Hardware Impaired Modify-and-Forward Relaying with Relay Selection: Reliability and Security

Noname manuscript No.
(will be inserted by the editor)

Hardware Impaired Modify-and-Forward Relaying with Relay Selection: Reliability and Security

Hongxing Peng · Hongyan Qi · Xingwang Li · Yuan Ding · Jun Wu · Varun G Menon

Received: date / Accepted: date

Abstract In this paper, we consider the physical layer security of cooperative multiple relays networks, where the source tries to communicate the destination via modify-and-forward (MF) relaying in the presence of eavesdropper. More practical, transceiver residual hardware impairments (TRHIs) and channel estimation errors (CEEs) are taken into account. To improve secure performance and energy efficiency, the $K-th$ best relay is selected since the best relay is not available due to some schedule and/or other reasons. More specifically, we investigate the reliability and security by invoking the outage probability(OP) and intercept probability(IP). To obtain more useful insights, the asymptotic behaviors for the OP are examined in the high signal-to-noise ratio (SNR) regime, followed by the diversity orders. The numeric results show that: 1) The secure performance is improved by employing MF compared with decode-and-forward (DF); 2) The reliability increases as the total number of relays increases; 3) There is an error floor for the outage probability due to the CEEs.

Keywords Modify-and-forward · physical layer security · hardware impairments · $K-th$ best relay selection

Hongxing Peng · Hongyan Qi · Xingwang Li · Jun Wu
School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454000, China
E-mail: {phx, lixingwang, wujun}@hpu.edu.cn, 311502010201@home.hpu.edu.cn

Yuan Ding
School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, Scotland, UK
E-mail: yuan.ding@hw.ac.uk

Varun G Menon
Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam, India
E-mail: varungmenon46@gmail.com

1 Introduction

With the development of Internet-of-Things (IoT) and Mobile Internets (MIN), the future beyond fifth generation (B5G) mobile communication networks will meet the demands of massive connections and ultra-reliable low-latency communications (URLLC) [1–3]. In order to achieve the above demands, secure communication has been identified as a crucial guarantee for the future wireless networks. Traditionally, secure communication is ensured by using encryption algorithms at the transmitter and decryption at the receiver. This not only imposes extra computational overhead and system complexity but also insecurity with the rapid development of computer technology. In light of this fact, Physical Layer Security (PLS) has been proposed as an effective way to ensure security of wireless communication network, which has sparked a great deal of interests from academia and industry [4, 5].

PLS, originally proposed by Wyner [6], investigated the reliable communication from the point of information theory, which has sparked a great deal of research interests [7–14]. In [7], authors derived analytical expressions for non-zero secrecy capacity and the secrecy outage probability of single-input single-output (SISO) systems over Rician/Nakagami-m fading channels. Authors in [8] focused on the PLS of single-input multiple-out (SIMO) systems, and a media-based modulation scheme was proposed. Extending multiple distributed antenna arrays, Forssell et al. proposed a new physical layer authentication approach of SIMO systems [9]. In [10], the opportunistic access point selection was used to discuss the outage performance for mobile edge computing (MEC) network, in which employed selection combining (SC) and switch-and-stay combining (SSC) two protocols. Regarding to multiple-input multiple-output (MIMO) cognitive wiretap system, Lei et al. has studied the secrecy outage probability performance of optimal antenna selection and suboptimal antenna selection schemes over Nakagami-m fading channel [11]. For MIMO system with unknown noise statistics, the authors developed a generalized maximum likelihood (ML) estimation to detect signals in [12]. For improving physical layer security, Yan et al. considered a multi-input multi-output cognitive radio (MIMO-CR) system and derived the secrecy outage probability analysis by proposed optimal antenna selection (OAS) and suboptimal antenna selection (SAS) schemes [13]. Employing the large scale antenna array can improve spectral efficiency and enhance wireless security, in [14] a large scale MIMO was introduced into the physical layer, with the purpose of tracking with the short range interception problem, the secrecy performance of amplify-and-forward (AF) and DF was analyzed.

Cooperative relaying is an effective way to provide diversity gain and enhance edge coverage. Thus, cooperative communication has received extensive research in wireless networks. In the [15], the performance of a multi-carrier cooperative underwater acoustic communication (UWAC), in which fixed features in the underwater channel, has been analyzed. Cao et al. introduced the cooperative relay technique into conventional underlay/overlay D2D communications, where proposed adaptive mode selection and spectrum allocation

schemes to ensure better performance of the cellular and D2D users [16]. With the advantage of improving network capacity, a Capacity-Optimized Cooperative topology control scheme, in which including the upper layer network capacity and the physical layer cooperative communications, has been proposed [17]. The security of cooperative communication networks has also attracted many researchers [18–20]. In a dual-hop cooperative AF relaying network, the expressions in terms of the secrecy outage probability and ergodic secrecy capacity have been derived, for the consideration, an effective secrecy diversity order has also been investigated [18]. Though small cell networks can meet the data traffic demands, it is constrained when converting between base stations. Based on this situation, the achievable sum rate, symbol error rate and outage probability in a cooperative transmission mechanism, have been explored by combining Rician/Gamma fading channels with zero-forcing receivers [19]. In the presence of an eavesdropper and co-channel interference, Vahidian et al. considered two opportunistic relay selection techniques to achieve physical layer security, where the first scheme was that the selected relay minimized the leakage information at the eavesdropper node, the second scheme was that the selected relay maximized achievable capacity of the destination node [20]. For cache-aided multi-relay networks, Xia et al. discussed secrecy outage performance in [21]. Though the multi-relay cooperative network can reduce the network complexity and improves the spatial diversity of the network, it does not make full use of the frequency band. Relay selection has been considered as an effective scheme to use frequency and ensure the secrecy and protect the source message in cooperative relay communication, which appears in rich literature [22–24]. In order to improve the PLS of cooperative wireless networks and prevent eavesdropping attacks, two protocols, where called AF and DF, were studied. Considering the existence of eavesdropping, the intercept probability expressions and the diversity order performance of relay selection was derived and evaluated, where using asymptotic intercept probability analysis [22]. Since the opportunistic relay selection has limits in the confidentiality, two scheme, where the one assumed that the eavesdropping CSI can be known at any time and the achievable secure rate can be maximized and the other one assumed a general understanding of the eavesdropper channel and was suitable for practical application, were proposed in cooperative networks [23]. Ikki et al. in [24] investigated the performance of the best-relay selection scheme in the cooperative networks, where the selected best relay needed to achieve the maximum SNR at the destination node, and also derived the expressions of the outage probability and average channel capacity. Fan et al. in [25] discussed the outage performance and optimized the cache placement with multiple amplify-and-forward relay networks, which applied the best relay. However, the best relay may not be available. The authors in [26] explored the OP and the throughput by employing a relay selection scheme, where the HIs and interference were considered. For enhancing work efficiency, Bao *et al*. adopted three opportunity relay selection schemes to analyze the PLS performance in [27].

In practice, radio frequency (RF) frond-ends are limited by some imperfections, such as residual hardware impairments (RHIs) [28,29], phase noise [30, 31], non-linear power amplify [32,33] and in-phase/quadrature phase (I/Q) imbalance [34]. For terrestrial relays that are interfered by co-channel interference (CCI), Guo *et al.* in [28] investigated outage probability (OP) and throughput performance of the considered system under HIs, where a partial relay selection scheme was used. Considering the impact of RHIs, the authors analyzed the achievable sum-rate of the unmanned aerial vehicle (UAV)-aided non-orthogonal multiple access (NOMA) multi-way in [29]. In [30], the authors focused on the analysis of average symbol error rate (ASER) by different fading scenarios, where random phase noise was considered. In [31], the authors proposed a physical layer authentication scheme of MIMO system by jointly utilizing channel and phase noise, analyzed the security, covertness, robustness of the proposed scheme, and estimated the channel gain and phase noise. Considering the high-power amplifier (HPA) non-linear, Balti *et al.* analyzed the outage probability (OP), the bit error rate, and the capacity of the cooperative relaying systems, in which the opportunistic relay selection with outdated CSI was used to select the best relay [32]. Taking the effect of the HPA, Belkacem *et al.* discussed the OP and ergodic sum rate in NOMA systems, and further explored the asymptotic OP in the high SNR region [33]. In this respect, Zhang et al. in [35] proposed four linear precoding techniques to mitigate I/Q imbalance of down-link massive MIMO systems, namely widely linear zero-forcing, widely linear matched filter, widely linear minimum mean-squared error and widely linear block-diagonalization. The security and reliability of the ambient backscatter NOMA system were studied by deriving analytical expressions for the outage probability and the intercept probability [34]. In addition, it is impossible to obtain perfect channel state information (CSI) due to channel estimation errors (CEEs) [36,5]. In [36], authors analyzed the security-reliability tradeoff of multiple DF relays networks, where the CEEs was taken into account. Li et al. in [5] investigated PLS of wireless-powered decode-and-forward (DF) multi-relay networks by joint considering non-linear energy harvesters, I/Q imbalance and CEEs.

To further improve the system secure performance, a MF protocol was originally proposed by Kim in [37], where relay first decodes the received information and then forwards the modified information to the receiver. The secure performance can be achieved that the secret can only be shared between relay and destination via unique CSI. However, eavesdropper can not decode information since the CSI of between relay and destination is not know in the eavesdropper. On this basis, the authors have investigated the PLS of MF cooperative communications [38–40]. Utilizing the principle of physical-layer-network coding, a novel secure physical layer network coding MF (SPMF) was proposed in cooperative relay network in [38], without CEEs. Compared with [38], Vien *et al.* in [39] discussed the analytical expressions for the secrecy outage probability of SPMF networks by considering both direct transmission or relaying transmission scenarios. The authors focused on the secure performance analysis of MF multi-relay and multi-eavesdropper networks, where

three relay selection criteria are considered according to the level of channel knowledge acquisition in [40], however, the RHIs was not considered.

The above studies on MF protocol security performance are based on ideal conditions, however, in real communication systems, this becomes impractical. Motivated by this, we focuses on the reliability and security performance of cooperative multi-relay networks, where the $K-th$ best relay is selected to communicate with destination by using MF protocol. In practice, RHIs and CEEs are considered. In this study, we assume that all nodes are equipped with single antenna and all links experience Rayleigh fading and path loss. Specifically, we derive the theoretical analytical expressions of outage probability and intercept probability. To get more insights, we also study the asymptotic expressions and the diversity order of the outage probability. Some research involved non-ideal HIs and imperfect CSI on DF relaying networks in [41–43]. Guo *et al*. in [41] evaluated the effect of HIs on DF multiple relaying networks, adopting switch-and-examine combining with post-selection (SECps) scheduling scheme. The authors discussed the OP with HIs in the DF terrestrial relays, where used a multi-relay selection (MRS) and single-relay selection (SRS) schemes in [42]. In [43], taking the HIs and CEEs two factors, the reliability performance for a cognitive satellite-terrestrial relay network (CSTRN) was investigated, and the half-duplex decode-and-forward (DF) mode was adopted. For the purpose of comparison, the results of DF protocol are provided. The main contributions of this paper are as follows:

- Different from the most existing works, considering RHIs and CEEs, we propose a K-th best relay selection scheme. This happens that the best relay is not available or the best relay is scheduled. Moreover, the MF protocol is considered by decoding the original information and forwarding the modified information the destination in the presence of eavesdropper.
- We investigate the reliability of the considered cooperative MF multi-relay networks by deriving the theoretical analytical expression for the outage probability. For the purpose of comparison, we consider both ideal conditions and non-ideal conditions.
- We investigate the security of the considered cooperative MF multi-relay networks by deriving the theoretical analytical expression for the intercept probability. For the purpose of comparison, the results of the considered systems with DF protocol are taken into account.
- We further study the asymptotic condition and the diversity order of the outage probability in the high signal-to-noise ratio (SNR) regime. It illustrates that outage probability has error floor at high SNRs in the presence of CEEs. It also indicates there is a tradeoff between the outage probability and the intercept probability in the presence of CEEs, RHIs. This means that the optimal can be obtained by carefully selecting parameter values.

The remainder of this paper is organized as follows. In Section 2, we present the system model of the considered networks. In section 3, we investigate the security and reliability by deriving the intercept probability and the outage probability both non-ideal conditions and ideal conditions. In section 4, we

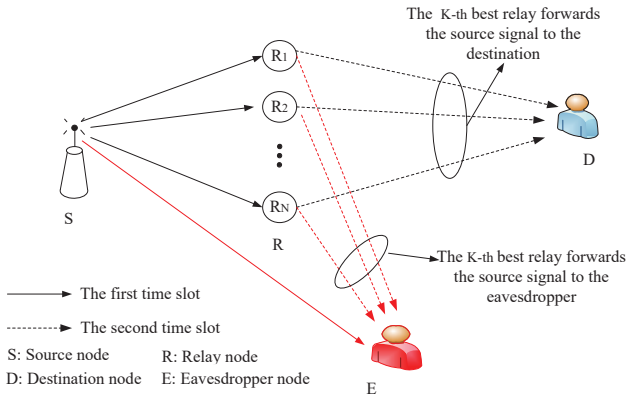

Fig. 1 Security analysis model of $K-th$ best relay selection for MF relaying

analyze and discuss the asymptotic behavior and diversity order of the outage probability under high SNRs. The numerical results are given in Section 5. Finally, the conclusions are drawn in Section 6.

2 System Model and Statistical Characteristics

We consider a cooperative MF relaying network as shown in Fig.1, which consists of one source S, one legitimate destination D, one illegitimate eavesdropper E, and N relays R_n, n=$\{1, 2, ..., N\}$. We assume that all nodes are equipped a single antenna, and the direct link between S and D is absent due to the heavy blockage [44]. For convenience, we also assume that channel coefficients about S to R_n, S to E, R_n to E, R_n to D are all marked as h_i, $i \in (SR_n, R_nD, R_nE, SE)$.

In practice, owing to CEEs, it is difficult to obtain a perfect CSI. In order to obtain CSI, some channel estimation algorithms are needed. Additionally, the path loss is also taken into account in considered networks. For this purpose, linear minimum mean square error (MMSE) is adopted [45]. Therefore, channels can be modeled as [46,47]:

$$\begin{aligned} g_i &= \frac{h_i}{\sqrt{d_i^{\alpha}}} \\ g_i &= \hat{g}_i + e_i \end{aligned} \tag{1}$$

where e_i, $i \in (SR_n, R_nD, R_nE, SE)$, is the CEE with $e_i \sim \mathcal{CN}(0, \sigma_{ei}^2)$, and $\hat{g}_i$ is the estimated channel of real channel g_i. d represents the distance from one node to another node, and α is corresponding path-loss exponent.

The whole communication process is divided into two time slots: 1) S broadcasts its own original signals x_1 to R_n and E; 2) R_n decodes and modifies

received signals from S, then sends x_2 to D and E. Here, x_2=x_1+∇x, ∇x is the difference of the the signals sent in the two time slots. For the considered MF network, in the second time slot, D and E have received modified signals, and D can recover original signals by the security key between the relays and the destination, while E cannot. This is because E has no security key between them, where the security key is the CSI of both relays and destination.

• *The first time slot:* S broadcasts signals to R_n and E with $E\left\{\left|x_{1SR_n}^2\right|\right\} = E\left\{\left|x_{1SE}^2\right|\right\} = 1$, the received signal at E, R_n can be uniformly expressed as:

$$y_{1i} = g_{1i}\left(\sqrt{P_1}x_{1i} + \eta_{t,1i}\right) + \eta_{r,1i} + n_{1i} \tag{2}$$

where P_1 is the transmit power in the first time slot. α is the path-loss exponent and d_i is the distance between nodes. $n_{1i} \sim \mathcal{CN}(0, N_0)$ is the single-sided-noise power spectral density. $\eta_{t,1i}$, $\eta_{r,1i}$ are the distortion noises of RHIs at the transmitter and the receiver, respectively. As stated in [48], the noise is defined as:

$$\eta_{t,1i} \sim \mathcal{CN}\left(0, \delta_{t,1i}^2 P_1\right), \eta_{r,1i} \sim \mathcal{CN}\left(0, \delta_{r,1i}^2 P_1 |g_{1i}|^2\right) \tag{3}$$

The power of the aggregated distortion at the receiver end is expressed as:

$$\begin{aligned} E_{\eta_{t,1i},\eta_{r,1i}} &= E\left\{\left|g_{1i}\eta_{t,1i} + \eta_{r,1i}\right|^2\right\} \\ &= g_{1i}^2 P_1 \delta_{t,1i}^2 + g_{1i}^2 P_1 \delta_{r,1i}^2 \\ &= g_{1i}^2 P_1 \left(\delta_{t,1i}^2 + \delta_{r,1i}^2\right) \end{aligned} \tag{4}$$

We can see from (4) that $\eta_{t,1i}$ and $\eta_{r,1i}$ are related to the transmission power and the channel gain g_{1i}. For the simplicity, the aggregated distortion noise can be written as η_{1i}. Thus, the received signals at E and R_n can be finally written as:

$$y_{1i} = g_{1i}\sqrt{P_1}x_{1i} + \eta_{1i} + n_{1i} \tag{5}$$

where $\eta_{1i} \sim \mathcal{CN}\left(0, \delta_{1i}^2 P_1\right)$ is the aggregated distortion noise at the transmitter and receiver with $\delta_{1i} = \sqrt{\delta_{t,1i}^2 + \delta_{r,1i}^2}$.

• *The second time slot:* the received signal at R_n is decoded and modified, then forwarded to D and E. Similarly, the received signals at D and E can be expressed as:

$$y_{2i} = g_{2i}\sqrt{P_2}x_{2i} + \eta_{2i} + n_{2i} \tag{6}$$

where $i \in (R_nD, R_nE)$, x_{2R_nD} and x_{2R_nE} are the signals sending to D and E with $E\left\{\left|x_{2R_nD}^2\right|\right\} = E\left\{\left|x_{2R_nE}^2\right|\right\} = 1$, respectively. $\eta_{2R_nE} \sim \mathcal{CN}\left(0, \delta_{2R_nE}^2 P_2\right)$, $\eta_{2R_nD} \sim \mathcal{CN}\left(0, \delta_{2R_nD}^2 P_2\right)$ are the aggregated distortion noise at the transmitter and receiver, respectively.

According to (2)−(6), the received effective signal-to-interference plus noise ratio (SINR) of the all links are expressed as:

$$\gamma_{ji} = \frac{\rho_j \left|\hat{h}_{ji}\right|^2 d_{ji}^{-a}}{\rho_j \left|\hat{h}_{ji}\right|^2 d_{ji}^{-a} \delta_{ji}^2 + \rho_j \sigma_{eji}^2 + \rho_j \sigma_{eji}^2 + \delta_{ji}^2 + 1} \tag{7}$$

where in the whole system, the signals transmissions is divided into j phases with $j \in (1, 2)$.

All channels are assumed to follow independently Rayleigh-distributed with the channel coefficients g_{ji}. $|g_{ji}|^2$ has an exponential distribution with the probability density function (PDF) and cumulative distribution function (CDF) denoted as

$$f_{|g_{ji}|^2}(x) = \frac{1}{\lambda_{ji}} e\left(-\frac{1}{\lambda_{ji}} x\right) \tag{8}$$

$$F_{|g_{ji}|^2}(x) = 1 - e\left(-\frac{1}{\lambda_{ji}} x\right) \tag{9}$$

where λ_{ji} is the expectation of channel power gain. According to Shannon's capacity formula, we can obtain the instantaneous channel capacity as:

$$C_{ji} = \frac{1}{2} \log_2 (1 + \gamma_{ji}) \tag{10}$$

where the factor $\frac{1}{2}$ can be explained that the transmission is completed in two time slots and γ_{ji} denotes the effective end-to-end SINR.

3 Reliability and Security Analysis

In this section, we study the reliability and security of the considered system in terms of the outage probability and the intercept probability, and the asymptotic analysis and the diversity orders are carried out. For comparison, the results of DF protocol are also presented in this section.

3.1 Outage Probability Analysis

According to DF protocol, the end-to-end channel capacity is the minimum of channel capacities both S to R_n and R_n to D. Thus, the expression can be presented as:

$$C_d = \min (C_{1SR_n}, C_{2R_nD}) \tag{11}$$

In the first time slot, MF is the same as DF scheme [40]. In the second time slot, DF relay first decodes the received signal and then forwards it with the same code word to both D and E, however, MF relay first decodes and modifies the received signal, and then sends the modified signal to D and E. For eavesdropper, the original information cannot be recovered from the modified information since it can not obtain the secret key between relay and destination. For destination, D can recover original information since it has the secret key between relay and itself according to the CSI between relay and destination [37]. Hence, for considered MF scheme in the whole transmission system, the signals sent in the two time slots are different, while the signals are the same for considered DF scheme.

In this work, a relay is selected based on $K-th$ the maximum minimum criteria [49], thus the instantaneous capacity for S to R_n and R_n to D link can be expressed as:

$$C_I = K^{th} \max_{n=1,2,\ldots,N} \min \left(C_{1SR_n}, C_{2R_nD} \right) \tag{12}$$

Outage probability: For a given threshold C_T, an interrupt event occurs when C_I is lower than C_T. The expression of outage probability can be presented as:

$$P_{out} = P_r \left(C_I < C_T \right) \tag{13}$$

Theorem 1 *For non-ideal conditions, the expression for OP is presented in (14), where* $\psi = \frac{(2^{2C_T}-1)(\rho_1\sigma^2_{e1SR_n}+\rho_1\sigma^2_{e1SR_n}\delta^2_{1SR_n}+1)}{\rho_1 \mathrm{d}^{-a}_{1SR_n} - \rho_1 \mathrm{d}^{-a}_{1SR_n}\delta^2_{1SR_n}(2^{2C_T}-1)}$,
$\upsilon = \frac{(2^{2C_T}-1)(\rho_2\sigma^2_{e2R_nD}+\rho_2\sigma^2_{e2R_nD}\delta^2_{2R_nD}+1)}{\rho_2 \mathrm{d}^{-a}_{2R_nD} - \rho_2 \mathrm{d}^{-a}_{2R_nD}\delta^2_{2R_nD}(2^{2C_T}-1)})$. *For ideal conditions, i.e.,* $\delta^2_{ji} = \sigma^2_{eji} = 0$, *the expression of OP is written in (15).*

$$P_{out} = \sum_{k=1}^{K} \binom{N}{k-1} \left(1 - e^{-\frac{1}{\lambda_{1SR_n}}(\psi)} \times e^{-\frac{1}{\lambda_{2R_nD}}(\upsilon)}\right)^{N-k+1} \times \left(e^{-\frac{1}{\lambda_{1SR_n}}(\psi)} \times e^{-\frac{1}{\lambda_{2R_nD}}(\upsilon)}\right)^{k-1} \tag{14}$$

and

$$P_{out} = \sum_{k=1}^{K} \binom{N}{k-1} \left(1 - e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}} + \frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)}\right)^{N-k+1} \times \left(e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}} + \frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)}\right)^{k-1} \tag{15}$$

Proof : See Appendix A.

Remark 1: We observe the OP under non-ideal conditions and ideal conditions are obtained from (14) and (15) for $\delta^2_{1SR_n} < \frac{1}{2^{2C_T}-1}$, $\delta^2_{2R_nD} < \frac{1}{2^{2C_T}-1}$, otherwise, the OP under non-ideal conditions and ideal conditions is equal to 1. We also observe that reliability performance is related to the number of relays, fading parameters and rate threshold. In addition, MF has the same maximum rate as DF.

3.2 Intercept Probability Analysis

This subsection studies the security of the considered network with MF and DF in terms of IP, where RHIs and CEEs are taken into account.

Intercept probability: For a given threshold C_T, IP is defined that the channel capacity at E is greater than the threshold C_T and it can be expressed as:

$$P_{\text{int}} = P_r\left(C_E > C_T\right) \tag{16}$$

where C_E represents the capacity on the eavesdropping.

The IP under MF protocol: Two signals are received at E, one modified by R and one sent by S. Since E does not know the key, the eavesdropping probability only needs to consider the message sent by S.

Theorem 2 *For non-ideal conditions, i.e.,*$\delta_{ji}^2 \neq 0, \sigma_{eji}^2 \neq 0$*, and for ideal conditions, i.e.,* $\delta_{ji}^2 = \sigma_{eji}^2 = 0$*, the expressions of IP under MF are given in (17) and (18), respectively.*

$$P_{\text{int}}=e^{-\frac{1}{\lambda_{1SE}}\frac{(2^{2C_T}-1)(\rho_1\sigma_{e1SE}^2+\rho_1\sigma_{e1SE}^2\delta_{1SE}^2+1)}{\rho_1 \mathrm{d}_{1SE}^{-a}-\rho_1 \mathrm{d}_{1SE}^{-a}\delta_{1SE}^2(2^{2C_T}-1)}} \tag{17}$$

$$P_{\text{int}}=e^{-\frac{1}{\lambda_{1SE}}\frac{2^{2C_T}-1}{\rho_1}} \tag{18}$$

The IP under DF protocol: Unlike MF scheme, for IP, the capacity of S to E and R_n to E need to be considered. For C_{SE} and C_{R_nE}, Selection Combing (SC) protocol is adopted,i.e.,

$$C_e = \max(C_{1SE}, C_{2R_nE}) \tag{19}$$

And the IP can be expressed as [49]:

$$P_{\text{int}} = P_r\left(C_e > C_T\right) \tag{20}$$

Theorem 3 *For non-ideal conditions, i.e.,*$\delta_{ji}^2 \neq 0, \sigma_{eji}^2 \neq 0$*, and for ideal conditions, i.e.,* $\delta_{ji}^2 = \sigma_{eji}^2 = 0$*, the expressions of IP under DF are written as (21) and (22), respectively.*

$$\begin{aligned} P_{\text{int}}= 1 &- \left(1 - e^{-\frac{1}{\lambda_{1SE}}\frac{(2^{2C_T}-1)(\rho_1\sigma_{e1SE}^2+\rho_1\sigma_{e1SE}^2\delta_{1SE}^2+1)}{\rho_1 \mathrm{d}_{1SE}^{-a}-\rho_1 \mathrm{d}_{1SE}^{-a}\delta_{1SE}^2(2^{2C_T}-1)}}\right) \\ &\times \left(1 - e^{-\frac{1}{\lambda_{2R_nE}}\frac{(2^{2C_T}-1)(\rho_2\sigma_{e2R_nE}^2+\rho_2\sigma_{e2R_nE}^2\delta_{2R_nE}^2+1)}{\rho_2 \mathrm{d}_{2R_nE}^{-a}-\rho_2 \mathrm{d}_{2R_nE}^{-a}\delta_{2R_nE}^2(2^{2C_T}-1)}}\right) \end{aligned} \tag{21}$$

$$P_{\text{int}}= 1 - \left(1 - e^{-\frac{1}{\lambda_{1SE}}\frac{2^{2C_T}-1}{\rho_1}}\right)\left(1 - e^{-\frac{1}{\lambda_{2R_nE}}\frac{2^{2C_T}-1}{\rho_2}}\right) \tag{22}$$

Proof : See Appendix B.

Remark 2: We find that when $\delta_{1SE}^2 < \frac{1}{2^{2C_T}-1}$ and $\delta_{2R_n\mathrm{E}}^2 < \frac{1}{2^{2C_T}-1}$, the IPs for the two cases are derived as (22) and (23), otherwise IP is equal to 1. We also find that the IP is not affected by the number of the realys, i.e., the security performance can not be improved by increasing or decreasing the number of relays.

4 Asymptotic Analysis and Diversity Order

To obtain useful insights, we investigate the asymptotic analysis and the diversity order of the OP.

4.1 Asymptotic Analysis

Corollary 1: At high SNRs, the asymptotic expressions of OP under the non-ideal case and ideal case are given as [50],

$$P_{out}^{\infty,ni} \approx \sum_{k=1}^{K} \binom{N}{k-1} (1-\tau)^{N-k+1} (\tau)^{k-1} \tag{23}$$

$$P_{out}^{\infty,id} \approx \binom{N}{K} \left(\frac{1}{\rho_1} \frac{2^{2C_T}-1}{\lambda_{1SR_n}} + \frac{1}{\rho_2} \frac{2^{2C_T}-1}{\lambda_{2R_nD}} \right)^{N-K} \tag{24}$$

Proof : See Appendix C.

Remark 3: We can observe the asymptotic behaviours of OP from Corollary 1: for non-ideal case, we see the asymptotic is a constant when SNR is in the high region; for ideal case, we can find the asymptotic OP varies with SNR.

4.2 Diversity Order Analysis

To gain further insights, we explore diversity order for OP, which defined as [51]:

$$\Delta = -\lim_{\rho \to 0} \frac{\log P_{out}^{\infty}}{\log \rho} \tag{25}$$

where ρ is the average transmit SNR and P_{out}^{∞} is the asymptotic analytical expression of OP.

Corollary 2: when $\rho_j \to \infty$, the diversity order under the non-ideal case and ideal case are written as, respectively

$$\begin{aligned} \Delta^{ni} &= -\lim_{\rho\to 0} \frac{\log P_{out}^{\infty,ni}}{\log \rho} = 0 \\ \Delta^{id} &= -\lim_{\rho\to 0} \frac{\log P_{out}^{\infty,id}}{\log \rho} = N - K \end{aligned} \tag{26}$$

Remark 4: Based on the definition of the diversity order, we have the following insights: 1) The diversity order for non-ideal case is zero due to fixed OP as the SNR grows to infinity. This means that at high SNR, the diversity order is irrelevant to system and fading parameters; 2) The diversity order for ideal case is a non-zero constant as the SNR grows to infinity. This means that the diversity order depends on the number of relay and the selected number.

5 Numerical Results and Discussion

In this section, we present the analytical and simulation results to verify our analysis in Sections 3 and 4. In all evaluations, unless otherwise explicitly specified, we assume that the parameters of those results are set as follows: $\sigma_{eji}^2 = \sigma_e^2$, $\alpha = 3$. Moreover, Monte-Carlo simulations have been conducted with 10^4 channels trials.

Fig.2 plots the OP and IP versus the average transmit SNR under the ideal and non-ideal conditions. We set N=6, K=2, $C_T = 0.5$, $\sigma_e^2 = 0.3$, δ_i= 0.15, $d_{1SR_n} = 1$, $d_{2R_nD} = 0.5$, $d_{2R_nE} = 0.5, d_{1SE} = 1$. Firstly, both MF and DF protocols have the same OP, while MF has better IP performance than DF. This means that the considered protocol can enhance the security without compromising reliability. In addition, we can also conclude that there exist error floors for the OP of the two protocols due to the fixed CEEs. Moreover, although distortion noise is deleterious to the OP of the considered networks, it can improve the security performance. Finally, it can be seen that the OP for the ideal case is lower than that in the non-ideal case, which indicates that the reliability performance is limited by the imperfect factors.

Fig.3 depicts the OP and IP versus the average transmit SNR for different numbers of better relays and the distance between the nodes. We set N=4, $C_T = 0.5$, $\sigma_e^2 = 0.1$, δ_{1SE}= 0.15, $\delta_{1SR_n} = \delta_{2R_nD}$=$\delta_{2R_nE}$= 0.1, $d_{1SR_n} = 1$, $d_{2R_nD} = 0.5$, $d_{2R_nE} = 0.5, d_{1SE} = 1$. It shows that the OP performance is better as K is smaller, while IP has no change as d=0.5, K=$\{1, 2, 3\}$. When K=2, d=$\{0.5, 0.8\}$, we can observe that the OP increases with the increase of d, while the IP decreases. Finally, it is shown that there is a tradeoff between reliability and security.

Fig.4 shows the OP and IP versus the average transmit SNR for different path-loss exponent and channel estimation errors (CEEs). We set N=4, K=2, C_T=0.5, $\sigma_e^2 = 0.1$, δ_{1SE}= 0.15, $\delta_{1SR_n} = \delta_{2R_nD}$=$\delta_{2R_nE}$= 0.1, $d_{1SR_n} = 1$,

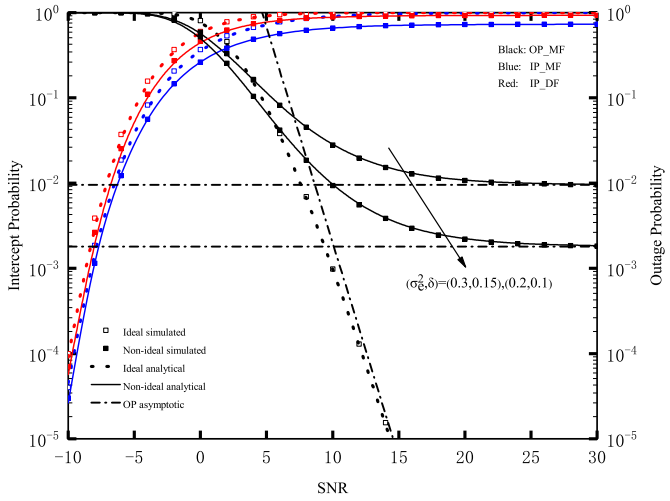

Fig. 2 OP and IP versus SNR under non-ideal and ideal case

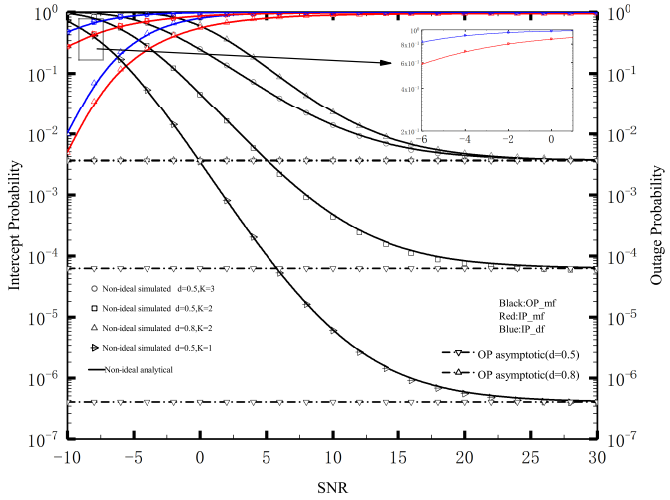

Fig. 3 OP and IP versus SNR for difference K and d ($d_{2R_nD} = d_{2R_nE} = d_{1SE} = d_{1SR_n} = d$)

$d_{2R_nD} = 0.5$, $d_{2R_nE} = 0.5, d_{1SE} = 1$. As can be seen that the OP increases as σ_e^2 grows and there exists an error floor under the non-ideal case. It can also be observed that CEEs have positive effects on the IP of the considered systems. When σ_e^2 is 0.3, IP is directly proportional to α, while OP is inversely proportional to α. No matter how the parameters change, IP under MF protocol is always lower than that under the DF protocol. This means that the considered protocol can enhance the security. Fig.5 presents that the OP versus the transmit SNR for different number of relays (N = 4, 5, 6) in the presence of

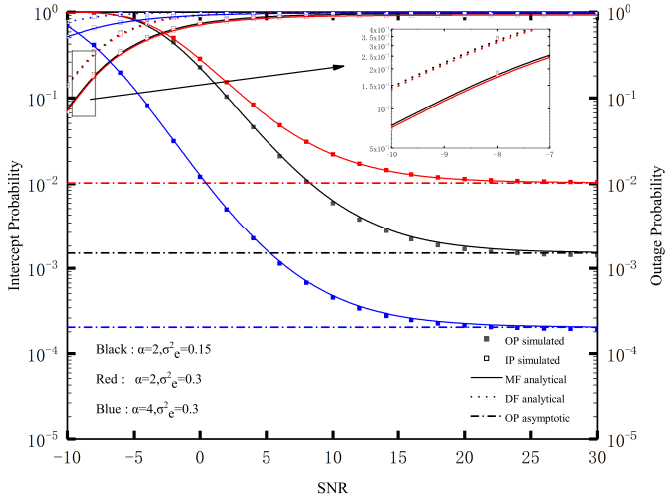

Fig. 4 OP and IP versus SNR for difference α and σ_e^2

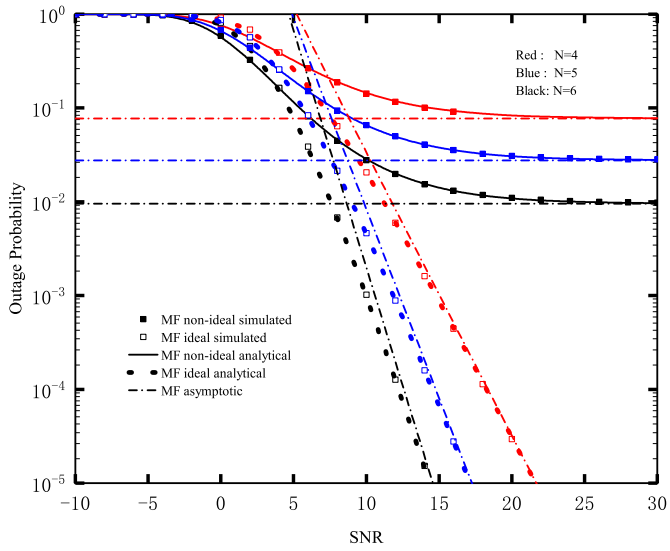

Fig. 5 OP versus SNR for different N

non-ideal and ideal conditions. We set K=2, σ_e^2 =0.3, C_T = 0.5, d_{1SR_n} = 1, d_{2R_nD} = 0.5, δ_{1SR_n}= 0.1, δ_{2R_nD}= 0.1. From Fig.5, we can conclude that the OP decreases as the number of relays increases. This means that the gain is proportional to the number of relays. Moreover, OP decreases linearly as the transmit SNR increase in the presence of ideal conditions.

Fig.6 shows the IP versus the transmit SNR for different values of σ_e^2. We set N=4, K=2, C_T=0.5, δ_{1SE}= 0.15, δ_{1SR_n} = δ_{2R_nD}=δ_{2R_nE}= 0.1, d_{2R_nE} =

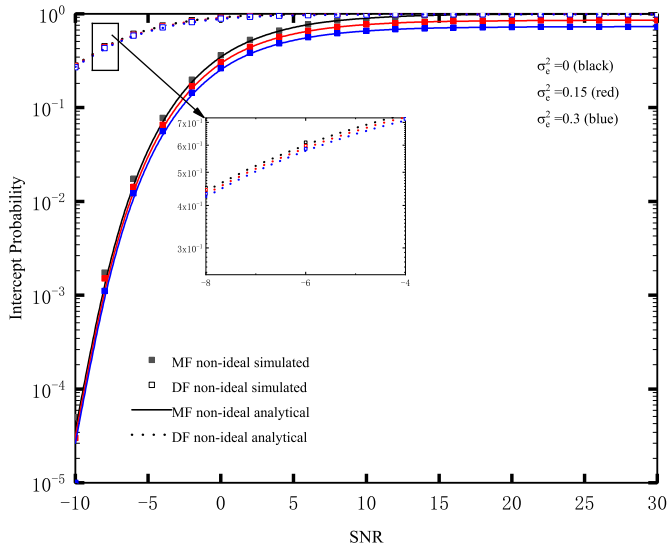

Fig. 6 IP versus SNR for different σ_e^2

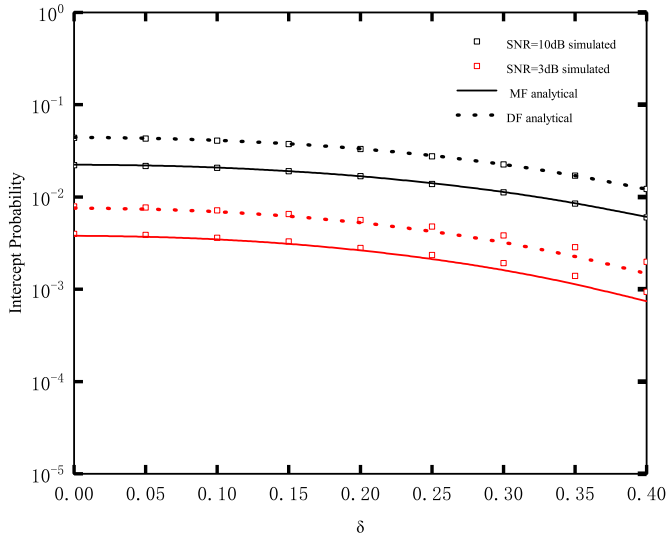

Fig. 7 IP versus δ for different SNR (δ_{1SE}=$\delta_{2R_nE} = \delta$)

0.5, $d_{1SE} = 1$. It can be observed that the effect of CEEs on the IP is relatively small, which means that the differences of IP among the three CEEs values can be ignored in high and low SNR regions. From Fig.6, we also have the following conclusions: 1) The considered MF protocol can significantly improve the security; 2) CEEs have positive effects on the IP of the considered systems.

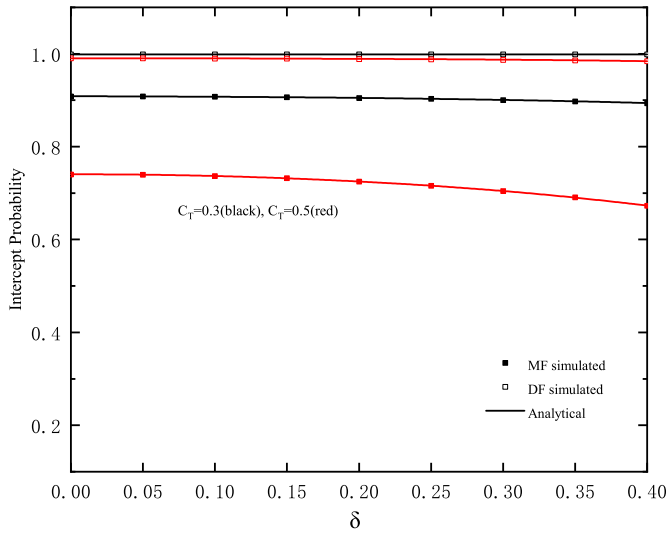

Fig. 8 IP versus δ for different C_T

In Fig.7, IP is plotted versus the RHIs for different averaged transmit SNR values. We set N=4, K=2, $C_T = 0.5$, σ_{e}^2 =0.3, $d_{2R_nE} = 0.5, d_{1SE} = 1$. From Fig.7, we can conclude that the ability to resist eavesdropping is enhanced with the increase of δ for both MF and DF. This also shows that MF protocol has better security than DF.

Fig.8 illustrates the IP versus distortion noise parameter for different C_T. N=4, K=3, σ_{e}^2 =0.2, $d_{2R_nE} = 0.5, d_{1SE} = 1$. We can observe that the IP decreases with the increase of C_T for both MF scheme and DF scheme, and we can also observe that IP is inversely proportional to hardware impairments. This means that the security can be enhanced by the increase of distortion noise.

6 Conclusion

In this paper, we consider the reliability and security of multi-relay networks by presenting a new MF protocol, where the two factors of RHIs and CEEs are taken into account. Specifically, the exact expressions of the OP and IP have been derived. Numerical results reveal that: (i) the MF is effective for system security compared with the DF; (ii) the Kth (Kth >1) best relay selection schemes can solve the best relay unavailable. (iii) RHIs and CEEs have detrimental impact on reliability; and (v) there exists error floors for the OP due to the CEEs.

Appendix A: Proof of Theorem 1

For non-ideal condition, we set $\delta_{ji}^2 \neq 0, \sigma_{eji}^2 \neq 0$, the proof starts by simplifying (13) to the following form as

$$\begin{aligned} P_{out} &= P_r\left(C_I < C_T\right) \\ &= P_r\left(\underset{n=1,2,\ldots,N}{K^{th}\max\min}\left(C_{1SR_n}, C_{2R_nD}\right) < C_T\right) \\ &= \sum_{k=1}^{K}\binom{N}{k-1}\left(\underbrace{P_r(\min(C_{1SR_n}, C_{2R_nD}) < C_T)}_{I_1}\right)^{N-k+1} \\ &\times \left(\underbrace{1 - P_r(\min(C_{1SR_n}, C_{2R_nD}) < C_T)}_{I_2}\right)^{k-1} \end{aligned} \tag{A.1}$$

where the whole calculation is divided into two parts, ie., I_1 and I_2. Firstly, I_1 can be represented as follows:

$$I_1 = 1 - \underbrace{P_r(Y_{1SR_n} \geq 2^{2C_T} - 1)}_{I_3}\underbrace{P_r(Y_{2R_nD} \geq 2^{2C_T} - 1)}_{I_4}. \tag{A.2}$$

From (A.2), it can be seen that I_1 is composed of I_3 and I_4. Next, we calculate I_3 and I_4, respectively.

$$I_3 = e^{-\frac{(2^{2C_T}-1)(\rho_1\sigma_{e1SR_n}^2 + \rho_1\sigma_{e1SR_n}^2\delta_{1SR_n}^2 + 1)}{\rho_1 \mathrm{d}_{1SR_n}^{-a} - \rho_1 \mathrm{d}_{1SR_n}^{-a}\delta_{1SR_n}^2(2^{2C_T}-1)}} \tag{A.3}$$

$$I_4 = e^{-\frac{(2^{2C_T}-1)(\rho_2\sigma_{e2R_nD}^2 + \rho_2\sigma_{e2R_nD}^2\delta_{2R_nD}^2 + 1)}{\rho_2 \mathrm{d}_{2R_nD}^{-\alpha} - \rho_2 \mathrm{d}_{2R_nD}^{-\alpha}\delta_{2R_nD}^2(2^{2C_T}-1)}}) \tag{A.4}$$

Substituting both (A.3) and (A.4) into (A.2), I_1 can be written as:

$$\begin{aligned} \psi &= \frac{(2^{2C_T}-1)(\rho_1\sigma_{e1SR_n}^2 + \rho_1\sigma_{e1SR_n}^2\delta_{1SR_n}^2 + 1)}{\rho_1 \mathrm{d}_{1SR_n}^{-a} - \rho_1 \mathrm{d}_{1SR_n}^{-a}\delta_{1SR_n}^2(2^{2C_T}-1)} \\ \upsilon &= \frac{(2^{2C_T}-1)(\rho_2\sigma_{e2R_nD}^2 + \rho_2\sigma_{e2R_nD}^2\delta_{2R_nD}^2 + 1)}{\rho_2 \mathrm{d}_{2R_nD}^{-a} - \rho_2 \mathrm{d}_{2R_nD}^{-a}\delta_{2R_nD}^2(2^{2C_T}-1)}) \\ I_1 &= 1 - e^{-\frac{1}{\lambda_{1SR_n}}(\psi)} \times e^{-\frac{1}{\lambda_{2R_nD}}(\upsilon)} \end{aligned} \tag{A.5}$$

Then, I_2 also can be obtained, it can be calculated as:

$$I_2 = e^{-\frac{1}{\lambda_{1SR_n}}(\psi)} \times e^{-\frac{1}{\lambda_{2R_nD}}(\upsilon)} \tag{A.6}$$

Substituting between (A.5) and (A.6) into (13), we can get the expression of (14), and we can obtain the expression of (15) by setting $\delta_{ji}^2 = \sigma_{eji}^2 = 0$. Then, we can get the proof for Theorem 1.

Appendix B: Proof of Theorem 3

We first simply (20), and then the (20) is presented as following:

$$\begin{aligned} P_{\text{int}} &= P_r\left(C_e > C_T\right) \\ &= P_r\left(\max(C_{1SE}, C_{2R_nE}) > C_T\right) \\ &= 1 - P_r\left(C_{2R_nE} \le C_T\right) P_r\left(C_{1SE} \le C_T\right) \end{aligned} \tag{B.1}$$

Substituting (9) and (10) into (B.1), then (21) and (22) can be obtained, respectively. And we can get the proof of Theorem 3.

Appendix C: Proof of Corollary 1

For OP in the non-ideal case, we first simplify (14) with SNR is in high region, and the expression of OP is written as follows:

$$\begin{aligned} P_{out}^{\infty,ni} &= \sum_{k=1}^{K} \binom{N}{k-1} \left(1-\tau e^{-\mu}\right)^{N-k+1} \times \left(\tau e^{-\mu}\right)^{k-1} \\ \xi_1 &= \frac{2^{2C_T}-1}{\mathrm{d}_{1SR_n}^{-a} - \mathrm{d}_{1SR_n}^{-a}\delta_{1SR_n}^2(2^{2C_T}-1)} \\ \xi_2 &= \frac{2^{2C_T}-1}{\mathrm{d}_{2R_nD}^{-a} - \mathrm{d}_{2R_nD}^{-a}\delta_{2R_nD}^2(2^{2C_T}-1)} \\ \mu &= \xi_1 \frac{1}{\lambda_{1SR_n}\rho_1} + \xi_2 \frac{1}{\lambda_{2R_nD}\rho_2} \\ \xi_3 &= \frac{\sigma_{e1SR_n}^2 + \sigma_{e1SR_n}^2\delta_{1SR_n}^2}{\mathrm{d}_{1SR_n}^{-a} - \mathrm{d}_{1SR_n}^{-a}\delta_{1SR_n}^2(2^{2C_T}-1)} \\ \xi_4 &= \frac{\sigma_{e2R_nD}^2 + \sigma_{e2R_nD}^2\delta_{2R_nD}^2}{\mathrm{d}_{2R_nD}^{-a} - \mathrm{d}_{2R_nD}^{-a}\delta_{2R_nD}^2(2^{2C_T}-1)} \\ W &= \xi_3 \frac{2^{2C_T}-1}{\lambda_{1SR_n}} + \xi_4 \frac{2^{2C_T}-1}{\lambda_{2R_nD}} \end{aligned} \tag{C.1}$$

where $\tau = e^{-W}$, its obvious that $\rho_j \to \infty$,i.e., $\mu \to 0$ and $e^{-\mu} \to 1$. Thus, the asymptotic expressions of OP with the non-ideal case can be presented in equation (23).

For OP in the ideal case, similarly, $e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)} \to 1$ is approximately equal to 1. Thus, we can derive the following formula:

$$\begin{aligned}
P_{out}^{\infty,id} &\approx \sum_{k=1}^{K}\binom{N}{k-1}\left(1-e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)}\right)^{N-k+1} \\
&\quad\times\left(e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)}\right)^{k-1} \\
&\approx \sum_{k=1}^{K}\binom{N}{k-1}\left(1-e^{-\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)}\right)^{N-k+1} \\
&\approx \sum_{k=1}^{K}\binom{N}{k-1}\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)^{N-k+1} \\
&\approx \binom{N}{K}\left(\frac{1}{\rho_1}\frac{2^{2C_T}-1}{\lambda_{1SR_n}}+\frac{1}{\rho_2}\frac{2^{2C_T}-1}{\lambda_{2R_nD}}\right)^{N-K}
\end{aligned} \tag{C.2}$$

After the approximate calculation, we can get the asymptotic expressions of OP with the ideal case.

References

1. Wu. Y, Gao. X, Zhou. S, Yang. W, Polyanskiy. Y and Caire. G, "Massive Access for Future Wireless Communication Systems," in IEEE Wireless Communications, vol. 27, no. 4, pp. 148-156, August 2020.
2. Sutton. G. J, Zeng. J, Liu. R. P, Ni. W, Nguyen. D. N, Jayawickrama. B. A, Huang. X, Abolhasan. M, Zhang. Z, Dutkiewicz. E, and Lv. T, "Enabling technologies for ultra-reliable and low latency communications: From PHY and MAC layer perspectives," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2488C2524, 3rd Quart., 2019.
3. Li Xingwang, Wang Qunshu, Liu Meng, Li Jingjing, Peng Hongxing, Piran Md Jalil, Li Lihua, "Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks with Hardware Impairments and Channel Estimation Errors, " IEEE Internet of Things Journal, 2020. 10.1109/JIOT.2020.3029754
4. Cao. K et al., "Improving Physical Layer Security of Uplink NOMA via Energy Harvesting Jammers," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 786-799, 2021.
5. Li Xingwang, Huang Mengyan, Liu Yuanwei, Menon Varun G, Paul Anand, Ding Zhiguo, "I/Q Imbalance Aware Nonlinear Wireless-Powered Relaying of B5G Networks: Security and Reliability Analysis," IEEE Transactions on Network Science and Engineering, pp. 1-1, Aug. 2020.
6. Wyner. A. D, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
7. Iwata. S, Ohtsuki. T and Kam. P. -, "Performance Analysis of Physical Layer Security over Rician/Nakagami-m Fading Channels," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, pp. 1-6, 2017.
8. Mao. T and Wang. Z, "Physical-Layer Security Enhancement for SIMO-MBM Systems," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, pp. 1-6, 2018.

9. Forssell. H, Thobaben. R and Gross. J, "Performance Analysis of Distributed SIMO Physical Layer Authentication," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, pp. 1-6, 2019.
10. Xia. J et al., "Opportunistic Access Point Selection for Mobile Edge Computing Networks," in IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 695-709, Jan. 2021.
11. Lei. H et al., "Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems Over Nakagami- m Channels," in IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2237-2250, March 2017.
12. He. K, He. L, "Learning based signal detection for MIMO systems with unknown noise statistics," IEEE Trans. Commun. no. 99, pp. 1-12, 2021.
13. Yan. P, Zou. Y and Zhu. J, "Transmit antenna selection to improve physical layer security for MIMO-CR systems," 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, pp. 1-4, 2016.
14. Chen. X, Lei. L, Zhang. H and Yuen. C, "Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?," in IEEE Transactions on Wireless Communications, vol. 14, no. 9, pp. 5135-5146, Sept. 2015.
15. Al-Dharrab. S, Uysal. M and Duman. T. M, "Cooperative underwater acoustic communications [Accepted From Open Call]," in IEEE Communications Magazine, vol. 51, no. 7, pp. 146-153, July 2013.
16. Cao. Y, Jiang. T and Wang. C, "Cooperative device-to-device communications in cellular networks," in IEEE Wireless Communications, vol. 22, no. 3, pp. 124-129, June 2015.
17. Guan. Q, Yu. F. R, Jiang. S, Leung. V. C. M and Mehrvar. H, "Topology control in mobile Ad Hoc networks with cooperative communications," in IEEE Wireless Communications, vol. 19, no. 2, pp. 74-79, April 2012.
18. Pandey. A and Yadav. S, "Physical Layer Security in Cooperative AF Relaying Networks With Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," in IEEE Transactions on Vehicular Technology, vol. 67, no. 11, pp. 10615-10630, Nov. 2018.
19. Li. X, Li. J, Li. L, Du. L, Jin. J and Zhang. D, "Performance analysis of cooperative small cell systems under correlated Rician/Gamma fading channels," in IET Signal Processing, vol. 12, no. 1, pp. 64-73, 2 2018.
20. Vahidian. S, Aissa. S and Hatamnia. S, "Relay Selection for Security-Constrained Cooperative Communication in the Presence of Eavesdropper's Overhearing and Interference," in IEEE Wireless Communications Letters, vol. 4, no. 6, pp. 577-580, Dec. 2015.
21. Xia. J et al., "Secure Cache-Aided Multi-Relay Networks in the Presence of Multiple Eavesdroppers," in IEEE Transactions on Communications, vol. 67, no. 11, pp. 7672-7685, Nov. 2019.
22. Zou. Y, Wang. X and Shen. W, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099-2111, October 2013.
23. Krikidis. I, "Opportunistic relay selection for cooperative networks with secrecy constraints," in IET Communications, vol. 4, no. 15, pp. 1787-1791, 15 Oct. 2010.
24. Ikki. S and Ahmed. M. H, "Performance analysis of adaptive decode-and-forward cooperative diversity networks with best-relay selection," in IEEE Transactions on Communications, vol. 58, no. 1, pp. 68-72, January 2010.
25. Fan. L, Zhao. N, Lei. X, Chen. Q, Yang. N and Karagiannidis. G. K, "Outage Probability and Optimal Cache Placement for Multiple Amplify-and-Forward Relay Networks," in IEEE Transactions on Vehicular Technology, vol. 67, no. 12, pp. 12373-12378, Dec. 2018.
26. Guo. K et al.,"Performance Analysis of Hybrid Satellite-Terrestrial Cooperative Networks With Relay Selection," in IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 9053-9067, Aug. 2020.
27. Bao. V. N. Q, Linh-Trung. N, and Debbah. M, "Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers," in IEEE Transactions on Wireless Communications, vol. 12, no. 12, pp. 6076-6085, December 2013.
28. Guo. K et al., "On the Performance of the Uplink Satellite Multiterrestrial Relay Networks With Hardware Impairments and Interference," in IEEE Systems Journal, vol. 13, no. 3, pp. 2297-2308, Sept. 2019.

29. Li. X, Wang. Q, Liu. Y, Tsiftsis.T. A, Ding. Z and Nallanathan. A, "UAV-Aided Multi-Way NOMA Networks With Residual Hardware Impairments," in IEEE Wireless Communications Letters, vol. 9, no. 9, pp. 1538-1542, Sept. 2020.
30. Silva. P. E. G, de Souza. R. A. A, da Costa. D. B, Moualeu. J. M and Yacoub. M. D, "Error Probability of M-Phase Signaling With Phase Noise Over Fading Channels," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6766-6770, June 2020.
31. Zhang. P, Shen. Y, Jiang. X and Wu. B, "Physical Layer Authentication Jointly Utilizing Channel and Phase Noise in MIMO Systems," in IEEE Transactions on Communications, vol. 68, no. 4, pp. 2446-2458, April 2020.
32. Balti. E and Guizani. M, "Impact of Non-Linear High-Power Amplifiers on Cooperative Relaying Systems," in IEEE Transactions on Communications, vol. 65, no. 10, pp. 4163-4175, Oct. 2017.
33. Belkacem. O. B. H, Ammari. M. L and Dinis. R, "Performance Analysis of NOMA in 5G Systems With HPA Nonlinearities," in IEEE Access, vol. 8, pp. 158327-158334, 2020.
34. Li. X, Zhao. M, Liu. Y, Li. L, Ding. Z and Nallanathan. A, "Secrecy Analysis of Ambient Backscatter NOMA Systems Under I/Q Imbalance," in IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12286-12290, Oct. 2020.
35. Zhang. W et al., "Widely Linear Precoding for Large-Scale MIMO with IQI: Algorithms and Performance Analysis," in IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 3298-3312, May 2017.
36. Ding. X, Zou. Y, Ding. F, Zhang. D and Zhang. G, "Opportunistic Relaying Against Eavesdropping for Internet-of-Things: A Security-Reliability Tradeoff Perspective," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8727-8738, Oct. 2019
37. Kim. S. W, "Modify-and-forward for securing cooperative relay communications", Proc.Int. Zurich Seminar Commun, pp. 136-139, Feb. 2014.
38. Vien. Q, Le. T. A, Nguyen. H. X and Phan. H, "A Secure Network Coding Based Modify-and-Forward Scheme for Cooperative Wireless Relay Networks," 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, pp. 1-5, 2016.
39. Vien. Q, Le. T. A and Duong. T. Q, "Opportunistic secure transmission for wireless relay networks with modify-and-forward protocol," 2017 IEEE International Conference on Communications (ICC), Paris, pp. 1-6, 2017.
40. Chu. S, "Secrecy Analysis of Modify-and-Forward Relaying With Relay Selection," in IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1796-1809, Feb. 2019.
41. Guo. K, Zhang. B, Huang. Y and Guo. D, "Outage Analysis of Multi-Relay Networks With Hardware Impairments Using SECps Scheduling Scheme in Shadowed-Rician Channel," in IEEE Access, vol. 5, pp. 5113-5120, 2017.
42. Wu. H et al., "Impact of Hardware Impairments on Outage Performance of Hybrid Satellite-Terrestrial Relay Systems," in IEEE Access, vol. 7, pp. 35103-35112, 2019.
43. Guo. K, An. K, Zhang. B, Huang. Y, Guo. D, "On the Performance of Cognitive Satellite-Terrestrial Relay Networks with Channel Estimation Error and Hardware Impairments," in Sensors Basel, Switzerland, vol. 18, Sep. 2018.
44. Salem. A, Hamdi.K. A and Rabie.K. M, "Physical Layer Security With RF Energy Harvesting in AF Multi-Antenna Relaying Networks," in IEEE Transactions on Communications, vol. 64, no. 7, pp. 3025-3038, July 2016.
45. Li. X, Huang. M, Li. J, Yu. Q, Rabie. K and Cavalcante. C. C, "Secure analysis of multi-antenna cooperative networks with residual transceiver HIs and CEEs," in IET Communications, vol. 13, no. 17, pp. 2649-2659, 2019.
46. Ma. B, Zhang. H and Zhang. Z, "Joint power allocation and mode selection for D2D communications with imperfect CSI," in China Communications, vol. 12, no. 7, pp. 73-81, July 2015.
47. Xu. F and Rui. X, "Impact of Imperfect Channel on the Performance of Relay Selection," 2015 International Conference on Network and Information Systems for Computers, Wuhan, pp. 151-154, 2015.
48. Bjornson. E, Matthaiou. M and Debbah. M, "A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments," in IEEE Transactions on Communications, vol. 61, no. 11, pp. 4512-4525, November 2013.
49. Zhang. J, Pan. G and Xie. Y, "Secrecy Analysis of Wireless-Powered Multi-Antenna Relaying System With Nonlinear Energy Harvesters and Imperfect CSI," in IEEE Transactions on Green Communications and Networking, vol. 2, no. 2, pp. 460-470, June 2018.

50. Liu. X, Yang. L, Chen. J and Zheng. F, "On the Performance of Nth Best Relay Selection Scheme for NOMA-Based Cooperative Relaying Networks with SWIPT," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, pp. 1-5, 2019.
51. Liu. Y, Ding. Z, Elkashlan. M and Poor. H. V, "Cooperative Non-orthogonal Multiple Access With Simultaneous Wireless Information and Power Transfer," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 4, pp. 938-953, April 2016.