IQ-Impaired Wireless-Powered Modify-and-Forward Relaying for IoT Networks: An In-Depth Physical Layer Security Analysis

IQ-Impaired Wireless-Powered Modify-and-Forward Relaying for IoT Networks: An In-Depth Physical Layer Security Analysis

Xingwang Li, Hongyan Qi, Dinh-Thuan Do, Zhang Hui, Yuan Ding, Mingfu Zhu, and Hongxing Peng

***Abstract*—With the large-scale commercialization of 5G networks, the era of Internet-of-Things (IoT), which is oriented towards the internet-of-everything (IoE), is coming. Under the circumstance, reliable and secure communication are the great challenges for future wireless network because of the broadcasting characteristics of electromagnetic wave. Physical layer security (PLS) is an effective way to ensure secure communication by exploiting random nature of fading channels. Motivated by this, we investigate PLS of the wireless-powered cooperative multi-relaying for IoT networks in the presence of eavesdropper with the estimation errors of channel (EEC) and imbalance between in-phase and quadrature-phase (IIQ). Specifically, the relays can be charged by the source with the aid of energy harvesters, and a novel more secure modify-and-forward (MF) relay protocol is proposed. For further improving energy efficiency and reducing extra interference, the K-th superior relay selection scheme is proposed since some best ones are not available due to some scheduling or failure. Based on the system under study, we derive the analytical expressions for the outage probability (OP), intercept probability (IP) and secrecy outage probability (SOP) to evaluate the reliable and secure performance of this consideration system. Particularly, we then analyze the asymptotic behaviors of the OP, IP and SOP, respectively. Through computer simulation, we show that: *i*) With EEC, the error floors of the OP and SOP are of presence; *ii*) Multiple relays lead to better OP and SOP performance; and *iii*) IIQ improves the security and is detrimental to the system reliability.**

***Index Terms*—Channel estimation errors, in-phase/quadrature-phase imbalance, power splitting, modify-and-forward, the K-th superior relay selection**

I. Introduction

With the rapid deployments of 5G networks, various applications enabled by 5G have been on the agenda, such as Internet-of-Thing (IoT), Internet-of-Vehicles (IoV), Augmented Reality (AR) and Virtual Reality (VR), etc. For these applications, massive connections, higher data rates, lower latency and quality of service (QoS) are key requirements for future wireless network. [1]. To meet the above demands, some promising disruptive approaches have been emerged, such as massive intelligent reflecting surface [2], ambient backscatter communication (AmBC) [3], ultra-reliable and low-latency communication (URLLC) [4] and millimeter wave (mmWave) [5]. The above technologies are the key enablers for the great deal of applications for IoT networks. However, communication security is an intractable problem for the above technologies because of the broadcast nature of electromagnetic waves, which has aroused a great interest from the academia and industry [6–8].

From the perspective of information theory, physical layer security (PLS) has been proposed to ensure secure wireless communication. In particular, PLS has been explored extensively, see [8–12]. In [8], Lei *et al.* investigated the PLS of single-input multiple-output (SIMO) systems over generalized-K fading channel by deriving theoretical expressions for security outage probability (SOP), average security capacity and the probability of strictly positive secrecy capacity. Emphasizing on visible light communication, Mostafa *et al.* in [9] proposed a beamforming scheme to analyze the effects of ideal channel knowledge at the eavesdropper due to location uncertainty. To extend the analysis of the security of multiple-input single-output (MISO) systems, the stochastic geometry and the perspective of space were employed to study SOP performance [10]. By extending the above work to cognitive networks, the authors in [12] analyzed the secrecy outage performance of SIMO underlay cognitive wiretap systems relying on the selection combining. The authors in [13, 14] have considered the effect of transmit antenna selection on the secure communications effects of MIMO systems. By considering whether the channel knowledge of the primary links and the listening link is known by source, the SOP was analyzed for two antenna schemes [15]. Regarding to full-duplex wireless powered IoT networks, authors in [16] designed a two stage suboptimal scheme to maximize the sum secrecy throughput, and the optimal variables involve transmission time slot and the beamforming vectors of the base station.

Cooperative communication is regarded as an effective technology to enhance coverage because direct connections between sources and destinations can be unavailable due to blockage or other practical reasons. For single relay assisted system transmissions, the related works can be found in [17, 18]. In [17], the impact of relay placement on the SOP was explored. Brante *et al.* adopted two schemes to consider the

Xingwang Li, Hongyan Qi, and Hongxing Peng are with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China (email: lixingwangbupt@gmail.com, 311502010201@home.hpu.edu.cn, phx@hpu.edu.cn).

Dinh-Thuan Do is with the Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan (email: dodinhthuan@asia.edu.tw).

Hui Zhang is with the Institute of Mining Engineering, Guizhou Institute of Technology, Guiyang 550003, China (email: caikuangzhang@163.com).

Y. Ding is with the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, Scotland, UK. e-mail: (email: yuan.ding@hw.ac.uk).

M. Zhu is with the Henan Chuitian Technology Co., Ltd., Hebi, 458000, China China (email: mfzhu@nled.cc).

PLS of single relay cooperative networks [18]. In addition, some multi-relay cooperative PLS system can be found in [19–21]. For amplify-and-forward (AF) relaying networks, three criteria were proposed and the effects of co-channel interference on network security were analyzed in [19]. Constrained by the transmission power of the whole system, an optimal power allocation strategy was developed to explore decode-and-forward (DF) relaying security communications [20]. For the AF and DF protocols mentioned above, the authors in [21] investigated system performance of the downlink hybrid satellite and terrestrial relaying systems, and studied two interception scenarios of non-colluding eavesdropper and colluding eavesdropper. However, multiple relays not only cause interference to affect the signal transmissions, but also cause energy waste. To this end, relay selection has received a great deal of focus [22–24]. The authors in [22] employed the optimal relay selection mechanism to analyze the impact on cooperative networks, and discussed the intercept probability (IP) performance. In [23], the partial relay selection was used to investigate the statistical behaviors and the bit error rate (BER) in multiple relays systems. From the perspective of improving performance, three relay selection schemes were adopted, and the SOP was considered in [24]. Vicario *et al*. investigated the outage performance and diversity order in DF cooperative system, which adopted opportunistic relay selection with outdated channel knowledge in [25]. Considering interference-limited case, the authors employed partial relay selection strategy and discussed outage performance in [26].

In practice, owing to the limited power of relays, the system efficiency is reduced. To this end, the simultaneous wireless information and power transfer technology (SWIPT) for cooperative systems has been discussed in [1, 27–30]. In [27], two practical SWIPT protocols, i.e., time switching (TS) and power splitting (PS), were proposed and the rate-energy performance was analyzed under energy harvesting (EH). In [28], Nasir *et al.* proposed an adaptive time-switching EH protocol without channel knowledge at the transmitter. The authors in [29] designed a PS relay scheme to optimize throughput, and took a greedy algorithm to obtain trade-off between performance and complexity. Considering two practical factors of estimation errors of channel (EEC) and hardware impairments, the performance of NOMA relaying B5G IoT networks was investigated by using time TS protocol in [1]. For the two-way AF relay network, Liu *et al.* employed PS protocol to investigate the outage performance, where the transceiver hardware impairments (HIs) and selection combining scheme were considered to process the signals [30]. Beyond the traditional TS and PS, many researchers have extended the application of SWIPT into cooperative systems [31–33]. A distributed power splitting (DPS) was developed according to game theory to study SWIPT network performance of relay channel interference, in which the AF and DF protocols were considered [31]. The [32] and [33] have proposed the TS relaying (TSR) and PS relaying (PSR) protocols and evaluated the security performance of multi-antenna relay networks. Moreover, the SWIPT was extended into cooperative NOMA networks [34, 35]. The authors in [34] focused on the system throughput and fairness improvement in wireless-Powered NOMA networks by considering two decoding order strategies.

All the above discussions are based on the ideal conditions. In fact, there are various non-ideal HIs caused by imperfect components in wireless communications [36–40]. Inspired by the residual HIs and EEC, Li *et al.* explored their effects on the system and analyzed the security and reliability performance [36]. Additionally, imbalance between in-phase and quadrature-phase (IIQ) has also attracted a lot of attention [37–41]. For enhancing the proposed system performance, a new low complexity technology was developed, and the impact of IIQ on reliability of low-cost device was discussed [37]. For narrowband IoT (NB-IoT), a novel IIQ mitigation scheme was proposal by utilizing the inactive subcarriers of index modulation orthogonal frequency division multiplexing (IM-OFDM) systems [38]. The authors in [39] have derived the outage probability (OP) of AF relaying networks with IIQ at transceivers. Considering both SWIPT and IIQ, the two relay schemes were employed to evaluate the outage and intercept performance of the wireless-powered multi-relay networks by employing non-linear EHs [40]. Li *et al.* have analyzed the OP performance in full-duplex (FD) NOMA networks under IIQ, and the results have showed that the existence of IIQ is detrimental to OP performance in [41].

A. Motivation and Contribution

Previous literature studies have largely overlooked PLS performance of the modify-and-forward (MF) protocol. From the view of security keys, in [42], Kim firstly proposed a new protocol, namely MF, where relay can modify the decoded information according to channel knowledge between the relay and destination. Compared with traditional AF and DF, MF can enhance the system security performance. Based these, some literatures on the MF cooperative systems have been emerged [43–45]. In [43], Vien *et al.* studied the security of the considered network in two schemes, without EEC. The authors in [44] explored the system SOP performance based on the channel knowledge acquisition, however, the IIQ was not taken into account. By extending the application of the traditional MF, Vien *et al.* developed a secure network coding (NC)-based MF (SPMF) strategy and studied the SOP performance, where this strategy can deal with the non-ideal modified message sharing [45]. By employing unique nature of wireless fading channels as the keys, a more secure MF protocol is adopted to hinder illegitimate to recover the intercepted information. Based on this, we investigate the reliable and secure performance of wireless-powered relaying network. In addition, for practical network scenarios, we consider two practical imperfect factors, namely IIQ and EEC. To future enhance communication efficiency, the K-th superior relay selection scheme is considered. Specially, we obtain the theoretical expressions for the OP, IP and SOP. For further insights, we also analyze the asymptotic behaviors for the OP and SOP at high SNRs and the IP at high main-to-eavesdropper ratio (MER), respectively. The main work of our article is presented summarily as follows:

- Different from the existing works, i.e, [43–45], we studied

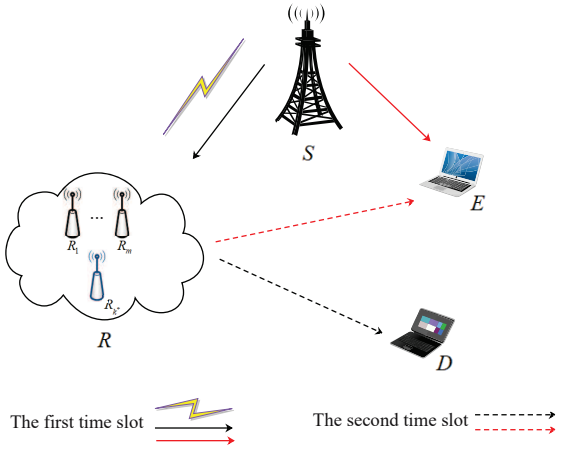

Fig. 1. System model for SWIPT aided MF cooperative

the secure and reliable performance of the wireless-powered MF based multiple relaying for IoT networks, where the selected relay can be charged by the source via PS strategy. Moreover, two non-ideal factors in practical systems are introduced, which is known as IIQ and EEC.

- For the reliability, we derive theoretical expressions for the OP under the conditions of IIQ and EEC for both MF and DF protocols. To gain insights, the asymptotic analysis is carried out in regard to the outage performance in the high SNR region. The analysis results show that the error floors is of existence for OP under EEC.
- For the security, we deduce exact expressions to the IP and SOP under IIQ and EEC for both MF and DF protocols. In addition, the asymptotic results for the SOP as SNR grow into infinity are obtained as well as the IP in the high MER, respectively.

B. Organization

The remain of our paper is arranged as follows. Section II, the proposed networks model is presented. Section III deduces the theoretical formulas for the OP, IP and SOP, then discusses the asymptotic behaviors in terms of both OP and SOP at high SNRs and the asymptotic result for the diversity orders and the asymptotic IP at high MERs. In Section IV, numerical simulation results verify our theoretical analyses. And in Section V, we illustrate a conclusion of this paper.

II. System Model

We consider a cooperative wireless-powered MF relaying IoT network, where one source S aims to communicate with one legitimate IoT device D with an eavesdropper E via M IoT devices as relays R_m, m=$\{1, 2, ..., M\}$, as shown in Fig. 1. It is assumed that all IoT nodes are single antenna devices and the IoT relay nodes are constrained in power. Moreover, the relays can be charged from the source by employing PS strategy. The link of $S \to D$ is absent due to obstacle or shadow fading. EEC and IIQ existed in practical networks are taken into account.

Channel estimation is generally used to obtain CSI. In this paper, the channel coefficient is expressed as $g_i = \hat{g}_i + e_i$,

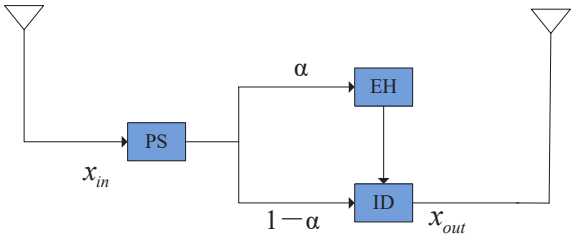

Fig. 2. Power-splitting structure of considering system

$i \in (SR_m, R_mD, R_mE, SE)$, $\hat{g}_i$ denotes the estimated channel coefficient, and e_i is the EEC with $e_i \sim \mathcal{CN}(0, \sigma_{ei}^2)$. All channel links experience Rayleigh fading, β_i is the channel variance.

In a practical communication environment, the modeling of the radio frequency front end is not accurate enough, so the two branches of I and Q are not perfectly matched, which causes the mismatch of the two branch of both phase and amplitude. Under this situation, the radio frequency signals is modeled as [46]:

$$x_{IIQ} = \varsigma_{t/r} x_s + \zeta_{t/r} x_s^* \tag{1}$$

where $x_s = \sqrt{P_S} x_i$, x_i is the corresponding transmitter signal at TX with $E\left\{|x_i|^2\right\} = 1$. P_S is the transmit power at S. $\varsigma_t = \frac{1}{2}\left(1 + \mu_t e^{i\phi_t}\right)$, $\varsigma_r = \frac{1}{2}\left(1 + \mu_r e^{-i\phi_r}\right)$, $\zeta_t = \frac{1}{2}\left(1 - \mu_t e^{-i\phi_t}\right)$ and $\zeta_r = \frac{1}{2}\left(1 - \mu_r e^{i\phi_r}\right)$. $\mu_{t/r}$ and $\phi_{t/r}$ are the amplitude and phase mismatch. For ideal case, $\mu_{t/r} = 1$ and $\phi_{t/r} = 0°$.

The entire communication has two time slots: 1) S transmits signals to R_m and E, simultaneously relays harvest transmitted energy from S; 2) R_m modifies signals, and forwards them to D and E.

1) The 1st time slot: During the first time slot, S sends its own signals to R_m and E, and R_m can harvest energy from S. From Fig. 2, the harvested energy at the relays is given as:

$$E_{R_m} = \alpha \eta P_S |g_{SR_m}|^2 \tag{2}$$

where α, $0 \le \alpha \le 1$, and αP_S is for collecting energy, η presents energy conversion coefficient. g_{SR_m} is the channel coefficient between the S and R_m.

The obtained signals at R_m and E are expressed as

$$y_{SR_m} = \varsigma_{rSR_m} \Im_{SR_m} + \varsigma_{rSR_m} \Im_{SR_m}^* \tag{3}$$

$$\begin{aligned} y_{SE} = {} & \varsigma_{rSE}\left[g_{SE}\left(\varsigma_{tSE}\sqrt{P_S}x + \zeta_{tSE}\sqrt{P_S}x^*\right) + n\right] \\ & + \zeta_{rSE}\left[g_{SE}\left(\varsigma_{tSE}\sqrt{P_S}x + \zeta_{tSE}\sqrt{P_S}x^*\right) + n\right]^* \end{aligned} \tag{4}$$

where $\Im_{SR_m} = g_{SR_m}\left(\varsigma_{tSR_m}\sqrt{(1-\alpha)P_S}x + \zeta_{tSR_m}\sqrt{(1-\alpha)P_S}x^*\right) + n$, n is the complex additive white Gaussian noise (AWGN) with $n \sim \mathcal{CN}(0, N)$, $(1-\alpha)P_S$ is for transmitting information.

2) The 2nd time slot: In the following time slot, relays modify signals and forward them to destination D and eavesdropper$E$, and the received signals at both nodes are presented as, respectively

$$y_{R_mD} = \varsigma_{rR_mD} \partial_{R_mD} + \zeta_{rR_mD} \partial_{R_mD}^* \tag{5}$$

$$y_{R_mE} = \varsigma_{rR_mE}\tilde{\partial}_{R_mE} + \zeta_{rR_mE}\tilde{\partial}^*_{R_mE} \quad (6)$$

where $\partial_{R_mD} = g_{R_mD}\left(\varsigma_{tR_mD}\sqrt{\alpha P_S}x + \zeta_{tR_mD}\sqrt{\alpha P_S}x^*\right) + n$, $\tilde{\partial}_{R_mE} = g_{R_mE}\left(\varsigma_{tR_mE}\sqrt{\alpha P_S}\tilde{x} + \zeta_{tR_mE}\sqrt{\alpha P_S}\tilde{x}^*\right) + n$, and $\tilde{x}$ is modified message, y_{R_mE} cannot recover the original information due to not knowing the unique channel state between relays and destination [42].

The obtained signal-to-interference-plus-noise ratios (SINRs) between two nodes are written as

$$\gamma_{SE} = \frac{A_{SE}}{B_{SE}} \quad (7)$$

$$\gamma_{SR_m} = \frac{\tilde{\vartheta}_{SR_m}}{\vartheta_{SR_m}} \quad (8)$$

where $A_{SE} = \bar{\gamma}_{SE}|\hat{g}_{SE}|^2 t_{SE}$, $B_{SE} = \bar{\gamma}_{SE}|\hat{g}_{SE}|^2 p_{SE} + \bar{\gamma}_{SE}p_{SE}\sigma^2_{eSE} + \bar{\gamma}_{SE}t_{SE}\sigma^2_{eSE} + \nu_{SE}$, $\tilde{\vartheta}_{SR_m} = \bar{\gamma}_{SR_m}|\hat{g}_{SR_m}|^2 t_{SR_m}(1-\alpha)$, $\vartheta_{SR_m} = \bar{\gamma}_{SR_m}|\hat{g}_{SR_m}|^2 p_{SR_m}(1-\alpha) + \bar{\gamma}_{SR_m}p_{SR_m}\sigma^2_{eSR_m}(1-\alpha) + \bar{\gamma}_{SR_m}t_{SR_m}\sigma^2_{eSR_m}(1-\alpha) + \nu_{SR_m}$, $\bar{\gamma}_{SE} = \bar{\gamma}_{SR_m} = \frac{P_S}{N}$ is the average SNR.

$$\gamma_j = \frac{\tilde{\tau}_j}{\tau_j} \quad (9)$$

where $\tau_j = \bar{\gamma}_j|\hat{g}_j|^2 p_j\alpha + \bar{\gamma}_j p_j\sigma^2_{ej}\alpha + \bar{\gamma}_j t_j\sigma^2_{ej}\alpha + \nu_j$, $\tilde{\tau}_j = \bar{\gamma}_j|\hat{g}_j|^2 t_j\alpha$, $j \in (R_mD, R_mE)$

To simplify the operation, we assume $t_i = |\varsigma_{ri}\varsigma_{ti} + \zeta_{ri}\zeta^*_{ti}|^2$, $p_i = |\varsigma_{ri}\zeta_{ti} + \zeta_{ri}\varsigma^*_{ti}|^2$, $\nu_i = |\varsigma_{ri} + \zeta_{ri}|^2$ and $\bar{\gamma}_i = \frac{P_S}{N}$ is the average SNR.

As discussed above, the channel capacity between two nodes is obtained by

$$C_i = \frac{1}{2}\log(1+\gamma_i) \quad (10)$$

where $i \in (SR_m, R_mD, R_mE, SE)$.

In MF protocol, the maximum capacity of reliable communication is given by

$$C_D = \min(C_{SR_m}, C_{R_mD}) \quad (11)$$

Considering the eavesdropper cannot recover the information modified via the relays, the maximum capacity at E with MF protocols is given by $C_E = C_{SE}$. The instantaneous secrecy capacity (SC) between the source and the destination is expressed as

$$C_S = \{C_D - C_E, 0\}^+ \quad (12)$$

where $\{\cdot\}^+ = \max\{\cdot, 0\}$, C_E is the channel capacity at E.

III. PERFORMANCE ANALYSIS

This section carries out the OP, IP and SOP performance analysis, where EEC, IIQ and EHs are included. The exact analytical expressions in terms of OP, IP and SOP are derived with both MF and DF for non-ideal and ideal cases. Moreover, for more insights, we carry out the asymptotic analysis as well as diversity order.

A. Outage Probability Analysis

For a given transmission rate R_{th}, OP is obtained when the probability of the channel capacity of main links is smaller than R_{th}, see in (13),

$$P_{out} = P_r(C_D < R_{th}) \quad (13)$$

The OP under MF protocol: Considering the interference between multiple relays, the signal transmissions will be affected. Based on this reason, to improve the system efficiency, we deploy the K-th max min criterion to select a relay, in which this criterion can also generate corresponding capacity, i.e., $K^{th}\max\min C_D$ [47],

$$P_{out} = P_r\left(K^{th}\max\min(C_{SR_m}, C_{R_mD}) < R_{th}\right) \quad (14)$$
$$m = 1, 2, \ldots, M$$

Theorem 1. *For non-ideal case, the exact mathematical formula of the OP with MF scheme is written as in (15), displayed at the top of the next page.*
where $\Omega = \frac{\left(\bar{\gamma}_{SR_m}p\sigma^2_{eSR_m}(1-\alpha) + \bar{\gamma}_{SR_m}t\sigma^2_{eSR_m}(1-\alpha) + \nu\right)}{\bar{\gamma}_{SR_m}t(1-\alpha) - \bar{\gamma}_{SR_m}p(1-\alpha)\varepsilon}$, $\mho = \frac{\left(\bar{\gamma}_{R_mD}p\sigma^2_{eR_mD}\alpha + \bar{\gamma}_{R_mD}t\sigma^2_{eR_mD}\alpha + \nu\right)}{\bar{\gamma}_{R_mD}t\alpha - \bar{\gamma}_{R_mD}p\alpha\varepsilon}$ *and* $\varepsilon = 2^{2R_{th}-1}$. *Before we can solve for OP, we need to satisfy* $\varepsilon < \frac{t}{p}$, *otherwise the OP=1.*

Proof: See Appendix A. ∎

To better analyze the proposed system, the performance of DF protocol is also studied.

The OP under DF protocol: The OP under both MF protocol and DF protocol are equal, since S first sends its own signals to the relays and an eavesdropper under both protocols. D and E then receive modified information with the aid of MF protocol, while D can recover the message since it has knowledge the key between the R_m and D, while E cannot recover because the one is unknown. Therefore, OP under DF is the same as OP under MF.

Theorem 2. *For ideal case, i.e., t=1, p=0, v=1,* $\sigma^2_{ei} = 0$. *Then the expression of OP becomes*

$$P^{id}_{out} = \sum_{k=1}^{K}\binom{M}{k-1}\left(1-e^{-\frac{\Theta_1}{\bar{\gamma}}}\right)^{M-k+1}\left(e^{-\frac{\Theta_1}{\bar{\gamma}}}\right)^{k-1} \quad (16)$$

where $\Theta_1 = \frac{\varepsilon}{\beta_{SR_m}(1-\alpha)} + \frac{\varepsilon}{\beta_{R_mD}\alpha}$.

B. Intercept Probability Analysis

We study the IP of the proposed system, and for the purpose of further analysis, non-ideal and ideal cases for both MF and DF are discussed.

For transmission rate R_{th}, the definition of IP is the probability of the channel maximum rate of the eavesdropper is more than R_{th}, see in (17),

$$P_{in} = P_r(C_E > R_{th}) \quad (17)$$

Theorem 3. *For the IP of MF protocol, we only need the link information of S to E, and we use the selection combining algorithm to process the two received information at E in terms of IP for DF protocol.*

• *Non-ideal conditions*

$$P_{out}^{ni,MF}=\sum_{k=1}^{K}\binom{M}{k-1}\left(1-e^{-\frac{\varepsilon}{\beta_{SR_m}}\Omega-\frac{1}{\beta_{R_mD}}\varepsilon\mho}\right)^{M-k+1}\left(e^{-\frac{1}{\beta_{SR_m}}\varepsilon\Omega-\frac{1}{\beta_{R_mD}}\varepsilon\mho}\right)^{k-1} \tag{15}$$

In this situation, the expressions of IP under MF and DF can be given as, respectively

$$P_{in}^{ni,MF}=e^{-\frac{\varepsilon\left(\bar{\gamma}\sigma_{eSE}^2p+t\bar{\gamma}\sigma_{eSE}^2+\nu\right)}{\beta_{SE}\bar{\gamma}(t-p\varepsilon)}} \tag{18}$$

and

$$P_{in}^{ni,DF}=1-\left(1-e^{-\frac{\varepsilon\left(\bar{\gamma}\sigma_{eSE}^2p+t\bar{\gamma}\sigma_{eSE}^2+\nu\right)}{\beta_{SE}\bar{\gamma}(t-p\varepsilon)}}\right)\times\left(1-e^{-\frac{\varepsilon\left(\bar{\gamma}\sigma_{eR_mE}^2p\alpha+\bar{\gamma}\sigma_{eR_mE}^2t\alpha+\nu\right)}{\beta_{R_mE}\bar{\gamma}(t\alpha-p\varepsilon\alpha)}}\right) \tag{19}$$

where for both two protocols, we need to ensure $\varepsilon<\frac{t}{p}$, otherwise the IP=1.

• *Ideal conditions*

For ideal conditions: t=1, p=0, v=1, $\sigma_{ei}^2=0$. The expressions of IP with two protocols can be respectively written as

$$P_{in}^{id,MF}=e^{-\frac{\varepsilon}{\beta_{SE}\bar{\gamma}}} \tag{20}$$

and

$$P_{in}^{id,DF}=1-\left(1-e^{-\frac{\varepsilon}{\beta_{SE}\bar{\gamma}}}\right)\left(1-e^{-\frac{\varepsilon}{\beta_{R_mE}\bar{\gamma}\alpha}}\right) \tag{21}$$

C. Secrecy Outage Probability Analysis

We explore the SOP under both MF and DF protocols for non-ideal and ideal cases.

The SOP under MF protocol: In light of MF protocol, we only consider the link information on $S\to E$. Hence, according to the K-best relay selection, the SOP is defined as

$$P_{sout}^{MF}=P_r\left(K^{th}\max C_S<R_{th}\right)\quad m=1,2,\ldots,M \tag{22}$$

The SOP under DF protocol: Due to the two links information of both $S\to E$ and $R_m\to E$, we take the approach of processing information separately [47], its expression is

$$P_{sout}^{DF}=P_r\left(\left(K^{th}\max\min\Psi\right)<R_{th}\right)\quad m=1,2,\ldots,M \tag{23}$$

where $\Psi=(C_{SR_m}-C_{SE},C_{R_mD}-C_{R_mE})$.

Theorem 4. *For non-ideal case, the analytical approximate expressions of SOP with MF and DF are presented as (24) and (25), respectively, shown at the top of next page. We adopt the Gaussian-Chebyshev quadrature to obtain SOP, for $\varepsilon<\frac{t}{p}$, otherwise SOP=1, where $\omega_1=\frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L}s_1s_2\sqrt{1-\delta_q^2}$, $\omega_3=\frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L}s_1s_4\sqrt{1-\delta_q^2}$, L is a Complex accuracy trade-off parameter, $\delta_q=\cos\left(\frac{(2q-1)\pi}{2L}\right)$, $s_1=e^{-\frac{x\left(\bar{\gamma}\sigma_{eSE}^2p+\bar{\gamma}\sigma_{eSE}^2t+v\right)}{\bar{\gamma}\beta_{SE}(t-px)}}$, $x=\frac{\lambda(\delta_q+1)}{2}$, $\xi(x)=2^{2R_{th}}(1+x)-1$, $s_2=1-e^{-\frac{\xi(x)\left(\bar{\gamma}(1-\alpha)\sigma_{eSR_m}^2p+\bar{\gamma}(1-\alpha)\sigma_{eSR_m}^2t+v\right)}{\bar{\gamma}\beta_{SR_m}(t(1-\alpha)-p\xi(x)(1-\alpha))}}$, $s_4=1-e^{-\frac{\xi(x)\left(\bar{\gamma}\alpha\sigma_{eR_mD}^2p+\bar{\gamma}\alpha\sigma_{eR_mD}^2t+v\right)}{\bar{\gamma}\beta_{R_mD}(t\alpha-p\xi(x)\alpha)}}$.*

Proof: See Appendix B. ∎

and we adopt the Gaussian-Chebyshev quadrature to obtain SOP with DF for non-ideal case, and the two signals at E are processed separately, where $\omega_2=\frac{\pi\lambda}{2L\beta_{R_mE}}\sum_{q=0}^{L}s_3s_4\sqrt{1-\delta_q^2}$, $s_3=e^{-\frac{x\left(\bar{\gamma}\alpha\sigma_{eR_mE}^2p+\bar{\gamma}\alpha\sigma_{eR_mE}^2t+v\right)}{\bar{\gamma}\beta_{R_mE}(t\alpha-px\alpha)}}$. For $\varepsilon<\frac{t}{p}$, otherwise SOP=1.

Proof: See Appendix C. ∎

Theorem 5. *For ideal conditions: t=1, p=0, v=1, $\sigma_{ei}^2=0$. The Gaussian-Chebyshev quadrature is employed to calculate SOP, the expressions of SOP with both MF and DF can be respectively obtained by*

$$P_{sout}^{id,MF}\approx\sum_{k=1}^{K}\binom{M}{k-1}\left(\left(1-\omega_1^{\Delta}\right)\left(1-\omega_3^{\Delta}\right)\right)^{k-1}\times\left(1-\left(1-\omega_1^{\Delta}\right)\left(1-\omega_3^{\Delta}\right)\right)^{M-k+1} \tag{26}$$

$$P_{sout}^{id,DF}\approx\sum_{k=1}^{K}\binom{M}{k-1}\left(\left(1-\omega_1^{\Delta}\right)\left(1-\omega_2^{\Delta}\right)\right)^{k-1}\times\left(1-\left(1-\omega_1^{\Delta}\right)\left(1-\omega_2^{\Delta}\right)\right)^{M-k+1} \tag{27}$$

where $s_1^{\Delta}=e^{-\frac{x}{\bar{\gamma}\beta_{SE}}}$, $s_2^{\Delta}=1-e^{-\frac{\xi(x)}{\bar{\gamma}\beta_{SR_m}(1-\alpha)}}$, $s_3^{\Delta}=e^{-\frac{x}{\bar{\gamma}\beta_{R_mE}\alpha}}$, $s_4^{\Delta}=1-e^{-\frac{\xi(x)}{\bar{\gamma}\beta_{R_mD}\alpha}}$, $\omega_1^{\Delta}=\frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L}s_1^{\Delta}s_2^{\Delta}\sqrt{1-\delta_q^2}$, $\omega_3^{\Delta}=\frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L}s_1^{\Delta}s_4^{\Delta}\sqrt{1-\delta_q^2}$, $\omega_2^{\Delta}=\frac{\pi\lambda}{2L\beta_{R_mE}}\sum_{q=0}^{L}s_3^{\Delta}s_4^{\Delta}\sqrt{1-\delta_q^2}$.

D. Asymptotic Analysis

According to the analytical results, we explore the asymptotic behavior and the diversity order in the high SNRs.

Corollary 1. *The asymptotic expressions of OP are given as when $\bar{\gamma}\to\infty$:*

• *Non-ideal conditions*

$$P_{out}^{\infty,ni}\approx\sum_{k=1}^{K}\binom{M}{k-1}\left(1-e^{-\Theta_2-\Theta_3}\right)^{M-k+1}\left(e^{-\Theta_2-\Theta_3}\right)^{k-1} \tag{28}$$

• *Ideal conditions*

$$P_{out}^{\infty,id}\approx\sum_{k=1}^{K}\binom{M}{k-1}\left(\frac{\Theta_1}{\bar{\gamma}}\right)^{M-k+1} \tag{29}$$

where $\Theta_2=\frac{\varepsilon\left(p\sigma_{eSR_m}^2+t\sigma_{eSR_m}^2\right)}{\beta_{SR_m}(t-p\varepsilon)}$, $\Theta_3=\frac{\varepsilon\left(p\sigma_{eR_mD}^2+t\sigma_{eR_mD}^2\right)}{\beta_{R_mD}(t-p\varepsilon)}$.

$$P_{sout}^{ni,MF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(1-\left(1-\omega_1\right)\left(1-\omega_3\right)\right)^{M-k+1} \left(\left(1-\omega_1\right)\left(1-\omega_3\right)\right)^{k-1} \tag{24}$$

$$P_{sout}^{ni,DF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(1-\left(1-\omega_1\right)\left(1-\omega_2\right)\right)^{M-k+1} \left(\left(1-\omega_1\right)\left(1-\omega_2\right)\right)^{k-1} \tag{25}$$

Proof: See Appendix D. ∎

Corollary 2. *To further explore the interception behaviors, we adopt the MER as $\beta_{me} = \frac{\beta_{SR_m}}{\beta_{R_mE}}$ for the IP of DF protocol when $\beta_{me} \to \infty$, and for the IP of MF protocol we study it when $\bar{\gamma} \to 0$. Since $x \to 0$, $e^{-x} \to 1-x$, the expressions for both protocols are given by*

- *Non-ideal conditions*

$$P_{in}^{ni,MF} \approx 0 \tag{30}$$

and

$$P_{in}^{ni,DF} \approx 1 - \left(1 - e^{-\frac{\varepsilon\left(\bar{\gamma}\sigma_{eSE}^2 p + t\bar{\gamma}\sigma_{eSE}^2 + \nu\right)}{\beta_{SE}\bar{\gamma}(t-p\varepsilon)}}\right) \tag{31}$$

- *Ideal conditions*

$$P_{in}^{id,MF} \approx 0 \tag{32}$$

and

$$P_{in}^{id,DF} \approx 1 - \left(1 - e^{-\frac{\varepsilon}{\beta_{SE}\bar{\gamma}}}\right) \tag{33}$$

Corollary 3. *In case of high MER, the asymptotic expressions for SOP with two cases are given by*

- *Non-ideal case:*

$$P_{asout}^{ni,MF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(\left(1-\omega_1^{\Xi}\right)\left(1-\omega_3^{\Xi}\right)\right)^{k-1} \times \left(1-\left(1-\omega_1^{\Xi}\right)\left(1-\omega_3^{\Xi}\right)\right)^{M-k+1} \tag{34}$$

and

$$P_{asout}^{ni,DF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(\left(1-\omega_1^{\Xi}\right)\left(1-\omega_2^{\Xi}\right)\right)^{k-1} \times \left(1-\left(1-\omega_1^{\Xi}\right)\left(1-\omega_2^{\Xi}\right)\right)^{M-k+1} \tag{35}$$

where $\omega_1^{\Xi} = \frac{\pi\lambda}{2L\beta_{SE}} \sum_{q=0}^{L} e^{-\Theta_6}\left(1-E_1\right)\sqrt{1-\delta_q^2}$, $\omega_3^{\Xi} = \frac{\pi\lambda}{2L\beta_{SE}} \sum_{q=0}^{L} e^{-\Theta_6}\left(1-E_3\right)\sqrt{1-\delta_q^2}$, $\omega_2^{\Xi} = \frac{\pi\lambda}{2L\beta_{R_mE}} \sum_{q=0}^{L} e^{-\Theta_8}\left(1-E_3\right)\sqrt{1-\delta_q^2}$, $\Theta_6 = \frac{x\left(p\sigma_{eSE}^2+t\sigma_{eSE}^2\right)}{\beta_{SE}(t-px)}$, $\Theta_8 = \frac{x\left(p\sigma_{eR_mE}^2+t\sigma_{eR_mE}^2\right)}{\beta_{R_mE}(t-px)}$, $E_1 = e^{-\frac{\xi(x)\left(p\sigma_{eSR_m}^2+t\sigma_{eSR_m}^2\right)}{\beta_{SR_m}(t-p\xi(x))}}$, $E_3 = e^{-\frac{\xi(x)\left(p\sigma_{eR_mD}^2+t\sigma_{eR_mD}^2\right)}{\beta_{R_mD}(t-p\xi(x))}}$.

Proof: See Appendix E. ∎

- *Ideal case:*

$$P_{asout}^{id,MF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(\left(1-\omega_1^{\Gamma}\right)\left(1-\omega_3^{\Gamma}\right)\right)^{k-1} \times \left(1-\left(1-\omega_1^{\Gamma}\right)\left(1-\omega_3^{\Gamma}\right)\right)^{M-k+1} \tag{36}$$

and

$$P_{asout}^{id,DF} \approx \sum_{k=1}^{K} \left(\begin{array}{c} M \\ k-1 \end{array} \right) \left(\left(1-\omega_1^{\Gamma}\right)\left(1-\omega_2^{\Gamma}\right)\right)^{k-1} \times \left(1-\left(1-\omega_1^{\Gamma}\right)\left(1-\omega_2^{\Gamma}\right)\right)^{M-k+1} \tag{37}$$

where $\omega_1^{\Gamma} = \frac{\pi\lambda}{2L\beta_{SE}} \sum_{q=0}^{L} \frac{\xi(x)}{\beta_{SR_m}\bar{\gamma}(1-\alpha)}\sqrt{1-\delta_q^2}$, $\omega_3^{\Gamma} = \frac{\pi\lambda}{2L\beta_{SE}} \sum_{q=0}^{L} \frac{\xi(x)}{\beta_{R_mD}\bar{\gamma}\alpha}\sqrt{1-\delta_q^2}$, $\omega_2^{\Gamma} = \frac{\pi\lambda}{2L\beta_{R_mE}} \sum_{q=0}^{L} \frac{\xi(x)}{\beta_{R_mD}\bar{\gamma}\alpha}\sqrt{1-\delta_q^2}$.

Proof: See Appendix F. ∎

E. Diversity Order

For further explore analysis, we study the diversity order of OP at high SNRs. The diversity order is defined by

$$d = -\lim_{\bar{\gamma}\to\infty} \frac{\log\left(P_{out}^{\infty}\right)}{\log\bar{\gamma}} \tag{38}$$

where P_{out}^{∞} and $\bar{\gamma}$ are the asymptotic expression of OP and the average SNR of the system, respectively.

Corollary 4. *The diversity orders in terms of OP with two cases are presented as*

- *Non-ideal conditions:*

$$d = -\lim_{\bar{\gamma}\to\infty} \frac{\log\left(P_{out}^{\infty,ni}\right)}{\log\bar{\gamma}} = 0 \tag{39}$$

and

- *Ideal conditions:*

$$d = -\lim_{\bar{\gamma}\to\infty} \frac{\log\left(P_{out}^{\infty,id}\right)}{\log\bar{\gamma}} = M - K \tag{40}$$

Remark 1. *This Corollary 4, in non-ideal case, illustrates that the diversity order of OP at high SNRs approaches zero. For the asymptotic OP is a positive number, this reveals that the proper average SNR contributes to reducing the OP for imperfect CSI and IIQ. For ideal case, this Corollary also shows that the diversity order in terms of OP depended on the number of relays.*

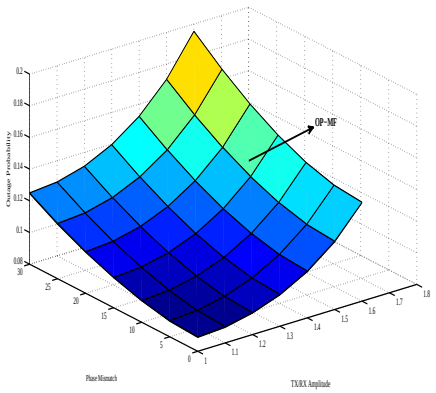

Fig. 3. The impact of IIQ on OP (ϕ_t=ϕ_r, μ_t=μ_r)

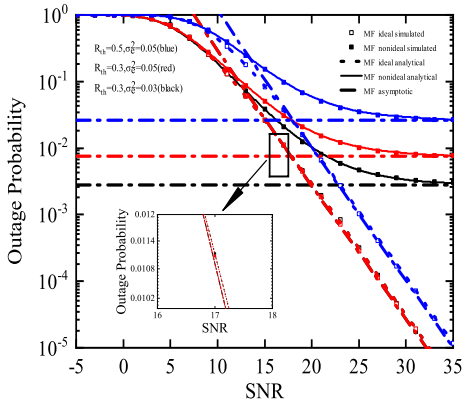

Fig. 5. OP for different transmission rates and EEC factors versus SNR

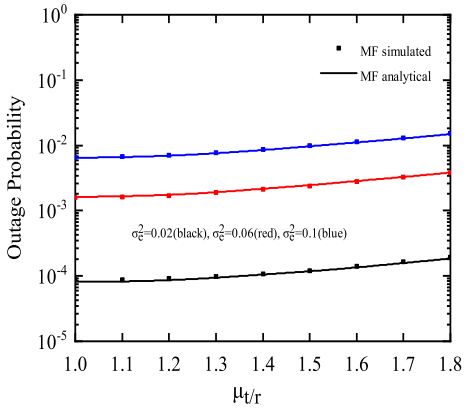

Fig. 4. OP for different EEC factors versus TX/RX amplitude

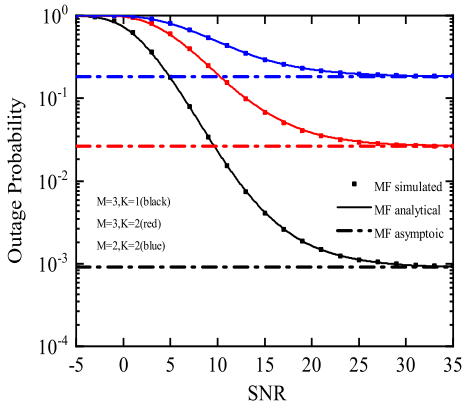

Fig. 6. OP in different relay values versus SNR

IV. Numerical Results

This section studies the OP, IP and SOP by numerical simulations. For the above theoretical analysis, we use Monte Carlo simulation to verify our analysis obtained in Section III. Unless otherwise specified, we assume that σ_{ei}^2=σ_e^2, N=1, μ_t=μ_r=1.1, ϕ_t=ϕ_r=5°, L=100.

Fig. 3 plots the impact of IIQ on OP, we assume that σ_e^2= 0.1, M=3, K=2, P_S=30dB, R_{th}=0.5, and α=0.4. As we can see that the OP is proportional to the size of both the phase mismatch and the TX/RX amplitude, it reveals that the OP becomes higher when the phase mismatch and the TX/RX amplitude increases.

Fig. 4 shows the OP versus TX/RX amplitude for different EEC factors (σ_e^2=$0.02, 0.06, 0.1$). We set M=3, K=1, R_{th}=0.5, α=0.4, P_S=30dB. we can see that the OP becomes deteriorated with the growth of the channel estimate error. The OP increases as $\mu_{t/r}$ increases, this means that TX/RX amplitude is detrimental to the system reliability.

Fig. 5 depicts the OP versus the SNR with MF protocol for different transmission rates and EEC factors $\left(R_{th}, \sigma_e^2\right)$=$((0.5, 0.05), (0.3, 0.05), (0.3, 0.03))$. We set α=0.2, M=3, and K=2. It can be observed that the OP becomes small with the R_{th} decreasing when σ_e^2=0.05, which reveals that the outage performance can be enhanced by the decreases of transmission rate. It can also be observed that the OP becomes large with the σ_e^2 increasing when R_{th}=0.3. In addition, we see that the an error floor for the OP appears because of the EEC, which implies that the system reliability performance is not improved via the decrease of EEC.

Fig. 6 presents the OP versus SNR for different number of relays (M, K)=$\{(3,1), (3,2), (2,2)\}$. We assume that σ_e^2=0.05, R_{th}=0.5, α=0.2. From Fig. 6, one can see that the OP decreases as the selected relay value becomes small when the total number of relays is fixed, which indicates that smaller K results in better outage performance. One can also see that the OP decreases with the M increasing, which indicates that cooperative communication is of benefit to improving system performance.

Fig. 7 plots the OP versus the power splitting, where $\left(\sigma_e^2, P_S\right)$=$\{(0.01, 15), (0.05, 15), (0.01, 10)\}$, M=3, K=2, and R_{th}=0.1. We can see that: (i) OP changes with respect to α; (ii) as α gets larger, OP shows parabolic state, and the parabolic shows convex, which means that PS protocol can be properly designed to minimize the OP; (iii) as P_S is a fixed value, the OP becomes larger with σ_e^2 increases, this indicates that system reliability degrades by increasing σ_e^2 value; (iv) when σ_e^2 is 0.01, the outage performance gets better as P_S grows, which implies that increasing proper P_S value is good for reliability performance.

Fig. 8 illustrates SOP versus SNR for two situations. We set R_{th}=0.2, α=0.3, σ_e^2=0.05, M=3, and K=1. In this simulation, we explore the SOP performance for DF protocol. As in

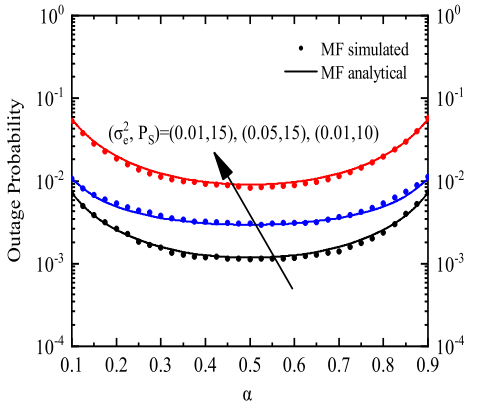

Fig. 7. OP in different EEC and P_S values versus α

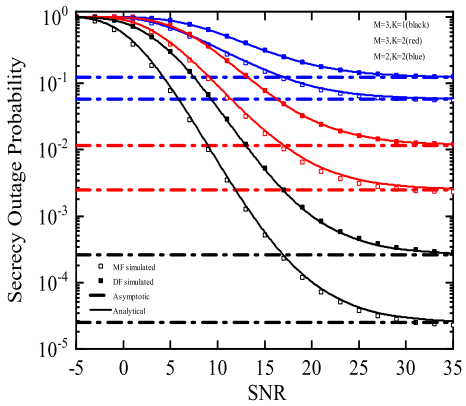

Fig. 10. SOP in different relay values M versus SNR

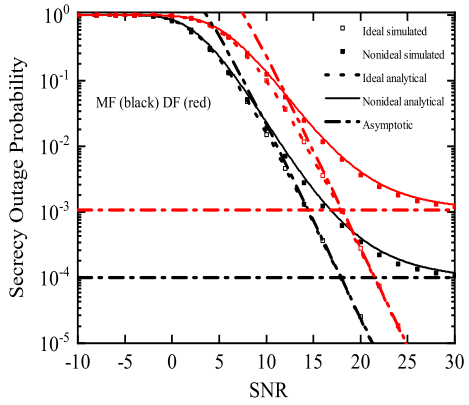

Fig. 8. SOP in non-ideal and ideal cases versus SNR

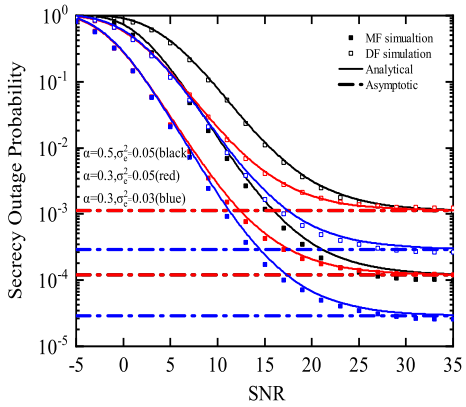

Fig. 11. SOP in different EEC and power splitting factor values versus SNR

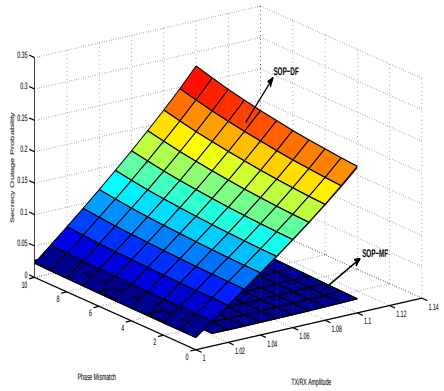

Fig. 9. The impact of IIQ on SOP (ϕ_t=ϕ_r, μ_t=μ_r)

Fig. 8, the secrecy outage performance is better in ideal case comparing with non-ideal case. In non-ideal case, the results reveal that the SOP has error floors, this is because the presence of the EEC. It also reveals that the SOP of DF protocol is more than the one of the MF protocol for both cases, i.e., MF protocol is contributed to enhancing the secrecy outage performance.

Fig. 9 shows the impact of IIQ on SOP. We assume that σ_e^2=0.01, P_S=30dB, M=3, K=1, α=0.2, R_{th}=1. From this figure, it can be seen that: (i) MF protocol can significantly enhance secrecy outage performance compared with DF protocol; (ii) the SOP is higher as the growth of $\mu_{t/r}$ and $\phi_{t/r}$. That is, the IIQ has proportional to the SOP for two protocols. In addition, it also provides the maximum degree of IIQ that our considered cooperative communication system can withstand for SOP.

The SOP versus SNR for different values of relay (M,K)=$\{(3,1),(3,2),(2,2)\}$ is shown in Fig. 10. Here, we set R_{th}=0.2, α=0.5, σ_e^2=0.03. The simulation shows that the K is proportional to SOP when the M value is fixed, and also shows that the SOP is inversely proportional to M. Finally, the SOP has error floor due to the EEC.

In Fig. 11, the SOP versus SNR is plotted for different EEC and power splitting factor values, where (α,σ_e^2)=$\{(0.5,0.05),(0.3,0.05),(0.3,0.03)\}$. It can be observed that the SOP of DF protocol is higher than the one in MF protocol for these three different combinations, which implies that our adopted protocol is beneficial to the system performance. It can also be observed that the SOP becomes higher with α increasing when σ_e^2 is 0.05, which implies that increasing α values is detrimental to the secrecy outage performance. Additionally, the SOP becomes small as σ_e^2 decreases when α is a fixed value, which indicates that the secrecy outage performance can be enhanced by decreasing σ_e^2 values.

In Fig. 12, the impact of phase mismatch and TX/RX amplitude on IP is demonstrated. We assume P_S=30dB, M=3,

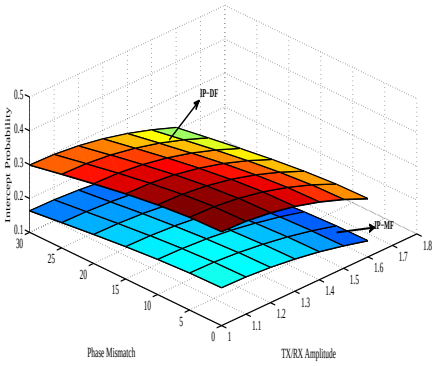

Fig. 12. The impact of IIQ on IP (ϕ_t=ϕ_r, μ_t=μ_r)

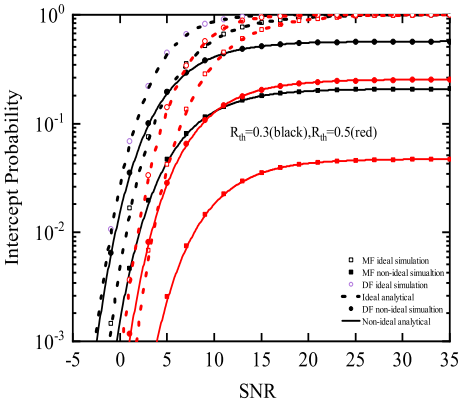

Fig. 13. IP in non-ideal and ideal cases versus SNR

K=2, σ_e^2=0.3, R_{th}=0.3, α=0.5. We can draw that the impact of IIQ on IP is inversely proportional to the OP and SOP, which indicates that the IIQ is effective to the security performance enhancement in appropriate IIQ regime.

In Fig. 13, the IP versus SNR for ideal case and non-ideal case is plotted, the parameters are set as follows σ_e^2=0.3, α=0.5, M=3, K=2, R_{th}=(0.3,0.5). We consider both IIQ and EEC in practical system, as well as the ideal case. The simulation results show that (i) the IP of the DF protocol is higher than the one of the MF protocol, which means that our employed protocol is effective for improving system security; (ii) the IP is inversely proportional to the R_{th}, which implies that we can enhance security performance by improve transmission rates; (iii) The ideal IP is higher than the non-ideal one for MF protocol and DF protocol. In addition, the IP becomes larger with the increase of the average SNR at two protocols, i.e., we cannot improve security performance by increasing SNR.

V. Conclusion

This paper investigated the PLS of wireless-powered cooperative multi-relay networks. We have considered two practical factors: IIQ and EEC. Particularly, the exact approximate expressions for the OP, IP and SOP have been derived. Moreover, we have further explored the asymptotic OP with high SNRs and SOP with high MER, and the OP's diversity orders. To further analyze system performance, we have also studied the performance for DF protocol. Simulation results verify the adopted scheme has outperformed the DF scheme, and contributed to the security performance improvement of the considered system.

Appendix A: Proof of Theorem 1

We first simplify (14), and then the following form as

$$P_{out}^{ni,MF} = \sum_{k=1}^{K} \binom{M}{k-1} \left(P_r\left(\min\left(C_{SR_m}, C_{R_m D}\right) < R_{th}\right)\right)^{M-k+1} \times \left(1 - P_r\left(\min\left(C_{SR_m}, C_{R_m D}\right) < R_{th}\right)\right)^{k-1} \quad \text{(A.1)}$$

Substituting (8) and (9) into (A.1), we can get the expression for the OP and verify the (15).

Appendix B: Proof of Theorem 4

For (22), we can obtain following:

$$P_{sout}^{ni,MF} = \sum_{k=1}^{K} \binom{M}{k-1} \left(P_r\left(C_S < R_{th}\right)\right)^{M-k+1} \times \left(1 - P_r\left(C_S < R_{th}\right)\right)^{k-1} \quad \text{(B.1)}$$

$$P_r\left(C_S < R_{th}\right) = 1 - \underbrace{P_r\left(C_{SR_m} - C_{SE} \geqslant R_{th}\right)}_{I_1} \times \underbrace{P_r\left(C_{R_m D} - C_{SE} \geqslant R_{th}\right)}_{I_2} \quad \text{(B.2)}$$

we first calculate I_1 in the following.

$$I_1 = P_r\left(\gamma_{SR_m} \geqslant 2^{2R_{th}}\left(1 + \gamma_{SE}\right) - 1\right) = 1 - \int_0^{+\infty} f_{\gamma_{SE}}(x) F_{\gamma_{SR_m}}\left(\xi(x)\right) dx \quad \text{(B.3)}$$

where we assume $\xi(x) = 2^{2R_{th}}(1+x) - 1$, it is difficult to solve (B.3). Thus, we employ the Gaussian-Chebyshev quadrature to find approximation solution, where is expressed by

$$\int_0^{\lambda} \tilde{m}(x) dx = \frac{\pi\lambda}{2L} \sum_{q=0}^{L} \tilde{m}\left(\frac{\lambda(\delta_q + 1)}{2}\right) \sqrt{1 - \delta_q^2} \quad \text{(B.4)}$$

based on (B.4), (B.3) can be obtained, i.e, $I_1 = 1 - \frac{\pi\lambda}{2\beta_{SE}L} \sum_{q=0}^{L} \tilde{m}_1(x) \sqrt{1-\delta_q^2}$, where

$$\tilde{m}_1(x) = \left(1 - e^{-\frac{\xi(x)\left(\bar{\gamma}(1-\alpha)\sigma_{eSR_m}^2 p + \bar{\gamma}(1-\alpha)\sigma_{eSR_m}^2 t + v\right)}{\bar{\gamma}\beta_{SR_m}(t(1-\alpha) - p\xi(x)(1-\alpha))}}\right) \times \left(e^{-\frac{x\left(\bar{\gamma}\sigma_{eSE}^2 p + \bar{\gamma}\sigma_{eSE}^2 t + v\right)}{\bar{\gamma}\beta_{SE}(t - px)}}\right)$$

Similarly, I_2 can be obtained, i.e., $I_2 = 1 - \frac{\pi\lambda}{2\beta_{SE}L} \sum_{q=0}^{L} \tilde{m}_2(x) \sqrt{1-\delta_q^2}$, $\tilde{m}_2(x) = \left(1 - e^{-\frac{\xi(x)\left(\bar{\gamma}\alpha\sigma_{eR_m D}^2 p + \bar{\gamma}\alpha\sigma_{eR_m D}^2 t + v\right)}{\bar{\gamma}\beta_{R_m D}(t\alpha - p\xi(x)\alpha)}}\right) \times \left(e^{-\frac{x\left(\bar{\gamma}\sigma_{eSE}^2 p + \bar{\gamma}\sigma_{eSE}^2 t + v\right)}{\bar{\gamma}\beta_{SE}(t - px)}}\right)$.

Substituting I_1 and I_2 into (B.2), the (B.5) is obtained, shown at the top of the next page.

$$P_{sout}^{ni,MF} \approx \sum_{k=1}^{K} \binom{M}{k-1} \left(1-\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_2\sqrt{1-\delta_q^2}\right)\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_4\sqrt{1-\delta_q^2}\right)\right)^{M-k+1} \times \left(\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_2\sqrt{1-\delta_q^2}\right)\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_4\sqrt{1-\delta_q^2}\right)\right)^{k-1} \tag{B.5}$$

$$P_{sout}^{ni,DF} \approx \sum_{k=1}^{K} \binom{M}{k-1} \left(1-\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_2\sqrt{1-\delta_q^2}\right)\left(1-\frac{\pi\lambda}{2\beta_{R_m E}L}\sum_{q=0}^{L} s_3 s_4\sqrt{1-\delta_q^2}\right)\right)^{M-k+1} \left(\left(1-\frac{\pi\lambda}{2\beta_{SE}L}\sum_{q=0}^{L} s_1 s_2\sqrt{1-\delta_q^2}\right)\left(1-\frac{\pi\lambda}{2\beta_{R_m E}L}\sum_{q=0}^{L} s_3 s_4\sqrt{1-\delta_q^2}\right)\right)^{k-1} \tag{C.3}$$

APPENDIX C: PROOF OF THEOREM 4

Based on (23), we can calculate following:

$$P_{sout}^{ni,DF} = \sum_{k=1}^{K} \binom{M}{k-1} \left(P_r\left(\min\Psi < R_{th}\right)\right)^{M-k+1} \times \left(1-P_r\left(\min\Psi < R_{th}\right)\right)^{k-1}, \tag{C.1}$$

and

$$P_r\left(\min\Psi < R_{th}\right) = 1 - \underbrace{P_r\left(\left(C_{SR_m} - C_{SE}\right) \geq R_{th}\right)}_{I_3} \times \underbrace{P_r\left(\left(C_{R_m D} - C_{R_m E}\right) \geq R_{th}\right)}_{I_4}, \tag{C.2}$$

where as can be seen from (C.2), $I_1 = I_3$, similar to solving for I_1, I_4 can be solved. I_4 is expressed by $I_4 = 1 - \frac{\pi\lambda}{2\beta_{R_m E}L}\sum_{q=0}^{L}\tilde{m}_3(x)\sqrt{1-\delta_q^2}$, $\tilde{m}_3(x) = \left(1-e^{-\frac{\xi(x)\left(\bar{\gamma}\alpha\sigma_{eR_m D}^2 p+\bar{\gamma}\alpha\sigma_{eR_m D}^2 t+v\right)}{\bar{\gamma}\beta_{R_m D}(t\alpha-p\xi(x)\alpha)}}\right) \times \left(e^{-\frac{x\left(\bar{\gamma}\alpha\sigma_{eR_m E}^2 p+\bar{\gamma}\alpha\sigma_{eR_m E}^2 t+v\right)}{\bar{\gamma}\beta_{R_m E}(t\alpha-px\alpha)}}\right)$.

Substituting I_1 and I_4 into (C.1), we can get (C.3), shown at the top of this page.

APPENDIX D: PROOF OF COROLLARY 1

At high SNRs regime, combined (15), the OP for non-ideal case is expressed by

$$P_{out}^{\infty,ni} = \sum_{k=1}^{K} \binom{M}{k-1} \left(1-e^{-\Theta_2-\Theta_3}e^{-\frac{(\Theta_4+\Theta_5)}{\bar{\gamma}}}\right)^{M-k+1} \times \left(e^{-\Theta_2-\Theta_3}e^{-\frac{(\Theta_4+\Theta_5)}{\bar{\gamma}}}\right)^{k-1}, \tag{D.1}$$

where $\Theta_4 = \frac{\varepsilon\nu}{\beta_{SR_m}(t(1-\alpha)-p\varepsilon(1-\alpha))}$, $\Theta_5 = \frac{\varepsilon\nu}{\beta_{R_m D}(t\alpha-p\varepsilon\alpha)}$. When $x \to 0$, then $e^{-x} \to 1$. Based on this, $e^{-\frac{(\Theta_4+\Theta_5)}{\bar{\gamma}}} \to 1$, and we can obtain (28).

Combing (16) and $x \to 0$, $e^{-x} \to 1$, we can obtain following:

$$P_{out}^{\infty,id} \approx \sum_{k=1}^{K} \binom{M}{k-1} \left(1-e^{-\frac{1}{\bar{\gamma}}\Theta_1}\right)^{M-k+1}, \tag{D.2}$$

where $\frac{\Theta_1}{\bar{\gamma}} \to 0$, $1-e^{-\frac{\Theta_1}{\bar{\gamma}}} \to \frac{\Theta_1}{\bar{\gamma}}$, then (29) can be obtained.

APPENDIX E:PROOF OF COROLLARY 3

We first simplify the SOP under two protocols in the non-ideal case, and its exact expressions are given by

$$P_{asout}^{ni,MF} = \sum_{k=1}^{K} \binom{M}{k-1} \left(\left(1-\Phi_1\right)\left(1-\Phi_3\right)\right)^{k-1} \times \left(1-\left(1-\Phi_1\right)\left(1-\Phi_3\right)\right)^{M-k+1}, \tag{E.1}$$

and

$$P_{asout}^{ni,DF} = \sum_{k=1}^{K} \binom{M}{k-1} \left(\left(1-\Phi_1\right)\left(1-\Phi_2\right)\right)^{k-1} \times \left(1-\left(1-\Phi_1\right)\left(1-\Phi_2\right)\right)^{M-k+1}, \tag{E.2}$$

where $\Phi_1 = \frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L} e^{-\Theta_6}e^{-\frac{\Theta_7}{\bar{\gamma}}}\left(1-E_1 e^{-\frac{E_2}{\bar{\gamma}}}\right)\sqrt{1-\delta_q^2}$, $\Phi_3 = \frac{\pi\lambda}{2L\beta_{SE}}\sum_{q=0}^{L} e^{-\Theta_6}e^{-\frac{\Theta_7}{\bar{\gamma}}}\left(1-E_3 e^{-\frac{E_4}{\bar{\gamma}}}\right)\sqrt{1-\delta_q^2}$, $\Phi_2 = \frac{\pi\lambda}{2L\beta_{R_m E}}\sum_{q=0}^{L} e^{-\Theta_8}e^{-\frac{\Theta_9}{\bar{\gamma}}}\left(1-E_3 e^{-\frac{E_4}{\bar{\gamma}}}\right)\sqrt{1-\delta_q^2}$, $\Theta_7 = \frac{x\nu}{\beta_{SE}(t-px)}$, $\Theta_9 = \frac{x\nu}{\beta_{R_m E}(t-px)}$, $E_2 = e^{-\frac{\xi(x)\nu}{\beta_{SR_m}(t(1-\alpha)-p(1-\alpha)\xi(x))}}$, $E_4 = e^{-\frac{\xi(x)\nu}{\beta_{R_m D}(t\alpha-p\alpha\xi(x))}}$.

As we can see that Θ_7 ,Θ_9, E_2 and E_4 are constants, and when $\bar{\gamma} \to \infty$, $e^{-\Theta_6}e^{-\frac{\Theta_7}{\bar{\gamma}}}\left(1-E_1 e^{-\frac{E_2}{\bar{\gamma}}}\right) \to e^{-\Theta_6}\left(1-E_1\right)$, $e^{-\Theta_6}e^{-\frac{\Theta_7}{\bar{\gamma}}}\left(1-E_3 e^{-\frac{E_4}{\bar{\gamma}}}\right) \to e^{-\Theta_6}\left(1-E_3\right)$, $e^{-\Theta_8}e^{-\frac{\Theta_9}{\bar{\gamma}}}\left(1-E_3 e^{-\frac{E_4}{\bar{\gamma}}}\right) \to e^{-\Theta_8}\left(1-E_3\right)$, thus we can obtain the SOP in the high MER regime for non-ideal case.

APPENDIX F:PROOF OF COROLLARY 3

Based on (26) and (27), when SNRs are in high regime, $s_1^{\Delta} \to 1$, $s_3^{\Delta} \to 1$, $s_2^{\Delta} \to \frac{\xi(x)}{\beta_{SR_m}\bar{\gamma}(1-\alpha)}$, $s_4^{\Delta} \to \frac{\xi(x)}{\beta_{R_m D}\bar{\gamma}\alpha}$, $\omega_1^{\Delta} \approx \omega_1^{\Gamma}$, $\omega_2^{\Delta} \approx \omega_2^{\Gamma}$ and $\omega_3^{\Delta} \approx \omega_3^{\Gamma}$.

After algebra operations, we can get the SOP for ideal case.

REFERENCES

[1] M. L. J. L. H. P. P. M. J. L. L. X. Li, Q. Wang, "Cooperative wireless-powered NOMA relaying for B5G IoT networks with hardware impairments and channel estimation errors," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5453–5467, Apr. 2021.

[2] M. Zeng, X. Li, G. Li, W. Hao, and O. A. Dobre, "Sum Rate Maximization for IRS-Assisted Uplink NOMA," *IEEE Communications Letters*, vol. 25, no. 1, pp. 234–238, . 2021.

[3] 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 Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021.

[4] S. Gallenmller, J. Naab, I. Adam, and G. Carle, "5g urllc: A case study on low-latency intrusion prevention," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 35–41, Oct. 2020.

[5] X. Li, J. Fang, H. Li, and P. Wang, "Millimeter wave channel estimation via exploiting joint sparse and low-rank structures," *IEEE Transactions on Wireless Communications*, vol. 17, no. 2, pp. 1123–1133, Feb. 2018.

[6] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[7] R. Zhao, H. Lin, Y. He, D. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

[8] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO Generalized-K fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[9] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[10] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving physical layer security for MISO systems via using artificial noise," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.

[11] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Beamforming optimization for physical layer security in MISO wireless networks," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, Jul. 2018.

[12] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 126–10 132, Dec. 2016.

[13] Q. Yang, H. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7547–7560, Nov. 2016.

[14] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[15] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[16] R. Rezaei, S. Sun, X. Kang, Y. L. Guan, and M. R. Pakravan, "Secrecy throughput maximization for full-duplex wireless powered iot networks under fairness constraints," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6964–6976, Aug. 2019.

[17] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[18] G. Brante, H. Alves, R. D. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1330–1342, Apr. 2015.

[19] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[20] J. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 28–38, Jan. 2016.

[21] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2488–2501, Mar. 2019.

[22] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[23] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Communications Letters*, vol. 12, no. 4, pp. 235–237, Apr. 2008.

[24] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[25] J. L. Vicario, A. Bel, J. A. Lopez-salcedo, and G. Seco, "Opportunistic relay selection with outdated CSI: outage probability and diversity analysis," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

[26] S. Kim, Y. Ko, and J. Heo, "Outage analysis of amplify-and-forward partial relay selection scheme with multiple interferers," *IEEE Communications Letters*, vol. 15, no. 12, pp. 1281–1283, Dec. 2011.

[27] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.

[28] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1607–1622, May. 2015.

[29] Z. Zhou, M. Peng, Z. Zhao, W. Wang, and R. S. Blum, "Wireless-powered cooperative communications: Power-splitting relaying with energy accumulation," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 969–982, Apr. 2016.

[30] Z. Liu, G. Lu, Y. Ye, and X. Chu, "System outage probability of PS-SWIPT enabled two-way AF relaying with hardware impairments," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 532–13 545, Nov. 2020.

[31] H. Chen, Y. Li, Y. Jiang, Y. Ma, and B. Vucetic, "Distributed power splitting for SWIPT in relay interference channels using game theory," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 410–420, Jan. 2015.

[32] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[33] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[34] P. D. Diamantoulakis, K. N. Pappi, Z. Ding, and G. K. Karagiannidis, "Wireless-powered communications with Non-Orthogonal Multiple Access," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8422–8436, Dec. 2016.

[35] Z. Yang, Z. Ding, P. Fan, and N. Al-Dhahir, "The impact of power allocation on cooperative Non-orthogonal Multiple Access networks with SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4332–4343, Jul. 2017.

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

[37] A. A. Boulogeorgos, V. M. Kapinas, R. Schober, and G. K. Karagiannidis, "I/Q-Imbalance self-interference coordination," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4157–4170, Jun. 2016.

[38] A. Tusha, S. Doan, and H. Arslan, "IQI mitigation for narrowband iot systems with ofdm-im," *IEEE Access*, vol. 6, pp. 44 626–44 634, 2018.

[39] J. Li, M. Matthaiou, and T. Svensson, "I/Q imbalance in AF Dual-Hop relaying: Performance analysis in Nakagami-m fading," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 836–847, Mar. 2014.

[40] X. Li, H. Mengyan, 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 Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[41] X. Li, M. Liu, C. Deng, P. T. Mathiopoulos, Z. Ding, and Y. Liu, "Full-duplex cooperative NOMA relaying systems with I/Q imbalance and imperfect SIC," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 17–20, 2020.

[42] S.W.Kim, "Modify-and-forward for securing cooperative relay communications," in *Proc. Int. Zurich Seminar Commun, Zurich, Switzerland*, Feb 2014, pp. 136–139.

[43] Q. Vien, T. A. Le, H. X. Nguyen, and H. Phan, "A secure network coding based modify-and-forward scheme for cooperative wireless relay networks," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1–5.

[44] S. Chu, "Secrecy analysis of modify-and-forward relaying with relay selection," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1796–1809, Feb. 2019.

[45] Q. Vien, T. A. Le, and T. Q. Duong, "Opportunistic secure transmission for wireless relay networks with modify-and-forward protocol," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[46] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 286–12 290, Oct. 2020.

[47] J. Zhang, G. Pan, and Y. Xie, "Secrecy analysis of wireless-powered multi-antenna relaying system with nonlinear energy harvesters and imperfect CSI," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 460–470, Jun. 2018.