Secrecy Performance Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems

MAHENDRA K. SHUKLA, HA H. NGUYEN, AND OM JEE PANDEY

1Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK S7N 5A9, Canada
2Department of Electronics and Communication Engineering, School of Engineering and Applied Sciences, SRM University, Amaravati 522502, India

Corresponding author: Mahendra K. Shukla (m.shukla@usask.ca)

ABSTRACT This paper studies physical layer security for two-way relay non-orthogonal multiple access systems. Specifically, by employing a decode-and-forward relay and considering both the maximum-ratio combining and selection combining schemes at the eavesdropper, instantaneous end-to-end signal-to-interference-plus-noise ratios are first formulated and approximated for the interference-limited scenario. Then analytical expressions for the secrecy outage probability and the intercept probability are obtained. Moreover, we analyze the effective secrecy diversity order and demonstrate that the eavesdropper severely degrades the secrecy performance, and even reduces the diversity order to zero. Numerical and simulation results verify our derivations and reveal that, due to information leakage in the first time phase, there exists a secrecy performance floor. It is also demonstrated that the secrecy outage probability performance degrades when the eavesdropper is closer to either of the users. Between the two combining schemes, the results demonstrate that the secrecy outage probability performance is better when the selection combining scheme is employed by the eavesdropper.

INDEX TERMS Physical layer security, non-orthogonal multiple access (NOMA), two-way relay networks, secrecy outage probability, intercept probability, decode-and-forward (DF).

I. INTRODUCTION

With the increasing demand for wireless communications services and applications, non-orthogonal multiple access (NOMA) has attracted significant attention in 5G research community owing to its superior spectrum efficiency [1]–[3]. In contrast to the traditional orthogonal multiple access, NOMA exploits the power domain in addition to the time or frequency domain [4] to manage signal transmissions by multiple users. In NOMA, users are allocated different powers depending on the channel conditions, and the transmitter employs superposition coding to transmit the combined signal to users [5]. Further, to extract the desired message from the combined received signal, successive interference cancellation is performed at the receivers [6], [7].

Recently, NOMA has been introduced in cooperative relaying which offers enhanced coverage, throughput, and reliability [8], [9], especially for the users with bad channel conditions [11]–[21]. In cooperative relaying communications, to achieve the spatial diversity, communication between transmitter and receiver is done via a relay node [10]. For a cooperative NOMA system, the authors in [11] have derived the exact outage probability and simple bounds for the multi-user scenario. Further, the authors in [12] have investigated the performance by considering both direct and indirect links between the base station and far users. Moreover, to facilitate the far user, decode-and-forward (DF) relaying is used in both full-duplex (FD) and half-duplex (HD) modes. In [13], the authors have proposed two-stage superimposed transmission with finite time slots and evaluated the ergodic sum rate and outage probability of a cooperative NOMA system. The authors in [14] have proposed a two-stage relay selection scheme and evaluate the outage performance. The energy efficiency and delay issue for a cooperative NOMA system have been addressed in [15]. The authors in [16] have utilized the max-min selection method to satisfy the quality-of-service of users and obtained the sum rate and outage probability. In [17], the system performance in delay-limited and delay-tolerant transmission modes for a full-duplex cooperative NOMA system is analyzed.

It is pointed out that all the aforementioned research works [8]–[17] have investigated NOMA system performance under
one-way relaying only. In comparison to one-way relaying, two-way relaying (TWR) has emerged as a more spectrally efficient technique [22]–[24]. Recently, by considering TWR, the authors in [18]–[21] have investigated performance of NOMA systems. In particular, the authors in [18] have analyzed performance of a TWR-NOMA system by considering both perfect and imperfect successive interference cancellation. The authors in [19] have investigated a jointly-optimized power and time allocation scheme to minimize the system outage probability. Further, the authors in [20] have introduced a hybrid TWR method to evaluate the bit error rate and system throughput. In [21], hardware impairments are considered in performance analysis of TWR-NOMA systems.

Although the introduction of NOMA in cooperative relaying offers coverage, throughput, and reliability enhancement, information security remains a major concern due to the broadcast nature of wireless communications. The eavesdroppers may overhear the private and sensitive information of the legitimate sources and present a security threat to NOMA systems [25]. To combat such problems, generally higher-layer encryption protocols and algorithms are provided, which may not be good enough with the growing computational power and capability [26] of eavesdroppers. An alternative method to provide security at physical layer was proposed by Wyner, which exploits characteristics of the physical layer [27].

For NOMA systems, the authors in [28] have obtained an SOP expression by considering artificial noise, whereas the authors in [29] have analyzed the secrecy outage probability (SOP) when the max–min transmit antenna selection (TAS) scheme is used in a MIMO-NOMA system. Further, considering the transmit antenna selection, SOP performance is examined in [30]. In the context of cooperative relay networks using NOMA, only a few works have studied the problem of physical layer security [31]–[39]. Specifically, in [31], the authors have evaluated SOP for NOMA systems by considering both amplify-and-forward (AF) and DF protocols, whereas in [32] and [33], the authors have examined SOP for multiple-relay assisted NOMA systems. Further, by considering multiple eavesdroppers, SOP performance has been evaluated under the multi-relay scenario in [34] and [35]. In [36], the authors have examined the effects of residual hardware impairment on the intercept probability and SOP. To improve the secrecy performance, the authors in [37] have considered jammer-aided cooperative NOMA systems and obtained a SOP expression. In [38], a two-stage FD-jamming is proposed to provide secure transmission. Again, it is noted that all the aforementioned studies have considered only one-way relay NOMA systems. Only recently, the secrecy energy efficiency and ergodic secrecy rate are evaluated in [39] and [40], respectively, for TWR-NOMA systems. To the best of the authors’ knowledge, there is no work in the literature that studies the secrecy outage performance of TWR-NOMA systems. Therefore, the objective of this paper is to fill this important research gap.

In light of preceding discussions, in this paper, we consider a TWR-NOMA system where two single-antenna users communicate with each other with the help of a single-antenna DF relay in the presence of a single-antenna eavesdropper. The contributions of this paper are summarized as follows.

• For the considered TWR-NOMA system, we first formulate the instantaneous end-to-end signal-to-interference-plus-noise ratios (SINRs) by examining both maximum ratio combining (MRC) and selection combining (SC) schemes at the eavesdropper. In the interference-limited scenario, the SINRs are well approximated by the signal-to-interference ratios by ignoring thermal noise. Based on such approximations, novel tight closed-form analytical expressions for the SOP are derived.

• We investigate the intercept probability as a special case of SOP, where the channel capacity of the main link falls below link channel capacity of the eavesdropper. The intercept probability expressions are provided for both cases of MRC and SC schemes at the eavesdropper.

• We analyze the effective secrecy diversity order to obtain useful information about the system secrecy performance. We demonstrate that the eavesdropper severely degrades the secrecy performance, and even reduces the diversity order to zero.

• We study the effects of the main link, eavesdropper link, target secrecy rate and power allocation coefficient on the SOP performance. It is demonstrated that a single eavesdropper can severely deteriorate the SOP performance and there exists a secrecy performance floor. It is also demonstrated that the secrecy outage probability gets worse when the eavesdropper is closer to either of the users and the SOP performance is better when the SC scheme is employed instead of the MRC scheme at the eavesdropper.

The remainder of this paper is organized as follows. In Section II, we describe the secure TWR-NOMA system considered in the paper. In Section III, we first formulate and approximate the end-to-end SINRs and derive the expressions of the SOP and intercept probability. The effective secrecy diversity order is also analyzed in Section III. Section IV presents numerical and simulation results. Finally, the conclusions are drawn in Section V.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider a NOMA-based wireless system in which two single-antenna users, $U_1$ and $U_2$, exchange information bidirectionally via a single-antenna, half-duplex DF relay $R$ under the malicious attempt of a single-antenna passive eavesdropper $E$. The two-way communication takes place in two time phases and in each phase $E^1$ overhears the information transmitted by $U_1$, $U_2$, $1$In this paper, we consider only one eavesdropper. The case of multiple eavesdroppers can also be analyzed for the considered system model. For such a case, it is expected that the secrecy performance will further degrade due to higher chances of information leakage [34], [35].
where the legitimate terminals have some prior knowledge about the CSI of users. Moreover, such consideration is also more challenging than the case where the legitimate terminals are absent and all the channels are reciprocal and subject to independent quasi-static frequency-flat Rayleigh fading. The direct links between $U_1$ and $U_2$ are assumed to be absent and all the channels are modeled as $CN(0, \Omega_1)$, where $X \sim CN(a, b)$ denote a complex Gaussian random variable (RV) $X$ with mean $a$ and variance $b$. Likewise, the channel coefficients $h_1$ and $h_2$ for the links $R \rightarrow U_1$ and $R \rightarrow U_2$ are modeled as $CN(0, \Omega_1)$, respectively. Moreover, it is assumed that the relay linearly combines the decoded messages of $U_1$ and $U_2$ as $CN(0, \Omega_R)$, respectively. Finally, additive white Gaussian noise (AWGN) for each link is modeled as $CN(0, N_0)$.

**TABLE 1.** Frequently used parameters/symbols.

<table>
<thead>
<tr>
<th>Parameters/Symbols</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N_0$</td>
<td>AWGN variance at each link</td>
</tr>
<tr>
<td>$U_1, U_2$, and $R$</td>
<td>User 1, User 2, and relay, respectively</td>
</tr>
<tr>
<td>$P_1, P_2$, and $P_R$</td>
<td>Transmission power of User 1, User 2, and relay, respectively</td>
</tr>
<tr>
<td>$\Omega_i$</td>
<td>Variance of the $i^{th}$ link</td>
</tr>
<tr>
<td>$a_i$</td>
<td>Power allocation coefficients for the messages of the $i^{th}$ transmission</td>
</tr>
<tr>
<td>$R(\cdot)$</td>
<td>Absolute value</td>
</tr>
<tr>
<td>$u(\cdot)$ and $d(\cdot)$</td>
<td>Heaviside step function and Dirac delta function</td>
</tr>
<tr>
<td>$F_i(\cdot)$</td>
<td>Gauss hypergeometric function [47, eq. (9.14.2)]</td>
</tr>
<tr>
<td>$E_i(\cdot)$</td>
<td>Exponential integral [47, eq. (8.211.1)]</td>
</tr>
<tr>
<td>$R_x$</td>
<td>Target secrecy rate (in bps/Hz)</td>
</tr>
<tr>
<td>$f_X(\cdot)$</td>
<td>Probability density function of $X$</td>
</tr>
<tr>
<td>$P_X(\cdot)$</td>
<td>Cumulative distribution function of $X$</td>
</tr>
<tr>
<td>$CM$</td>
<td>Capacity of the main link</td>
</tr>
<tr>
<td>$CE$</td>
<td>Capacity of the eavesdropper link</td>
</tr>
</tbody>
</table>

**A. INSTANTANEOUS END-TO-END SINRS**

1) **INSTANTANEOUS END-TO-END SINRS OF MAIN LINKS**

The complete two-way information exchange between $U_1$ and $U_2$ takes two transmission phases. In the first phase (see Fig. 1(a)), both legitimate users $U_1$ and $U_2$ simultaneously transmit their respective messages of unit-variance, $x_1$ and $x_2$, to the relay. Therefore, the received signal at $R$ is given as

$$y_R = \sqrt{a_{1,R}}Ph_1x_1 + \sqrt{a_{2,R}}Ph_2x_2 + n_R,$$

where $n_R$ is AWGN at $R$, $a_{1,R}$ and $a_{2,R}$ are the power allocation coefficients for the messages $x_1$ and $x_2$, respectively, which satisfy $0 < a_{1,R}, a_{2,R} < 1$ and $a_{1,R} + a_{2,R} = 1$ [8]. Moreover, we have considered the total power constraint to control the inter-cell and inter-pair interference in a hybrid NOMA system [6], [8]. Without loss of generality, it is assumed that the channel condition of $U_1$ is better than that of $U_2$ (i.e., $\Omega_1 \geq \Omega_2$) [1], [8], [34]. Following the principle of SIC as presented in [12], [34], [37] the relay decodes message $x_1$ before recovering $x_2$, as $U_1$ is the stronger user. Hence, the SINR to extract $x_1$ at $R$ is expressed as

$$\Lambda_{1,R} = \frac{a_{1,R}P_R|h_1|^2}{a_{2,R}P_R|h_2|^2+1},$$

where $P_R = P_1 = P_2$. Then, by subtracting the interference from $U_1$, the received SNR to extract $x_2$ at $R$ is

$$\Lambda_{2,R} = a_{2,R}P_R|h_2|^2.$$

Moreover, for successful decoding of messages $x_1$ and $x_2$ at the relay, the corresponding data rates of $U_1$ and $U_2$ should be lower than $\log_2(1+a_{2,R}P_R|h_2|^2)$ and $\log_2 \left(1 + \frac{a_{1,R}P_R|h_1|^2}{a_{2,R}P_R|h_2|^2+1}\right)$, respectively [41].

During the second transmission phase (see Fig. 1(b)), both legitimate users $U_1$ and $U_2$ communicate with the relay $R$ by simultaneously transmitting their respective messages $x_1$ and $x_2$. The relay linearly combines the decoded messages of $U_1$ and $U_2$ and then broadcasts the resultant signal to $U_1$ and $U_2$ with a total power $P_R$. Therefore, the received signal at $U_1$ and $U_2$ can be expressed, respectively, as

$$y_{R,1} = h_1(\sqrt{a_{1,R}P_R}|x_1| + \sqrt{a_{2,R}P_R}|x_2|) + n_{R,1},$$

$$y_{R,2} = h_2(\sqrt{a_{1,R}P_R}|x_1| + \sqrt{a_{2,R}P_R}|x_2|) + n_{R,2},$$

where $n_{R,1}$ and $n_{R,2}$ are AWGN at $U_1$ and $U_2$, respectively. The strong user supports the high data rate application such as live streaming, whereas the weak user supports the low data rate application such as text messaging [35].

In this paper, perfect SIC is considered to provide an intuitive view on the SOP performance of the considered TWR-NOMA system. The case of imperfect SIC is left for future work.

2Such CSI consideration is more practical because the CSI corresponding to the passive eavesdropper link is usually not known to the intended users. Moreover, such consideration is also more challenging than the case where the legitimate terminals have some priori knowledge about the CSI corresponding to the passive eavesdropper link.
where $n_{R,1}$ and $n_{R,2}$ are AWGNS at $U_1$ and $U_2$ respectively, $a_{R,1}$ and $a_{R,2}$ are the power allocation coefficients corresponding to transmission of $R$ to $U_1$ and $U_2$, respectively, such that $a_{R,1}, a_{R,2} > 0$ and $a_{R,1} + a_{R,2} = 1$. Further, users $U_1$ and $U_2$ subtract their own messages from $y_{R,1}$ and $y_{R,2}$, respectively. Hence, the SNRs for decoding $x_2$ and $x_1$ at $U_1$ and $U_2$ can be obtained, respectively, as

$$
\Lambda_{R,1} = a_{R,2} \rho_R |h_1|^2, \\
\Lambda_{R,2} = a_{R,1} \rho_R |h_2|^2,
$$

where $\rho_R = \frac{E}{N_0}$. Furthermore, to maximize the SINRs of the wiretap $U_1 \rightarrow E$ and $U_2 \rightarrow E$ links, $E$ combines the received signals using two popular combining schemes, namely MRC and SC. The instantaneous end-to-end SINRs at $E$ under MRC and SC schemes are discussed in following subsections.\textsuperscript{5}

2) INSTANTANEOUS END-TO-END SINRs AT $E$ UNDER MRC SCHEME

In the first phase (see Fig. 1(a)), $E$ intercepts the messages transmitted by $U_1$ and $U_2$. Therefore, the received signal at $E$ can be given as

$$
y_E = \sqrt{a_{1,E} P_1} h_{1,E} x_1 + \sqrt{a_{2,E} P_2} h_{2,E} x_2 + n_E,
$$

where $n_E$ is AWGN at $E$. In this work, we assume that the eavesdropper has the same detection capability as the legitimate users, i.e., it detects the desired signal by considering the signal from the other user as interference.\textsuperscript{6} Hence, in the first phase, the SINRs for decoding $x_1$ and $x_2$ at $E$ can be obtained, respectively, as

$$
\Lambda_{1,E}^{(1)} \approx \frac{a_{1,E} |h_{1,E}|^2}{a_{2,E} |h_{2,E}|^2 + 1} \approx \frac{a_{1,E} |h_{1,E}|^2}{a_{2,E} |h_{2,E}|^2}, \\
\Lambda_{2,E}^{(1)} \approx \frac{a_{2,E} |h_{2,E}|^2}{a_{1,E} |h_{1,E}|^2 + 1} \approx \frac{a_{2,E} |h_{2,E}|^2}{a_{1,E} |h_{1,E}|^2},
$$

It is pointed out that the approximations made in the above two expressions essentially approximate SINRs by their upper bounds, which are the signal-to-interference ratios (SIRs). Such approximations are valid and widely adopted in the literature (see, e.g. [43]) when performance analysis is focused on the interference-limited case in which the thermal noise is negligible compared to the aggregate interference from the other transmitters [42].

In the second phase (see Fig. 1(b)), $E$ again intercepts the information broadcasted by $R$. Therefore, the received signal at $E$ in the second phase can be expressed as

$$
y_{R,E} = h_{R,E} \left( \sqrt{a_{R,1} P_1} x_1 + \sqrt{a_{R,2} P_2} x_2 \right) + n_{R,E}.
$$

where $n_{R,E}$ is AWGN at $E$. Thus, in the second phase, the SINRs for decoding $x_1$ and $x_2$ at $E$ are determined and approximated, respectively, as

$$
\Lambda_{1,E}^{(2)} = \frac{a_{R,2} \rho_R |h_{R,E}|^2}{a_{R,1} \rho_R |h_{R,E}|^2 + 1} \approx \frac{a_{R,2}}{a_{R,1}}, \\
\Lambda_{2,E}^{(2)} = \frac{a_{R,1} \rho_R |h_{R,E}|^2}{a_{R,2} \rho_R |h_{R,E}|^2 + 1} \approx \frac{a_{R,1}}{a_{R,2}},
$$

Moreover, under the MRC scheme, the instantaneous SINRs of the wiretap $U_1 \rightarrow E$ and $U_2 \rightarrow E$ links are approximated, respectively, as

$$
\Lambda_{1,E}^{(MRC)} \approx \frac{a_{1,E} |h_{1,E}|^2}{a_{2,E} |h_{2,E}|^2}, \\
\Lambda_{2,E}^{(MRC)} \approx \frac{a_{2,E} |h_{2,E}|^2}{a_{1,E} |h_{1,E}|^2},
$$

Remark: It can be clearly observed from (14) and (15) that $\Lambda_{1,E}^{(MRC)}$ and $\Lambda_{2,E}^{(MRC)}$ do not depend on the channel gain of the $R \rightarrow E$ link, i.e., $|h_{R,E}|^2$. Therefore, in the second phase, the information leakage by $E$ is negligible, and channel gains of legitimate links are dominant.

3) INSTANTANEOUS END-TO-END SINRS AT $E$ UNDER SC SCHEME

Under the SC scheme, the instantaneous SINRs of the wiretap $U_1 \rightarrow E$ and $U_2 \rightarrow E$ links are approximated, respectively, as

$$
\Lambda_{1,E}^{(SC)} \approx \max \left\{ \frac{a_{1,E} |h_{1,E}|^2}{a_{2,E} |h_{2,E}|^2} \right\}, \\
\Lambda_{2,E}^{(SC)} \approx \max \left\{ \frac{a_{2,E} |h_{2,E}|^2}{a_{1,E} |h_{1,E}|^2} \right\}.
$$

4) SECRECY CAPACITY OF THE DF-BASED NOMA SYSTEM

The secrecy capacity of the DF-based NOMA system can be depicted as

$$
C_{\text{SEC}}^{(\theta)} = \left[ C_{\text{fit}}^{(\theta)} - \text{CE}_{\text{fit}}^{(\theta)} \right]^+, \quad \text{for } \theta \in \{\text{MRC}, \text{SC}\},
$$

where $\theta \in \{1, 2\}$ and $[z]^+ = \max\{0, z\}$. It then follows that the capacity of the main channels of users $U_1$ and $U_2$ can be given, respectively, as $C_{\text{fit}}^{(\theta)} = \frac{1}{2} \log_2(1 + \zeta_1)$ and $C_{\text{fit}}^{(\theta)} = \frac{1}{2} \log_2(1 + \zeta_2)$, where $\zeta_1 = \min(\Lambda_{2,R}, \Lambda_{R,1})$ and $\zeta_2 = \min(\Lambda_{1,R}, \Lambda_{R,2})$. The extra multiplications by $\frac{1}{2}$ is due to the fact that the overall information exchange is taking place in two different time phase of same duration. Moreover, the capacities related to the wiretap $U_2 \rightarrow E$ and $U_1 \rightarrow E$ links under MRC and SC schemes are generally given as $C_{\text{fit}}^{(\theta)} = \frac{1}{2} \log_2(1 + \Lambda_{1,E}^{(\theta)})$ and $C_{\text{fit}}^{(\theta)} = \frac{1}{2} \log_2(1 + \Lambda_{2,E}^{(\theta)})$, for $\theta \in \{\text{MRC}, \text{SC}\}$.

The secrecy rate of the weakest terminal defines the overall secrecy capacity and can be written as

$$
C_{\text{SEC}}^{(\theta)} = \min\{C_{\text{SEC},1}^{(\theta)}, C_{\text{SEC},2}^{(\theta)}\}. \quad \text{(19)}
$$
where $c_{SEC,j}^{(g)}$ is expressed as
\[
C_{SEC,j}^{(g)} = CM_j - CE_j^{(g)} = \frac{1}{2} \log_2 \psi_j^{(g)}, \quad j = 1, 2,
\] (20)
where $\psi_1^{(g)} = \frac{1+\zeta_1}{1+\zeta_2}$ and $\psi_2^{(g)} = \frac{1+\zeta_2}{1+\zeta_1}$.

In the next section, we discuss the secrecy performance of TWR-NOMA system. Specifically, we investigate the scenario where eavesdropper applies MRC scheme, and then we examine the scenario where eavesdropper applies SC scheme. We also present the effective secrecy diversity order to get some useful information about system performance. Moreover, the comparison between these two schemes are presented in Section IV.

III. SECRECY PERFORMANCE ANALYSIS

This section provides new tight closed-form expressions for the SOP of the DF-based NOMA systems for both the cases of MRC and SC schemes at $E$ under Rayleigh fading channels. We also provide closed-form expressions of the intercept probability for the considered system, which is a special case of SOP. Moreover, to get useful insights, we present effective secrecy diversity order.

A. SECRECY OUTAGE PROBABILITY

By definition, the secrecy outage event takes place when the instantaneous capacity difference of the main and eavesdropper links drops below a certain target secrecy rate $R_s$ (in bps/Hz). Mathematically, the SOP is written and calculated as
\[
SOP^{(g)}(\gamma_h) = \Pr \left[ \frac{C_{SEC}^{(g)}}{R_s} < \gamma_h \right] = \Pr \left[ \min(\psi_1^{(g)}, \psi_2^{(g)}) < \gamma_h \right] = 1 - \left[ 1 - F_1^{(g)}(\gamma_h) \right] \left[ 1 - F_2^{(g)}(\gamma_h) \right],
\] (21)
where $\gamma_h = 2R_s$ is the SNR threshold. In the above expression, the terms $F_1^{(g)}(\gamma_h)$ and $F_2^{(g)}(\gamma_h)$ are the SOPs of users $U_1$ and $U_2$, respectively. In the following subsections, we derive closed-form SOP expressions when MRC and SC schemes are applied at the eavesdropper, respectively.

1) MRC SCHEME AT $E$

A closed-form expression of SOP, when the MRC scheme is employed at $E$ can be evaluated in the following theorem.

**Theorem 1:** Under Rayleigh fading, a closed-form expression for the SOP of the TWR-NOMA is given as
\[
SOP^{(MRC)}(\gamma_h) = 1 - \left[ 1 - F_{\psi_1}^{(MRC)}(\gamma_h) \right] \left[ 1 - F_{\psi_2}^{(MRC)}(\gamma_h) \right],
\] (22)
where
\[
F_{\psi_1}^{(MRC)}(\gamma_h) = \mathcal{W}_1 \left( \frac{a_{r,1}}{\rho_{1,1}^2} \right) \text{E}_1(2, 1; 2; - \frac{a_{r,1}}{\rho_{1,1}}) + \mathcal{W}_2 \left( \frac{C_{1} \gamma_h}{a_{r,1}} \right) e^{\frac{C_{1} \rho_{1,1}}{a_{r,1}}},
\] (23)
and
\[
F_{\psi_2}^{(MRC)}(\gamma_h) = \mathcal{W}_3 \left( \frac{a_{r,2}}{\rho_{2,1}^2} \right) 2F_1(2, 1; 2; - \frac{a_{r,2}}{\rho_{2,1}}) + \mathcal{W}_4 \left( \frac{A_{1}}{a_{s,1}^2} \right) \left( - \frac{D_{1} \gamma_h a_{r,1}}{a_{r,2}} - \frac{D_{1} \gamma_h a_{s,1}}{a_{s,1}} \right) + \mathcal{W}_5 \left( \frac{A_{2}}{a_{s,2}^2} \right) \left( - \frac{D_{2} \gamma_h a_{r,2}}{a_{r,1}} - \frac{D_{2} \gamma_h a_{s,1}}{a_{s,1}} \right),
\] (24)
with $C_1 = \frac{a_{r,1} \rho_{1,1}^2 + a_{r,2} \rho_{2,1}^2}{a_{r,1} \rho_{1,1} + a_{r,2} \rho_{2,1}}$, $C_2 = a_{r,1}^2 a_{r,2} \rho_{1,1}^2$, $C_3 = a_{r,1} a_{r,2} \rho_{1,1} \rho_{2,2}$, $C_4 = a_{r,1} a_{r,2} \rho_{2,1} \rho_{2,2}$, $C_5 = a_{r,1}^2$, $D_1 = a_{r,1} a_{r,2} \rho_{1,1} \rho_{2,2}$, $D_2 = a_{r,1} a_{r,2}^2 \rho_{1,1}^2$, $D_3 = a_{r,1} a_{r,2} \rho_{1,1}^2$, $D_4 = a_{r,1} a_{r,2}^2$.

Proof: See Appendix A.

2) SC SCHEME AT $E$

To obtain a closed-form expression of SOP when the SC scheme is employed at $E$ we first evaluate the term $F_{\psi_1}^{(SC)}(\gamma_h)$ given in (21) as follows:
\[
F_{\psi_1}^{(SC)}(\gamma_h) = \int_0^\infty F_1(\gamma_h(1 + y) - 1) f_{\psi_1}^{(SC)}(y) dy.
\] (25)
As before, to obtain $f_{\psi_1}^{(SC)}(z)$ we first obtain $F_{\psi_1}^{(SC)}(z)$ as
\[
F_{\psi_1}^{(SC)}(z) = \Pr \left( \max \left( \frac{a_{r,2}^2 \rho_{2,2}^2}{a_{r,1}^2 \rho_{1,1}^2}, \frac{a_{r,2}}{a_{r,1}} \right) < z \right) = F_{\Delta_1}(z) F_{\Delta_2}(z)
\] (26)
where $u(z)$ is the Heaviside step function, $\Delta_1 = \frac{a_{r,2}^2 \rho_{2,2}^2}{a_{r,1}^2 \rho_{1,1}^2}$, and $\Delta_2 = \frac{a_{r,2}}{a_{r,1}}$. Differentiating (26) with respect to $z$ gives
\[
f_{\psi_1}^{(SC)}(z) = \delta(z - \frac{a_{r,2}}{a_{r,1}}) - \frac{a_{r,2}}{a_{r,1}} \rho_{2,2} \delta(z - \frac{a_{r,2}}{a_{r,1}}) + \frac{a_{r,2} \rho_{2,2}^2}{a_{r,1}^2 \rho_{1,1}^2} \delta(z - \frac{a_{r,2}}{a_{r,1}}) + \frac{a_{r,2}}{a_{r,1}} \rho_{2,2} \delta(z - \frac{a_{r,2}}{a_{r,1}}) + \frac{a_{r,2} \rho_{2,2}^2}{a_{r,1}^2 \rho_{1,1}^2} \delta(z - \frac{a_{r,2}}{a_{r,1}}).
\] (27)
where $\delta(\cdot)$ is the Dirac delta function. By substituting the CDF of $\zeta_1$ from (37) and the PDF of $\Lambda_{SC}^{(1,2)}(\cdot)$ from (27) into (25), and carrying out the required integration using $\Gamma(\alpha, x) = \int_0^\infty \alpha^\alpha e^{-\alpha x} \text{d}t$ [47, eq. (8.350.2)], we obtain

$$
F_{\zeta_1}^{(SC)}(\gamma_1h) = 1 - e^{\zeta_1(\gamma_1h-1)}\left(\left(\mu_2 \gamma_1h + \mu_3 \gamma_1h \Gamma(-1, \mu_5 \gamma_1h)\right) - \mu_1 \zeta_1 \Gamma(-1, \mu_5 \gamma_1h)\right)
$$

where $\mu_1 = \frac{\zeta_1 a_1, R}{a_{R, 2}}, \mu_2 = \frac{a_{2, R, a_1, a_2, R, 1} \Omega_{2, E}}{a_{R, 2} \Omega_{1, E}}, \mu_3 = \frac{a_{2, R, a_1, a_2, R, 1} \Omega_{1, E}}{a_{R, 2} \Omega_{1, E}} + \frac{a_{2, R, a_2, R, 1} \Omega_{1, E}}{a_{R, 2} \Omega_{1, E}}, \mu_4 = \frac{a_{2, R, a_2, R, 2} \Omega_{2, E}}{a_{R, 2} \Omega_{1, E}} + \frac{a_{1, R, a_2, R, 2} \Omega_{2, E}}{a_{R, 2} \Omega_{1, E}}, \mu_5 = \frac{a_{1, R, a_2, R, 2} \Omega_{2, E}}{a_{R, 2} \Omega_{1, E}} + \frac{a_{1, R, a_2, R, 2} \Omega_{2, E}}{a_{R, 2} \Omega_{1, E}}$. Likewise, the CDF of $\phi_2$ can be evaluated as

$$
F_{\phi_2}^{(SC)}(\gamma_2h) = \int_0^\infty F_{\phi_1}^{(SC)}(\gamma_2h + 1) \text{d}y
$$

For this, $f_{\phi_1}^{(SC)}(c)$ can be obtained by using a similar approach as used to obtain (27) as

$$
f_{\phi_1}^{(SC)}(c) = \delta \left( z - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2}} \right) - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} + a_{1, R} \Omega_1, E \delta (\gamma_1h + 1) \Gamma(-1, \gamma_1h) + a_{1, R} \Omega_1, E \delta \left( \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right)
$$

By substituting the CDF of $\zeta_2$ from (46) and the PDF of $\Lambda_{SC}^{(1,2)}(\cdot)$ from (30) into (29), and carrying out the required integration with the aid of partial fractions and making use of [47, eq. (8.350.2)], we obtain the SOP of user $U_2$ as

$$
F_{\zeta_2}^{(SC)}(\gamma_2h) = 1 - a_{1, R} \Omega_1, E \delta \left( z - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right) - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} + a_{1, R} \Omega_1, E \delta \left( \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right)
$$

where $\gamma_2 = a_{1, R} \Omega_1, E \delta \Omega_1, E \delta \delta \left( z - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right) - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} + a_{1, R} \Omega_1, E \delta \left( \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right)$.

$$
B_3 = \frac{(\gamma_1, \gamma_2) \Omega_1, E \delta \Omega_1, E \delta \delta \left( z - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right) - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} + a_{1, R} \Omega_1, E \delta \left( \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right)}{(a_{1, R} \Omega_1, E \delta \Omega_1, E \delta \delta \left( z - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right) - \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} + a_{1, R} \Omega_1, E \delta \left( \frac{a_{1, R} \Omega_1, E \delta}{a_{R, 2} \Omega_2, E \delta} \right))}
$$

Similarly, for the case of having SC at the eavesdropper, a closed-form expression for the intercept probability is given as

$$
F_{\zeta_2}^{(SC)}(\gamma_2h) = 1 - \left(1 - F_{\zeta_2}^{(MRC)}\right)\left(1 - F_{\zeta_2}^{(SC)}\right)
$$

where $F_{\zeta_2}^{(MRC)}$ and $F_{\zeta_2}^{(SC)}$ can be obtained by substituting $\gamma_2h = 1$ into (23) and (24), respectively.

C. EFFECTIVE SECRECY DIVERSITY ORDER

To get a better insight from the obtained SOP in (21), here we analyze the effective secrecy diversity order for the considered TWR-NOMA system. According to the information outage probability concept, the diversity order can be defined as [44]

$$
d_{\text{SOP}}^{(\theta)}(\gamma_1h) = -\lim_{\text{SNR} \to \infty} \frac{\log F_{\zeta_2}^{(SC)}(\gamma_1h)}{\log \text{SNR}},
$$

where $\theta \in \{\text{MRC}, \text{SC}\}$. To demonstrate the effective secrecy diversity order, Fig. 2 plots the magnitude of the slope of...

![FIGURE 2. Effective secrecy diversity order versus SNR.](image-url)
SOP versus the SNR $\rho_3 = \rho_5$ (in dB) when $\Omega_1 = 10$, $\Omega_2 = 5$, $\Omega_{1,E} = 5$, $\Omega_{2,E} = 1$, $a_{1,R} = 0.9$, $a_{R,1} = 0.6$, and $R_s = 2$ bps/Hz under both the MRC and SC schemes at E. It can be seen from Fig. 2 that the effective secrecy diversity order reduces to zero as SNR increases. This indicates that the overall system secrecy performance will be limited by the dominance of information leakage in the first time slot and even a single eavesdropper significantly deteriorates the system performance in a TWR-NOMA system. Such behavior can also be seen through the plots presented in Section IV (numerical results and discussions), where the SOP performance reaches to an error floor as SNR increases.

### IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we present numerical results to corroborate our analytical findings and to provide valuable insights on the secrecy performance of the considered system. Specifically, we study effects of the main link, eavesdropper link, target secrecy rate and power allocation coefficient on the SOP performance. We perform Monte-Carlo simulations for $10^6$ independent trials. Further, the SNR is $\rho_3 = \rho_5$.

![FIGURE 3. Effect of the main link on the SOP performance.](image)

Fig. 3 plots SOP performance versus SNR for different values of $\Omega_1$ ($\Omega_1$ is the variance of $U_1 \rightarrow R$ link) when $a_{1,R} = 0.9$, $a_{R,1} = 0.6$, $\Omega_2 = 5$, $\Omega_{1,E} = 2$, $\Omega_{2,E} = 1$, $\Omega_{R,E} = 1$, and $R_s = 0.5$ bps/Hz under both the MRC and SC schemes at E. It can be seen from the figure that the analytical SOP results with MRC and SC schemes match perfectly with the simulation results. Moreover, the figure reveals that, as the channel quality of the main link ($U_1 \rightarrow R$) increases, the SOP decreases. For instance, the SOP decreases as $\Omega_1$ increases from 10 to 15. Therefore, when the legitimate user is closer to the relay, the SOP performance improves. Similar observation can also be made for the case when the quality of the main link ($U_2 \rightarrow R$) increases. It can be seen that the SOP performance deteriorates drastically due to eavesdropper and performance floors can be observed at high SNR. Moreover, the SOP performance under the MRC scheme at E is worse than that under the SC scheme. This is expected since the eavesdropper is able to fetch more information with the MRC than with the SC, but at the cost of increased hardware complexity.

![FIGURE 4. Effect of the target secrecy rate on the SOP performance.](image)

The impact of target secrecy rate $R_t$ (in bps/Hz) on the SOP performance is shown Fig. 4 when $a_{1,R} = 0.9$, $a_{R,1} = 0.6$, $\Omega_1 = 10$, $\Omega_2 = 5$, $\Omega_{1,E} = 2$, $\Omega_{2,E} = 1$, and $\Omega_{R,E} = 1$, under both the MRC and SC schemes at E. It can be seen that the SOP performance degrades as the target secrecy rate $R_t$ increases, which is because the power requirement increases to support the higher $R_t$. The plots demonstrate that the SOP gets saturated in the high SNR regime due to the presence of the eavesdropper. Moreover, we have also compared the SOP performance of the TWR-NOMA system with that of the traditional TWR orthogonal multiple access (TWR-OMA) system with the same system setup, albeit the relay forwards the signal to the respective sources using two time slots in the second phase. It can be seen from the figure that the SOP performance of the TWR-NOMA system is better than that of the TWR-OMA system in the medium to high SNR regions. Such performance behavior can be explained by the fact that in a TWR-NOMA system the information leakage in the second phase is less since the relay broadcasts the combined signal in the same time slot, whereas in a TWR-OMA system, the information leakage is larger in the second phase because the relay forwards the signal to the respective sources in two different time slots. Therefore as compared to a TWR-NOMA system, for a TWR-OMA system the SINR at the eavesdropper increases with the SNR.

In Fig. 5, effect of the wiretap link on SOP performance is illustrated by plotting the SOP curves for different values of $\Omega_{1,E}$ when $\Omega_1 = 10$, $\Omega_2 = 5$, $\Omega_{2,E} = 1$, $\Omega_{R,E} = 1$, $R_s = 0.5$, $a_{1,R} = 0.8$, and $a_{R,1} = 0.6$. It is evident from the figure that when the quality of the wiretap link ($U_1 \rightarrow E$) increases, the SOP also increases. For instance, the SOP

\[^7\text{Note that the link variance can be represented as } \Omega = d^{-\nu}, \text{ where } d \text{ is the distance and } \nu \text{ is the path-loss exponent.}\]
increases as $\Omega_{1,E}$ increases from 2 to 5. Therefore, when the eavesdropper is closer to the legitimate user, the SOP performance degrades. Similar observation can also be made for the case when the quality of the eavesdropper link ($U_2 \rightarrow E$) increases.

Influence of the power allocation coefficient on the SOP performance is depicted in Fig. 6, where SOP curves for different values of $a_{1,R}$ are plotted when $\Omega_1 = 10$, $\Omega_2 = 5$, $\Omega_{1,E} = 5$, $\Omega_{2,E} = 1$, $R_s = 0.5$, and $a_{R,1} = 0.6$. It can be seen from the figure that as $a_{1,R}$ increases, the SOP decreases. This is due to the fact that large $a_{1,R}$ may result in large secrecy transmission rate, and hence better SOP performance is observed.

Finally, in Fig. 7, we compare the interception probabilities and SOP for different values of SNR when $a_{1,R} = 0.9$, $a_{R,1} = 0.6$, $\Omega_1 = 10$, $\Omega_2 = 5$, $\Omega_{1,E} = 2$, $\Omega_{2,E} = 1$, $R_s = 1$ bps/Hz under both the MRC and SC schemes at $E$. It can be seen from the figure that the analytical SOP and intercept probability results with MRC and SC schemes are in a perfect agreement with the simulation results. As can be seen from the figure, similar to SOP, the intercept probability decreases as SNR increases. However, at high SNR, performance error floor can be observed due to the information leakage.

V. CONCLUSION

In this paper, we have considered a TWR-NOMA system and studied its secrecy performance in the presence of an eavesdropper. Closed-form expressions of the SOP are derived for both cases of having MRC and SC schemes employed at the eavesdropper. The intercept probability is also investigated as a special case of the SOP. Moreover, the effective secrecy diversity order is analyzed to demonstrate that the eavesdropper severely degrades the secrecy performance, and even reduces the diversity order to zero. This means that the SOP reaches an error floor in the high SNR regime. The analytical findings were corroborated with Monte Carlo simulations. Effects of the main link and eavesdropper link on the SOP performance are also investigated. It is demonstrated that when any of the user is closer to the relay and/or when the eavesdropper is further away from the legitimate user, the SOP performance of the considered TWR-NOMA system improves. Performance comparison in terms of the SOP between the TWR-NOMA and conventional TWR-OMA systems is also presented and confirms the superiority of the TWR-NOMA system. It was also shown that the SOP performance is better when the SC scheme is employed at the eavesdropper instead of the MRC scheme. The research findings obtained can be useful to provide design guidelines for secure TWR-NOMA systems and its applications in IoT networks.

Given that this is the first work that has analyzed secrecy outage performance of a TWR-NOMA system, one direct step forward as a future direction for this line of research would be on the secrecy enhancement, especially using jamming and artificial noise schemes in the considered system. Furthermore, the effects of imperfect CSI and SIC deserve further studies, as well as the optimal power allocation scheme. Finally, given the expectation on scalability
of NOMA-based systems, extending our proposed system and analysis to the case of multiple users and/or multiple eavesdroppers is worthwhile.

APPENDIX A

PROOF OF THEOREM 1

With the MRC scheme employed at $E$, $F_{\psi_1}(y_{th})$ can be expressed as

$$F_{\psi_1}(y_{th}) = \frac{\min(\Lambda_{2,E}, \Lambda_{1,E})}{\Lambda_{2,E}} < y_{th}$$

$$= \int_0^\infty F_{\xi_1}(y_{th}(1 + y)) \left( -f_{AMC}(y) \right) dy.$$  \hspace{1cm} (35)

To proceed further, we first evaluate the CDF of $\xi_1$ as

$$F_{\xi_1}(z) = \frac{\min(\Lambda_{2,E}, \Lambda_{1,E})}{\Lambda_{2,E}} \times \Psi_{1}$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (36)

Differentiating (39) with respect to $\Lambda_{2,E}$, we obtain the CDF of $\Lambda_{2,E}$ as

$$F_{\Lambda_{2,E}}(z) = \frac{1}{\Lambda_{2,E}} \times \Psi_{1}$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (37)

where $\Lambda_{1,E} = \frac{a_{2,E} \Omega_1 + a_{2,R} \Omega_2}{a_{2,E} \Omega_1 + a_{2,R} \Omega_2 + a_{2,E} \Omega_2}$.

Next, to obtain $f_{\Lambda_{2,E}}(z)$ we first obtain $F_{\Lambda_{2,E}}(z)$ as

$$F_{\Lambda_{2,E}}(z) = \frac{\min(\Lambda_{2,E}, \Lambda_{1,E})}{\Lambda_{2,E}} \times \Psi_{1}$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (38)

Under Rayleigh fading channels, we can express $F_{\phi}(y) = 1 - \frac{1}{\psi_{1}} \times \Psi_{1}$ and $F_{\Lambda_{2,E}}(z) = \frac{1}{\Lambda_{2,E}} \times \Psi_{1}$. Substituting these into (36), and simplifying, we get the CDF of $\Lambda_{2,E}$ as

$$F_{\Lambda_{2,E}}(z) = \frac{1}{\Lambda_{2,E}} \times \Psi_{1}$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (39)

Then, by differentiating (39) with respect to $z$, we obtain

$$f_{\Lambda_{2,E}}(z) = \frac{\Lambda_{2,E}}{\Lambda_{2,E}} \times \Psi_{1}$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (40)

where $\Lambda_{2,E} = \frac{a_{2,E} \Omega_1 + a_{2,R} \Omega_2}{a_{2,E} \Omega_1 + a_{2,R} \Omega_2 + a_{2,E} \Omega_2}$.

Substituting the CDF of $\Lambda_{2,E}$ from (37) and the PDF of $\Lambda_{2,E}$ from (40) into (35), (36) can be computed as

$$F_{\psi_1}(y_{th}) = W_1 \int_{\frac{a_{2,R}}{\alpha_{2,E}}}^{\infty} \frac{1}{(1 + \beta(y))^2} dy$$

$$= \int_0^\infty F_{\xi_1}(y_{th}(1 + y)) \left( -f_{AMC}(y) \right) dy.$$  \hspace{1cm} (41)

where $W_1 = \frac{c_2}{(c_4 - c_3 a_{2,E}^2)^2}$, $W_2 = \frac{c_2 e^{-c_1(y_{th} - 1)^2} c_7 (c_4 - c_3 a_{2,E}^2)^2}{a_{2,R} c_{1}}$, $\beta_1 = \frac{c_5}{(c_4 - c_3 a_{2,E}^2)^2}$, and $\beta_2 = \frac{c_5}{c_{1}}$. The term $J_1$ can be obtained by carrying out the required integration with the help of [47, eq. (3.194.2)] and it is given as

$$J_1 = \left( \frac{a_{2,R}}{a_{2,E} \beta_2} \right) \frac{c_7}{c_{1}} e^{-c_{5} y_{th}} dy $$

Similarly, $J_2$ can be obtained by carrying out the required integration with the help of [47, eq. (3.535.3)] as

$$J_2 = \left( \frac{c_{5} y_{th}}{a_{2,E} \beta_2} \right) e^{-c_{5} y_{th}} dy$$

Finally, substituting (42) and (43) into (41), we obtain

$$F_{\psi_1}(y_{th}) = \frac{W_1(\psi_{1})}{(1 + \beta(y))^2} dy.$$  \hspace{1cm} (44)

We first evaluate the CDF of $\psi_2$ as

$$F_{\psi_2}(y_{th}) = \frac{W_2(\psi_{1})}{(1 + \beta(y))^2} dy.$$  \hspace{1cm} (45)

Under Rayleigh fading channels, we can express the CDFs of $\psi_{1}$ and $\psi_{2}$ as $F_{\psi_{1}}(y_{th}) = 1 - \frac{1}{\psi_{1} \times \Psi_{1}}$ and $F_{\psi_{2}}(y_{th}) = 1 - \frac{1}{\psi_{2} \times \Psi_{2}}$. By inserting these into (45), and simplifying, we get

$$F_{\psi_{1}}(y_{th}) = 1 - \left( \frac{a_{2,R} \Omega_1}{a_{2,E} \Omega_2 + a_{2,R} \Omega_1} \right) e^{-2 \psi_{1}}$$

where $\psi_{2} = \frac{a_{2,E} \Omega_1 + a_{2,R} \Omega_2}{a_{2,E} \Omega_1 + a_{2,R} \Omega_2 + a_{2,E} \Omega_2}$ and $\psi_{1} = \frac{a_{2,E} \Omega_1 + a_{2,R} \Omega_2}{a_{2,E} \Omega_1 + a_{2,R} \Omega_2 + a_{2,E} \Omega_2}$.

Moreover, by following the same approach as used to obtain (40), $f_{\psi_{1}}$ can be evaluated as

$$f_{\psi_{1}}(y_{th}) = W_3 \int_{\frac{a_{2,R}}{\alpha_{2,E}}}^{\infty} \left( 1 + \beta(y) \right)^2 dy$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (47)

where $W_3 = \frac{D_2}{(D_4 - D_3 a_{2,E})^2}$, $W_4 = D_2 a_{2,E} \Omega_1 e^{-2 \psi_{1}}$, $\alpha_1 = \frac{D_3}{(D_4 - D_3 a_{2,E})^2}$, $\alpha_2 = a_{2,E} \Omega_2 (y_{th} - 1) + a_{2,E} \Omega_1$, $\alpha_3 = a_{2,E} \Omega_2 y_{th}$, and $\alpha_5 = D_3 a_{2,E}$. The term $I_1$ can be obtained by carrying out the required integration with the help of [47, eq. (3.194.2)] as

$$I_1 = \left( \frac{a_{2,R}}{a_{2,E} \beta_2} \right) f_{1}(2; 1; 2; - \frac{a_{2,R}}{a_{2,E} \beta_2})$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (48)

where $W_3 = \frac{D_2}{(D_4 - D_3 a_{2,E})^2}$, $W_4 = D_2 a_{2,E} \Omega_1 e^{-2 \psi_{1}}$, $\alpha_1 = \frac{D_3}{(D_4 - D_3 a_{2,E})^2}$, $\alpha_2 = a_{2,E} \Omega_2 (y_{th} - 1) + a_{2,E} \Omega_1$, $\alpha_3 = a_{2,E} \Omega_2 y_{th}$, and $\alpha_5 = D_3 a_{2,E}$. The term $I_1$ can be obtained by carrying out the required integration with the help of [47, eq. (3.194.2)] as

$$I_1 = \left( \frac{a_{2,R}}{a_{2,E} \beta_2} \right) f_{1}(2; 1; 2; - \frac{a_{2,R}}{a_{2,E} \beta_2})$$

$$= \int_0^\infty F_{\phi}(y) \times f_{AMC}(y) dy.$$  \hspace{1cm} (49)
Moreover, $I_2$ can be obtained by performing the required integration with the help of the partial fraction and using [47, eqs. (3.352.2), (3.353.1)] as

$$I_2 = \frac{A_1}{\alpha_5} - \frac{e^{-\frac{D_1 y_{th} a_{d,1}}{\alpha_5}}}{\alpha_5} \frac{D_1 y_{th} a_{d,1}}{\alpha_5} - \frac{D_1 y_{th} a_{d,2}}{\alpha_5}$$

$$+ \frac{A_2}{(\alpha_3)^2} \left( e^{-\frac{D_1 y_{th} a_{d,1}}{\alpha_5}} \frac{D_1 y_{th} a_{d,1}}{\alpha_5} - \frac{D_1 y_{th} a_{d,2}}{\alpha_5} \right)$$

$$+ \frac{A_3}{\alpha_3} \left( e^{-\frac{D_1 y_{th} a_{d,2}}{\alpha_5}} \frac{D_1 y_{th} a_{d,2}}{\alpha_5} - \frac{D_1 y_{th} a_{d,1}}{\alpha_5} \right).$$

Finally, substituting $F^{(\text{MRC})}_{1}(\gamma_{th})$ from (41) and $F^{(\text{MRC})}_{2}(\gamma_{th})$ from (48) into (21), we obtain a final expression for the SOP (22) when the MRC scheme is employed at $E$.

**ACKNOWLEDGMENT**

The authors would like to thank the Editor and anonymous reviewers for their constructive comments, which helped improving the clarity of this article.

**REFERENCES**


MAHENDRA K. SHUKLA received the Ph.D. degree in electronics and communication engineering from the Indian Institute of Information Technology Allahabad, Prayagraj, India, in 2018. He is currently working as a Postdoctoral Fellow with the Communications Theories Research Group (CTRG), Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK, Canada. His research interests include cooperative relaying, physical layer security, non-orthogonal multiple access, energy harvesting, and signal processing. He is also a regular Reviewer of premier journals, including the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, the IEEE SYSTEMS JOURNAL, the IEEE COMMUNICATIONS LETTERS, and IET Communications.

HA H. NGUYEN (Senior Member, IEEE) received the B.Eng. degree from the Hanoi University of Technology (HUT), Hanoi, Vietnam, in 1995, the M.Eng. degree from the Asian Institute of Technology (AIT), Bangkok, Thailand, in 1997, and the Ph.D. degree from the University of Manitoba, Winnipeg, MB, Canada, in 2001, all in electrical engineering. He joined the Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK, Canada, in 2001, where he became a Full Professor, in 2007, and he is currently the NSERC/Cisco Industrial Research Chair of low-power wireless access for sensor networks. He has coauthored, with an editor Shwedyk, the textbook A First Course in Digital Communications (Cambridge University Press). His research interests include communication theory, wireless communications, and statistical signal processing. He is a Fellow of the Engineering Institute of Canada (EIC) and a Registered Member of the Association of Professional Engineers and Geoscientists of Saskatchewan (APEGS). He was the Co-Chair of the Multiple Antenna Systems and Space-Time Processing Track of IEEE Vehicular Technology Conferences (Fall 2010, Ottawa, ON, Canada, and Fall 2012, Quebec, QC, Canada), the Lead Co-Chair of the Wireless Access Track of IEEE Vehicular Technology Conferences (Fall 2014, Vancouver, BC, Canada), the Lead Co-Chair of the Multiple Antenna Systems and Cooperative Communications Track of the IEEE Vehicular Technology Conference (Fall 2016, Montreal, QC, Canada), and the Technical Program Co-Chair of the Canadian Workshop on Information Theory (St. John’s, NL, Canada, in 2015). He was an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS, from 2007 to 2011 and from 2011 to 2016, respectively. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

OM JEE PANDEY (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University, Lucknow, India, in 2008, the M.Tech. degree in digital communications from the ABV-Indian Institute of Information Technology and Management Gwalior, Gwalior, India, in 2013, and the Ph.D. degree from the Department of Electrical Engineering, IIT Kanpur, Kanpur, India, in 2019. From 2008 to 2011, he worked with Escorts Limited and FANUC India Private Limited. He was a Senior Lecturer with the Jaipur Engineering College and Research Center, Jaipur, from 2013 to 2014. He also worked as a Postdoctoral Fellow with the Communications Theories Research Group (CTRG), Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK, Canada, after completion of his Ph.D. program. He is currently working as an Assistant Professor with the Department of Electronics and Communication Engineering, SRM University AP, Amaravati. His research interest includes the signal processing for wireless networks with a specific focus on robust sensor node localization and tracking over wireless ad hoc networks. He also works on related areas such as low-latency data transmission, data aggregation, and distributed detection and estimation in wireless sensor networks. He also works as a Reviewer of various reputed journals of IEEE, including IEEE TVT, IEEE ACCESS, IEEE IoT, and IEEE TCOM.

* * *