

# Secrecy Outage Probability of Energy-Harvesting Cooperative NOMA Transmissions with Relay Selection

Abdelhamid Salem, *Member, IEEE*, Leila Musavian, *Member, IEEE*,  
Eduard Jorswieck, *Senior Member, IEEE*, and Sonia Aïssa, *Fellow, IEEE*

**Abstract**—Three relay selection techniques, aiming at achieving secure non-orthogonal multiple access in cooperative energy-harvesting (EH) communications, are proposed and compared. In the cooperative relaying system, the source node communicates with multiple users through amplify-and-forward EH relays in the presence of a passive eavesdropper. The relay selection is a two-stage strategy, where the first stage aims at achieving the users' target data rate, and the second aims at optimizing the secrecy outage probability. New explicit analytical expressions for the secrecy outage probability are derived for three operating scenarios: i) when the channel state information (CSI) of the eavesdropper is unknown, and a two-stage conventional relay selection scheme is considered, ii) when CSI of the eavesdropper is known, and a two-stage optimal relay selection scheme is used, and iii) when multiple relays participate in forwarding the signal to the end users. Monte-Carlo simulations are provided to confirm the derivations, and the effects of the main system parameters on its secrecy are investigated. In particular, it is shown that the optimal relay selection scheme outperforms the conventional and the multiple-relays schemes in terms of secrecy outage probability, and that this superiority becomes more obvious when the number of the relays increases.

**Index Terms**—NOMA, cooperative communications, energy harvesting, secrecy outage probability, physical-layer security.

## I. INTRODUCTION

Non-orthogonal multiple access (NOMA) is a promising technology to enhance the efficiency of wireless communication systems [1]. The main idea of NOMA is to serve multiple users with different power levels. More specifically, the source superimposes the signals of the users in the same frequency, time and code domains, but with different power levels. In this way, NOMA opportunistically explores the multi-user diversity, e.g., users with poor channel conditions are served with higher transmission power levels.

A. Salem is with the Department of Electronic and Electrical Engineering, University College London, London, WC1E 7JE, U.K. (e-mail: a.salem@ucl.ac.uk). L. Musavian is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK. (e-mail: Leila.musavian@essex.ac.uk). E. Jorswieck is with the Department of Information Theory and Communication Systems, TU Braunschweig, Germany (e-mail: e.jorswieck@tu-bs.de). S. Aïssa is with the Institut National de la Recherche Scientifique (INRS-EMT), University of Quebec, Montreal, QC, H5A 1K6, Canada. (e-mail: aissa@emt.inrs.ca).

This work is supported in parts by the UK EPSRC under grant EP/N032268/1, and the German Research Foundation (DFG) under grant JO 801/23-1.

These users can detect their signals by treating the other users' signals as noise. On the other hand, the users with strong channel conditions can apply successive interference cancellation (SIC) technique, in which they detect their own signals by removing the weaker users' signals [1].<sup>1</sup> The impact of NOMA technique on the performance of communication systems has been investigated in several works. For instance, [2] demonstrated that NOMA can achieve better sum-rate and outage performance than the traditional orthogonal multiple access (OMA) when the power coefficients and users' rates are carefully chosen. A power allocation strategy to maximize the sum-rate in NOMA systems with quality-of-service (QoS) constraints was investigated in [3]. The impact of the availability of the channel state information (CSI) at the source on the performance of NOMA systems was also studied in [4]. In addition, different forms of cooperative NOMA systems have been studied in the literature. In [5], it was shown that NOMA in coordinated direct and relayed transmission can enhance the system performance compared to NOMA in non-coordinated transmission. The achievable average rate of cooperative NOMA systems is analyzed in [6] for independent Rayleigh fading channels. In the same context, the outage performance of cooperative NOMA networks is evaluated in [7], where a simultaneous wireless information and power transfer (SWIPT) technique is adopted at the near users to forward the far user's signals. Further work in [8] considered NOMA in multi-antenna relaying systems, where the relay's antenna that optimizes the signal-to-interference-plus-noise ratio (SINR) is selected to forward the signal; the results in this work demonstrate the superiority of NOMA over OMA. In [9], the authors consider a cooperative NOMA system, in which the source communicates with the users through an energy harvesting (EH) relay node, and the impact of power allocation on the considered SWIPT system is investigated. In this direction, a cooperative SWIPT-NOMA protocol where users near the source work as EH relays to help the farther users is proposed in [10].

Moreover, due to the vulnerability of wireless channels,

<sup>1</sup>Hereafter, a user with stronger channel condition is referred to as stronger user. Also, a user with poorer channel condition is referred to as weaker user.

attention to the issue of security in wireless communication systems has increased rapidly. Physical-layer security, which is based on the physical characteristics of the channels, has been extensively considered to enhance the security performance of wireless communication networks. This concept was introduced in [11], which shows that a secure communication can be achieved if the eavesdropper/wiretap channel is noisier than a legitimate destination/main channel. Very recently, physical-layer security has been studied to perform secure transmission in NOMA systems. In this trend, physical-layer security in NOMA systems was studied in [12], with the aim to maximize the NOMA secrecy rate subject to QoS requirements. In [13], the security of NOMA in large-scale networks was considered, and new analytical expressions for the secrecy outage probability were derived. The security in a downlink NOMA transmission system, in which the users are grouped in clusters was studied in [14]. The secrecy rate optimization problem for a downlink NOMA system subject to SIC constraints has been studied in [15]. Application of NOMA to a multi-user system with both multi- and uni-cast messages was investigated in [16]. Since the uni-cast message can be received by all users, secure NOMA transmission to prevent multi-cast destinations from decoding the uni-cast signal has also been considered in [16]. Also, an optimal NOMA design subject to QoS and secrecy outage constraints was considered in [17]. In this direction, the secrecy outage probability of a NOMA system with different transmit antenna selection schemes was studied in [18].

In this paper, different relay selection schemes are investigated to enhance the secrecy performance of cooperative SWIPT-NOMA against any passive eavesdropping attack. In the considered system, the source and the users have fixed power supplies. The relays, on the other hand, are EH nodes that harvest energy from the received source signal and then amplify-and-forward (AF) this signal to the users. Three relay selection schemes are considered in this work. The first is based on scenarios where the CSI of the eavesdropper channel is unknown at the legitimate nodes, in which case we study conventional relay selection. The second relay selection scheme is based on full knowledge of the main and the eavesdropper's CSI. Here, an optimal relay selection scheme is proposed. Thirdly, we consider the case when multiple relays are used to amplify-and-forward the source signal to the users.<sup>2</sup>

Therefore, the major contributions of this work are twofold. Firstly, novel relay selection schemes are proposed to enhance the secrecy performance of cooperative SWIPT-NOMA systems for the three aforementioned cases. Secondly, although the performance analysis of such co-

<sup>2</sup>It is important to mention that these three cases/schemes are investigated in order to explain the effect of the channel knowledge on the system performance, and not simply for comparison purpose. A two-stage selection strategy is considered in each relay selection scheme. The goal of the first stage is to realize the users' target data rate, and the second stage aims at optimizing the secrecy outage probability at the strongest user.

operative systems is hard and challenging, in this paper, new explicit analytical expressions for the secrecy outage probability are derived for the three relay selection schemes. Furthermore, the impact of the main system parameters on the secrecy performance of the proposed relay selection schemes are examined. Results show that optimal relay selection outperforms the conventional and the multiple-relay schemes. It is also shown that increasing the SNR and the number of relaying nodes enhances the secrecy performance, whereas an increase of the total number of users and their target data rates results in a deterioration of the system security in terms of secrecy outage probability.

Next, Section II describes the system under consideration. Sections III and IV derive the analytical expressions for the secrecy outage probability when CSI of the eavesdropper is unknown or fully known, respectively. Section V, derives the secrecy outage probability when multiple relays are used to forward the source message. Numerical and simulation results are presented and discussed in Section VI. Finally, the main conclusions of this work are stated in Section VII.

## II. SYSTEM MODEL AND PRELIMINARIES

Consider a downlink relaying system consisting of a source transmitter,  $N$  EH-AF relays and  $M$  legitimate users, operating in the presence of a passive eavesdropper. Each node in the system is equipped with a single antenna and operates in half-duplex mode. The source and users' equipments have fixed power supplies, while the relays are EH nodes solely relying on their harvested energy. Each relay implements a power-splitting EH protocol, as described in [19], to harvest energy and process information from the received observations. The channel coefficient between the source and a relay  $n$  is denoted by  $h_{sr_n}$ , and the channel coefficients between a relay  $n$  and user  $i$  and the eavesdropper are denoted  $h_{r_n u_i}$  and  $h_{r_n e}$ , respectively. The channels are assumed to be independent and identically distributed (i.i.d.) Rayleigh fading channels.<sup>3</sup> The distances between the nodes are denoted by  $d_{sr_n}$  (source to relay  $n$ ),  $d_{r_n u_i}$  (relay  $n$  to user  $i$ ), and  $d_{r_n e}$  (relay  $n$  to eavesdropper). Due to deep shadowing, the communication in the system is achieved through the EH-relay node(s), and the direct links (source to legitimate users, and source to eavesdropper) are assumed not available, e.g., the users and the eavesdropper are not in the coverage area of the source. This assumption has been widely adopted in the literature pertaining to cooperative systems [22]–[24].

Therefore, the source and the users communicate with each other over two phases. During Phase-I, following the principle of NOMA, the source node transmits a superimposed signal to the users, which is received firstly by all the relays. Part of the received signal energy will be harvested by the relays to charge their batteries using the power splitting technique, while the other part of the received

<sup>3</sup>The Rayleigh fading model has been widely considered in the literature of EH systems, see e.g. [1], [7], [9], [10], [19]–[22].

signal energy will be allocated for information processing. The second phase (Phase-II), consists in the forwarding of signals through AF relaying.

### A. First Transmission Phase

In Phase-I, the source transmits the signal using superposition coding,  $s = \sum_{i=1}^M \sqrt{\alpha_i P_s} x_i$ , where  $P_s$  is the source power,  $x_i$  is the signal for user  $i$ , and  $\alpha_i$  is the power allocation coefficient for user  $i$ , with  $\sum_{i=1}^M \alpha_i = 1$ . The users are ordered based on their average channel gains, which in the considered scenario is the same as path loss. The path loss does not vary fast compared to the small-scale fading. Thus, the distance-based users' ranking can simplify the design of power allocation and rate adaptation for NOMA. The application of distance-based users' ranking in NOMA systems has been thoroughly discussed in [25]–[28]. With such ordering, user  $M$  is the closest user to the source, and is thus the strongest one. The observation at the  $n^{\text{th}}$  relay is hence given by

$$y_{r_n} = h_{sr_n} \sum_{i=1}^M \sqrt{\frac{\alpha_i P_s}{d_{sr_n}^m}} x_i + n_{r_n}, \quad (1)$$

where  $m$  is the path-loss exponent, and  $n_{r_n}$  is the additive white Gaussian noise (AWGN) at relay  $n$  with variance  $\sigma_{r_n}^2$ , i.e.,  $n_{r_n} \sim \mathcal{CN}(0, \sigma_{r_n}^2)$ . We define  $\beta_{r_n}$  as the fraction of the received power allocated for the EH, and  $(1 - \beta_{r_n})$  as the part allocated for the information processing. Consequently, the received signal at the relay's EH receiver is

$$y_{r_n}^{\text{EH}} = h_{sr_n} \sum_{i=1}^M \sqrt{\frac{\beta_{r_n} \alpha_i P_s}{d_{sr_n}^m}} x_i + n_{r_n}. \quad (2)$$

Neglecting the noise power, the harvested energy at relay  $n$  can be estimated as  $\mathcal{E}_{r_n} = \frac{T \eta_{r_n} \beta_{r_n} P_s |h_{sr_n}|^2}{2 d_{sr_n}^m}$ , where  $\eta_{r_n}$  is the EH efficiency and  $T$  is the time required to transmit the signal from the source to the users. The received signal at the information receiver (IR) of relay  $n$  is

$$y_{r_n}^{\text{IR}} = h_{sr_n} \sum_{i=1}^M \sqrt{\frac{(1 - \beta_{r_n}) \alpha_i P_s}{d_{sr_n}^m}} x_i + n_{r_n}. \quad (3)$$

### B. Second Transmission Phase

In Phase-II, the relay transmits a scaled version of the received signal,  $x_{r_n} = G_{r_n} y_{r_n}^{\text{IR}}$ , where  $G_{r_n}$  is the relay gain. Given that  $\sum_{i=1}^M \alpha_i = 1$ , the relay gain is defined by

$$G_{r_n} = \sqrt{\frac{P_{r_n}}{\frac{(1 - \beta_{r_n}) P_s}{d_{sr_n}^m} |h_{sr_n}|^2 + \sigma_{r_n}^2}}. \quad (4)$$

where  $P_{r_n}$  is the harvested power at relay  $n$  which is  $P_{r_n} = \frac{\eta_{r_n} \beta_{r_n} P_s |h_{sr_n}|^2}{2 d_{sr_n}^m}$ . Now substituting  $P_{r_n}$  in (4) we get

$$G_{r_n} = \sqrt{\frac{\eta_{r_n} \beta_{r_n} P_s |h_{sr_n}|^2}{(1 - \beta_{r_n}) P_s |h_{sr_n}|^2 + d_{sr_n}^m \sigma_{r_n}^2}}. \quad (5)$$

Therefore, the received signals at user  $u_i$  and at the eavesdropper via relay  $n$  are given by (6) and (7) respectively, where  $n_{u_i}$  is the AWGN at user  $u_i$  with variance  $\sigma_{u_i}^2$ , i.e.,  $n_{u_i} \sim \mathcal{CN}(0, \sigma_{u_i}^2)$ , and  $n_e$  is the AWGN at the eavesdropper with variance  $\sigma_e^2$ , i.e.,  $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ . Similar to the strongest user in conventional NOMA systems, user  $M$  will carry out SIC, i.e., user  $M$  first detects all the other users' signals and then subtracts them from its observation before decoding its own message  $x_M$ .

### C. SINR Derivations

The SINR at user  $M$  to detect the  $k^{\text{th}}$  user message,  $x_k$ , where  $1 \leq k < M$ , via relay  $n$ , is given by (8). After all signals are detected successfully, user  $M$  removes these messages and detects its own message,  $x_M$ , with SINR given by

$$\gamma_{n,M} = \frac{(1 - \beta_{r_n}) P_s G_{r_n}^2 \alpha_M |h_{sr_n}|^2 |h_{r_n u_M}|^2}{G_{r_n}^2 |h_{r_n u_M}|^2 d_{sr_n}^m \sigma_{r_n}^2 + d_{sr_n}^m d_{r_n u_M}^m \sigma_{u_M}^2}. \quad (9)$$

Similar to the weak users in conventional NOMA systems, user  $k$  detects its message,  $x_k$ , by treating the other stronger users' messages,  $\sum_{i=k+1}^M x_i$ , as noise. Therefore, the SINR for detecting the messages  $x_j$  at user  $k$ , where  $j \in [1 : k]$ , using relay  $n$ , is given by (10).

The worst-case scenario is taken into account, in which the eavesdropper always performs SIC successfully and targets the strong user, i.e., user  $M$ , [12]. Therefore, the SINR at the eavesdropper to detect  $x_M$  through relay  $n$  is given by

$$\gamma_{n,e} = \frac{(1 - \beta_{r_n}) P_s G_{r_n}^2 \alpha_M |h_{sr_n}|^2 |h_{r_n e}|^2}{G_{r_n}^2 |h_{r_n e}|^2 d_{sr_n}^m \sigma_{r_n}^2 + d_{sr_n}^m d_{r_n e}^m \sigma_e^2}. \quad (11)$$

Similarly, the SINR at the eavesdropper to detect the  $k^{\text{th}}$  user's signal is given by (12).

In the next three sections, three scenarios are considered to optimize the secrecy performance of user  $M$ , when only one relay is selected to forward the signal and the eavesdropper's CSI is unknown or fully known, or when multiple relays are chosen to forward the signal.

## III. CONVENTIONAL RELAY SELECTION

In this scenario, the CSI pertaining to the eavesdropper is assumed to be unknown at the legitimate nodes. Conventional relay selection strategy is proposed in this scenario. The selected relay, active in the second transmission phase, is the one that can provide the maximum SINR at the intended user,  $u_M$ , while at the same time providing the required data rates to the other users. Hence, the aim of this scheme is to (i) maximize the SINR at the intended

$$\begin{aligned}
y_{n,u_i} &= G_{r_n} \frac{h_{r_n u_i}}{\sqrt{d_{r_n u_i}^m}} \left( h_{sr_n} \sum_{k=1}^M \sqrt{\frac{(1-\beta_{r_n}) \alpha_k P_s}{d_{sr_n}^m}} \mathbf{x}_k + n_{r_n} \right) + n_{u_i}, \\
&= \sqrt{\frac{(1-\beta_{r_n}) P_s}{d_{sr_n}^m d_{r_n u_i}^m}} G_{r_n} h_{r_n u_i} h_{sr_n} \left( \sum_{k=1}^M \sqrt{\alpha_k} \mathbf{x}_k \right) + \sqrt{\frac{1}{d_{r_n u_i}^m}} G_{r_n} h_{r_n u_i} n_{r_n} + n_{u_i}, \tag{6}
\end{aligned}$$

$$y_{n,e} = \sqrt{\frac{(1-\beta_{r_n}) P_s}{d_{sr_n}^m d_{r_n e}^m}} G_{r_n} h_{r_n e} h_{sr_n} \left( \sum_{k=1}^M \sqrt{\alpha_k} \mathbf{x}_k \right) + \sqrt{\frac{1}{d_{r_n e}^m}} G_{r_n} h_{r_n e} n_{r_n} + n_e, \tag{7}$$

---


$$\gamma_{n,x_k \rightarrow M} = \frac{(1-\beta_{r_n}) P_s G_{r_n}^2 \alpha_k |h_{sr_n}|^2 |h_{r_n u_M}|^2}{(1-\beta_{r_n}) P_s G_{r_n}^2 |h_{sr_n}|^2 |h_{r_n u_M}|^2 \sum_{i=k+1}^M \alpha_i + G_{r_n}^2 |h_{r_n u_M}|^2 d_{sr_n}^m \sigma_{r_n}^2 + d_{sr_n}^m d_{r_n u_M}^m \sigma_{u_M}^2}. \tag{8}$$


---

$$\gamma_{n,x_j \rightarrow k} = \frac{(1-\beta_{r_n}) P_s G_{r_n}^2 \alpha_j |h_{sr_n}|^2 |h_{r_n u_k}|^2}{(1-\beta_{r_n}) P_s G_{r_n}^2 |h_{sr_n}|^2 |h_{r_n u_k}|^2 \sum_{i=j+1}^M \alpha_i + G_{r_n}^2 |h_{r_n u_k}|^2 d_{sr_n}^m \sigma_{r_n}^2 + d_{sr_n}^m d_{r_n u_k}^m \sigma_{u_k}^2}. \tag{10}$$


---

$$\gamma_{n,x_k \rightarrow e} = \frac{(1-\beta_{r_n}) P_s G_{r_n}^2 \alpha_k |h_{sr_n}|^2 |h_{r_n e}|^2}{(1-\beta_{r_n}) P_s G_{r_n}^2 |h_{sr_n}|^2 |h_{r_n e}|^2 \sum_{i=k+1}^M \alpha_i + G_{r_n}^2 |h_{r_n e}|^2 d_{sr_n}^m \sigma_{r_n}^2 + d_{sr_n}^m d_{r_n e}^m \sigma_e^2}. \tag{12}$$


---

user, and (ii) serve the other users with their required data rates.

Firstly, we select a sub-set of the EH-relays ( $N_r$ ) that satisfy the following conditions:

$$N_r = \left\{ n : 1 \leq n \leq N, \frac{1}{2} \log(1 + \gamma_{n,M}) > \bar{R}_M, \right.$$

$$\left. \frac{1}{2} \log(1 + \gamma_{n,k}) > \bar{R}_k, \frac{1}{2} \log(1 + \gamma_{n,x_k \rightarrow j}) > \bar{R}_k \right\}, \tag{13}$$

where  $k \in \{1, 2, \dots, M-1\}$ ,  $j \in \{k+1, k+2, \dots, M\}$ ,  $\log(\cdot)$  represents logarithm of base-2,  $\bar{R}_M$  and  $\bar{R}_k$  are the target data rates at user  $M$  and user  $k$ , respectively, and the size of  $N_r$  is denoted by  $|N_r|$ .

From this sub-set  $N_r$ , the best relay ( $n^*$ ) is selected as the one that maximizes the SINR at user  $M$ , hence,  $\gamma_{n^*,M} = \max\{\gamma_{n,M}, n \in N_r\}$ .

#### A. Performance Analysis

Here, we will characterize the secrecy outage probability for the conventional relay selection scheme. The secrecy outage probability is the probability that the secrecy rate is less than a target secrecy rate  $R_0$  [29]. Therefore, the

secrecy outage probability in this scheme can be calculated by

$$P_{\text{sop}} = \underbrace{\Pr(|N_r| = 0)}_{O_1} \cup \underbrace{\Pr\left(\frac{1 + \max_{n \in N_r} \{\gamma_{n,M}\}}{1 + \gamma_{n,e}} < \zeta, N_r > 0\right)}_{O_2}, \tag{14}$$

where  $O_1$  is the probability that all the relays cannot provide the required data rates to the users, i.e.,  $N_r = \emptyset$ , and  $O_2$  is the probability that the secrecy rate at user  $M$  is less than the threshold value  $R_o$ , in which  $\zeta = 2^{2R_o}$ .

**Lemma 1.** From (13),  $O_1$  can be found as

$$O_1 = \prod_{n=1}^N \left\{ 1 - \Pr(R_{n,M} > \bar{R}_M) \prod_{k=1}^{M-1} \left[ \Pr(R_{n,k} > \bar{R}_k) \prod_{j=k+1}^M \Pr(R_{n,k \rightarrow j} > \bar{R}_k) \right] \right\}, \tag{15}$$

where

$$\Pr(R_{n,k} > \bar{R}_k) = \int_{\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}^{\infty} e^{-\left(z + \frac{\zeta_k a_4 z + a_5 \zeta_k}{z^2 (a_1 - a_2 \zeta_k) - a_3 z \zeta_k}\right)} dz, \tag{16}$$

$$O_2 = \sum_{Q=1}^N \underbrace{\left\{ \sum_{l=1}^Q \Pr(n^* = l) \Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma_{l,e}\zeta - 1 \mid |N_r| = Q, n^* = l \right) \right\}}_{S_1} \underbrace{\Pr(|N_r| = Q)}_{S_2}. \quad (22)$$

which can be expressed at high SNRs as [19]

$$\Pr(R_{n,k} > \bar{R}_k) \approx w_1 J_1[w_1] e^{-\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}, \quad (17)$$

where  $\zeta_k = 2^{2\bar{R}_k}$  and  $J_1[\cdot]$  is the first-order modified Bessel function of the second kind [30], and

$$\Pr(R_{n,k \rightarrow j} > \bar{R}_k) = \int_{\frac{b_3 \zeta_k}{b_1 - b_2 \zeta_k}}^{\infty} e^{-\left(z + \frac{\zeta_k b_4 z + b_5 \zeta_k}{z^2(b_1 - b_2 \zeta_k) - b_3 z \zeta_k}\right)} dz. \quad (18)$$

At high SNRs, (18) can be written as

$$\Pr(R_{n,k \rightarrow j} > \bar{R}_k) \approx w_2 J_1[w_2] e^{-\frac{b_3 \zeta_k}{b_1 - b_2 \zeta_k}}. \quad (19)$$

Also, we have

$$\Pr(R_{n,M} > \bar{R}_M) = \int_{\frac{c_2 \zeta_M}{c_1}}^{\infty} e^{-\left(z + \frac{\zeta_M c_3 z + c_4 \zeta_M}{z^2 c_1 - c_2 z \zeta_M}\right)} dz, \quad (20)$$

which, at high SNRs, can be expressed by

$$\Pr(R_{n,M} > \bar{R}_M) \approx w_3 J_1[w_3] e^{-\frac{c_2 \zeta_M}{c_1}}. \quad (21)$$

*Proof:* The proof is provided in Appendix A. ■

**Lemma 2.**  $O_2$  in (14) can be calculated using the law of total probability as in (22), where

$$\begin{aligned} \Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma \zeta - 1 \right) &= \\ &\int_0^{\infty} \prod_{\substack{n=1 \\ n \neq l}}^Q \left\{ 1 - \int_{\frac{c_2(\zeta + \gamma \zeta - 1)}{c_1}}^{\infty} e^{-\left(z + \frac{(\zeta + \gamma \zeta - 1)c_3 z + c_4(\zeta + \gamma \zeta - 1)}{z^2 c_1 - c_2 z(\zeta + \gamma \zeta - 1)}\right)} dz \right\} \\ &\times \left\{ \int_{\epsilon_1}^{\epsilon_2} \left[ \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 e_1 - e_2 \theta \gamma)}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} \right] e^{-\theta} d\theta \right. \\ &+ \int_{\epsilon_2}^{\infty} \left[ 1 - e^{-\left(\frac{(\zeta + \gamma \zeta - 1)c_3 \theta + c_4(\zeta + \gamma \zeta - 1)}{(\theta^2 c_1 - c_2 \theta(\zeta + \gamma \zeta - 1))}\right)} \right] \\ &\times \left. \left[ \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 e_1 - e_2 \theta \gamma)}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} \right] e^{-\theta} d\theta \right\} d\gamma. \quad (23) \end{aligned}$$

At high SNRs, we have

$$\begin{aligned} \Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma \zeta - 1 \right) &= \\ &\sum_{i=1}^n H_i e^{\gamma_i} \prod_{\substack{n=1 \\ n \neq l}}^Q \left\{ 1 - w_4 J_1[w_4] e^{-\frac{c_2(\zeta + \gamma_i \zeta - 1)}{c_1}} \right\} \\ &\times \left\{ e^{-\left(\frac{\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i}{\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i}\right)} \times \right. \\ &\frac{(\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i) (\epsilon_2 - \epsilon_1) e_1 \left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e^{-\frac{\epsilon_2 + \epsilon_1}{2}}}{\gamma_i \left(\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i\right)^2} \\ &+ \sum_{j=1}^n H_j \left\{ 1 - e^{-\left(\frac{(\zeta + \gamma_i \zeta - 1)c_3 \theta_j + c_4(\zeta + \gamma_i \zeta - 1)}{(\theta_j^2 c_1 - c_2 \theta_j(\zeta + \gamma_i \zeta - 1))}\right)} \right\} \times \\ &\left. \left\{ \frac{1}{\gamma_i} e^{-\left(\frac{\gamma_i e_3 \theta_j + e_4 \gamma_i}{(\theta_j^2 e_1 - e_2 \theta_j \gamma_i)}\right)} \frac{(\gamma_i e_3 \theta_j + e_4 \gamma_i) \theta_j^2 e_1}{(\theta_j^2 e_1 - e_2 \theta_j \gamma_i)^2} \right\} \right\}, \quad (24) \end{aligned}$$

where  $\gamma_i$  and  $H_i$  are the  $i^{\text{th}}$  abscissa and weight of the  $n^{\text{th}}$  order Laguerre polynomial, respectively, [30, eq. (25.4.45)]. The probability that relay  $l$  is selected,  $\Pr(n^* = l) = p_l$ , is given by

$$\begin{aligned} p_l &= \sum_{i=1}^n H_i e^{x_i} \left( \int_{\frac{c_2 x}{c_1}}^{\infty} \frac{(c_3 z + c_4) z^2 c_1}{(z^2 c_1 - c_2 z x)^2} e^{-\left(z + \frac{x c_3 z + c_4 x}{z^2 c_1 - c_2 z x}\right)} dz \right) \\ &\times \prod_{\substack{n=1 \\ l \neq n}}^Q \left( 1 - \int_{\frac{c_2 x}{c_1}}^{\infty} e^{-\left(z + \frac{x c_3 z + c_4 x}{z^2 c_1 - c_2 z x}\right)} dz \right), \quad (25) \end{aligned}$$

which, at high SNRs, is expressed as

$$\begin{aligned} p_l &= \sum_{i=1}^n H_i e^{x_i} \times \\ &\left( \frac{4\gamma_M c_3 J_0 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} \right] e^{-\frac{c_2 x}{c_1}}}{2x c_1} + \frac{c_2 x w_5 J_1 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} \right] e^{-\frac{c_2 x}{c_1}}}{c_1} \right) \\ &\times \prod_{\substack{n=1 \\ l \neq n}}^Q \left( 1 - \sqrt{\frac{4x c_3}{c_1}} J_1 \left[ \sqrt{\frac{4x c_3}{c_1}} \right] e^{-\frac{c_2 x}{c_1}} \right), \quad (26) \end{aligned}$$

where  $x_i$  and  $H_i$  are the  $i^{\text{th}}$  abscissa and weight of the  $n^{\text{th}}$  order Laguerre polynomial, respectively, [30, eq. (25.4.45)]. In addition,  $S_2$  in (22) can be calculated using

$$\Pr(|N_r| = Q) = \binom{N}{Q} P_1^{N-Q} (1 - P_1)^Q, \quad (27)$$

where  $P_1 = \Pr(|N_r| = 0)$ .

*Proof:* The proof is provided in Appendix B. ■

**Theorem 3.** *The secrecy outage probability achieved by the two-stage conventional relay selection strategy can be calculated as*

$$P_{\text{sop}} = O_1 \cup O_2, \quad (28)$$

where  $O_1$  and  $O_2$  are derived in Lemma 1 and Lemma 2, respectively.

#### IV. OPTIMAL RELAY SELECTION

In certain cases, where a user can play dual role as a legitimate receiver for some messages and as an eavesdropper for others, e.g., in a time-division multiple access (TDMA) environment, the legitimate nodes can know the eavesdropper's CSI [31], [32]. In other words, the eavesdropper is a user of the system and has an ongoing communication with the source, i.e., the eavesdropper is not a hidden node and is not necessarily a malicious user. Instead, it is an active node participating in the communication exchange with the source. When CSI of both the wiretap and the main links is known, the relay node that maximizes the secrecy rate is considered to be the optimal relay. Therefore, in this scenario, we consider an optimal relay selection scheme, in which the best selected relay is the one that can provide the maximum secrecy rate at user  $M$  and, at the same time, can provide the required data rates to the other users. In this scheme, we select a sub-set,  $N_r$ , of the EH-relays that satisfy the users data rates, as explained in the previous section in (13). Then, from this sub-set,  $N_r$ , the best relay  $n^*$  that optimizes the secrecy rate at user  $M$  is selected. Hence,

$$C_{s,M}^* = \max \{C_{s,M}^n, n \in N_r\}, \quad (29)$$

where  $C_{s,M}^n$  is the secrecy rate of user  $M$  via relay  $n$ .

**Theorem 4.** *The secrecy outage probability achieved by the two-stage optimal relay selection strategy can be calculated as*

$$P_{\text{sop}} = O_1 \cup \sum_{Q=1}^N \left\{ \Pr \left( \max_{n \in Q} \{C_{s,M}^n\} < R_o \mid |N_r| = Q \right) \Pr(|N_r| = Q) \right\} \quad (30)$$

where  $O_1$  is given in Lemma 1,  $\Pr(|N_r| = Q)$  is expressed in (27), and

$$\begin{aligned} & \Pr \left( \max_{n \in Q} \{C_{s,M}^n\} < R_o \mid |N_r| = Q \right) = \\ & \int_0^{\infty} \prod_{\substack{n=1 \\ n \neq l}}^Q \left\{ 1 - \int_0^{\infty} e^{-\left( z + \frac{(\zeta + \gamma \zeta - 1)c_3 z + c_4(\zeta + \gamma \zeta - 1)}{(z^2 c_1 - c_2 z(\zeta + \gamma \zeta - 1))} \right)} dz \right\} \\ & \times \left\{ \int_{\epsilon_1}^{\epsilon_2} \left\{ \frac{1}{\gamma} e^{-\left( \frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)} \right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} \right\} e^{-\theta} d\theta \right. \\ & \left. + \int_{\epsilon_2}^{\infty} \left\{ 1 - e^{-\left( \frac{(\zeta + \gamma \zeta - 1)c_3 \theta + c_4(\zeta + \gamma \zeta - 1)}{(\theta^2 c_1 - c_2 \theta(\zeta + \gamma \zeta - 1))} \right)} \right\} \times \right. \\ & \left. \left\{ \frac{1}{\gamma} e^{-\left( \frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)} \right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} \right\} e^{-\theta} d\theta \right\} d\gamma. \end{aligned} \quad (31)$$

At high SNRs, the expression above can be approximated as follows:

$$\begin{aligned} & \Pr \left( \max_{n \in Q} \{C_{s,M}^n\} < R_o \mid |N_r| = Q \right) = \\ & \prod_{n=1}^Q \sum_{i=1}^n H_i e^{\gamma_i} \left\{ \left( e^{-\left( \frac{\gamma e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma}{\left( \left( \frac{\epsilon_2 + \epsilon_1}{2} \right)^2 \epsilon_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma \right)} \right)} \right. \right. \\ & \times \left. \frac{(\gamma e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma) (\epsilon_2 - \epsilon_1) \left( \frac{\epsilon_2 + \epsilon_1}{2} \right)^2 e_1}{\gamma \left( \left( \frac{\epsilon_2 + \epsilon_1}{2} \right)^2 \epsilon_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma \right)^2} \right) \\ & \left. + \sum_{j=1}^n H_j \left\{ 1 - e^{-\left( \frac{(\zeta + \gamma \zeta - 1)c_3 \theta_j + c_4(\zeta + \gamma \zeta - 1)}{(\theta_j^2 \epsilon_1 - c_2 \theta_j(\zeta + \gamma \zeta - 1))} \right)} \right\} \right\} \\ & \times \left\{ \frac{1}{\gamma_i} e^{-\left( \frac{\gamma_i e_3 \theta_j + e_4 \gamma_i}{(\theta_j^2 \epsilon_1 - e_2 \theta_j \gamma_i)} \right)} \frac{(\gamma_i e_3 \theta_j + e_4 \gamma_i) \theta_j^2 e_1}{(\theta_j^2 \epsilon_1 - e_2 \theta_j \gamma_i)^2} \right\}. \end{aligned} \quad (32)$$

*Proof:* The proof is provided in Appendix C. ■

#### V. COMMUNICATION WITH MULTIPLE RELAYS

In this scenario, in order to avoid the imperfect SIC at the users due to the effect of simultaneous multiple relays transmissions, an orthogonal transmission technique, such as TDMA, is employed in the second phase. Specifically, each relay transmits its message in a specific time slot in the second phase. In addition, the users apply maximum ratio combining (MRC) technique to maximize their total SINR. Consequently, taking into account that the CSI of

the eavesdropper is unknown and that  $l$  relays are used to forward the signal to the users, the rates at user  $M$  and at the eavesdropper can be written as

$$R_M = a \log \left( 1 + \sum_{n=1}^l \gamma_{n,M} \right), \quad R_e = a \log \left( 1 + \sum_{n=1}^l \gamma_{n,e} \right), \quad (33)$$

where  $a = \frac{1}{l+1}$ . We can now define a set  $\Phi$  which contains all the possible subsets of the available relay combinations that can provide the target data rates at the users,  $\Phi = [\Phi_1, \dots, \Phi_n, \dots, \Phi_C]$ , where  $\Phi_n$  is the  $n^{\text{th}}$  subset that contains a possible combination of the available relays, with the number of relays being  $|\Phi_n| = l_n$  and the number of subsets being  $|\Phi| = C$ .

#### A. Performance Analysis

Here, we will analyze the secrecy outage probability achieved by using multiple relays to amplify-and-forward the source signal to the users. The secrecy outage probability in this scheme can be calculated as

$$P_{\text{sop}} = \underbrace{\Pr(|\Phi| = 0)}_{A_1} \cup \underbrace{\Pr(C_{s,M} < R_o, |\Phi| \neq 0)}_{A_2}, \quad (34)$$

where  $A_1$  is the probability that all the relay sub-sets cannot provide the required data rates to the users, i.e., when  $\Phi = \emptyset$ , and  $A_2$  is the probability that the secrecy rate at user  $M$  is less than the threshold value.

**Lemma 5.** From (34), the probability  $A_1$  can be calculated by

$$A_1 = \prod_{n=1}^C \left\{ 1 - \Pr(R_{\Phi_n, M} > \bar{R}_M) \prod_{k=1}^{M-1} \Pr(R_{\Phi_n, k} > \bar{R}_k) \right\}, \quad (35)$$

where  $R_{\Phi_n, M}$  is the rate at user  $M$  using the relays in subset  $\Phi_n$ , and

$$\Pr(R_{\Phi_n, M} > \bar{R}_M) = 1 - \frac{2^{-Q} e^{\frac{A}{2}}}{\gamma_M} \sum_{q=0}^Q \binom{Q}{q} \sum_{n=0}^{N+q} \frac{(-1)^n}{\beta_n} \Re \left( \frac{\mathcal{M}_{\varphi_M} \left( \frac{A + 2\pi j n}{2\gamma_M} \right)}{\frac{A + 2\pi j n}{2\gamma_M}} \right) + E(A, N, Q), \quad (36)$$

where  $j^2 = -1$ ,  $\Re\{\cdot\}$  denotes the real part;  $A$ ,  $N$  and  $Q$  are positive integers used to control accuracy and satisfy the condition that a remainder error term  $E(A, N, Q)$  is negligible compared with the first term,

$$|E(A, N, Q)| = \frac{e^{-A}}{1 - e^{-A}} + \left| \frac{2^{-Q} e^{\frac{A}{2}}}{\gamma_M} \sum_{q=0}^Q (-1)^{N+1+q} \binom{Q}{q} \Re \left( \frac{\mathcal{M}_{\varphi} \left( \frac{A + 2\pi j (N + q + 1)}{2\gamma_M} \right)}{\frac{A + 2\pi j (N + q + 1)}{2\gamma_M}} \right) \right|, \quad (37)$$

$$\beta_n = \begin{cases} 2 & n = 0 \\ 1 & n = 1, 2, \dots, N + q \end{cases},$$

and

$$\mathcal{M}_{\varphi_M}(s) = \prod_{n=1}^{l_n} \int_0^{\infty} \frac{e^{-s\gamma_M}}{\gamma_M} \times \left\{ \int_{\frac{c_2\gamma_M}{c_1}}^{\infty} e^{-\left(x_n + \frac{\gamma_M c_3 x_n + c_4 \gamma_M}{(x_n^2 c_1 - c_2 x_n \gamma_M)}\right)} \frac{(\gamma_M c_3 x_n + c_4 \gamma_M) x^2 c_1}{(x_n^2 c_1 - c_2 x_n \gamma_M)^2} dx \right\} d\gamma_M. \quad (38)$$

At high SNR, we get

$$\mathcal{M}_{\varphi_M}(s) = \prod_{n=1}^{l_n} \sum_{r=1}^K \frac{H_r}{s} \times \left( \frac{sw_3^2 J_0[w_3] e^{-\frac{c_2\gamma_{Mr}}{sc_1}}}{2\gamma_{Mr}} + \frac{sc_2\gamma_{Mr} w_3 J_1[w_3] e^{-\frac{c_2\gamma_{Mr}}{sc_1}}}{\gamma_{Mr} c_1} \right), \quad (39)$$

where  $H_r$  and  $\gamma_{Mr}$  are the  $r^{\text{th}}$  abscissa and weight, respectively, of the  $r^{\text{th}}$  order Laguerre polynomial. Similarly, the probabilities  $\Pr(R_{\Phi_n, k} > \bar{R}_k)$  and  $\Pr(R_{\Phi_n, k \rightarrow j} > \bar{R}_k)$  can be calculated using (36) with moment-generating functions (MGFs) given, respectively, by

$$\mathcal{M}_{\varphi_k}(s) = \prod_{n=1}^{l_n} \int_0^{\infty} \frac{e^{-s\gamma_k}}{\gamma_k} \left\{ \int_{\frac{a_3\gamma_k}{a_1 - a_2\gamma_k}}^{\infty} e^{-\left(x + \frac{\gamma_k a_4 x + a_5 \gamma_k}{(x^2(a_1 - a_2\gamma_k) - a_3x\gamma_k)}\right)} \times \left( \frac{(\gamma_k a_4 x + a_5 \gamma_k) (2x(a_1 - a_2\gamma_k) - a_3\gamma_k)}{(x^2(a_1 - a_2\gamma_k) - a_3x\gamma_k)^2} - \frac{\gamma_k a_4}{(x^2(a_1 - a_2\gamma_k) - a_3x\gamma_k)} - 1 \right) dx \right\} d\gamma_k, \quad (40)$$

which, at high SNR, becomes

$$\mathcal{M}_{\varphi_k}(s) = \prod_{n=1}^{l_n} \sum_{r=1}^K \frac{H_r}{s} \times$$

$$\left( \frac{sw_1^2 J_0[w_1] e^{-\frac{a_3 \gamma_{k_r}}{a_1 - a_2 \gamma_k}}}{2\gamma_{k_r}} + \frac{sa_3 \gamma_{k_r} w_1 J_1[w_1] e^{-\frac{a_3 \gamma_{k_r}}{a_1 - a_2 \gamma_k}}}{\gamma_{k_r} a_2} \right), \quad (41)$$

and

$$\begin{aligned} \mathcal{M}_{\varphi_j}(s) &= \prod_{n=1}^{l_n} \int_0^\infty \frac{e^{-s\gamma_k}}{\gamma_k} \left\{ \int_{\frac{b_3 \gamma_k}{b_1 - b_2 \gamma_k}}^\infty e^{-\left(x + \frac{\gamma_k b_4 x + b_5 \gamma_k}{(x^2 (b_1 - b_2 \gamma_k) - b_3 x \gamma_k)}\right)} \right. \\ &\quad \times \left( \frac{(\gamma_k b_4 x + b_5 \gamma_k) (2x (b_1 - b_2 \gamma_k) - b_3 \gamma_k)}{(x^2 (b_1 - b_2 \gamma_k) - b_3 x \gamma_k)^2} \right. \\ &\quad \left. \left. - \frac{\gamma_k b_4}{(x^2 (b_1 - b_2 \gamma_k) - b_3 x \gamma_k)} - 1 \right) dx \right\} d\gamma_k, \quad (42) \end{aligned}$$

which, at high SNR, is given by

$$\begin{aligned} \mathcal{M}_{\varphi_j}(s) &= \prod_{n=1}^{l_n} \sum_{r=1}^K \frac{H_r}{s} \times \\ &\left( \frac{sw_2^2 J_0[w_2] e^{-\frac{b_3 \gamma_{k_r}}{b_1 - b_2 \gamma_{k_r}}}}{2\gamma_{k_r}} + \frac{sb_3 \gamma_{k_r} w_2 J_1[w_2] e^{-\frac{b_3 \gamma_{k_r}}{b_1 - b_2 \gamma_{k_r}}}}{\gamma_{k_r} b_2} \right). \quad (43) \end{aligned}$$

*Proof:* The proof is provided in Appendix D. ■

Alternatively, to find simpler expressions for the probabilities in (35), these probabilities can be upper-bounded using the fact that [21, (40)],  $\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,M} < \gamma_M\right) \leq \prod_{n=1}^{l_n} \Pr(\gamma_{n,M} < \gamma_M)$ ,

$\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,k} < \gamma_k\right) \leq \prod_{n=1}^{l_n} \Pr(\gamma_{n,k} < \gamma_k)$ , and  $\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,k \rightarrow j} < \gamma_k\right) \leq \prod_{n=1}^{l_n} \Pr(\gamma_{n,k \rightarrow j} < \gamma_k)$ , where  $\Pr(\gamma_{n,M} < \gamma_M)$ ,  $\Pr(\gamma_{n,k} < \gamma_k)$  and  $\Pr(\gamma_{n,k \rightarrow j} < \gamma_k)$  are derived in the previous sections.

**Lemma 6.**  $A_2$  in (34) can be derived in this scenario given that  $\Phi = \Phi_n$ , as

$$\begin{aligned} A_2 &= \sum_{n=1}^C \underbrace{\Pr\left(C_{s,M}^{\Phi_n} < R_o\right)}_{P_{\Phi_n}} \\ &= \sum_{n=1}^C \Pr\left(\underbrace{\sum_{n=1}^{l_n} \gamma_{n,M} < \zeta + \zeta \sum_{n=1}^{l_n} \gamma_{n,e} - 1}_{P_{\Phi_n}}\right), \quad (44) \end{aligned}$$

where  $C_{s,M}^{\Phi_n}$  is the secrecy rate of user  $M$  via subset  $\Phi_n$ , and  $P_{\Phi_n}$  is the  $P_{\text{sop}}$  using the subset  $\Phi_n$ . Conditioning on  $h_{sr}$ ,  $P_{\Phi_n}$  is derived as

$$\begin{aligned} P_{\Phi_n} &= \int_0^\infty \left\{ \left[ \int_{\epsilon_{1,1}}^{\epsilon_{2,1}} \dots \int_{\epsilon_{1,l_n}}^{\epsilon_{2,l_n}} f_{\gamma_e}(\gamma) f_{|h_{sr}|^2}(\theta_1, \dots, \theta_{l_n}) d\theta_1 \dots d\theta_{l_n} \right. \right. \\ &\quad \left. \left. + \int_{\epsilon_{2,1}}^\infty \dots \int_{\epsilon_{2,l_n}}^\infty F_{\gamma_M}(\zeta + \gamma\zeta - 1) \times \right. \right. \\ &\quad \left. \left. f_{\gamma_e}(\gamma) f_{|h_{sr}|^2}(\theta_1, \dots, \theta_{l_n}) d\theta_1 \dots d\theta_{l_n} \right] \right\} d\gamma. \quad (45) \end{aligned}$$

The probability in (45) requires at least  $l_n + 1$ -fold integrals, which makes it hard if not impossible to find a closed-form solution. For simplicity and to gain some insights, we consider the cases where the relays are identical and located at the same distance from the source, such as when the relays are located at the boundary of the cell and the source (base-station) is located at the center of the cell, or in sensors network when the access point is located at the center of the network.

*Remark 7.* If the relays are identical nodes, the expression of  $P_{\Phi_n}$  can be simplified to

$$\begin{aligned} P_{\Phi_n} &= \int_0^\infty \left\{ \left[ \int_{\epsilon_1}^{\epsilon_2} f_{\gamma_e}(\gamma) f_{|h_{sr}|^2}(\theta) d\theta + \right. \right. \\ &\quad \left. \left. \int_{\epsilon_2}^\infty F_{\gamma_M}(\zeta + \gamma\zeta - 1) f_{\gamma_e}(\gamma) f_{|h_{sr}|^2}(\theta) d\theta \right]^{l_n} \right\} d\gamma, \quad (46) \end{aligned}$$

From the derivation in Appendix D, the conditional cumulative distribution function (CDF),  $F_{\gamma_M}(\zeta + \gamma\zeta - 1)$  can be written as

$$\begin{aligned} F_{\gamma_M}(\varsigma) &= \frac{2^{-Q} e^{\frac{A}{2}}}{\varsigma} \sum_{q=0}^Q \binom{Q}{q} \sum_{n=0}^{N+q} \frac{(-1)^n}{\beta_n} \\ &\times \Re \left( \frac{\mathcal{M}_\varphi\left(\frac{A + 2\pi j n}{2\varsigma}\right)}{\frac{A + 2\pi j n}{2\varsigma}} \right) + E(A, N, Q) \quad (47) \end{aligned}$$

where  $\varsigma = \zeta + \gamma\zeta - 1$  and

$$\begin{aligned} \mathcal{M}_\varphi(s) &= \prod_{n=1}^{l_n} \int_0^\infty e^{-s\varsigma} \left\{ e^{-\left(\frac{\varsigma c_3 \theta + c_4 \varsigma}{(\theta^2 c_1 - c_2 \theta \varsigma)}\right)} \frac{(c_3 \theta + c_4) \theta^2 c_1}{(\theta^2 c_1 - c_2 \theta \varsigma)^2} \right\} d\varsigma \\ &\approx \prod_{n=1}^{l_n} \sum_{i=1}^n \text{H}_i e^{\varsigma_i (1-s)} \left\{ e^{-\left(\frac{\varsigma_i c_3 \theta + c_4 \varsigma_i}{(\theta^2 c_1 - c_2 \theta \varsigma_i)}\right)} \frac{(c_3 \theta + c_4) \theta^2 c_1}{(\theta^2 c_1 - c_2 \theta \varsigma_i)^2} \right\}, \quad (48) \\ &\quad (49) \end{aligned}$$



The probability density function (PDF)  $f_{\gamma_e}(\gamma)$  can be obtained with the inverse Laplace transform as  $f_{\gamma_e}(\gamma) = \mathcal{L}^{-1}(\mathcal{M}_{\gamma_e}(s))$  [33], [34]. Using the formula in [34], the PDF of the SINR at the eavesdropper can be obtained according to

$$f_{\gamma_e}(\gamma) = \frac{2^{-Q} e^{\frac{A}{2}}}{\gamma} \sum_{q=0}^Q \binom{Q}{q} \sum_{n=0}^{N+q} \frac{(-1)^n}{\beta_n} \times \Re \left( \mathcal{M}_{\gamma_e} \left( \frac{A + 2\pi j n}{2\gamma} \right) \right) + E(A, N, Q), \quad (50)$$

where

$$\begin{aligned} \mathcal{M}_{\gamma_e}(s) &= \prod_{n=1}^{l_n} \int_0^{\infty} e^{-s\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 e_1 - e_2 \theta \gamma)}\right)} \frac{(e_3 \theta + e_4) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} d\gamma \\ &\approx \prod_{n=1}^{l_n} \sum_{i=1}^n \text{H}_i e^{\gamma_i(1-s)} e^{-\left(\frac{\gamma_i e_3 \theta + e_4 \gamma_i}{(\theta^2 e_1 - e_2 \theta \gamma_i)}\right)} \frac{(e_3 \theta + e_4) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma_i)^2}. \end{aligned} \quad (51)$$

It is worth to mention that, the conditional CDF,  $F_{\gamma_M}(\zeta + \gamma\zeta - 1)$ , and the conditional PDF,  $f_{\gamma_e}(\gamma)$ , can be derived as upper-bounds using the same identity as in [21],  $\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,M} < \zeta + \zeta\gamma - 1\right) \leq \prod_{n=1}^l \Pr(\gamma_{n,M} < \zeta + \zeta\gamma - 1)$  and  $\Pr\left(\sum_{n=1}^l \gamma_{n,e} < \gamma\right) \leq \prod_{n=1}^l \Pr(\gamma_{n,e} < \gamma)$ .

**Theorem 8.** *The secrecy outage probability achieved by the two-stage conventional relay selection strategy can be calculated as*

$$P_{\text{sop}} = \Lambda_1 \cup \Lambda_2, \quad (52)$$

where  $\Lambda_1$  and  $\Lambda_2$  can be calculated using Lemma 5 and Lemma 6.

*Remark 9.* All the probabilities in this work are provided in closed-form exact expressions, and approximated expressions based on high SNRs.<sup>4</sup> Each probability expression describes part of the total system performance. For instance,  $\Pr(R_{n,k} > \bar{R}_k)$  gives insight on the performance of user  $k$ , and the term  $\Pr(R_{n,M} > \bar{R}_M)$  gives clear insight on the performance of user  $M$ . In addition, from these expressions the impact of different system parameters on the overall system performance can be clearly observed. For instance, from (17), (19) and (21), it is clear that, when  $\beta_{r_n}$  is large the secrecy outage probability can be enhanced because the relays can harvest higher power. A larger  $\beta_{r_n}$  can also degrade the secrecy outage probability because it leaves a smaller power fraction to process the data. Therefore, there is an optimal value of  $\beta_{r_n}$  that results in optimal system performance. This optimal value can be obtained easily using the expressions derived in this paper. For instance, the

<sup>4</sup>The performance analysis of the case when the number of relays goes to infinity can also give insights about the secrecy outage probability. Due to the paper length limitation, this case will be investigated in future work.

problem can be formulated as:  $\min_{0 < \beta_{r_n} < 1} P_{\text{sop}}$ . One method to solve this problem and find the optimal value of  $\beta_{r_n}$  is using line search techniques such as the golden section method [35].

## VI. NUMERICAL RESULTS

In this section, in order to examine the secrecy performance of the proposed schemes, some numerical and simulation results corresponding to the derived expressions are presented. The analytical results are illustrated by carrying out Monte-Carlo simulations, which were executed over  $10^5$  independent trials. Unless stated otherwise, the noise power at all nodes are set as  $\sigma^2 = 0$  dBW, the path-loss exponent  $m = 2.7$ ,  $\eta = 0.8$  [35],  $\text{SNR} = \frac{P}{\sigma^2}$ , the power allocation coefficients  $\alpha_i^2 = \frac{M-i+1}{\mu}$ , with  $\mu$  chosen to satisfy  $\sum_{i=1}^M \alpha_i^2 = 1$ , the number of users  $M = 3$ , and the number of relays  $|N_r| = 4$ . For illustration purposes, we consider a 2D system topology where the source, the users and the eavesdropper are located at  $(x_{ds}, y_{ds}) = (0, 0)$ ,  $(x_{du1}, y_{du1}) = (0, 2)$ ,  $(x_{du2}, y_{du2}) = (1.5, 0)$ ,  $(x_{dM}, y_{dM}) = (1, 0)$ , and  $(x_{de}, y_{de}) = (0, 1)$ , respectively, and the relays are located at  $(x_{dRe1}, y_{dRe1}) = (1, 0.5)$ ,  $(x_{dRe2}, y_{dRe2}) = (1.5, 0.5)$ ,  $(x_{dRe3}, y_{dRe3}) = (1, 1.5)$  and  $(x_{dRe4}, y_{dRe4}) = (1.5, 1.5)$ . Due to the symmetry between the strongest user and the eavesdropper paths, this topology can explain the benefit of the relay selection schemes. Such topology has been considered in [36], [37]. Please note that the selected topology is used for the sake of presentation and that the enhancements of the proposed selection schemes hold for all possible configurations [37]. For clarity, some results for the case when the users are randomly distributed inside a circle area with a radius of 10m and the source node is located at the center of this area are also presented.

### A. Effect of Target Secrecy Rate and Number of Relays

To demonstrate the impact of the target secrecy rate  $R_o$  and of the number of relays on the secrecy outage probability, we plot Fig. 1, which represents  $P_{\text{sop}}$  versus  $R_o$  for different values of the number of relays in the three selection schemes. It should be pointed out that in this figure,  $R_{e2}$  and  $R_{e3}$  are used when two relays are assumed in the system. In the case of multiple-relays scheme, two scenarios are considered: when only two relays (one subset) and when four relays subsets are used. It is evident from these results that  $P_{\text{sop}}$  increases as the target secrecy rate increases, and that increasing the number of the relays results in a degradation of  $P_{\text{sop}}$  in the three considered schemes. In addition, comparing the three schemes for each value of the number of relays, one can notice that the optimal relay selection scheme outperforms the other two schemes.<sup>5</sup> This improvement in performance can be clearly

<sup>5</sup>This is because in the optimal relay selection, the best relay has been selected based on the knowledge of the CSI of the eavesdropper, which is not the case in the other two schemes.

seen when  $R_o$  is small and  $|N_r| = 4$ , while in the case of  $|N_r| = 2$  the optimal scheme has the best performance when  $R_o$  is approximately between 0 and 1.2. After that, the optimal and conventional schemes inclined to achieve similar secrecy performance. On the other hand, using multiple relays results in the worst secrecy performance when  $C = 1$  compared to the optimal and conventional schemes. This is because,  $l$  relays are used to forward the signal to the users by TDMA. In this case,  $l + 1$  slots are needed to achieve the end-to-end communication, which is represented by  $a$  in (33). In conventional and optimal relay selection techniques,  $l = 1$ . Having said that, when  $C = 4$  the multiple relay scheme outperforms the conventional scheme only at low values of the target secrecy rate  $0 < R_o < 0.5$ . It is also worth noticing that increasing the number of relay sub-sets  $|\Phi| = C$  enhances the system security.

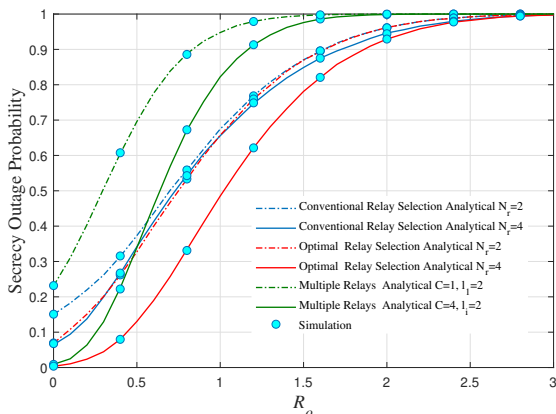


Figure 1: Secrecy outage probability versus  $R_o$  for different values of  $|N_r|$  when SNR = 30 dB.

### B. Effect of Target Secrecy Rate and SNR

Fig. 2 depicts some simulated and numerical results of  $P_{sop}$  as a function of the target secrecy rate  $R_o$  for different SNR values when only two relays,  $R_{e1}$  and  $R_{e2}$ , are used in the system. From the results in this figure, we can clearly observe that increasing the SNR always enhances  $P_{sop}$  in the three schemes. When SNR=10 dB, the conventional relay selection scheme performs similarly to the optimal relay selection scheme. On the other hand, when SNR=30 dB and SNR=60 dB, the optimal relay selection scheme outperforms the conventional scheme. The performance gap between the three schemes increases as the SNR increases, where the multiple-relays scheme always has the worst secrecy performance.

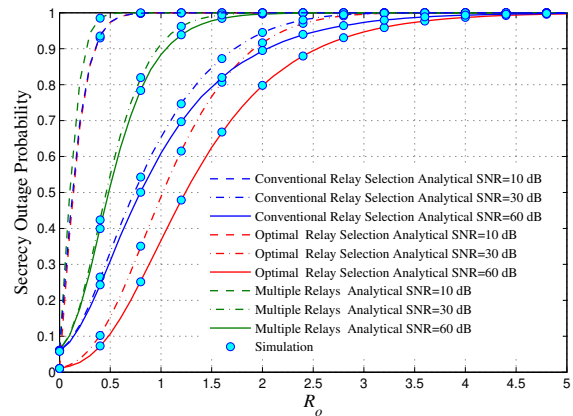


Figure 2: Secrecy outage probability versus  $R_o$  for different values of SNR when  $|N_r| = 2$ ,  $C = 1$ , and  $|\Phi| = 2$ .

### C. Effect of Users' Target Data Rate and Number of Users

In this subsection, we capture the influence of the users' target data rate, the number of users, and the SNR, on the system secrecy performance. Fig. 3 presents  $P_{sop}$  versus SNR for different combinations of  $M$  and the users' target data rates, for the three schemes. In general, it is seen that increasing the SNR enhances  $P_{sop}$  for all the studied configurations. In addition, comparing the studied combinations for each scheme, it can be seen that, for a given SNR the secrecy performance improves as the number of users and the target rates decrease. This enhancement becomes smaller at high SNR. In addition, it is interesting to notice that increasing the target rates of the users,  $\bar{R}_1$  and  $\bar{R}_2$  in case  $M = 3$ , has almost similar impact on the system secrecy. In contrast, when  $M = 2$  increasing the target rate  $\bar{R}_1$  of the first user (weakest) impacts essentially the system security.

To compare the secrecy performance of the three schemes for these system features, we plot Fig. 3d and Fig. 3e. These figures illustrate that the gap between the conventional and optimal schemes is tight at low SNR, and becomes wider as the SNR goes higher. This can be explained as discussed for Fig. 1 and Fig. 2; the gain attained by the optimal relay selection scheme increases as the number of relays and/or the SNR increase. In addition, the multiple-relays scheme has the worst secrecy performance for all the combinations considered in this figure.

### D. Randomness of the Users Locations

In this subsection, we present in Fig. 4 some results when the number of users  $M = 8$ , and the users are uniformly distributed inside a circle area with a radius of 10m and the source node is located at the center of this area. In addition, the number of the relays  $N = 4$ , which are located 5m away from the source in different directions, e.g.,  $(x_{dRe1}, y_{dRe1}) = (5, 5)$ ,  $(x_{dRe2}, y_{dRe2}) = (-5, 5)$ ,  $(x_{dRe3}, y_{dRe3}) = (-5, -5)$  and  $(x_{dRe4}, y_{dRe4}) = (5, -5)$ . It is clear from these results that high transmission power is needed to achieve secure communication, due to large

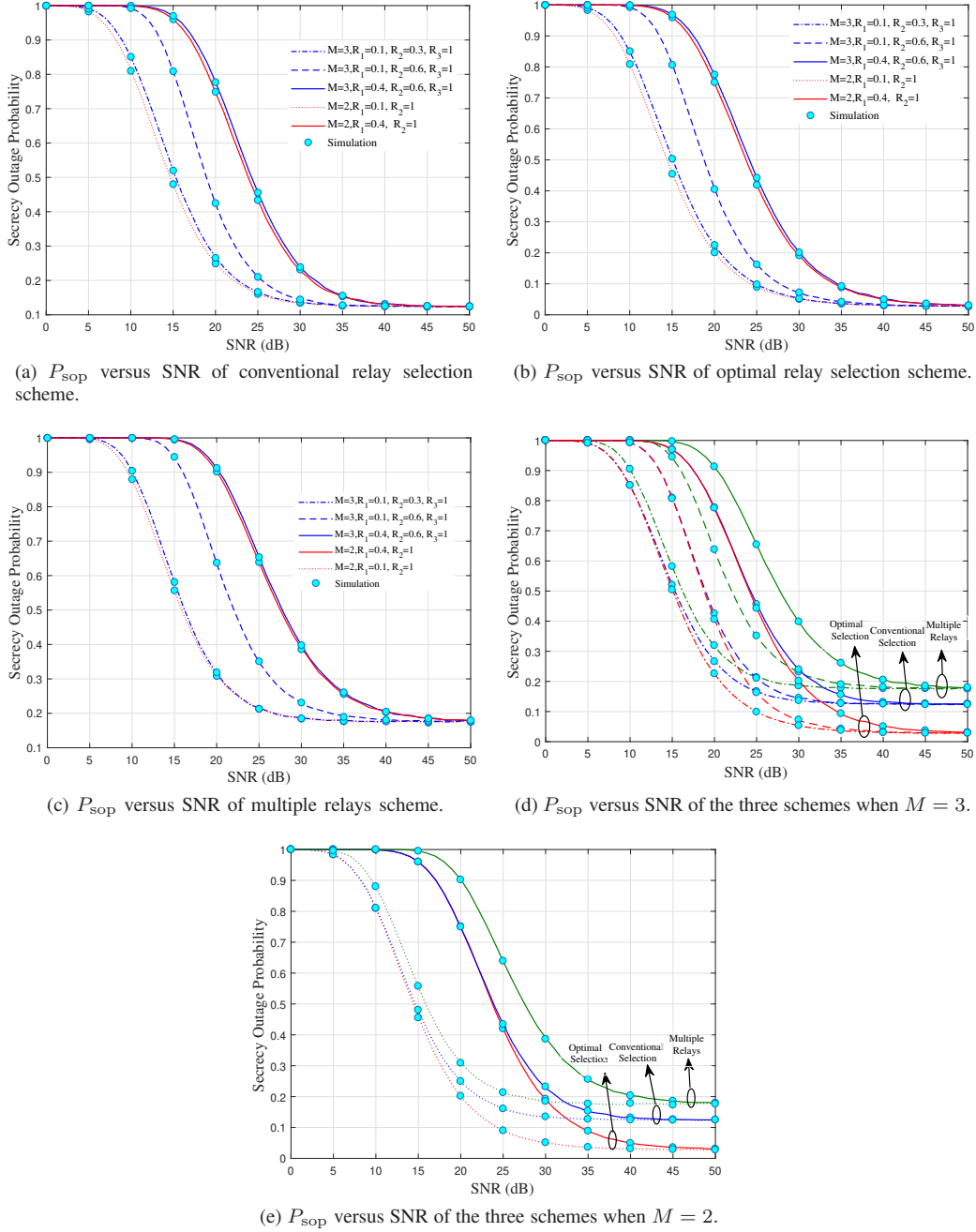


Figure 3: Secrecy outage probability versus SNR of the three schemes for different values of  $M$ ,  $\bar{R}_1$ ,  $\bar{R}_2$ ,  $\bar{R}_3$  when  $R_o = 0.2$ .

path-loss. Furthermore, the optimal relay selection scheme always has the best performance, and multiple relay scheme has better performance than the conventional scheme only at low target secrecy rate, as it is noted in Fig. 1.

### E. Impact of Eavesdropper Location

Here, we investigate the impact of the eavesdropper's location on the secrecy outage probability. The position of the eavesdropper is varied on the x-axis from (0, 1) meters to (4, 1) meters, i.e., the eavesdropper moves horizontally from

the original location (0, 1). Fig. 5 shows the secrecy outage probability as a function of the eavesdropper location, when  $\text{SNR}=30$  dB and only two relays are used, i.e.,  $R_{e1}$  and  $R_{e3}$ . From this figure, we observe that  $P_{\text{sop}}$  is at its maximum when the eavesdropper is approximately at (1, 1), i.e., when it is located between the two relays. Also,  $P_{\text{sop}}$  decreases as the eavesdropper moves away. This phenomena can be justified by the fact that, when the eavesdropper is between the two relays, the distance between the eavesdropper and the two relays will be short. Thus, the received information signal at the eavesdropper will be strong, and as a result the

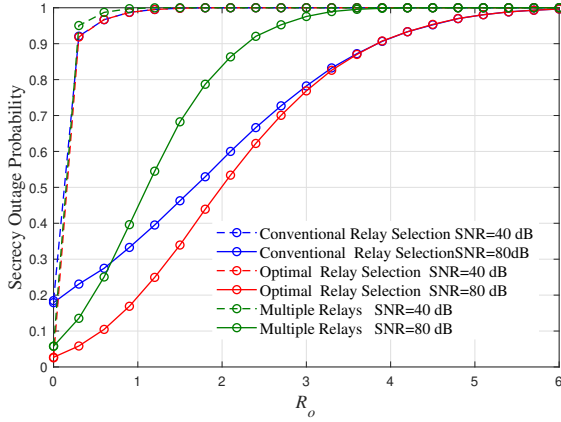


Figure 4: Secrecy outage probability versus  $R_o$  for different values of SNR when  $|N_r| = 4$ ,  $C = 4$ ,  $|\Phi_i| = 2$ .

secrecy outage probability will be very high. In addition, in case the distances between the eavesdropper and the source and the relays are long, the received signal at the eavesdropper will be weak due to the large path-loss, and this results in smaller secrecy outage probability.

## VII. CONCLUSION

In this paper, we investigated the secrecy performance of different relay selection schemes in cooperative NOMA systems when a source node communicates with multiple users via multiple energy-harvesting relay nodes in the presence of a passive eavesdropper. We have derived new explicit analytical expressions for the secrecy outage probability considering three different relay selection schemes: 1) when the CSI of the eavesdropper is unknown, 2) when the CSI of the eavesdropper is known, and 3) when multiple relays are used to forward the signal to the users. The results in this work demonstrated that no matter what the values of the system parameters are, the optimal relay selection scheme strictly outperforms the other two selection schemes, and that the performance gap between the proposed schemes depends essentially on the system setup. Furthermore, it was shown that increasing the SNR and the number of relay nodes can enhance the secrecy performance, while as the users' target data rates and the number of users increase, the system security gets degraded.

## APPENDIX A

For the derivation of Lemma 1, substituting (5) into (10), we can express  $\gamma_{n,k}$  as

$$\gamma_{n,k} = \frac{a_1 x_n^2 y_n}{a_2 x_n^2 y_n + a_3 x_n y_n + a_4 x_n + a_5}, \quad (53)$$

where  $x_n = |h_{sr_n}|^2$ ,  $y_n = |h_{r_n u_k}|^2$ ,  $a_1 = \beta_{r_n} (1 - \beta_{r_n}) P_s^2 \alpha_k \eta_{r_n}$ ,  $a_2 = \beta_{r_n} (1 - \beta_{r_n}) P_s^2 \eta_{r_n} \sum_{i=k+1}^M \alpha_i$ ,  $a_3 = d_{sr_n}^m \beta_{r_n} P_s \eta_{r_n} \sigma_{r_n}^2$ ,  $a_4 = d_{sr_n}^m d_{r_n u_k}^m (1 - \beta_{r_n}) P_s \sigma_{u_k}^2$ , and  $a_5 = d_{sr_n}^{2m} \sigma_{r_n}^2 d_{r_n u_k}^m \sigma_{u_k}^2$ . Therefore,

$$\Pr(R_{n,k} > \bar{R}_k) = 1 -$$

$$\Pr\left(\frac{a_1 x_n^2 y_n}{a_2 x_n^2 y_n + a_3 x_n y_n + a_4 x_n + a_5} < \zeta_k\right), \quad (54)$$

where  $\zeta_k = 2^{2\bar{R}_k}$ , and  $\bar{R}_k$  is the target rate for user  $k$ , which can be written as

$$\Pr(R_{n,k} > \bar{R}_k) = 1 -$$

$$\Pr(y_n (x_n^2 (a_1 - a_2 \zeta_k) - a_3 x_n \zeta_k) < \zeta_k a_4 x_n + a_5 \zeta_k). \quad (55)$$

The right-hand-side (RHS) of Eq. (55) can be written as follows:

$$\Pr(y_n (x_n^2 (a_1 - a_2 \zeta_k) - a_3 x_n \zeta_k) < \zeta_k a_4 x_n + a_5 \zeta_k) =$$

$$\begin{cases} \Pr\left(y_n > \frac{\zeta_k a_4 x_n + a_5 \zeta_k}{(x_n^2 (a_1 - a_2 \zeta_k) - a_3 x_n \zeta_k)}\right) = 1, x_n < \frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k} \\ \Pr\left(y_n < \frac{\zeta_k a_4 x_n + a_5 \zeta_k}{(x_n^2 (a_1 - a_2 \zeta_k) - a_3 x_n \zeta_k)}\right), x_n > \frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k} \end{cases} \quad (56)$$

In this expression, if  $x_n < \frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}$ , then the term  $\frac{\zeta_k a_4 x_n + a_5 \zeta_k}{(x_n^2 (a_1 - a_2 \zeta_k) - a_3 x_n \zeta_k)}$  will be negative, while  $y_n$  is always positive  $y_n > 1$ , so the probability in this case is 1. By conditioning on  $x_n$ , we can obtain (57), where  $F_{y_n}(\cdot)$  is the CDF of  $y_n$ , and  $f_{x_n}(\cdot)$  is the PDF of  $x_n$ . Since  $x_n$  and  $y_n$  are both exponentially distributed, we get

$$\Pr(R_{n,k} > \bar{R}_k) = \int_{\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}^{\infty} e^{-\left(z + \frac{\zeta_k a_4 z + a_5 \zeta_k}{(z^2 (a_1 - a_2 \zeta_k) - a_3 z \zeta_k)}\right)} dz, \quad (58)$$

At high SNR, the last term in the denominator of the SINR expression in (53) can be neglected, because it is included the product of the two noise variance, i.e.,  $a_5 = 0$ . Thus, the expression in (58) becomes

$$\Pr(R_{n,k} > \bar{R}_k) = \int_{\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}^{\infty} e^{-\left(z + \frac{\zeta_k a_4}{(z(a_1 - a_2 \zeta_k) - a_3 \zeta_k)}\right)} dz. \quad (59)$$

Let  $\mathcal{Y} = z(a_1 - a_2 \zeta_k) - a_3 \zeta_k$ , then we can approximate (59) as

$$\Pr(R_{n,k} > \bar{R}_k) = \frac{e^{-\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}}{a_1 - a_2 \zeta_k} \int_0^{\infty} e^{-\left(\frac{\mathcal{Y}}{a_1 - a_2 \zeta_k} + \frac{\zeta_k a_4}{\mathcal{Y}}\right)} d\mathcal{Y}, \quad (60)$$

which can be found as

$$\Pr(R_{n,k} > \bar{R}_k) \approx w_1 \mathbf{J}_1[w_1] e^{-\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}, \quad (61)$$

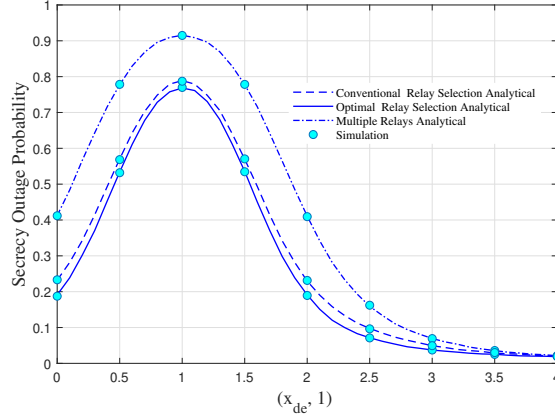


Figure 5: Secrecy outage probability versus  $x_{de}$  of the three schemes, when SNR=30 dB and  $R_o = 0.2$ .

$$\Pr(R_{n,k} > \bar{R}_k) = 1 - \left\{ \int_0^{\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}} f_{x_n}(z) dz + \int_{\frac{a_3 \zeta_k}{a_1 - a_2 \zeta_k}}^{\infty} F_{y_n} \left( \frac{\zeta_k a_4 z + a_5 \zeta_k}{(z^2 (a_1 - a_2 \zeta_k) - a_3 z \zeta_k)} \right) f_{x_n}(z) dz \right\}, \quad (57)$$

where  $w_1 = \sqrt{\frac{4\zeta_k a_4}{a_1 - a_2 \zeta_k}}$ , and  $J_1[\cdot]$  is the first-order modified Bessel function of the second kind [19], [30]. Similarly, we can write  $\gamma_{n,x_k \rightarrow j}$  as follows:

$$\gamma_{n,x_k \rightarrow j} = \frac{b_1 x_n^2 y_n}{b_2 x_n^2 y_n + b_3 x_n y_n + b_4 x_n + b_5}, \quad (62)$$

where  $x_n = |h_{sr_n}|^2$ ,  $y_n = |h_{rn,u_j}|^2$ ,  $b_1 = \beta_{r_n} (1 - \beta_{r_n}) P_s^2 \alpha_k \eta_{r_n}$ ,  $b_2 = \beta_{r_n} (1 - \beta_{r_n}) P_s^2 \eta_{r_n} \sum_{i=k+1}^M \alpha_i$ ,  $b_3 = d_{sr_n}^m \beta_{r_n} P_s \eta_{r_n} \sigma_{r_n}^2$ ,  $b_4 = d_{sr_n}^m d_{rn,u_j}^m (1 - \beta_{r_n}) P_s \sigma_{u_j}^2$ , and  $b_5 = d_{rn,u_j}^m \sigma_{u_j}^2 d_{sr_n}^m \sigma_{r_n}^2$ . Following similar steps, we can find

$$\Pr(R_{n,k \rightarrow j} > \bar{R}_k) = \int_{\frac{b_3 \zeta_k}{b_1 - b_2 \zeta_k}}^{\infty} e^{-\left(z + \frac{\zeta_k b_4 z + b_5 \zeta_k}{(z^2 (b_1 - b_2 \zeta_k) - b_3 z \zeta_k)}\right)} dz. \quad (63)$$

At high SNRs, by following similar steps as in (59), (60) and (61), (63) can be written as

$\Pr(R_{n,k \rightarrow j} > \bar{R}_k) \approx w_2 J_1[w_2] e^{-\frac{b_3 \zeta_k}{b_1 - b_2 \zeta_k}}$ , where  $w_2 = \sqrt{\frac{4\zeta_k b_4}{b_1 - b_2 \zeta_k}}$ . Now, to derive  $\Pr(R_{n,M} > \bar{R}_M)$ , we write the SINR at user  $M$  as

$$\gamma_{n,M} = \frac{c_1 x_n^2 y_n}{c_2 x_n y_n + c_3 x_n + c_4}, \quad (64)$$

where  $x_n = |h_{sr_n}|^2$ ,  $y_n = |h_{rn,u_M}|^2$ ,  $c_1 = \beta_{r_n} (1 - \beta_{r_n}) P_s^2 \alpha_M \eta_{r_n}$ ,  $c_2 = d_{sr_n}^m \beta_{r_n} P_s \eta_{r_n} \sigma_{r_n}^2$ ,  $c_3 = d_{sr_n}^m d_{rn,u_M}^m (1 - \beta_{r_n}) P_s \sigma_{u_M}^2$ , and  $c_4 = d_{rn,u_j}^m \sigma_{u_j}^2 d_{sr_n}^m \sigma_{r_n}^2$ . Therefore,

$$\Pr(R_{n,M} > \bar{R}_M) = 1 - \Pr\left(\frac{c_1 x_n^2 y_n}{c_2 x_n y_n + c_3 x_n + c_4} < \zeta_M\right), \quad (65)$$

where  $\zeta_M = 2^{2\bar{R}_M}$  and  $\bar{R}_M$  is the target rate for user  $M$ . This probability can be written as

$$\Pr(R_{n,M} > \bar{R}_M) = 1 -$$

$$\Pr(y_n (x_n^2 c_1 - c_2 x_n \zeta_M) < \zeta_M c_3 x_n + c_4 \zeta_M), \quad (66)$$

and further expressed as

$$\Pr(R_{n,M} > \bar{R}_M) = \int_{\frac{c_2 \zeta_M}{c_1}}^{\infty} e^{-\left(z + \frac{\zeta_M c_3 z + c_4 \zeta_M}{z^2 c_1 - c_2 z \zeta_M}\right)} dz. \quad (67)$$

At high SNRs, by following similar steps as in (59), (60) and (61),  $\Pr(R_{n,M} > \bar{R}_M)$  can be expressed by  $\Pr(R_{n,M} > \bar{R}_M) \approx w_3 J_1[w_3] e^{-\frac{c_2 \zeta_M}{c_1}}$ , where  $w_3 = \sqrt{\frac{4\zeta_M c_3}{c_1}}$ . Finally, substituting (58), (63) and (67) into (15), we find  $O_1$ .

## APPENDIX B

Here, we provide the proof of Lemma 2. First,  $O_2$  in (14) can be calculated by

$$O_2 = \Pr\left(\frac{1 + \max_{n \in N_r} \{\gamma_{n,M}\}}{1 + \gamma_{n,e}} < \zeta, |N_r| > 0\right)$$

$$= \Pr\left(\max_{n \in N_r} \{\gamma_{n,M}\} < \zeta + \gamma_{n,e} \zeta - 1, |N_r| > 0\right). \quad (68)$$

Using the law of total probability, we get (69). To find  $S_1$ , from order statistics [38] we can find (70). By conditioning on  $|h_{sr_l}|^2 = \theta$  and  $\gamma_{l,e} = \gamma$ , we get (71). From (67), we can find

$$\begin{aligned}
O_2 &= \sum_{Q=1}^N \left\{ \underbrace{\Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma_{n,e}\zeta - 1 \mid |N_r| = Q \right)}_{S_1} \right\} \underbrace{\Pr(|N_r| = Q)}_{S_2} \\
&= \sum_{Q=1}^N \left\{ \sum_{l=1}^Q \underbrace{\Pr(n^* = l) \Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma_{l,e}\zeta - 1 \mid |N_r| = Q, n^* = l \right)}_{S_1} \right\} \underbrace{\Pr(|N_r| = Q)}_{S_2}. \quad (69)
\end{aligned}$$

$$\begin{aligned}
F_{\max_{n \in Q} \{\gamma_{n,M}\}}(\zeta + \gamma_{l,e}\zeta - 1) &= \Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma_{l,e}\zeta - 1 \mid |N_r| = Q, n^* = l \right) \\
&= \prod_{n=1}^Q \Pr(\gamma_{n,M} < \zeta + \gamma_{l,e}\zeta - 1). \quad (70)
\end{aligned}$$

$$\begin{aligned}
&\Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma_{l,e}\zeta - 1 \mid \gamma_{l,e} = \gamma, |h_{sr_l}|^2 = \theta \right) = \\
&\int_0^\infty \int_0^\infty F_{\max_{n \in Q} \{\gamma_{n,M}\}}(\zeta + \gamma\zeta - 1 \mid |h_{sr_l}|^2 = \theta) f_{\gamma_{l,e}}(\gamma \mid |h_{sr_l}|^2 = \theta) f_{|h_{sr_l}|^2}(\theta) d\theta d\gamma. \quad (71)
\end{aligned}$$

Consequently, the PDF can be found as follows:

$$\Pr(\gamma_{n,M} < \zeta + \gamma\zeta - 1) = 1 -$$

$$\int_{\frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}}^\infty e^{-\left(z + \frac{(\zeta + \gamma\zeta - 1)c_3 z + c_4(\zeta + \gamma\zeta - 1)}{(z^2 c_1 - c_2 z(\zeta + \gamma\zeta - 1))}\right)} dz. \quad (72)$$

At high SNRs, following similar steps as in (59), (60) and (61), we obtain  $F_{\{\gamma_{n,M}\}}(\zeta + \gamma\zeta - 1) \approx 1 - w_4 J_1[w_4] e^{-\frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}}$ , where  $w_4 = \sqrt{\frac{4(\zeta + \gamma\zeta - 1)c_3}{c_1}}$ , and

$$\Pr(\gamma_{l,M} < \zeta + \gamma\zeta - 1 \mid |h_{sr_l}|^2 = \theta) = 1 -$$

$$e^{-\left(\frac{(\zeta + \gamma\zeta - 1)c_3\theta + c_4(\zeta + \gamma\zeta - 1)}{\theta^2 c_1 - c_2\theta(\zeta + \gamma\zeta - 1)}\right)}, \quad \theta > \frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}. \quad (73)$$

To find the PDF of  $\gamma_{l,e}$ ,  $f_{\gamma_{l,e}}(\gamma)$ , we can write the SINR at the eavesdropper as

$$\gamma_{l,e} = \frac{e_1 x_l^2 y_l}{e_2 x_l y_l + e_3 x_l + e_4}, \quad (74)$$

where  $x_l = |h_{sr_l}|^2$ ,  $y_l = |h_{rl}|^2$ ,  $e_1 = \beta_{rl}(1 - \beta_{rl})P_s^2 \alpha_M \eta_{rl}$ ,  $e_2 = d_{sr_l}^m \beta_{rl} P_s \eta_{rl} \sigma_{rl}^2$ ,  $e_3 = d_{sr_l}^m d_{rl}^m (1 - \beta_{rl}) P_s \sigma_e^2$ , and  $e_4 = d_{sr_l}^m \sigma_{rl}^2$ . Therefore, the conditional CDF of  $\gamma_{l,e}$  is given by

$$F_{\gamma_{l,e}}(\gamma \mid x_l = \theta) = 1 - e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{\theta^2 c_1 - c_2 \theta \gamma}\right)}, \quad \theta > \frac{e_2 \gamma}{e_1}. \quad (75)$$

$$f_{\gamma_{l,e}}(\gamma \mid x_l = \theta) = \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{\theta^2 c_1 - c_2 \theta \gamma}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2}. \quad (76)$$

Since  $|h_{sr_l}|^2$  is exponentially distributed,  $f_{|h_{sr_l}|^2}(\theta) = e^{-\theta}$ . By conditioning on  $|h_{sr_l}|^2$  and  $\gamma_{l,e}$ , Eq. (71) can be formulated as in (77), (78) and (79), where  $\epsilon_1 = \frac{e_2 \gamma}{e_1}$  and  $\epsilon_2 = \frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}$ . Using Gaussian-Quadrature rules, in which

$$\int_0^\infty e^{-x} f(x) dx = \sum_{i=1}^n H_i f(x_i) + R(i) \quad (80)$$

where  $x_i$  and  $H_i$  are the  $i^{th}$  abscissa and weight of the  $n^{th}$  order Laguerre polynomial tabulated in [30, eq. (25.4.45)], respectively, and the remainder  $R(i)$  is negligible for  $n > 15$ , then the expression in (79) can be approximated as in (81) where  $\gamma_i$  and  $H_i$  are the  $i^{th}$  abscissa and weight of the  $n^{th}$  order Laguerre polynomial, respectively [30, eq. (25.4.45)]. The probability that relay  $l$  is selected,

$$\Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma\zeta - 1 \right) = \int_0^\infty \prod_{\substack{n=1 \\ n \neq l}}^Q \Pr(\gamma_{n,M} < \zeta + \gamma\zeta - 1) \\ \times \left\{ \int_0^\infty \Pr(\gamma_{l,M} < \zeta + \gamma\zeta - 1 \mid |h_{sr_l}|^2 = \theta) f_{\gamma_{l,e}}(\gamma \mid |h_{sr_l}|^2 = \theta) f_{|h_{sr_l}|^2}(\theta) d\theta \right\} d\gamma \quad (77)$$

$$\Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma\zeta - 1 \right) = \int_0^\infty \prod_{\substack{n=1 \\ n \neq l}}^Q \Pr(\gamma_{n,M} < \zeta + \gamma\zeta - 1) \times \left\{ \int_{\epsilon_1}^{\epsilon_2} f_{\gamma_{l,e}}(\gamma \mid |h_{sr_l}|^2 = \theta) f_{|h_{sr_l}|^2}(\theta) d\theta \right. \\ \left. + \int_{\epsilon_2}^\infty \Pr(\gamma_{l,M} < \zeta + \gamma\zeta - 1 \mid |h_{sr_l}|^2 = \theta) \times f_{\gamma_{l,e}}(\gamma \mid |h_{sr_l}|^2 = \theta) f_{|h_{sr_l}|^2}(\theta) d\theta \right\} d\gamma \quad (78)$$

$$= \int_0^\infty \prod_{\substack{n=1 \\ n \neq l}}^Q \left\{ 1 - \int_{\frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}}^\infty e^{-\left(z + \frac{(\zeta + \gamma\zeta - 1)c_3 z + c_4(\zeta + \gamma\zeta - 1)}{z^2 c_1 - c_2 z(\zeta + \gamma\zeta - 1)}\right)} dz \right\} \times \left\{ \int_{\epsilon_1}^{\epsilon_2} \left\{ \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 \epsilon_1}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)^2} \right\} e^{-\theta} d\theta \right. \\ \left. + \int_{\epsilon_2}^\infty \left\{ 1 - e^{-\left(\frac{(\zeta + \gamma\zeta - 1)c_3 \theta + c_4(\zeta + \gamma\zeta - 1)}{(\theta^2 c_1 - c_2 \theta(\zeta + \gamma\zeta - 1))}\right)} \right\} \times \left\{ \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 \epsilon_1}{(\theta^2 \epsilon_1 - e_2 \theta \gamma)^2} \right\} e^{-\theta} d\theta \right\} d\gamma, \quad (79)$$

$$\Pr \left( \max_{n \in Q} \{\gamma_{n,M}\} < \zeta + \gamma\zeta - 1 \right) \approx \sum_{i=1}^n H_i e^{\gamma_i} \prod_{\substack{n=1 \\ n \neq l}}^Q \left\{ 1 - w_4 J_1[w_4] e^{-\frac{c_2(\zeta + \gamma_i \zeta - 1)}{c_1}} \right\} \\ \times \left\{ e^{-\left(\frac{\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i}{\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 \epsilon_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i}\right)} \frac{(\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i) (\epsilon_2 - \epsilon_1) \epsilon_1 \left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e^{-\frac{\epsilon_2 + \epsilon_1}{2}}}{\gamma_i \left(\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 \epsilon_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i\right)^2} \right. \\ \left. + \sum_{j=1}^n H_j \left\{ 1 - e^{-\left(\frac{(\zeta + \gamma_i \zeta - 1)c_3 \theta_j + c_4(\zeta + \gamma_i \zeta - 1)}{(\theta_j^2 c_1 - c_2 \theta_j(\zeta + \gamma_i \zeta - 1))}\right)} \right\} \times \left\{ \frac{1}{\gamma_i} e^{-\left(\frac{\gamma_i e_3 \theta_j + e_4 \gamma_i}{(\theta_j^2 \epsilon_1 - e_2 \theta_j \gamma_i)}\right)} \frac{(\gamma_i e_3 \theta_j + e_4 \gamma_i) \theta_j^2 \epsilon_1}{(\theta_j^2 \epsilon_1 - e_2 \theta_j \gamma_i)^2} \right\} \right\}, \quad (81)$$

$\Pr(n^* = l) = p_l$ , can be given by

$$p_l = \prod_{\substack{n=1 \\ l \neq n}}^Q \Pr(\gamma_{l,M} > \gamma_{n,M}) = \Pr \left( \gamma_{l,M} > \max_{l \neq n} (\gamma_{n,M}) \right) \\ = \int_0^\infty f_{\gamma_{l,M}}(x) \prod_{\substack{n=1 \\ l \neq n}}^Q F_{\gamma_{n,M}}(x) dx \\ = \sum_{i=1}^n H_i e^{x_i} f_{\gamma_{l,M}}(x_i) \prod_{\substack{n=1 \\ l \neq n}}^Q F_{\gamma_{n,M}}(x_i), \quad (82)$$

where  $x_i$  and  $H_i$  are the  $i^{\text{th}}$  abscissa and weight of the  $n^{\text{th}}$  order Laguerre polynomial, respectively [30, eq. (25.4.45)], and  $F_{\gamma_{n,M}}(x) = 1 - \int_{\frac{c_2 x}{c_1}}^\infty e^{-\left(z + \frac{x c_3 z + c_4 x}{z^2 c_1 - c_2 z x}\right)} dz$ . At high

SNR, by following similar steps as in (59), (60) and (61),

$$\text{we get } F_{\gamma_{n,M}}(x) \approx \left\{ 1 - \sqrt{\frac{4xc_3}{c_1}} J_1 \left[ \sqrt{\frac{4xc_3}{c_1}} e^{-\frac{c_2 x}{c_1}} \right] \right\}. \\ \text{Also, } f_{\gamma_{l,M}}(x) = \int_{\frac{c_2 x}{c_1}}^\infty \frac{(c_3 z + c_4) z^2 c_1}{(z^2 c_1 - c_2 z x)^2} e^{-\left(z + \frac{x c_3 z + c_4 x}{z^2 c_1 - c_2 z x}\right)} dz,$$

$$\text{which becomes } f_{\gamma_{l,M}}(x) \approx \left( \frac{4\gamma_M c_3 J_0 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} e^{-\frac{c_2 x}{c_1}} \right]}{2xc_1} + \frac{c_2 x w_5 J_1 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} e^{-\frac{c_2 x}{c_1}} \right]}{c_1} \right)$$

at high SNR. Finally,  $S_2$  in (69) which is the probability of having  $Q$  relays in a sub-set  $N_r$  of the EH-relays of size  $|N_r|$ , can be obtained using the expression

$$\Pr(|N_r| = Q) = \binom{N}{Q} P_1^{N-Q} (1 - P_1)^Q, \quad \text{where} \\ P_1 = \Pr(|N_r| = 0).$$

$$\Pr \left( \max_{n \in Q} \left\{ \frac{1 + \gamma_{n,M}}{1 + \gamma_{n,e}} \right\} < \zeta \mid |h_{sr_n}|^2 = \theta \right) = \underbrace{\prod_{n=1}^Q \int_0^\infty \int_0^\infty F_{\gamma_{n,M}} \left( \zeta + \gamma\zeta - 1 \mid |h_{sr_n}|^2 = \theta \right) f_{\gamma_{n,e}} \left( \gamma \mid |h_{sr_n}|^2 = \theta \right) f_{|h_{sr_n}|^2}(\theta) d\theta d\gamma}_{\text{sop of user M using relay n}}, \quad (85)$$

## APPENDIX C

In this appendix, we present the proof of Theorem 4. The secrecy outage probability in this scheme can be calculated as

$$P_{\text{sop}} = \underbrace{\Pr(|N_r| = 0)}_{O_1} \cup \underbrace{\Pr \left( \max_{n \in N_r} \{C_{s,M}^n\} < R_o, |N_r| > 0 \right)}_{O_3}, \quad (83)$$

where  $R_o$  is the target secrecy rate. The term  $O_1 = \Pr(|N_r| = 0)$  was derived in the previous section as per (15). Now, we derive the term  $O_3$  of (83) as

$$O_3 = \sum_{Q=1}^N \underbrace{\Pr \left( \max_{n \in Q} \{C_{s,M}^n\} < R_o \mid |N_r| = Q \right)}_{\Delta_1} \times \underbrace{\Pr(|N_r| = Q)}_{\Delta_2}. \quad (84)$$

Firstly,  $\Delta_2$  is given by (27). Now, we can find  $\Delta_1$  conditionally on  $|h_{sr_n}|^2$  according to (85) where  $\zeta = 2^{2R_o}$ , and the conditional CDF of the SINR at user  $M$ , and the PDF of the SINR at the eavesdropper, are respectively given by

$$\Pr \left( \gamma_{n,M} < \zeta + \gamma\zeta - 1 \mid |h_{sr_n}|^2 = \theta \right) = 1 - e^{-\left( \frac{(\zeta + \gamma\zeta - 1)c_3\theta + c_4(\zeta + \gamma\zeta - 1)}{(\theta^2 c_1 - c_2\theta)(\zeta + \gamma\zeta - 1)} \right)}, \theta > \frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}. \quad (86)$$

$$f_{\gamma_{n,e}} \left( \gamma \mid |h_{sr_n}|^2 = \theta \right) = \frac{1}{\gamma} e^{-\left( \frac{\gamma e_3 \theta + e_4 \gamma}{\theta^2 e_1 - e_2 \theta \gamma} \right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2}. \quad (87)$$

Therefore,  $\Pr \left( \max_{n \in Q} \left\{ \frac{1 + \gamma_{n,M}}{1 + \gamma_{n,e}} \right\} < \zeta \mid |h_{sr_n}|^2 = \theta \right)$  can be found as in (88) and (89). where  $\epsilon_1 = \frac{e_2 \gamma}{c_1}$  and  $\epsilon_2 = \frac{c_2(\zeta + \gamma\zeta - 1)}{c_1}$ . The expression (89) can be approximated using Gaussian Quadrature rules as in (90) where  $\gamma_i, \theta_j$  and  $H_i, H_j$  are the  $i^{\text{th}}, j^{\text{th}}$  abscissas and weights of the  $n^{\text{th}}$  order Laguerre polynomial, respectively [30, eq. (25.4.45)].

## APPENDIX D

Here we provide the proof of Lemma 5. Firstly,

$$\Pr \left( R_{\Phi_n, M} > \bar{R}_M \right) = 1 - \Pr \left( \sum_{n=1}^{l_n} \gamma_{n,M} < \gamma_M \right), \quad (91)$$

where  $\gamma_M = 2^{a\bar{R}_M} - 1$ . As we can see from (91) the overall SINR in this scenario is the summation of multiple random variables. Therefore, derivation of the PDF and CDF of the overall SINR is typically more complicated and a closed-form expression is tedious to obtain, if not infeasible. On the other hand, the MGF-based approach has been recognized as an efficient and effective way for the outage analysis.

The MGF of  $\varphi = \sum_{n=1}^{l_n} \gamma_{n,M}$  can be found as [39]

$$\mathcal{M}_\varphi(s) = \prod_{n=1}^{l_n} \mathcal{M}_{\gamma_{n,M}}(s), \quad (92)$$

where  $\mathcal{M}_{\gamma_{n,M}}(s)$  is given by (93), and  $f_{\gamma_{l,M}}(x) = \int_0^\infty \frac{c_2 x}{c_1} \frac{(c_3 z + c_4) z^2 c_1}{(z^2 c_1 - c_2 z x)^2} e^{-\left( z + \frac{x c_3 z + c_4 x}{z^2 c_1 - c_2 z x} \right)} dz$ . At high SNR, by ignoring the last term in the denominator of the  $\gamma_{n,M}$  expression, and following similar steps as in (59), (60) and (61), the PDF becomes  $f_{\gamma_{l,M}}(x) \approx \left( \frac{4\gamma_M c_3 J_0 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} \right] e^{-\frac{c_2 x}{c_1}}}{2x c_1} + \frac{c_2 x w_5 J_1 \left[ \sqrt{\frac{4\gamma_M c_3}{c_1}} \right] e^{-\frac{c_2 x}{c_1}}}{c_1} \right)$ .

Thus, the MGF in (93) at high SNR is

$$\mathcal{M}_{\gamma_{n,M}}(s) = \int_0^\infty e^{-s\gamma_M} \times \left( \frac{w_5^2 J_0[w_5] e^{-\frac{c_2 \gamma_M}{c_1}}}{2\gamma_M} + \frac{c_2 \gamma_M w_5 J_1[w_5] e^{-\frac{c_2 \gamma_M}{c_1}}}{\gamma_M c_1} \right) d\gamma_M, \quad (94)$$

where  $w_5 = \sqrt{\frac{4\gamma_M c_3}{c_1}}$ . Equation (94) can be expressed in terms of the weights and abscissas of a Laguerre polynomial as

$$\mathcal{M}_{\gamma_{n,M}}(s) = \sum_{r=1}^K \frac{H_r}{s}$$



$$\begin{aligned}
\Pr\left(\max_{n \in Q} \left\{ \frac{1 + \gamma_{n,M}}{1 + \gamma_{n,e}} \right\} < \zeta \mid |h_{sr_n}|^2 = \theta\right) &= \prod_{n=1}^Q \int_0^{\infty} \left\{ \int_{\epsilon_1}^{\epsilon_2} f_{\gamma_{n,e}}(\gamma \mid |h_{sr_n}|^2 = \theta) f_{|h_{sr_n}|^2}(\theta) d\theta \right. \\
&\quad + \int_{\epsilon_2}^{\infty} F_{\gamma_{n,M}}(\zeta + \gamma\zeta - 1 \mid |h_{sr_n}|^2 = \theta) \\
&\quad \left. \times f_{\gamma_{n,e}}(\gamma \mid |h_{sr_n}|^2 = \theta) f_{|h_{sr_n}|^2}(\theta) d\theta \right\} d\gamma, \tag{88}
\end{aligned}$$

$$\begin{aligned}
\Pr\left(\max_{n \in Q} \left\{ \frac{1 + \gamma_{n,M}}{1 + \gamma_{n,e}} \right\} < \zeta \mid |h_{sr_n}|^2 = \theta\right) &= \prod_{n=1}^Q \int_0^{\infty} \left\{ \int_{\epsilon_1}^{\epsilon_2} \left( e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{\theta^2 e_1 - e_2 \theta \gamma}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{\gamma (\theta^2 e_1 - e_2 \theta \gamma)^2} \right) e^{-\theta} d\theta \right. \\
&\quad \left. + \int_{\epsilon_2}^{\infty} \left( 1 - e^{-\left(\frac{(\zeta + \gamma\zeta - 1)c_3 \theta + c_4(\zeta + \gamma\zeta - 1)}{\theta^2 c_1 - c_2 \theta (\zeta + \gamma\zeta - 1)}\right)} \right) \times \left( \frac{1}{\gamma} e^{-\left(\frac{\gamma e_3 \theta + e_4 \gamma}{\theta^2 e_1 - e_2 \theta \gamma}\right)} \frac{(\gamma e_3 \theta + e_4 \gamma) \theta^2 e_1}{(\theta^2 e_1 - e_2 \theta \gamma)^2} \right) e^{-\theta} d\theta \right\} d\gamma, \tag{89}
\end{aligned}$$

$$\begin{aligned}
&\Pr\left(\max_{n \in Q} \left\{ \frac{1 + \gamma_{n,M}}{1 + \gamma_{n,e}} \right\} < \zeta \mid |h_{sr_n}|^2 = \theta\right) \approx \\
&\prod_{n=1}^Q \sum_{i=1}^n H_i e^{\gamma_i} \left\{ \left( e^{-\left(\frac{\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i}{\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i}\right)} \frac{(\gamma_i e_3 \frac{\epsilon_2 + \epsilon_1}{2} + e_4 \gamma_i) (\epsilon_2 - \epsilon_1) \left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e_1}{\gamma_i \left(\left(\frac{\epsilon_2 + \epsilon_1}{2}\right)^2 e_1 - e_2 \frac{\epsilon_2 + \epsilon_1}{2} \gamma_i\right)^2} \right) \right. \\
&\quad \left. + \sum_{j=1}^n H_j \left\{ 1 - e^{-\left(\frac{(\zeta + \gamma\zeta - 1)c_3 \theta_j + c_4(\zeta + \gamma\zeta - 1)}{\theta_j^2 c_1 - c_2 \theta_j (\zeta + \gamma\zeta - 1)}\right)} \right\} \times \left\{ \frac{1}{\gamma_i} e^{-\left(\frac{\gamma_i e_3 \theta_j + e_4 \gamma_i}{\theta_j^2 e_1 - e_2 \theta_j \gamma_i}\right)} \frac{(\gamma_i e_3 \theta_j + e_4 \gamma_i) \theta_j^2 e_1}{(\theta_j^2 e_1 - e_2 \theta_j \gamma_i)^2} \right\} \right\}. \tag{90}
\end{aligned}$$

$$\begin{aligned}
\mathcal{M}_{\gamma_{n,M}}(s) &= \int_0^{\infty} e^{-s\gamma_{n,M}} f_{\gamma_{n,M}}(\gamma_M) d\gamma_M, \\
&= \int_0^{\infty} \frac{e^{-s\gamma_M}}{\gamma_M} \left\{ \int_{\frac{c_2 \gamma_M}{c_1}}^{\infty} e^{-x_n - \frac{\gamma_M c_3 x_n + c_4 \gamma_M}{(x_n^2 c_1 - c_2 x_n \gamma_M)}} \frac{(\gamma_M c_3 x_n + c_4 \gamma_M) x^2 c_1}{(x_n^2 c_1 - c_2 x_n \gamma_M)^2} dx \right\} d\gamma_M. \tag{93}
\end{aligned}$$

$$\begin{aligned}
&\times \left( \frac{sw_{5_r}^2 J_0[w_{5_r}] e^{-\frac{c_2 \gamma_{M_r}}{sc_1}}}{2\gamma_{M_r}} + \frac{sc_2 \gamma_{M_r} w_{5_r} J_1[w_{5_r}] e^{-\frac{c_2 \gamma_{M_r}}{sc_1}}}{\gamma_{M_r} c_1} \right), \quad = \frac{1}{2\pi j} \int_{\varrho - j\infty}^{\varrho + j\infty} \frac{\mathcal{M}_{\varphi}(s)}{s} e^{s\gamma_M} ds, \tag{96}
\end{aligned}$$

where  $H_r$  and  $\gamma_{M_r}$  are the  $r^{th}$  abscissa and weight, respectively, of the  $K^{th}$  order Laguerre polynomial, and  $w_{5_r} = \sqrt{\frac{4\gamma_{M_r} c_3}{c_1}}$ . Subsequently, the exact probability  $\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,M} < \gamma_M\right)$  can be obtained with the inverse Laplace transform as

$$\Pr\left(\sum_{n=1}^{l_n} \gamma_{n,M} < \gamma_M\right) = \mathfrak{L}^{-1}\left(\frac{\mathcal{M}_{\varphi}(s)}{s}\right)$$

where  $\mathfrak{L}^{-1}$  denotes the inverse Laplace transform, and  $\varrho$  is chosen in the region of convergence of the integral in the complex  $s$  plane. The integral in (96) can be evaluated numerically efficiently using the available mathematical softwares or by applying numerical techniques. Several methods for evaluating the inverse Laplace transform have been introduced in the literature. A valuable summary of these methods is provided in [33], [34]. Using (11) in [34], the CDF of the summation of SINRs can be mapped directly from the MGF using (97).

$$\Pr \left( \sum_{n=1}^l \gamma_{n,M} < \gamma_M \right) = \frac{2^{-Q} e^{\frac{A}{2}}}{\gamma_M} \sum_{q=0}^Q \binom{Q}{q} \sum_{n=0}^{N+q} \frac{(-1)^n}{\beta_n} \Re \left( \frac{\mathcal{M}_\varphi \left( \frac{A + 2\pi j n}{2\gamma_M} \right)}{\frac{A + 2\pi j n}{2\gamma_M}} \right) + E(A, N, Q). \quad (97)$$

## REFERENCES

- [1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Maga.*, vol. 55, pp. 185–191, Feb. 2017.
- [2] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Sig. Proc. Let.*, vol. 21, pp. 1501–1505, Dec. 2014.
- [3] J. Zhu, J. Wang, Y. Huang, S. He, X. You, and L. Yang, "On optimal power allocation for downlink non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, pp. 2744–2757, Dec. 2017.
- [4] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," *IEEE Trans. Commun.*, vol. 64, pp. 654–667, Feb. 2016.
- [5] J. B. Kim and I. H. Lee, "Non-orthogonal multiple access in coordinated direct and relay transmission," *IEEE Commun. Let.*, vol. 19, pp. 2037–2040, Nov. 2015.
- [6] J. B. Kim and I. H. Lee, "Capacity analysis of cooperative relaying systems using non-orthogonal multiple access," *IEEE Commun. Let.*, vol. 19, pp. 1949–1952, Nov. 2015.
- [7] N. T. Do, D. B. D. Costa, T. Q. Duong, and B. An, "A BNBF user selection scheme for NOMA-based cooperative relaying systems with SWIPT," *IEEE Commun. Let.*, vol. 21, pp. 664–667, Mar. 2017.
- [8] J. Men and J. Ge, "Non-orthogonal multiple access for multiple-antenna relaying networks," *IEEE Commun. Let.*, vol. 19, pp. 1686–1689, Oct. 2015.
- [9] 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 Trans. Wireless Commun.*, vol. 16, pp. 4332–4343, Jul. 2017.
- [10] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 34, pp. 938–953, Apr. 2016.
- [11] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- [12] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Let.*, vol. 20, pp. 930–933, May. 2016.
- [13] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 1656–1672, Mar. 2017.
- [14] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, pp. 7563–7567, Aug. 2017.
- [15] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems," *IEEE Sig. Proc. Let.*, vol. 24, pp. 1113–1117, Aug. 2017.
- [16] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, pp. 3151–3163, Jul. 2017.
- [17] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, pp. 2196–2206, Oct. 2017.
- [18] H. Lei, J. Zhang, K. H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
- [19] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 3622–3636, Jul. 2013.
- [20] A. Salem and K. A. Hamdi, "Wireless power transfer in multi-pair two-way AF relaying networks," *IEEE Trans. Commun.*, vol. 64, pp. 4578–4591, Nov. 2016.
- [21] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Wireless information and power transfer in cooperative networks with spatially random relays," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 4440–4453, Aug. 2014.
- [22] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J.Sel. Areas Commun.*, vol. 31, pp. 2099–2111, Oct. 2013.
- [23] H. Hui, A. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, pp. 1147–1151, Aug. 2015.
- [24] A. Ozgur, O. Leveque, and D. Tse, "Hierarchical cooperation achieves optimal capacity scaling in Ad Hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, pp. 3549–3572, Oct. 2007.
- [25] Z. Shi, S. Ma, H. ElSawy, G. Yang, and M. Alouini, "Cooperative HARQ-assisted NOMA scheme in large-scale D2D networks," *IEEE Transactions on Communications*, vol. 66, pp. 4286–4302, Sep. 2018.
- [26] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 938–953, Apr. 2016.
- [27] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 4438–4454, Jun. 2016.
- [28] H. Chingoska, Z. Hadzi-Velkov, I. Nikoloska, and N. Zlatanov, "Resource allocation in wireless powered communication networks with non-orthogonal multiple access," *IEEE Wireless Communications Letters*, vol. 5, pp. 684–687, Dec. 2016.
- [29] J. K. Y W Peter Hong, Pang Chang Lan C C, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. SpringerBriefs in Electrical and Computer Engineering, NY, USA, 2010.
- [30] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tabl.* Washington, D.C.: U.S. Dept. Commerce, 1972.
- [31] 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, pp. 6054–6067, Nov. 2014.
- [32] H. Lei, J. Zhang, K. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
- [33] J. Abate and W. Whitt, "Numerical inversion of laplace transforms of probability distributions," *ORSA J. Computing*, vol. 7, no. 1, pp. 36–43, 1995.
- [34] Y.-C. Ko, M. S. Alouini, and M. K. Simon, "Outage probability of diversity systems over generalized fading channels," *IEEE Trans. Commun.*, vol. 48, pp. 1783–1787, Nov. 2000.
- [35] A. Salem, L. Musavian, and K. A. Hamdi, "Wireless power transfer in distributed antenna systems," *IEEE Transactions on Communications*, vol. 67, pp. 737–747, Jan. 2019.
- [36] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.
- [37] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, pp. 1787–1791, Oct. 2010.
- [38] H. David., *Order Statistics*. 1970:John Wiley and Sons.
- [39] S. M. ROSS, *Introduction to probability models 10ed*. 2010.