th}\right)}{A_3^3}\left(\frac{\left(A_4B_2-A_3B_3\right)Ba_{RA}\left(1-\varepsilon_5\gamma_{th}\right)}{a_{RB}A_3+a_{RA}A_4}+\frac{\left(\left(A_4B_2-A_3B_3\right)B\gamma_{th}+A_3B_2\right)\ln\left(\varepsilon_5\gamma_{th}\right)}{A_3}\right)\Bigg]\end{aligned} \quad (48)$$

Substituting (47) and (48) into (22), $SOP_{Asy}^{(SC)}$ can be expressed. From the asymptotical expression of SOPs, it can be observed that the terms *A* is approximately 0, $F_{\varphi_A}^{Asy(SC)}$ has a trend of monotonic decline when SNR increases. When the SNR is large enough, $F_{\varphi_A}^{Asy(SC)}$ is infinitely close to 0. Consequently, the approximate SOP under SC scheme is close to $F_{\varphi_B}^{Asy(SC)}$ gradually.

The asymptotical secrecy outage probabilities under MRC scheme are shown as

$$F_{\varphi_A}^{Asy(MRC)} = \frac{G_1 a_{RB}}{H_1 a_{RB} + H_1^2 a_{RA}} - \frac{m_1\left(1 - A\left(\frac{\gamma_{th}}{a_{RB}} - 1\right)\right)}{H_2 a_{RB} m_2^2} - \frac{A m_1 \gamma_{th}\left(1 - A\left(\frac{\gamma_{th}}{a_{RB}} - \frac{H_2\gamma_{th}}{a_{RB}} - 1\right)\right)}{a_{RB}^2 m_2^2} \ln\left(\frac{A H_2 \gamma_{th}}{a_{RB}}\right) \tag{49}$$

$$F_{\varphi_B}^{Asy(MRC)} = \frac{G_3 a_{RA}}{H_3 a_{RA} + H_3^2 a_{RB}} + A_1 m_4 \left[\frac{B_1}{n_2}\left(1 - B\left(\gamma_{th} - 1\right) + W_2\right)\ln\left(W_1 + W_2\right) - \frac{B_2 W_3\left(1 - B\left(\gamma_{th} - 1\right) - W_1\right)}{n_4^2\left(W_1 + W_3\right)} + \frac{a_{RA} B_3\left(1 - B\left(\gamma_{th} - 1\right) - W_1\right)}{n_4\left(a_{RB} n_4 + a_{RA} n_3\right)} - \frac{\left(B_2\left(1 + W_3\right) - B_3 B\gamma_{th}\right)}{n_4^2}\left(1 - B\left(\gamma_{th} - 1\right) + W_3\right)\ln\left(W_1 + W_3\right)\right] \tag{50}$$

Substituting (49) and (50) into (22), $SOP_{Asy}^{(MRC)}$ can be gained. From the above two expressions, we can discover that the approximate SOP under MRC scheme is approximately equal to $F_{\varphi_B}^{Asy(MRC)}$ when the SNR is very large. Another interesting finding is that there exists secrecy performance floor in this system, which mainly relies on the NOMA protocol.

5. Numerical Results

In this part, some insightful simulative and analytical results are supplied to evaluate the secrecy performance of this wireless sensor networks. The distances[1] are normalized (i.e., $d_{AR} + d_{BR} = 1$, $d_{AE} + d_{BE} = 1$) for this simulation. The derived numerical results consistent with Monte-Carlo simulations, where verifies the correctness of our research. We set values for the fixed parameters, as shown in **Table 2**.

Table 2. Parameters for numerical results

Parameter	Value
Times of Monte-Carlo simulation	10^6
Mean channel power gain for h_{AR}	$g_{AR} = 10$
Mean channel power gain for h_{BR}	$g_{BR} = 5$
Mean channel power gain for h_{RE}	$g_{RE} = 1$
Mean channel power gain for h_{AE}	$g_{AE} = 2$
Mean channel power gain for h_{BE}	$g_{BE} = 1$
Exponent for path loss	$\alpha = 3$
Noise power	$N_0 = 1$

Fig. 2 is plotted to depict SOP of this wireless sensor networks utilizing SC and MRC strategies for different target transmission rates with $d_{AR} = 0.3$, $d_{AE} = 0.6$, $d_{RE} = 0.5$, $\beta = 0.4$, $a_{AR} = 0.7$ and $a_{RA} = 0.6$. The red crosses and solid lines represent SOP of SC algorithm for two-step TWR-NOMA systems. The blue asterisks and dash lines demonstrate exact SOP of MRC algorithm. The asymptotic SOP is drawn using the black dotted line for these two schemes. In addition, the triangles in two different colors stand for SC and MRC schemes

[1] The unit of normalized distance can be m or km, depending on the network deployment. The unit m is used for indoor or hotspot deployment scenarios, and km for cellular scenarios.

without considering power splitting [39]. In order to be fair, path loss is included in the simulation of this paper. For any size of SNR, the performance of SC scheme is superior to MRC scheme at *Eve*. In addition, the secrecy performance of two schemes under $R_{th} = 0.3$ bps/Hz outperforms the SOP under $R_{th} = 0.6$ bps/Hz, respectively. Therefore, the security outage behaviors for two kinds of schemes can be affected by changing the target transmission rate of sensor nodes. As the value of target transmission rate reduces, these two schemes provide better outage performance. When compared with the system model without power splitting, it can be found that SC and MRC schemes with considering power splitting in this paper can obtain better secrecy performance, respectively. It is observed that the approximate SOPs in high SNR region overlap with accurate SOPs perfectly, but these two corresponding lines are deviated in low SNR region due to our approximation employed in high SNR regime, which also verifies the result of approximate SOPs in previous research.

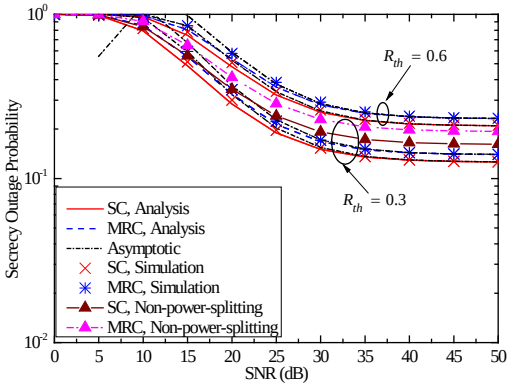

Fig. 2. SOP versus the transmit SNR with $R_{th} = 0.3$ and $R_{th} = 0.6$.

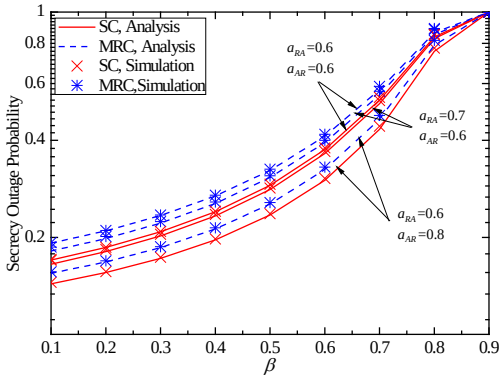

Fig. 3. SOP versus the β with different power allocation coefficients.

In **Fig. 3**, we compare the SOP of SC and MRC schemes for wireless sensor networks with different power distribution coefficients. When the time allocation parameter β becomes larger, the security performance becomes worse distinctly. This is because there is no transmission of information in the first time slot and more time is allocated to this phase, resulting in a waste of resources. Therefore, when the time allocation parameter increases, secrecy outage probability decreases significantly. Another phenomenon can be obtained obviously that the security behaviors of $a_{AR} = 0.8$ are superior to $a_{AR} = 0.6$ with the same a_{RA}. The reason for this situation is that a_{AR} is related to energy harvesting. For the strong channel link $A \to R$, the larger a_{AR} is, the more energy is collected at *R*. And the value of a_{RA} also has an effect on SOP for this model. The security performance for $a_{RA} = 0.7$ is better than $a_{RA} = 0.6$ with the same a_{AR} in this wireless sensor networks. Thus, the secure behavior can be improved by changing the value of power allocation coefficients a_{RA} and a_{AR}.

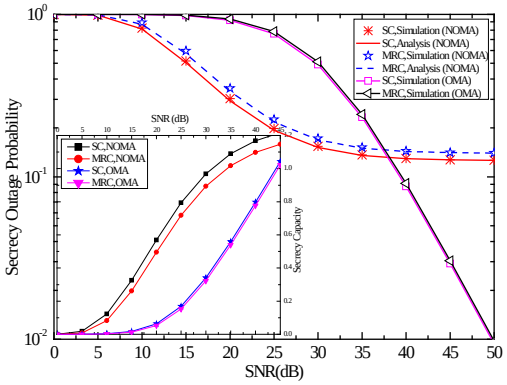

Fig. 4. SOP and secrecy capacity versus the transmit SNR with NOMA and OMA.

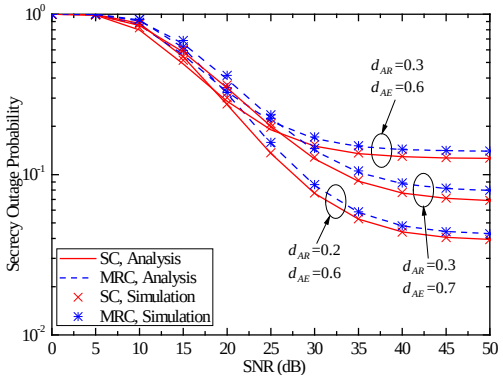

Fig. 5. SOP versus the transmit SNR with different distances.

Fig. 4 paints the SOP for TWR-NOMA systems and TWR−OMA systems under MRC and SC schemes at *Eve* with $R_{th} = 0.3$ bps/Hz. The secrecy capacity of wireless sensor networks is also described aimed at better expressing the advantages of this proposed system. For the traditional OMA systems, a complete process of information exchange requires four stages. So, comparing with the SOP of the traditional OMA systems, the NOMA systems have better performance in low and medium SNR region and higher channel capacity. The reasons for this phenomenon can be explained that the information leakage is larger in the two-way relay OMA systems in low and medium SNR region when the relay forwards signals to the respective nodes in two different stages. What's more, we can also find that secrecy performance floor appears in high SNR environments for this TWR-NOMA system because of the limit of NOMA protocol. For TWR-NOMA systems, the exchange of messages for two wireless sensor nodes can save time since it only takes two steps to complete an exchange of information, but the whole commutative process spends a long time for the traditional OMA systems.

In **Fig. 5**, secrecy outage probabilities of TWR-NOMA systems employing SC and MRC strategies at *Eve* for different distances are plotted with $a_{AR} = 0.7$, $a_{RA} = 0.6$, $R_{th} = 0.5$ bps/Hz, $d_{RE} = 0.5$, $\beta = 0.4$ and $\lambda = 0.2$. The distances for d_{AR}, d_{BR} and d_{AE}, d_{BE} are normalized. In addition, $d_{AR} < d_{BR}$ and $d_{AE} > d_{BE}$, because the link $A \to R$ has strong channel conditions, whereas the link $B \to R$ has weak channel conditions. We can observe that security performance of SC strategy is better than MRC strategy at any distance. The reason for this situation is that SC scheme is to select the maximum information eavesdropped in two time slots, while MRC scheme is to sum up the signals eavesdropped in two stages. For SC scheme, a portion of the information wiretapped is omitted, thus resulting in better security performance. It is also worth noting that altering d_{AR} and d_{AE} has a noticeable change on security performance. When the relay is close to wireless sensor node *A* or the eavesdropper is far away from wireless sensor node *A*, the security performance will be better. What's more, adjusting the distance of the link $A \to R$ has a great influence on security performance than altering the value of d_{AE}. Another phenomenon can be clearly obtained that the security behaviors for these two kinds of schemes with $d_{AE} = 0.7$ is inferior to these schemes with $d_{AE} = 0.6$ respectively when SNR < 26 dB. The security behaviors of SC and MRC schemes with $d_{AE} = 0.7$ starts enhancing and exceeds the security behaviors of these schemes with $d_{AE} = 0.6$ respectively when SNR > 26 dB. The figure also demonstrates that the SOP gets saturated due to the application of NOMA.

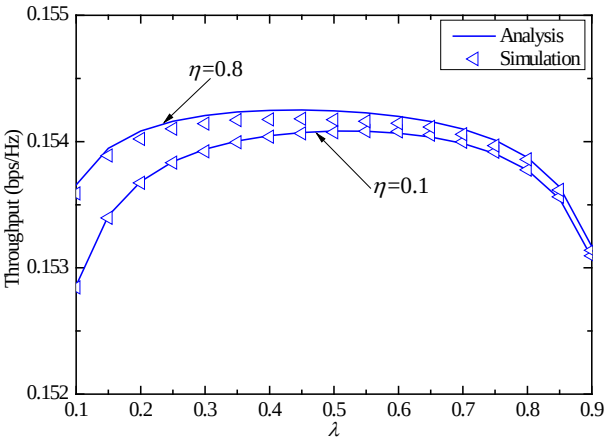

Fig. 6. Throughput versus λ with different energy conversion efficiencies η.

Fig. 6 illustrates the end-to-end throughput against the power splitting factor λ with different values of η. The blue curves indicate the accurate throughput for half-duplex based TWR-NOMA systems. The Monte-Carlo simulations are plotted using blue triangles for this systemic throughput. The lines of theoretical throughput are in accordance with the simulative results. It is evident from these curves that the throughput increases firstly and then decreases with the increasing of λ. Therefore, there exist certain value of λ that maximizes throughput. This phenomenon can be illustrated that throughput is related to P_{outR}, and the monotony of throughput is contrary to P_{outR} versus λ. In addition, as can be seen from this figure, the end-to-end throughput with $\eta = 0.8$ is superior to the throughput with $\eta = 0.1$, this phenomenon can be understood that the bigger energy conversion efficiency is, the more energy is collected at *R*. Therefore, throughput of this system can be improved by proper adjustment of transmission power.

5. Conclusion

This paper has investigated the security behaviors of this TWR-NOMA system for wireless sensor networks over independent Rayleigh distribution. The closed-form formulas of SOP and end-to-end throughput are derived employing SC and MRC schemes at eavesdropper. To better understand the performance of this system, the approximate derivations of SOP in high SNR region are also studied. The theoretical analyzes are corroborated with Monte-Carlo simulations. It is demonstrated that SC scheme can achieve the better secure performance comparing with MRC strategy at eavesdropper. Further analysis shows that when the eavesdropper keeps away from the legitimate sensor node *A* or the relay verges on node *A*, the security behaviors of this proposed TWR-NOMA systems improve. Moreover, the SOP can be enhanced by changing the value of power allocation coefficient, time allocation parameter, transmission power, and transmission rate. However, what needs illustration is that secrecy performance floors emerge for two combined strategies that cannot be eliminated because of the application of NOMA systems. The research achievements can provide a design concept for secure communication when applying to practice.

Appendix A

Proof of Theorem 1

The calculation method is similar to $F_{\varphi_A}^{(SC)}$, and the term $F_{\varphi_B}^{(SC)}$ can be obtained as

$$F_{\varphi_B}^{(SC)}(\gamma_{th}) = \int_0^{\infty} F_{\gamma_B}\left(\gamma_{th}(1+x)-1\right) f_{\gamma_{AE}}^{(SC)}(x)\,dx \tag{A.1}$$

According to the above analysis, $f_{\gamma_{AE}}^{(SC)}$ need to be derived firstly. The CDF of $\gamma_{AE}^{(SC)}$ can be obtained as

$$\begin{aligned} F_{\gamma_{AE}}^{(SC)}(y) &= \Pr\left(\max\left(\gamma_{AEA},\gamma_{REA}\right) < y\right) \\ &= \Pr\left(\gamma_{AEA} < y, \gamma_{REA} < y\right) \\ &= \left(1-\frac{A_4}{A_4+A_3 y}\right) u\left(y-\frac{a_{RB}}{a_{RA}}\right) \end{aligned} \tag{A.2}$$

Therefore, the PDF of $\gamma_{AE}^{(SC)}$ can be calculated as

$$f_{\gamma_{AE}}^{(SC)}(y) = \delta\left(y-\frac{a_{RB}}{a_{RA}}\right) - \frac{A_4}{A_4+A_3 y}\delta\left(y-\frac{a_{RB}}{a_{RA}}\right) + \frac{A_3 A_4}{\left(A_4+A_3 y\right)^2} u\left(y-\frac{a_{RB}}{a_{RA}}\right) \tag{A.3}$$

According to (24) and (A.3), $F_{\varphi_B}^{(SC)}$ is rewritten as

$$\begin{aligned} F_{\varphi_B}^{(SC)}(\gamma_{th}) &= 1 - \int_0^{\infty} \frac{A_1 e^{-B(\gamma_{th}(1+x)-1)} f_{\gamma_{AE}}^{(SC)}(x)}{A_2(\gamma_{th}(1+x)-1)+A_1}\,dx \\ &= 1 - e^{-B(\gamma_{th}-1)}\left(\frac{A_1}{\varepsilon_1\gamma_{th}+\varepsilon_2}\left(1-\frac{A_4}{\varepsilon_3}\right)e^{-\frac{B\gamma_{th}a_{RB}}{a_{RA}}} + \underbrace{\int_{\frac{a_{RB}}{a_{RA}}}^{\infty} \frac{A_1 A_3 A_4 e^{-B\gamma_{th}x}dx}{(A_2(\gamma_{th}(1+x)-1)+A_1)(A_3x+A_4)^2}}_{I_1}\right) \end{aligned} \tag{A.4}$$

where $\varepsilon_1 = A_2/a_{RA}$, $\varepsilon_2 = A_1 - A_2$, $\varepsilon_3 = A_3 a_{RB}/a_{RA} + A_4$.

Then, using factorization, the term I_1 can be calculated as

$$I_1 = \underbrace{\int_{\frac{a_{RB}}{a_{RA}}}^{\infty} \frac{B_1 e^{-B\gamma_{th}x}}{A_2(\gamma_{th}(1+x)-1)+A_1}dx}_{\theta_1} - \underbrace{\int_{\frac{a_{RB}}{a_{RA}}}^{\infty} \frac{(B_2x+B_3)e^{-B\gamma_{th}x}}{(A_3x+A_4)^2}dx}_{\theta_2} \tag{A.5}$$

where $B_1 = \frac{A_2 B_2 \gamma_{th}}{A_3^2}$, $B_2 = \frac{A_1 A_2 A_3^3 A_4 \gamma_{th}}{\left[\left(A_3-A_4\right)A_2\gamma_{th}+\left(A_1-A_2\right)A_3\right]^2}$, $B_3 = \frac{A_2 A_4^2 B_2 \gamma_{th} - A_1 A_3^3 A_4}{\left(A_2\gamma_{th}-A_2+A_1\right)A_3^2}$.

Making use of [37, eq. (3.352.2)], θ_1 can be expressed as

$$\theta_1 = \frac{B_1}{A_2\gamma_{th}} e^{\varepsilon_4 + B\gamma_{th}} Ei\left(-\varepsilon_4 - \frac{B\gamma_{th}}{a_{RA}}\right) \tag{A.6}$$

where $\varepsilon_4 = \varepsilon_2 B/A_2$.

Utilizing the substitution rule for definite integrals, $Ei(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t}dt, x<0$ [37, eq. (8.211.1)] and [37, eq. (3.351.4)], the term θ_2 can be obtained as

$$\theta_2 = \frac{1}{A_3^3} e^{\frac{A_4 B\gamma_{th}}{A_3}} \left(\frac{\left(A_4B_2 - A_3B_3\right)Be^{-\varepsilon_5\gamma_{th}}}{\varepsilon_5} + \left(\left(A_4B_2 - A_3B_3\right)B\gamma_{th} + A_3B_2\right)Ei\left(-\varepsilon_5\gamma_{th}\right)\right) \tag{A.7}$$

where $\varepsilon_5 = \left(a_{RB}/a_{RA} + A_4/A_3\right)B$.

Combining with the above formulas, $F_{\varphi_B}^{(SC)}$ can be derived.

Appendix B

Proof of Theorem 2

The term $F_{\varphi_B}^{(MRC)}$ can be obtained as

$$F_{\varphi_B}^{(MRC)}\left(\gamma_{th}\right) = \int_0^{\infty} F_{\gamma_B}\left(\gamma_{th}\left(1+x\right)-1\right) f_{\gamma_{AE}}^{(MRC)}\left(x\right)dx \tag{B.1}$$

Then, referring to the derivation of $\gamma_{BE}^{(MRC)}$, The CDF of $\gamma_{AE}^{(MRC)}$ can be given as

$$f_{\gamma_{AE}}^{(MRC)}\left(y\right) = \frac{m_4}{\left(m_6 + m_5\left(a_{RA}y - a_{RB}\right)\right)^2} \tag{B.2}$$

where $m_4 = A_3A_4a_{RA}^2$, $m_5 = A_3$, $m_6 = A_4a_{RA}$.

Combining with (24), (B.1) and (B.2), $F_{\varphi_B}^{(MRC)}$ can be calculated by using a similar method, and expressed as

$$F_{\varphi_B}^{(MRC)}(\gamma_{th}) = G_3\int_{\frac{a_{RB}}{a_{RA}}}^{\infty}\frac{1}{(1+H_3x)^2}dx - G_4\underbrace{\int_{\frac{a_{RB}}{a_{RA}}}^{\infty}\frac{e^{-B\gamma_{th}x}}{(n_1x+n_2)(n_4x+n_3)^2}dx}_{\theta_3} \tag{B.3}$$

where $G_3 = \frac{m_4}{\left(m_6 - m_5a_{RB}\right)^2}$, $G_4 = A_1m_4e^{-B(\gamma_{th}-1)}$, $H_3 = \frac{m_5a_{RA}}{m_6 - m_5a_{RB}}$, $n_1 = A_2\left(\gamma_{th}-1\right) + A_1$, $n_2 = A_2\gamma_{th}$, $n_3 = m_6 - m_5a_{RB}$, $n_4 = m_5a_{RA}$.

Then, employing [37, eq. (3.353.1)], the first term of $F_{\varphi_B}^{(MRC)}$ in (B.3) can be obtained as

$$G_3\int_{\frac{a_{RB}}{a_{RA}}}^{\infty}\frac{1}{\left(1+H_3x\right)^2}dx = \frac{G_3a_{RA}}{H_3a_{RA} + H_3^2a_{RB}} \tag{B.4}$$

Utilizing factorization, the term θ_3 can be rewritten as

$$\theta_3 = \int_{\frac{a_{RB}}{a_{RA}}}^{\infty} e^{-B\gamma_{th}x}\left(\frac{C_1}{n_1 + n_2x} - \frac{C_2x + C_3}{\left(n_3 + n_4x\right)^2}\right)dx \tag{B.5}$$

where $C_1 = \frac{n_2^2}{\left(n_2n_3 - n_1n_4\right)^2}$, $C_2 = \frac{n_2n_4^2}{\left(n_2n_3 - n_1n_4\right)^2}$, $C_3 = \frac{n_4\left(2n_2n_3 - n_1n_4\right)}{\left(n_2n_3 - n_1n_4\right)^2}$.

The expression of (B.5) can be calculated referring to [37, eq. (3.352.2)] and [37, eq. (3.353.1)], θ_3 can be obtained by

$$\begin{aligned}\theta_3 = &\frac{C_1}{n_2}\left(-e^{W_2}Ei\left(-\left(W_1+W_2\right)\right)\right) + \frac{C_2W_3e^{-W_1}}{n_4^2\left(W_1+W_3\right)} - \frac{a_{RA}C_3e^{-W_1}}{n_4\left(a_{RB}n_4 + a_{RA}n_3\right)}\\ &+\frac{e^{W_3}\left(C_2\left(1+W_3\right) - C_3B\gamma_{th}\right)}{n_4^2}Ei\left(-\left(W_1+W_3\right)\right)\end{aligned} \tag{B.6}$$

where $W_1 = \frac{a_{RB}B\gamma_{th}}{a_{RA}}$, $W_2 = \frac{n_1B\gamma_{th}}{n_2}$, $W_3 = \frac{n_3B\gamma_{th}}{n_4}$.

Finally, combining the above formulas, the closed-form expression of $F_{\varphi_B}^{(MRC)}$ is given.

References

[1] R. Chopra, C. R. Murthy, and R. Annavajjala, "Physical Layer Security in Wireless Sensor Networks Using Distributed Co-Phasing," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2662–2675, Oct. 2019. Article (CrossRef Link)

[2] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, "Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network With SWIPT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10786–10798, Dec. 2019. Article (CrossRef Link)

[3] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit Beamforming for Layered Physical Layer Security," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9747–9760, Oct. 2019. Article (CrossRef Link)

[4] H. Shi and G. Wang, "Physical Layer Security in the Untrusted EH Relay Networks with the Cooperative Jammer," in *Proc. of 2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, pp. 899–903, 2020. Article (CrossRef Link)

[5] S. Jia, J. Zhang, H. Zhao, and Y. Xu, "Performance analysis of physical layer security over --- fading channels," *China Commun.*, vol. 15, no. 11, pp. 138–148, Nov. 2018. Article (CrossRef Link)

[6] Y. Zhong, X. Ge, T. Han, Q. Li, and J. Zhang, "Tradeoff Between Delay and Physical Layer Security in Wireless Networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1635–1647, Jul. 2018. Article (CrossRef Link)

[7] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial internet of things," *China Commun.*, vol. 17, no. 1, pp. 73–88, Jan. 2020. Article (CrossRef Link)

[8] H. Li, Y. Chen, M. Zhu, J. Sun, D.-T. Do, V. G. Menon, and S. P. G., "Secrecy Outage Probability of Relay Selection Based Cooperative NOMA for IoT Networks," *IEEE Access*, vol. 9, pp. 1655–1665, Dec. 2020. Article (CrossRef Link)

[9] X. Li, M. Huang, Y. Liu, V. G. Menon, A. Paul, and Z. Ding, "I/Q Imbalance Aware Nonlinear Wireless-Powered Relaying of B5G Networks: Security and Reliability Analysis," *IEEE Trans. Network Sci. Eng.*, vol. 8, no. 4, pp. 2995-3008, 2021. Article (CrossRef Link)

[10] H. Lee, K.-J. Lee, H. Kim, and I. Lee, "Joint Transceiver Optimization for MISO SWIPT Systems with Time Switching," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3298–3312, May 2018. Article (CrossRef Link)

[11] D.-T. Do, A.-T. Le, Y. Liu and A. Jamalipour, "User Grouping and Energy Harvesting in UAV-NOMA System With AF/DF Relaying," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11855-11868, Nov. 2021. Article (CrossRef Link)

[12] Z. Ding, C. Zhong, D. Wing Kwan Ng, M. Peng, H. A. Suraweera, R. Schober, and H. V. Poor, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, Apr. 2015. Article (CrossRef Link)

[13] H. H. Jang, K. W. Choi, and D. I. Kim, "Novel Frequency-Splitting SWIPT for Overcoming Amplifier Nonlinearity," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 826–829, Jun. 2020. Article (CrossRef Link)

[14] P. V. Tuan and I. Koo, "Optimizing Efficient Energy Transmission on a SWIPT Interference Channel Under Linear/Nonlinear EH Models," *IEEE Syst. J.*, vol. 14, no. 1, pp. 457–468, Mar. 2020. Article (CrossRef Link)

[15] D.-T. Do, M.-S. Van Nguyen, M. Voznak, A. Kwasinski and J. N. de Souza, "Performance Analysis of Clustering Car-Following V2X System with Wireless Power Transfer and Massive Connections," *IEEE Internet Things J.*, pp. 1-18, Apr. 2021. Article (CrossRef Link)

[16] C. K. Singh, V. Singh, P. K. Upadhyay and M. Lin, "Energy Harvesting in Overlay Cognitive NOMA Systems With Hardware Impairments," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2648-2659, 2022. Article (CrossRef Link)

[17] S. P. Ngoc and K. H. Yun, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Commun.*, vol. 9, no. 17, pp. 2131–2139, 2015. Article (CrossRef Link)
[18] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013. Article (CrossRef Link)
[19] M. Alageli, A. Ikhlef, and J. Chambers, "SWIPT Massive MIMO Systems With Active Eavesdropping," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 233–247, Jan. 2019. Article (CrossRef Link)
[20] M.-S. Van Nguyen, D.-T. Do, S. Al-Rubaye, S. Mumtaz, A. Al-Dulaimi and O. A. Dobre, "Exploiting Impacts of Antenna Selection and Energy Harvesting for Massive Network Connectivity," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7587-7602, Nov. 2021. Article (CrossRef Link)
[21] Y. Liu, L. Wang, M. Elkashlan, T. Q. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," in *Proc. of 2014 IEEE Global Communications Conference*, Austin, TX, USA, pp. 4030–4035, Dec. 2014. Article (CrossRef Link)
[22] D. Do, T. Nguyen, K. M. Rabie, X. Li and B. M. Lee, "Throughput Analysis of Multipair Two-Way Replaying Networks With NOMA and Imperfect CSI," *IEEE Access*, vol. 8, pp. 128942-128953, Jul. 2020. Article (CrossRef Link)
[23] A. Rauniyar, P. E. Engelstad, and O. N. sterb, "On the Performance of Bidirectional NOMA-SWIPT Enabled IoT Relay Networks," *IEEE Sens. J.*, vol. 21, no. 2, pp. 2299–2315, Jan. 2021. Article (CrossRef Link)
[24] L. Shi, Y. Ye, R. Q. Hu, and H. Zhang, "System Outage Performance for Three-Step Two-Way Energy Harvesting DF Relaying," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3600–3612, Apr. 2019. Article (CrossRef Link)
[25] N. T. P. Van, S. F. Hasan, X. Gui, S. Mukhopadhyay, and H. Tran, "Three-Step Two-Way Decode and Forward Relay With Energy Harvesting," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 857–860, Apr. 2017. Article (CrossRef Link)
[26] F. Jameel, S. Wyne, and Z. Ding, "Secure Communications in Three- Step Two-Way Energy Harvesting DF Relaying," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 308–311, Feb. 2018. Article (CrossRef Link)
[27] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, "Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network With SWIPT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 786–10 798, Dec. 2019. Article (CrossRef Link)
[28] K. Lee, J.-P. Hong, H.-H. Choi, and T. Q. S. Quek, "Wireless-Powered Two-Way Relaying Protocols for Optimizing Physical Layer Security," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 162–174, Jan. 2019. Article (CrossRef Link)
[29] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Y. Chen, "Modeling and Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 3784–3796, Sep. 2018. Article (CrossRef Link)
[30] Z. Fang, S. Shen, J. Liu, W. Ni, and A. Jamalipour, "New NOMA-Based Two-Way Relay Networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15314–15324, Dec. 2020. Article (CrossRef Link)
[31] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426– 1440, Jul. 2018. Article (CrossRef Link)
[32] J. G. Proakis, *Digital Communications*, 4th ed. Boston, MA, USA: McGraw-Hill, 2001.
[33] C. K. Singh and P. K. Upadhyay, "Overlay Cognitive IoT-Based Full-Duplex Relaying NOMA Systems with Hardware Imperfections," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6578-6596, May 2022. Article (CrossRef Link)
[34] E. Soleimani-Nasab, M. Matthaiou, M. Ardebilipour, and G. K. Karagiannidis, "Two-Way AF Relaying in the Presence of Co-Channel Interference," *IEEE Trans. Commun.*, vol. 61, no. 8, pp.

3156–3169, Aug. 2013. Article (CrossRef Link)
[35] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R. Q. Hu, "Security- Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 83–96, Jan. 2019. Article (CrossRef Link)
[36] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y. Yao, "Secrecy Outage Probability Analysis of Friendly Jammer Selection Aided Multiuser Scheduling for Wireless Networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, May 2019. Article (CrossRef Link)
[37] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., Burlington, MA, USA: Elsevier, 2007.
[38] X. Li, M. Zhao, M. Zeng, S. Mumtaz, V. G. Menon, Z. Ding, and O. A. Dobre, "Hardware Impaired Ambient Backscatter NOMA Systems: Reliability and Security," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021. Article (CrossRef Link)
[39] M. K. Shukla, H. H. Nguyen and O. J. Pandey, "Secrecy Performance Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," *IEEE Access*, vol. 8, pp. 39502-39512, 2020. Article (CrossRef Link)

Hui Li received the Ph.D. degrees from information and communication engineering in 2008 in Nanjing University of Science and Technology. He is currently a Professor with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo China. His research interests include wireless communication, intelligent signal processing.

Yaping Chen received the B.Sc. degree in Henan Polytechnic University in 2019. She is currently pursuing the M.Sc. degree in the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo China. Her research interests include physical layer security, cooperative communication, and simultaneous wireless information and power transfer.

Borong Zou received the M.Sc. degree in theoretical physics from the Shanxi Normal University in 2008. Her research interests include wireless communications and intelligent signal processing.