Relay Selection for Improving Physical Layer Security in D2D Underlay Communications

MAJID H. KHOSHAFA1, (Member, IEEE), TELEX M. N. NGATCHED2, (Senior Member, IEEE), AND MOHAMED H. AHMED3, (Senior Member, IEEE)

1Department of Electrical and Computer Engineering, Queen’s University, Kingston, ON K7L 3N6, Canada
2Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John’s, NL A1B 3X5, Canada
3School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada

Corresponding author: Majid H. Khoshafa (mhk5@queensu.ca)

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada under its Discovery Grant (DG) Program under Grant RGPINs 2019-04626 and Grant 2021-03323.

ABSTRACT This paper investigates the physical layer security of inband underlay Device-to-Device (D2D) communication, where the direct link between D2D users is not available. In this respect, optimal relay and suboptimal relay selections are utilized to secure the D2D transmission. The eavesdropper uses either maximal-ratio combining or selection combining to increase the wiretapped signals. The D2D secrecy performance analysis is performed regarding the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity, and closed-form expressions are provided for both relay selection approaches and verified using Monte-Carlo simulation. From the numerical results, it is shown that increasing the number of D2D relays enhances the secrecy performance of D2D communications. Moreover, the exact asymptotic analysis of the SOP is provided. It turns out that the diversity order of both relay selection approaches is the same.

INDEX TERMS Physical layer security, D2D communications, secrecy outage probability, optimal and suboptimal relay selection, maximal-ratio combining, selection combining.

I. INTRODUCTION Mobile wireless communication has experienced rapid development in data traffic due to the dramatic growth of smart devices. According to Cisco, the average number of mobiles per capita will be 3.6 by 2023 [3]. Thus, spectrum scarcity is a crucial issue in wireless networks. Device-to-Device (D2D) communication, which allows nearby pairs to communicate directly rather than routing into a base station (BS), has received important consideration as a leading technology in future cellular communications to increase spectrum efficiency [4]. The benefits of D2D communications are high spectral efficiency, short delay, and low power consumption [5]. New mobile services for various proximity-based applications are offered via D2D communications such as content sharing, social networking, and multiplayer gaming. Based on the spectrum band exploitation, two approaches of D2D communications are presented; inband and out-band D2D communications. The D2D users are allowed to share the spectrum band with the cellular users in the former, whereas the unlicensed spectrum band is utilized by the D2D users in the latter [6]. The inband D2D communication can be further subdivided into two categories: overlay and underlay. Specifically, the spectrum band of the cellular network is divided into non-overlapping frequency sets in overlay D2D communications, where the cellular users utilize one set while the D2D users use the other one. Hence, in overlay D2D communications, interference management between cellular and D2D users is not required. In underlay D2D communications, however, the same frequency is utilized by the cellular and D2D users; therefore, interference management is crucial [7].

A. RELATED WORK Nowadays, wireless networks have been widely utilized in daily life applications to transmit essential and secure information. Consequently, security is considered a critical issue
for future fifth-generation (5G) and beyond wireless networks due to the broadcasting nature of the open wireless medium [8]. Traditionally, security depends on higher layers’ cryptographic encryption techniques and related protocols to guarantee information security. Nevertheless, with the development of mobile Internet, traditional cryptographic techniques may be inadequate or even inappropriate as an extra secure channel is needed for private key exchanges [9]. More importantly, due to novel improvements in the computational power of devices and optimization approaches for cracking encryption codes, new security strategies from information theory fundamentals, which focus on the propagation channel’s secrecy capacity, are essential to protect information from unauthorized devices [10].

Physical layer security (PLS), first explored by Wyner [11], is considered a novel strategy for improving wireless security by only exploiting the characteristics of wireless channels, e.g., noise, interference, and fading. Compared to traditional cryptography techniques, the benefits of applying PLS strategies for 5G and beyond wireless networks are twofold. First, PLS is independent of the computational complexity compared to cryptography in the higher layers [12]. Accordingly, even though eavesdroppers have highly powerful computational abilities, secure and reliable communications can be guaranteed. The second one is that PLS strategies have high scalability [13]. It is important to remark that PLS can be employed as a supplementary level of security on top of the current security approaches. Specifically, PLS can be integrated with the other security solutions to provide confidential and private communication data in 5G and beyond wireless networks [14], [15]. Many techniques, such as cooperative beamforming [16], artificial noise [17], and multi-antenna beamforming [18], have been investigated to degrade the quality of the wiretapped signals at the eavesdropper.

In PLS, the benefits of cooperative communications have been considerably investigated. More particularly, cooperative jamming (CJ) techniques have been extensively employed to enhance secrecy and decrease the amount of information that eavesdroppers can wiretap in wireless transmission [19], [20]. Even though jamming signals can be considered undesirable interference for legitimate users, they can be utilized to secure wireless communication transmissions. Several CJ strategies were comprehensively reported in [19] and the references therein. The authors in [20] proposed a secure full-duplex relaying protocol utilizing a friendly jammer to enhance the security level of the cellular network. Secure communications are significant in sixth-generation (6G) wireless networks. For instance, achieving secure communications using intelligent reflecting surfaces as a friendly jammer was investigated in [21], [22], and [23].

The importance of PLS techniques in relay networks lies in the fact that an intermediate relay node is more vulnerable to wiretapping than any other terminal. Signal relaying has also been considerably used to increase the quality of service in cellular networks. Relaying techniques provide many advantages, including extended coverage and a higher data rate. The benefits of cooperative relaying systems in the context of PLS have been widely investigated [24], [25], [26], [27], [28], [29]. In [24], the PLS was investigated for the cooperative non-orthogonal multiple access (NOMA) system, where power allocation approaches were proposed for the legitimate and jamming signals. The authors in [30] proposed two relay selection techniques, namely energy-aware relay selection and non-energy-aware relay selection, to reduce the overhearing by multiple eavesdroppers in cognitive radio transmission. The trade-off of security vs reliability was studied for wireless communications in [25], where an opportunistic relay selection approach was introduced to increase the secrecy capacity of the cellular network. In this regard, the relay selection of a cooperative scenario was analyzed in [26] to guarantee a secure transmission for the cellular network. Towards this end, the relay selection approach was proposed for guarding wireless transmissions against eavesdropping attacks. The authors in [27] studied the PLS of energy harvesting for cognitive radio networks using the cooperative relaying technique. In [28], the PLS of cooperative dual-hop NOMA for internet-of-things networks was investigated. The PLS of underlay multihop D2D relaying was investigated in [29].

The benefits of using D2D relays over direct D2D communications have been investigated in [31], [32], and [33] especially when there is a long distance between D2D users or poor link quality. As a result of sharing the same spectrum band, interference is a serious issue for both D2D and cellular users. Thus, interference management is necessary to mitigate the effects of interference [7]. However, the interference can be utilized to increase the secrecy level for cellular and D2D communications by confounding the eavesdropped signal [34], [35]. To maximize the wiretapped signal quality, the eavesdropper can utilize either maximum-ratio combining (MRC) or selection combining (SC) [36]. For the PLS in underlay D2D communications, many approaches can be used to increase the security level of D2D communications. More specifically, artificial noise and guard zone were used to guarantee a secure transmission for the D2D communications [37]. To secure D2D transmission, the BS was used as a friendly jammer to confuse the wiretapper by producing artificial noise [38]. Nevertheless, the quality of service of cellular users should be taken into consideration. In order to improve the PLS, spectrum partition and mode selection for D2D inband communications were investigated in [39]. The D2D relay guarantees a high-security cellular transmission by sending jamming signals toward an eavesdropper to compensate for sharing the spectrum. As a result, the benefits for cellular and D2D users are achieved, i.e., security enhancement for the former and high reliability and robustness for the latter [40].

B. MOTIVATION AND CONTRIBUTIONS

In this work, the PLS of the D2D communication is investigated. Unlike the existing work on the PLS of the cellular
networks, we investigate the PLS of the D2D relaying, where the D2D transmission is more likely to be eavesdropped due to the low resources at the D2D communications side. All works mentioned above study the case where direct links are available between D2D nodes. Nevertheless, in some practical scenarios, the channel conditions and distance may be unfavorable for direct D2D communication. In such conditions, the performance of the D2D communication can be enhanced by utilizing relay-aided transmission. Although the works mentioned above have presented some techniques to enhance the security of the direct inband underlay D2D communications from the PLS perspective, they only focus on enhancing the security of the cellular network. It is important to emphasize that due to the limited computational potential of the D2D user equipment, the transmissions of the D2D communications are weaker and susceptible to eavesdropping attacks. Therefore, the security improvement of D2D relaying is worthy of being investigated. To the best of our knowledge, no work has been reported in the open literature studying the PLS of relay-aided underlay D2D communication. Driven by this observation, in this paper, the secrecy capacity of the D2D relaying is investigated, where the D2D pair utilize DF relays to overcome the far distance and increase the quality of the D2D links. Taking into account the interference produced by the BS, the impact of the D2D relaying on the D2D security is evaluated. Two combining techniques at the eavesdropper are investigated. The main contributions of this paper are listed as follows:

- The D2D secrecy outage probability (SOP), the D2D probability of non-zero secrecy capacity (PNSC), and the cellular outage probability are investigated. In this regard, exact closed-form expressions are derived for the SOP, PNSC, and cellular outage probability. With this in mind, for maximizing the secrecy capacity of D2D communications, two relay selection schemes are utilized, namely, optimal relay selection (ORS) and suboptimal relay selection (SRS).
- The effect of D2D relays on the D2D secrecy performance is evaluated. More specifically, two practical combining approaches, MRC and SC, are examined on the eavesdropper side. Furthermore, an antenna selection at the BS is proposed to improve the reliability of the cellular network.
- Accurate expressions for the asymptotic SOP for the D2D communications are derived in the high-SNR regime. The upshot is that the secrecy diversity order is the same for both combining techniques as well as for relay selection schemes.
- Monte-Carlo simulations are utilized to verify and confirm the provided analytical expressions.

The remaining part of the paper is organized as follows. In Section II, the system model is described. The outage probability of the cellular network is analyzed in Section III. Section IV analyzes the SOP of D2D communications with respect to two different relay selection schemes, namely, OSR and SRS. Section V investigates the PNSC of D2D communications. The main results are discussed in Section VI. Finally, Section VII concludes the paper by outlining the significant contributions and results of this work.

II. SYSTEM MODEL

We consider a downlink transmission scenario in D2D relay communication as illustrated in Fig. 1, where the cellular network shares its spectral band with the D2D network in a particular environment. The D2D network consists of a D2D transmitter, $T$, $N_B$ decode-and-forward (DF) D2D relays ($R_k | k = 1, \ldots, N_R$), a D2D receiver, $D$, each equipped with a single antenna, and a multi-antenna eavesdropper, $E$, equipped with $N_E$ antennas. We consider a cellular network consisting of a BS, equipped with multiple antennas $N_B$, communicating with a single antenna cellular user, $C$. It is worth mentioning that, as a result of severe shadowing, the direct link between the D2D pair is unavailable in the proposed scenario. Thus, communication from $T$ to $D$ can only be set through the relays. Thus, the D2D transmissions require two phases. The received signals from $T$ are fully decoded in the first phase by the D2D relays. In the second phase, based on the highest secrecy capacity, the best D2D relay is selected from the set of the D2D relays to forward the decoded signal to $D$. During this phase, $E$ may wiretap the transmission of $R_k$. The BS transmits in both phases. Furthermore, we assume that all communication channels experience flat fading with a Rayleigh distribution.

The channel coefficients for the $T \rightarrow R_k$, $T \rightarrow C$, $BS \rightarrow C$, $BS \rightarrow E$, $R_k \rightarrow E$, $BS \rightarrow R_k$, $BS \rightarrow D$, and $R_k \rightarrow D$ links are denoted as $h_{trk}$, $h_{tc}$, $h_{bc}$, $h_{be}$, $h_{brk}$, $h_{brd}$, $h_{bd}$, and $h_{rd}$, respectively. In addition, the channel power gains are indicated by $|h_{ab}|^2$, which are independent and exponentially distributed random variables with a mean of $\lambda_{ab}$, where $ab \in \{trk, tc, bc, be, rxe, brk, bd, rd\}$. Additionally, the Euclidean distance is denoted as $d_{ab}$. Also, the variances of the additive white Gaussian noise (AWGN) at $R_k$, $D$, $C$, and $E$ are denoted by $\sigma_{r_k}^2$, $\sigma_{d}^2$, $\sigma_{c}^2$, and $\sigma_{e}^2$, respectively.
We assume that the D2D nodes, \( T \) and \( R_k \), transmit with equal power \( P \). In the first phase, the received signal at \( R_k \) is given by
\[
y_{R_k} = \sqrt{P} \left( \frac{d_{rk}}{d_o} \right)^{-\frac{\gamma}{2}} h_{rk} x_d + \sqrt{P_b} \left( \frac{d_{brk}}{d_o} \right)^{-\frac{\gamma}{2}} h_{brk} x_b + n_{r_k},
\]
where \( d_o \) is a reference distance, \( \eta \) denotes the path loss exponent, \( P \) and \( P_b \) are the D2D and BS transmitted power, respectively, \( x_d \) and \( x_b \) are the BS and D2D signals, respectively, with \( \mathbb{E} \left( |x_d|^2 \right) = \mathbb{E} \left( |x_b|^2 \right) = 1 \), where \( \mathbb{E} (\cdot) \) is the expectation operator, and \( n_{r_k} \) is the AWGN at \( R_k \). In the second phase, a D2D relay, \( R_k \), is chosen to maximize the secrecy capacity of the D2D link. The received signal at \( D \) is given by
\[
y_{D} = \sqrt{P} \left( \frac{d_{rd}}{d_o} \right)^{-\frac{\gamma}{2}} h_{rd} x_d + \sqrt{P_b} \left( \frac{d_{bd}}{d_o} \right)^{-\frac{\gamma}{2}} h_{bd} x_b + n_d,
\]
where \( n_d \) is the AWGN at \( R_k \). The received signal at \( C \), in the second phase, can be expressed as
\[
y_C = \sqrt{P_b} \left( \frac{d_{bc}}{d_o} \right)^{-\frac{\gamma}{2}} h_{bc} x_b + \sqrt{P} \left( \frac{d_{rc}}{d_o} \right)^{-\frac{\gamma}{2}} h_{rc} x_d + n_c,
\]
where \( n_c \) is the AWGN at \( C \). The eavesdropped signal, in the second phase, can be expressed as
\[
y_E = \sqrt{P} \left( \frac{d_{re}}{d_o} \right)^{-\frac{\gamma}{2}} h_{re} x_d + \sqrt{P} \left( \frac{d_{be}}{d_o} \right)^{-\frac{\gamma}{2}} h_{be} x_b + n_e,
\]
where \( n_e \) is the AWGN at \( E \). It is worth mentioning that, due to the powerful resources that are available at the BS where advanced security techniques such as beamforming can be implemented to secure the cellular transmission, we assume in this work that the cellular user is unlikely to be wiretapped. However, D2D transmission is more likely to be eavesdropped as a result of the low resources at the D2D communications side. Consequently, we only investigate the PLS of D2D communications. The instantaneous signal-to-interference-and-noise ratio (SINR) at \( R_k \), in the first phase, is given by
\[
y_{TR_k} = \frac{P \left( \frac{d_{rk}}{d_o} \right)^{-\eta} |h_{rk}|^2}{\sigma^2 + P_b \left( \frac{d_{brk}}{d_o} \right)^{-\eta} |h_{brk}|^2} = \frac{y_{rk}}{1 + \gamma_{brk}},
\]
where
\[
y_{rk} = \bar{y}_{rk} \left( \frac{d_{rk}}{d_o} \right)^{-\eta} |h_{rk}|^2 \quad \text{and} \quad \gamma_{brk} = \bar{y}_{brk} \left( \frac{d_{brk}}{d_o} \right)^{-\eta} |h_{brk}|^2,
\]
The channel capacity of the \( T \rightarrow R_k \) link is given by
\[
C_{TR_k} = \frac{1}{2} \log_2 \left( 1 + y_{TR_k} \right).
\]
The SINR at \( D \), in the second phase, is given by
\[
y_{RD} = \frac{P \left( \frac{d_{rd}}{d_o} \right)^{-\eta} |h_{rd}|^2}{\sigma^2 + P_b \left( \frac{d_{bd}}{d_o} \right)^{-\eta} |h_{bd}|^2} = \frac{y_{rd}}{1 + \gamma_{bd}},
\]
where
\[
y_{rd} = \bar{y}_{rd} \left( \frac{d_{rd}}{d_o} \right)^{-\eta} |h_{rd}|^2 \quad \text{and} \quad \gamma_{bd} = \bar{y}_{bd} \left( \frac{d_{bd}}{d_o} \right)^{-\eta} |h_{bd}|^2.
\]
The SINR at \( C \), \( \gamma_C \), in the second phase, is given by
\[
y_C = \frac{P_b \left( \frac{d_{bc}}{d_o} \right)^{-\eta} |h_{bc}|^2}{\sigma^2 + P \left( \frac{d_{rc}}{d_o} \right)^{-\eta} |h_{rc}|^2} = \frac{y_{rc}}{1 + \gamma_{rc}},
\]
where \( h_{bc} \) represents the channel coefficients between the selected antenna at the BS and \( C \). \( \gamma_{rc} = \bar{y}_{rc} \left( \frac{d_{bc}}{d_o} \right)^{-\eta} |h_{bc}|^2 \), \( \gamma_{rc} = \bar{y}_{rc} \left( \frac{d_{bc}}{d_o} \right)^{-\eta} |h_{bc}|^2 \), and \( \gamma_{rc} = \bar{y}_{rc} \left( \frac{d_{bc}}{d_o} \right)^{-\eta} |h_{bc}|^2 \). Let us define \( \mu_1 = \bar{y}_{rc} \left( \frac{d_{bc}}{d_o} \right)^{-\eta} \gamma_{rc} \), and \( \mu_2 = \bar{y}_{rc} \left( \frac{d_{bc}}{d_o} \right)^{-\eta} \gamma_{rc} \). Moreover, the SINR at \( E \) is given by
\[
y_{RE} = \frac{P \left( \frac{d_{re}}{d_o} \right)^{-\eta} |h_{re}|^2}{\sigma^2 + P_b \left( \frac{d_{be}}{d_o} \right)^{-\eta} |h_{be}|^2} = \frac{y_{re}}{1 + \gamma_{be}},
\]
where
\[
y_{re} = \bar{y}_{re} \left( \frac{d_{re}}{d_o} \right)^{-\eta} |h_{re}|^2 \quad \text{and} \quad \gamma_{be} = \bar{y}_{be} \left( \frac{d_{be}}{d_o} \right)^{-\eta} |h_{be}|^2.
\]
Similarly, we define \( \omega_3 = \bar{y}_{re} \left( \frac{d_{re}}{d_o} \right)^{-\eta} \gamma_{re} \), and \( \omega_4 = \bar{y}_{be} \left( \frac{d_{be}}{d_o} \right)^{-\eta} \gamma_{be} \). At the \( E \) side, two combining techniques are utilized to maximize the SNR at \( E \), namely, MRC and SC.

### III. Cellular Outage Probability

The cellular outage probability, \( P_{out} \), is defined by
\[
P_{out} = \Pr \left( \gamma_{BC} \leq \theta_c \right) = F_{\gamma_{BC}}(\theta_c),
\]
where \( \gamma_{BC} \) is the instantaneous SNR at \( C \) and \( \theta_c = 2^{R_c} - 1 \), \( R_c \) being the data transmission rate. Antenna selection approach is employed at the BS to avoid the high hardware complexity while maintaining the diversity and reliability advantages from multiple antennas. More specifically, the importance of using the antenna selection approach lies in the fact that the power consumption and the complexity of signal processing overhead are low as compared with other techniques such as beamforming techniques. In this regards, the transmitting antenna at BS is selected for the best data transmission performance. Moreover, the maximum channel gain can be determined by using
\[
|h_{bc}|^2 = \max_{i=1,...,N_B} |h_{bc}|^2.
\]
The probability density function (PDF) of $|h_{bc}|^2$ is given by [41]

$$f_{|h_{bc}|^2}(\gamma) = \frac{N_B}{\kappa_{bc}} \exp\left(-\frac{\gamma}{\kappa_{bc}}\right) \left(1 - \exp\left(-\frac{\gamma}{\kappa_{bc}}\right)\right)^{N_B-1}. \quad (12)$$

To derive the PDF of $\gamma_{bc}$, we use [42]

$$f_{\gamma_{bc}}(\gamma) = \int_0^\infty (\gamma + 1)f_{\gamma_{bc}}(\gamma(\gamma + 1))f_{\gamma_s}(\gamma) d\gamma. \quad (13)$$

The PDF of $\gamma_{bc}$ can be expressed in terms of the binomial expansion as [43, eq. (1.111)]

$$f_{\gamma_{bc}}(\gamma) = \frac{N_B}{\mu_1} \sum_{i=0}^{N_B-1} (-1)^i \binom{N_B-1}{i} \exp\left(-\frac{\gamma(i+1)}{\mu_1}\right), \quad (14)$$

and $f_{\gamma_s}(\cdot)$ is given by

$$f_{\gamma_s}(\gamma) = \frac{1}{\mu_2} \exp\left(-\frac{\gamma}{\mu_2}\right). \quad (15)$$

By plugging (14) and (15) into (13), the PDF of $\gamma_{bc}$, after some algebraic manipulations, can be obtained as

$$f_{\gamma_{bc}}(\gamma) = \frac{N_B}{\mu_1 \mu_2} \sum_{i=0}^{N_B-1} (-1)^i \binom{N_B-1}{i} \exp\left(-\frac{\gamma(i+1)}{\mu_1}\right) \times \frac{1 + \frac{\gamma(i+1)}{\mu_1} + 1}{\left(1 + \frac{\gamma(i+1)}{\mu_1} + 1\right)^2}. \quad (16)$$

From (16), $F_{\gamma_{bc}}(\gamma)$ is easily obtained as

$$F_{\gamma_{bc}}(\gamma) = N_B \sum_{i=0}^{N_B-1} \frac{(-1)^i \binom{N_B-1}{i}}{(i+1)} \left[1 - \frac{\exp\left(-\frac{\gamma(i+1)}{\mu_1}\right)}{1 + \frac{\gamma(i+1)}{\mu_1}}\right]. \quad (17)$$

By substituting (17) in (10), $P_{out}$ can be obtained.

**IV. D2D SECRECY OUTAGE PROBABILITY**

To examine the D2D secrecy capacity, $C_S$, the SOP is investigated in this subsection. The SOP can be defined as the probability that the achievable secrecy rate is less than a predefined target secrecy rate, $R_s$, for the D2D transmission. Mathematically speaking, it can be expressed as [44]

$$\text{SOP} = \Pr(C_S \leq R_s). \quad (18)$$

**A. OPTIMAL RELAY SELECTION**

The ORS is achieved when the relay selection is based on the particular D2D relay having the highest secrecy capacity [45], [46]. The channel state information (CSI) is assumed to be known for the main and wiretap links. Practically, the CSI of the wiretapped link can be estimated by observing the transmissions of the eavesdropper [44], [47]. For the ORS, the criterion of the relay selection is given by [26]

$$\theta = \arg \max_{k \in N_R} \left[C_{R_kD} - C_{R_kE}\right]^{+}. \quad (19)$$

where the index $\theta$ signifies the selected relay, $R_\theta$, for the ORS, $C_{R_kD}$ and $C_{R_kE}$ are the channel capacities of the $R_k \to D$ and $R_k \to E$ links, respectively, and $[x]^+ = \max(x, 0)$. The channel capacities of the $R_k \to D$ and $R_k \to E$ links are given by

$$C_{R_kD} = \frac{1}{2} \log_2 \left(1 + \gamma_{R_kD}\right), \quad (20)$$

and

$$C_{R_kE} = \frac{1}{2} \log_2 \left(1 + \gamma_{R_kE}\right). \quad (21)$$

Mathematically speaking, the secrecy capacity, $C_S^{\text{ORS}}$, can be expressed as

$$C_S^{\text{ORS}} = \max_{k \in N_R} \left[C_{R_kD} - C_{R_kE}\right]^{+}. \quad (22)$$

Using (22), the SOP can be expressed as

$$\text{SOP}^{\text{ORS}} = \Pr(C_S^{\text{ORS}} \leq R_s) = \Pr\left(\max_{k \in N_R} \left[C_{R_kD} - C_{R_kE}\right]^{+} \leq \gamma_s\right) \leq \gamma_s \right) \leq \gamma_{s}\right). \quad (23)$$

where $u \in \{\text{MRC}, \text{SC}\}$ and $\gamma_s = 2^{2\gamma_s}$. The probability density function (PDF) of the $R_\theta \to D$ link, $F_{\gamma_{R_\theta D}}(\cdot)$, can be obtained as

$$F_{\gamma_{R_\theta D}}(\gamma) = 1 - \frac{\exp\left(-\frac{\gamma}{\alpha_1}\right)}{1 + \frac{\alpha_2}{\alpha_1} \gamma}. \quad (24)$$

1) **EAVESDROPPER CHANNEL WITH MRC**

In this approach, the received signals are coherently combined. Hence, the channel gain between the selected relay and $E$ can be obtained as

$$|h_{R_\theta E}|^2 = \sum_{m=1}^{N_E} |h_{R_mE}|^2. \quad (25)$$

**Lemma 1**: The expression $\mathcal{P}_k^{\text{MRC}}$ can be derived as in (26), as shown at the bottom of the next page, where $A_1 = \frac{d}{\alpha_1} + \frac{1}{\alpha_1}$, $A_2 = \frac{\alpha_3}{\alpha_2}$, $A_3 = \frac{\alpha_3}{\beta + \frac{\alpha_1}{\alpha_2}}$, $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function [43, eq. (8.350.2)], and $\mathcal{W}_{u, b}(\cdot)$ is the Whittaker function [43, eq. (9.220.4)].

**Proof**: See Appendix A. \hfill $\blacksquare$

Now, the $\text{SOP}^{\text{ORS}}_{\text{MRC}}$ can be obtained by plugging (26) into (23).
2) EAVESDROPPER CHANNEL WITH SC

In this approach, the signal with the highest instantaneous SNR is selected. Thus, the channel gain between the selected relay and $E$ can be obtained as

$$|h_{δE}|^2 = \max_{1 \leq m < N_E} |h_{δm}|^2.$$  \hspace{1cm} (27)

**Lemma 2:** The expression $P_k^{SC}$ can be derived as in (28), as shown at the bottom of the page, where $B_1 = \frac{(m+1)}{ω_3} \left(1 + \frac{ω_2}{ω_1}\right) - \frac{ω_β}{ω_1}$, $B_2 = \frac{m+1}{ω_3} + \frac{β}{ω_1}$, $B_3 = \frac{ω_1}{ω_1+1}$, $B_4 = \frac{(m+1)}{ω_3} \left(1 + \frac{ω_2}{ω_1}\right) - \left(1 + \frac{ω_1}{ω_2}\right)$, and $Ei(.)$ is the exponential integral function [43, eq. (8.21.1)].

**Proof:** See Appendix B. \hspace{1cm} Q.E.D.

Now, the SOP_{SC} can be obtained by plugging (28) into (23).

**B. SUBOPTIMAL RELAY SELECTION SCHEME**

In practice, the CSI of the eavesdropper is not available when it is passive. In this case, the relay selection is based on the best relay that maximizes the reliability of the D2D link in the second phase. That is, the relay selection is given by [26]

$$δ = \arg \max_{k \in N_E} C_{R_k D}.$$  \hspace{1cm} (29)

where the index $δ$ represents the selected relay, $R_δ$, for the SRS. Mathematically speaking, the secrecy capacity, $C_s$, can be expressed as

$$C_s^{SRS} = \left[ \max_{k \in N_E} C_{R_k D} - C_{RE} \right]^+ = \left[ \frac{1}{2} \log_2 (1 + γ_{SRS}) - \frac{1}{2} \log_2 (1 + γ_{R_k D}) \right]^+,$$  \hspace{1cm} (30)

where $γ_{SRS} = \max_{k \in N_E} γ_{R_k D}$. Using (30), the SOP_v can be expressed as

$$\text{SOP}_{v}^{SRS} = \Pr \left( C_s \leq R_δ \right) = \Pr \left( \left[ \max_{k \in N_E} C_{R_k D} - C_{RE} \right]^+ \leq R_δ \right).$$

Using (24), the PDF of the $R_δ \rightarrow D$ link, $F_{γ_{R_k D}}(.)$, can be obtained as

$$F_{γ_{R_k D}} (γ) = \frac{N_E - 1}{k} \left(1 + \frac{γ}{(k+1)ω_2}\right) \left(1 - \exp\left(-\frac{γ}{ω_2}\right)\right).$$  \hspace{1cm} (31)

1) EAVESDROPPER CHANNEL WITH MRC

In this subsection, the SOP_{MRC} will be derived for the SRS scheme. The SOP_{MRC} can be obtained by

$$\text{SOP}_{MRC} = \int_0^∞ F_{γ_{R_k D}} (βγ + α) f_{MRC}(γ) dγ.$$  \hspace{1cm} (32)

**Lemma 4:** The SOP_{MRC} can be derived as in (36), as shown at the bottom of the next page, where $Z_1 = \frac{(k+1)ω_2}{ω_1}$, $Z_2 = \frac{ω_1}{ω_2}$, $Z_3 = \frac{1}{β} \left(1 + \frac{ω_1}{ω_2}(k+1)\right)$, and $Z_4 = \frac{1}{β} \left(1 + \frac{ω_1}{ω_2}(k+1)\right)$.

**Proof:** See Appendix D. \hspace{1cm} Q.E.D.

2) EAVESDROPPER CHANNEL WITH SC

In this subsection, the SOP_{SC} is derived for the SRS scheme. The SOP_{SC} can be obtained by

$$\text{SOP}_{SC} = \int_0^∞ F_{γ_{R_k D}} (βγ + α) f_{SC}(γ) dγ.$$  \hspace{1cm} (33)

**Lemma 3:** The SOP_{SC} can be obtained as in (34), as shown at the bottom of the next page, where $E_1 = \frac{β(k+1)}{ω_1} + \frac{1}{ω_2}$, $E_2 = \frac{β}{ω_2}$, and $E_3 = \frac{1}{β} \left(1 + \frac{ω_1}{ω_2}(k+1)\right)$.

**Proof:** See Appendix C. \hspace{1cm} Q.E.D.
C. ASYMPTOTIC SECRECY OUTAGE ANALYSIS

Now, the SOP of the D2D communications at high SNR, i.e., when $\gamma_d \to \infty$, is investigated to gain more insight into the impact of the essential parameters of the system model. We consider a scenario where $D$ is much closer to the D2D relay than the eavesdropper, which can be mathematically described as $\omega_1 \gg \omega_3$. As $\omega_1 \to \infty$, the asymptotic expression of the SOP can be expressed by [48]

$$\text{SOP}^\infty = (G_d \omega_1)^{-\gamma_d} + O(\omega_1^{-\gamma_d}),$$

(37)

where $G_d$ is the secrecy diversity order, $G_a$ is the secrecy array gain, and $O(\cdot)$ is the higher order terms. To elaborate, one can conclude that the curve of SOP$^\infty$ is defined by $G_d$, and the SNR improvement of SOP$^\infty$ related to the reference curve $\omega_1^{-\gamma_d}$ is described by $G_a$.

1) EAVESDROPPER CHANNEL WITH MRC IN THE ORS SCHEME

To derive the asymptotic SOP for MRC, SOP$^\infty_{\text{MRC,ORS}}$, we first expand the exponential function and the polynomial in (24) with the help of [43, eq. (1.112.2)] and [43, eq. (1.211.1)], respectively. Then, we neglect the higher order terms. Now, the SOP$^\infty_{\text{MRC,ORS}}$ can be obtained using

$$\text{SOP}^\infty_{\text{MRC,ORS}} = \left(G_{\text{ORS}} \omega_1\right)^{-G_{\text{MRC}} \omega_1} + O(\omega_1^{-G_{\text{MRC}} \omega_1}),$$

(38)

where $G_{\text{ORS}} = N_R$ and $G_{\text{MRC}}$ can be derived as

$$G_{\text{MRC}} = \prod_{k=1}^{N_R} \left(\omega_2 + 1\right) \left(\alpha + \frac{N_E \omega_3 \beta}{\omega_4 \exp\left(\frac{1}{2\omega_2}\right)} \sum_{m=0}^{N_E} \frac{N_E!}{m!} \left(\frac{1}{\omega_4}\right)^m \sum_{v=0}^{N_E} \left(\frac{N_E + s - 1}{\omega_4}\right) \exp\left(-\frac{1}{\omega_4}\right) \sum_{j=1}^{N_E} \frac{N_E - j}{(H_3 - H_2)^{m+2-j}}ight) \right].$$

(39)

2) EAVESDROPPER CHANNEL WITH SC IN THE ORS SCHEME

Similarly, the asymptotic SOP for SC, SOP$^\infty_{\text{SC,ORS}}$, can be derived following a similar procedure to that given above as

$$\text{SOP}^\infty_{\text{SC,ORS}} = \left(G_{\text{ORS}} \omega_1\right)^{-G_{\text{SC}} \omega_1} + O(\omega_1^{-G_{\text{SC}} \omega_1}),$$

(40)

where $G_{\text{ORS}} = N_R$ and $G_{\text{SC}}$ is given by

$$G_{\text{SC}} = \prod_{k=1}^{N_E} \left(\omega_2 + 1\right) \left(\alpha + \frac{N_E \omega_3 \beta}{\omega_4 \exp\left(\frac{1}{2\omega_2}\right)} \sum_{m=0}^{N_E} \frac{N_E!}{m!} \left(\frac{1}{\omega_4}\right)^m \sum_{v=0}^{N_E} \left(\frac{N_E + s - 1}{\omega_4}\right) \exp\left(-\frac{1}{\omega_4}\right) \sum_{j=1}^{N_E} \frac{N_E - j}{(H_3 - H_2)^{m+2-j}}ight) \right].$$

(41)

3) EAVESDROPPER CHANNEL WITH MRC IN THE SRS SCHEME

The asymptotic SOP for MRC, SOP$^\infty_{\text{MRC,SRS}}$, can be obtained with the help of [43, eq. (1.112.2)] and [43, eq. (1.211.1)], respectively, and neglecting the higher order terms. Now, the SOP$^\infty_{\text{MRC,SRS}}$ can be obtained using

$$\text{SOP}^\infty_{\text{MRC,SRS}} = \left(G_{\text{ORS}} \omega_1\right)^{-G_{\text{MRC}} \omega_1} + O(\omega_1^{-G_{\text{MRC}} \omega_1}),$$

(42)

where $G_{\text{ORS}} = N_R$ and $G_{\text{MRC}}$ can be derived as

$$G_{\text{MRC}} = \prod_{k=1}^{N_R} \left(\omega_2 + 1\right) \left(\alpha + \frac{N_E \omega_3 \beta}{\omega_4 \exp\left(\frac{1}{2\omega_2}\right)} \sum_{m=0}^{N_E} \frac{N_E!}{m!} \left(\frac{1}{\omega_4}\right)^m \sum_{v=0}^{N_E} \left(\frac{N_E + s - 1}{\omega_4}\right) \exp\left(-\frac{1}{\omega_4}\right) \sum_{j=1}^{N_E} \frac{N_E - j}{(H_3 - H_2)^{m+2-j}}ight) \right].$$

(43)

$$\text{SOP}_{\text{MRC}} = N_R \sum_{k=0}^{N_E-1} \frac{(-1)^k (N_E-1) \Gamma(\gamma_2 + \gamma_3) \omega_1 \exp\left(-\frac{(k+1) \omega_1}{\omega_2 \omega_4 \beta (k+1)}\right)}{\omega_2 \omega_4 \beta (k+1)} \sum_{j=1}^{N_E} \frac{N_E - j}{(H_1 H_3) \Gamma(\gamma_2 + \gamma_3) \omega_1 \exp\left(-\frac{(k+1) \omega_1}{\omega_2 \omega_4 \beta (k+1)}\right)}{\omega_2 \omega_4 \beta (k+1)}.$$
4) EAVESDROPPER CHANNEL WITH SC IN THE SRS SCHEME
The asymptotic SOP for SC, SOP$_{SC, SRS}^{\infty}$, can be obtained with the help of [43, eq. (1.112.2)] and [43, eq. (1.211.1)], respectively, and neglecting the higher order terms. Now, the SOP$_{SC, SRS}^{\infty}$ can be obtained using

$$\text{SOP}_{SC, SRS}^{\infty} = \left( g_{\text{dsc}}^{\text{SRS}}(\omega_1) - g_{\text{dsc}}^{\text{SC}}(\omega_1) + \mathcal{O}(\omega_1^{-\infty}) \right),$$

where $g_{\text{dsc}}^{\text{SRS}} = N_R$ and $g_{\text{dsc}}^{\text{SC}}$ can be derived as in (45), as shown at the bottom of the page.

V. PROBABILITY OF NON-ZERO SECRECY CAPACITY
Considering the PNSC, non-zero secrecy capacity is achieved if $\gamma_R D > \gamma_R E$ [44].

A. THE ORS SCHEME
From (23), the PNSC for the ORS, PNSC$_{\text{vORS}}$, is given by

$$\text{PNSC}_{\text{vORS}} = \text{Pr}(C_S > 0) = 1 - \text{Pr}(C_S \leq 0) = 1 - \text{Pr}\left(\max_{k \in N} [C_{R_k D} - C_{R_k E}]^+ \leq 0\right) = 1 - \prod_{k \in N} \text{Pr}\left(\frac{1 + \gamma_{R_k D}}{1 + \gamma_{R_k E}} \leq 1 \right).$$

(46)

Following the same steps in the derivation of (26) and (28), $D_k'$ can be derived as in (47) and (48), as shown at the bottom of the next page, for MRC and SC, respectively, where $A_4 = \frac{1}{\omega_1} + \frac{1}{\omega_2}$, $A_5 = \frac{\omega_1}{\omega_2}$, $B_5 = \frac{(m+1)}{\omega_1} \left(\frac{m+1}{\omega_3} - \frac{\omega_2}{\omega_1 \omega_3}\right)$, $B_6 = \frac{m+1}{\omega_2} + \frac{1}{\omega_2}$, and $B_7 = \frac{(m+1)}{\omega_3} - \left(1 + \frac{1}{\omega_2}\right) \frac{\omega_2}{\omega_1}$.

B. THE SRS SCHEME
From (31), the PNSC for the SRS, PNSC$_{\text{vSRS}}$, can be formulated as

$$\text{PNSC}_{\text{vSRS}} = \text{Pr}\left(\frac{1 + \gamma_{R SRS}}{1 + \gamma_{RE}} > 1\right) = 1 - \int_0^\infty F_{\gamma_{SRS}}(\gamma) f_{\gamma_{RE}}(\gamma) d\gamma.$$  

(49)

Following the same steps in the derivation of (34) and (36), the PNSC$_{\text{SRS}}$ can be derived as in (50) and (51), as shown at the bottom of the next page, for MRC and SC, respectively, where $H_4 = \frac{(k+1)}{\omega_1} + \frac{1}{\omega_3}$, $H_5 = \frac{\omega_1}{\omega_2(2k+1)}$, $Z_5 = \frac{(k+1)}{\omega_1} + \frac{(m+1)}{\omega_3}$, and $Z_6 = \frac{\omega_1}{\omega_2(2k+1)}$.

$$G_{\text{dsc}}^{\text{ORS}} = \left[\frac{N_E}{\omega_3} \sum_{p=0}^{N_R} \frac{N_R}{p} \omega_2^p \Gamma(p+1) \sum_{k=0}^{N_R-1} (-1)^k \binom{N_E - 1}{m} \sum_{s=0}^{N_R} \binom{N_R}{s} \alpha^{N_R-s} \beta^s \exp\left(-\frac{1}{2 \omega_4}\right) \right] \times \left(\frac{\omega_3}{k+1}\right)^s \Gamma(s+1) \left(\frac{1}{\omega_4}\right)^{\frac{s+2}{2}} W_{\frac{s-2}{2}} \left(\frac{1}{\omega_4}\right) + \left(\frac{1}{\omega_4}\right)^{\frac{s+1}{2}} \left(\frac{1}{\omega_4}\right) \right]^{\frac{1}{\omega_4}}.$$  

(45)
plotted, and a perfect agreement with the exact result is noted as \( \omega_1 \to \infty \). From the asymptotic curves, it is noteworthy that \( \mathcal{G}_d \) and \( \mathcal{G}_d \) can be accurately predicted. It is also observed that \( \mathcal{G}_d \) is not affected by \( N_E \). These asymptotic results reveal that the SOP under both ORS and SRS has the same \( \mathcal{G}_d \) for both combining techniques at \( E \). Furthermore, the theoretical results and the simulation results agree exactly, confirming the correctness of the derived expressions.

In Fig. 3, the SOPSC of the D2D communications, is illustrated for the ORS and SRS schemes. It can be seen that the SOPSC increases with decreasing \( N_R \), implying an improvement in the D2D secrecy performance. From Figs. 2 and 3, one can observe that the high-security level for D2D communications is obtained when \( E \) employs SC in comparison to the MRC approach. This is because the MRC gives a higher SNR gain at \( E \) as compared to the SC approach.

\[
D_k^{\text{MRC}} = 1 - \frac{\omega_2}{\omega_3} \frac{N_E}{\omega_4} \sum_{m=0}^{N_E-1} \frac{B_3}{m!} \left[ \Gamma(m+1) \omega_3^{m+1} \right] \left[ \sum_{i=1}^{m+1} (-1)^{m+1-i} \frac{A_4^{\frac{N_E-i}{2}}}{A_2^{\frac{N_E-i}{2}}} \right] \exp \left( -\frac{A_4^{\frac{N_E-i}{2}}}{A_2^{\frac{N_E-i}{2}}} \right) 
\]

\[
D_k^{\text{SC}} = 1 - \frac{N_E}{\omega_3 \omega_4} \sum_{m=0}^{N_E-1} (-1)^m \left( \frac{N_E-1}{m} \right) \left[ \frac{B_6 E_i[-B_6 B_3] + 1}{B_3} + \frac{B_7}{B_6} \right] \exp \left( \frac{B_6}{\omega_1 - \omega_2} \right) \left[ \frac{E_i[-B_6 B_3]}{B_6} \right] 
\]

\[
PNSC_{\text{MRC}}^{\text{SRS}} = 1 - N_R \sum_{k=0}^{N_R-1} \left( \frac{N_E}{k} \right) \frac{B_3}{(k+1)} \left[ 1 - \sum_{m=0}^{N_E-1} \frac{B_6 E_i[-B_6 B_3]}{B_3} + \frac{1}{B_3} \right] \frac{\frac{N_E}{m} \Gamma(m+1) \omega_1}{(H_5 - H_2)^{m+2-j}} \exp \left( \frac{H_5 - H_2}{H_5 - H_2} \right) 
\]

\[
PNSC_{\text{SC}}^{\text{SRS}} = 1 - N_R \sum_{k=0}^{N_R-1} \left( \frac{N_E}{k} \right) \frac{B_3}{(k+1)} \left[ 1 - \omega_1 \sum_{m=0}^{N_E-1} \frac{B_6 E_i[-B_6 B_3]}{B_3} + \frac{1}{B_3} \right] \frac{\frac{N_E}{m} \Gamma(m+1) \omega_1}{(H_5 - H_2)^{m+2-j}} \exp \left( \frac{H_5 - H_2}{H_5 - H_2} \right) 
\]
Figures 4 and 5 show the influence of $N_E$ on the SOP for both selections combining versus $\omega_1$ for the OSC and SRS schemes. In addition, the asymptotic curves for both combining approaches and relay selection schemes are also illustrated. In Fig. 4, the SOP for both ORS and SRS schemes decreases with decreasing $N_E$ because the eavesdropper capacity, $C_E$, decreases with decreasing $N_E$. In Fig. 5, there is also a decrease in the SOP for both ORS and SRS schemes with decreasing $N_E$. As $N_E$ does not influence the diversity order, the array gain is responsible for increasing the SOP. From the results above, it can be verified that the SOP for both combining approaches and relay selection schemes have the same secrecy diversity order $N_R$. Again, numerical results are also seen to agree with the simulated ones, confirming the accuracy of the analysis carried out.

Fig. 6 plots the analytical and simulation results for the cellular outage probability, $P_{out}$, versus $\mu_1$ for different values of $N_B$ at the BS. It can be observed that $P_{out}$ decreases monotonically as $\mu_1$ increases. Interestingly, the reliability enhances significantly with increasing $N_B$. Thus, the data transmission of cellular communication improves due to employing multiple antennas as the BS as compared to a single antenna. Furthermore, it can be seen that analytical results are also found to match the simulated ones, validating the correctness of our analysis. Fig. 7 presents $P_{out}$ versus $N_B$, where the influence of $N_B$ at the BS is evaluated. The reliability in the D2D communication improves with increasing $N_B$ and $\mu_1$ as expected.

Figures 8 and 9 plot the PNSC versus $\omega_1$ for both selections combining techniques and both relay selection schemes. From these figures, one can see that the PNSC improves as...
The probability of non-zero secrecy capacity, \( \text{PNSC}_\text{SC} \), vs. SNR, \( \omega_1 \), for different \( N_R \), where \( \omega_2 = \omega_4 = 10 \text{ dB}, N_E = 3 \), and \( \tau_s = 1 \text{ b/s/Hz} \).

\[ \omega_1 \text{ increases. Further, it is also remarkable that the PNSC decreases as } N_E \text{ decreases. Thus, for the MRC approach, the PNSC is lower than that of the SC approach because the MRC gives a higher SNR gain at } E. \text{ Finally, it is worth emphasizing that the ORS scheme always outperforms the SRS scheme. Numerical results are also found to match the simulated ones, verifying our analysis.} \]

**VII. CONCLUSION**

In this paper, the ORS and SRS schemes are utilized to enhance the inband underlay D2D secrecy performance. Two practical combining approaches, MRC and SC, are used to increase the eavesdropped signals. For both combining techniques as well as relay selection schemes, new closed-form expressions for the D2D SOP and PNSC are derived. Most noteworthy in the obtained results is the fact that the ORS scheme always outperforms the SRS scheme, assuming that the CSI of the wiretapped link is available. That is, the ORS guarantees the optimal secrecy performance for D2D communications. Additionally, the impact of D2D relays is investigated. It is observed, under these combining techniques, that increasing \( N_R \) enhances the D2D secrecy performance. The asymptotic results, which give a better understanding of the influence of the main system parameters on the SOP, are provided. As revealed in our analysis and confirmed through simulations, the diversity order is equal to \( N_R \) for both combining approaches and relay selection schemes. These results also show that \( N_E \) does not influence the diversity order. Moreover, we verified that, under both ORS and SRS schemes, increasing \( N_E \) degrades the secrecy performance of D2D communications.

**APPENDIX A**

**DERIVATION OF LEMMA 1**

The expression \( P_k^\nu \) can be obtained by

\[
P_k^\nu = \int_0^\infty F_{Y_{R_k}} (\beta \gamma + \alpha) f_{Y_{R_k}}^\nu (\gamma) \, d\gamma, \tag{52}
\]

where \( \beta = 2^{R_k} \) and \( \alpha = \beta - 1 \). The PDF of \( Y_{R_k} \) for MRC can be derived using \([42]\) as

\[
f_{Y_{R_k}}^\text{MRC} (\gamma) = \int_0^\infty (\xi + 1) f_{Y_{R_k}}^\text{MRC} (\gamma (\xi + 1)) f_{Y_{R_k}} (\xi) \, d\xi, \tag{53}
\]

where \( f_{Y_{R_k}}^\text{MRC} (\cdot) \) is given by

\[
f_{Y_{R_k}}^\text{MRC} (\gamma) = \frac{\gamma^{N_k-1}}{\Gamma(N_k)} \frac{e^{-\gamma}}{\omega_3^{N_k}} \exp \left( \frac{-\gamma}{\omega_3} \right), \tag{54}
\]

and \( f_{Y_{R_k}} (\cdot) \) is given by

\[
f_{Y_{R_k}} (\gamma) = \frac{1}{\omega_4} \exp \left( \frac{-\gamma}{\omega_4} \right). \tag{55}
\]

By plugging (54) and (55) into (53), \( f_{Y_{R_k}}^\text{MRC} (\gamma) \) is obtained as

\[
f_{Y_{R_k}}^\text{MRC} (\gamma) = \frac{\gamma^{N_k-1} \exp \left( -\frac{\omega_3}{\omega_4} \right) \sum_{m=0}^{N_k} \frac{N_k - 1}{m} \exp \left( -\frac{N_k - 1}{m} \right) \exp \left( -\frac{\gamma (m+1)}{\omega_3} \right)}{\Gamma(N_k) \omega_3^{N_k}}. \tag{56}
\]

By substituting (24) and (56) in (52), with the help of the partial fraction expansion, then using \([43], \text{eq. (1.111)}\), \([43], \text{eq. (3.383.4)}\), \([43], \text{eq. (3.383.10)}\), and \([43], \text{eq. (3.381.3)}\), \( P_k^\nu \) can be derived as in (26).

**APPENDIX B**

**DERIVATION OF LEMMA 2**

The PDF of \( Y_{R_k} \), \( f_{Y_{R_k}}^\nu (\gamma) \), can be derived using \([42]\) as

\[
f_{Y_{R_k}}^\nu (\gamma) = \int_0^\infty (\xi + 1) f_{Y_{R_k}}^\nu (\gamma (\xi + 1)) f_{Y_{R_k}} (\xi) \, d\xi, \tag{57}
\]

where \( f_{Y_{R_k}}^\nu (\cdot) \) is given by

\[
f_{Y_{R_k}}^\nu (\gamma) = \frac{N_E}{\omega_3} \sum_{m=0}^{N_k-1} (-1)^m \left( \frac{N_k - 1}{m} \right) \exp \left( -\frac{\gamma (m+1)}{\omega_3} \right). \tag{58}
\]

By plugging (58) and (55) into (57), \( f_{Y_{R_k}}^\nu (\gamma) \) is obtained as

\[
f_{Y_{R_k}}^\nu (\gamma) = \frac{N_E}{\omega_3} \sum_{m=0}^{N_k-1} (-1)^m \left( \frac{N_k - 1}{m} \right) \exp \left( -\frac{\omega_3}{\omega_4} \left( 1 + \frac{\gamma (m+1)}{\omega_3} + \frac{1}{\omega_4} \right) \right). \tag{59}
\]

By plugging (24) and (59) into (52), and with the help of the partial fraction expansion, then with the help of \([43], \text{eq. (3.353.3)}\), \([43], \text{eq. (3.352.4)}\), \( P_k^\nu \) can be obtained as in (28).
\[ \text{SOP}^{\text{SRS}}_{\text{MRC}} = N_R \sum_{k=0}^{N_k-1} \frac{(-1)^k (N_k-1)}{(k+1)} \left[ 1 - \sum_{m=0}^{N_E} \frac{(N_E) \Gamma(m+1) \omega_1 \exp \left(-\frac{(k+1)\alpha}{\omega_1}\right)}{\Gamma(N_E) \omega_3 \omega_4 \beta (k+1)} \right] \]

\[ \int_0^\infty \frac{y^{N_E-1} \exp \left(-\frac{H_1}{H} + \gamma \} \right)}{(H_2 + \gamma)^{m+1} (H_3 + \gamma)^{\beta}} \, dy. \quad (60) \]

**APPENDIX C**

**DERIVATION OF LEMMA 3**

The SOP_{MRC} can be obtained by plugging (56) and (32) in (33), and after simple algebraic manipulations, it can be expressed as in (60), as shown at the top of the page, where 
\( H_1 = \frac{6(k+1)}{\alpha_3}, \quad H_2 = \frac{\alpha_1}{\omega_4}, \quad \text{and} \quad H_3 = \frac{1}{\beta} \left( \alpha + \frac{\alpha_1}{\omega_4(k+1)} \right). \)

In what follows, the integral in (60), \( I \), is evaluated. First, \( I \) can be rewritten in a more general form as
\[ I = \int_0^\infty \frac{y^{N_E-1}}{\exp \left(H_1 y \right) (H_2 + \gamma)^{s} (H_3 + \gamma)^{z}} \, dy. \quad (61) \]

where \( s \) and \( z \) are integers. The partial fraction expansion is utilized in (61) to obtain
\[ \Delta = \sum_{i=1}^{s} \frac{Q_i}{(H_2 + \gamma)^{i}} + \sum_{j=1}^{z} \frac{U_j}{(H_3 + \gamma)^{j}}, \quad (62) \]

where
\[ Q_i = \frac{(-1)^z}{(H_2 - H_3)^{s+z-i}} \left[ 1 - \xi_1 + \xi_1 \sum_{p_1=1}^{s+1-i} \ldots \sum_{p_1=1}^{1} \right], \]

where \( n = z - 1 \), and
\[ \xi_1 = \begin{cases} 0, & z = 1, \\ 1, & \text{elsewhere}, \end{cases} \]

and
\[ U_j = \frac{(-1)^z}{(H_2 - H_3)^{s+z-j}} \left[ 1 - \xi_2 + \xi_2 \sum_{p_1=1}^{c+1-j} \ldots \sum_{p_1=1}^{1} \right], \]

where \( q = s - 1 \), and
\[ \xi_2 = \begin{cases} 0, & s = 1, \\ 1, & \text{elsewhere}. \end{cases} \]

By plugging (62) into (61), we get
\[ I = \int_0^\infty \frac{y^{N_E-1}}{\exp \left(H_1 y \right) \left( \sum_{i=1}^{s} \frac{Q_i}{(H_2 + \gamma)^{i}} + \sum_{j=1}^{z} \frac{U_j}{(H_3 + \gamma)^{j}} \right)} \, dy. \quad (63) \]

From (61), we have \( s = m + 1 \) and \( z = 1 \). With the help of [43, eq. (3.383.4)], \( I \) can be obtained. Then, by plugging the result of \( I \) into (60), and after simple algebraic manipulations, SOP_{MRC} can be derived as in (34).

**VIII. DERIVATION OF LEMMA 4**

The SOP_{SC} can be obtained by substituting (59) and (32) in (34), and following a similar procedure in the derivation of Lemma 3. Then using [43, eq. (3.353.3)] and [43, eq. (3.352.4)], SOP_{SC} can be obtained as in (36).

**ACKNOWLEDGMENT**

An earlier version of this paper (optimal relay selection scheme analysis) was presented in part at the IEEE Vehicular Technology Conference (VTC2020-Fall) [1]. This work is a part of a Ph.D. thesis [2].

**REFERENCES**

[1] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “Secure transmission in underlay D2D communications using optimal relay selection,” in Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall), Victoria, BC, Canada, Nov. 2020, pp. 1–6.

[2] M. H. Khoshafa, “Physical layer security in 5G and beyond wireless networks enabling technologies,” Ph.D. dissertation, Memorial University of Newfoundland, St. John’s, NL, Canada, Feb. 2022.

[10] D. Wang, B. Bai, W. Zhao, and Z. Han, “A survey of optimization approaches for wireless physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Commun. Mag., vol. 84, no. 3, pp. 102–1053, 2nd Quart., 2016.

[11] D. Wang, B. Bai, W. Zhao, and Z. Han, “A survey of optimization approaches for wireless physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 1801–1819, Apr. 2014.

[13] J. Liu, N. Kato, J. Ma, and N. Kadowaki, “Device-to-device communication in LTE-advanced networks: A survey,” IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 1923–1940, Dec. 2015.

[14] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “Resource management for device-to-device communication: A physical layer security perspective,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 946–960, Apr. 2018.

[15] A. Asadi, Q. Wang, and V. Mancuso, “A survey on device-to-device communication in cellular networks,” IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1801–1819, Apr. 2014.

[16] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, “A survey of device-to-device communications: Research issues and challenges,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[17] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, “A survey on multiple-antenna techniques for physical layer security,” IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.

[18] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.

[19] D. Wang, B. Bai, W. Zhao, and Z. Han, “A survey of optimization approaches for wireless physical layer security,” IEEE Commun. Mag., vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[20] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[21] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550–1573, 2nd Quart., 2014.

[22] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[23] A. U. Makrifi, K. M. Rabie, O. Kawaiyarta, K. Adhikari, G. Naurzybayev, X. Li, and R. Kharel, “Toward physical-layer security for Internet of Vehicles: Interference-aware modeling,” IEEE Internet Things J., vol. 8, no. 1, pp. 443–457, Jan. 2021.
X. Jiang, P. Li, B. Li, Y. Zou, and R. Wang, “Intelligent jamming strategies for secure spectrum sharing systems,” IEEE Trans. Commun., vol. 70, no. 2, pp. 1153–1167, Feb. 2022.

C. Jeong, I.-M. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system,” IEEE Trans. Signal Process., vol. 60, no. 1, pp. 310–325, Jan. 2011.

H.-M. Wang, C. Wang, and D. W. K. Ng, “Artificial noise assisted secure transmission under training and feedback,” IEEE Trans. Signal Process., vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” IEEE Trans. Signal Process., vol. 59, no. 1, pp. 351–361, Jan. 2011.

F. Jahanel, S. Wyne, G. Kaddoum, and T. Q. Duong, “A comprehensive survey on cooperative relaying and jamming strategies for physical layer security,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.

M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, “Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications,” IEEE Access, vol. 8, pp. 53575–53586, 2020.

M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications,” IEEE Commun. Lett., vol. 25, no. 5, pp. 1443–1447, May 2021.

M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. R. Ndjiongue, “Active reconfigurable intelligent surfaces-aided wireless communication system,” IEEE Commun. Lett., vol. 25, no. 11, pp. 3699–3703, Nov. 2021.

A. U. Makarfi, K. M. Rabie, O. Kawaiyana, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Khare, “Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective,” 2020, arXiv:2004.11288.

Y. Cao, S. Wang, M. Jin, N. Zhao, C. Xing, Y. Chen, and Z. Ding, “Power optimization for enhancing secrecy of cooperative user relaying NOMA networks,” IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 8008–8012, Jul. 2020.

Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” IEEE Trans. Veh. Technol., vol. 63, no. 6, pp. 2653–2661, Nov. 2013.

J. Zhu, Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems,” IEEE Trans. Veh. Technol., vol. 65, no. 7, pp. 5825–5831, Jul. 2015.

M. H. Khoshafa, J. M. Moualeu, T. M. N. Ngatched, and M. H. Ahmed, “On the performance of secure underlay cognitive radio networks with energy harvesting and dual-antenna selection,” IEEE Commun. Lett., vol. 25, no. 6, pp. 1815–1819, Jun. 2021.

X. Li, M. Zhao, X.-C. Gao, L. Li, D.-T. Do, K. M. Rabie, and R. Khare, “Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance,” IEEE Trans. Veh. Technol., vol. 66, no. 9, pp. 8303–8314, Sep. 2017.

M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay multihop Device-to-Device relaying,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2019, pp. 1–6.

P. Yan, Y. Zou, X. Ding, and J. Zhu, “Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems,” IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5115–5128, May 2020.

R. Ma, N. Xia, H.-H. Chen, C.-Y. Chiu, and C.-S. Yang, “Mode selection, radio resource allocation, and power coordination in D2D communications,” IEEE Wireless Commun., vol. 24, no. 3, pp. 112–121, Feb. 2017.

R. Ma, Y.-J. Chang, H.-H. Chen, and C.-Y. Chiu, “On relay selection schemes for relay-assisted D2D communications in LTE-A systems,” IEEE Veh. Technol. Lett., vol. 66, no. 9, pp. 8303–8314, Sep. 2017.

M. Hasan, E. Hossain, and D. I. Kim, “Resource allocation under channel uncertainties for relay-aided device-to-device communication underlaying LTE-A cellular networks,” IEEE Wireless Commun., vol. 13, no. 4, pp. 2322–2338, Apr. 2014.

W. Wang, K. C. Teh, and K. H. Li, “Enhanced physical layer security in D2D spectrum sharing networks,” IEEE Wireless Commun. Lett., vol. 6, no. 1, pp. 106–109, Dec. 2016.

M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, “Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI,” IEEE Wireless Commun. Lett., vol. 9, no. 8, pp. 1216–1220, Apr. 2020.

R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, “Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI,” IEEE Trans. Commun., vol. 66, no. 2, pp. 546–559, Feb. 2018.

M. A. Kishik and H. S. Dhillon, “Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks,” IEEE Wireless Commun. Lett., vol. 6, no. 3, pp. 394–397, Jun. 2017.

Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yener, “Secure wireless powered and cooperative jamming D2D communications,” IEEE Trans. Green Commun. Netw., vol. 2, no. 1, pp. 1–13, Mar. 2018.

Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, “Mode selection and spectrum partition for D2D inbound communications: A physical layer security perspective,” IEEE Trans. Commun., vol. 67, no. 1, pp. 623–638, Jan. 2019.

M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, “On the physical layer security of underlay relay-aided device-to-device communications,” IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

Z. Chen, J. Yuan, and B. Vucetic, “Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels,” IEEE Trans. Veh. Technol., vol. 54, no. 4, pp. 1312–1321, Jul. 2005.

A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes. New York, NY, USA: McGraw-Hill, 2002.

I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products. New York, NY, USA: Academic, 2014.

M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” IEEE Trans. Commun., vol. 63, no. 1, pp. 215–228, Dec. 2014.

H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, “Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels,” IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

Y. L. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” IEEE Netw., vol. 29, no. 1, pp. 42–48, Jan. 2015.

L. Wang, M. Elkhashlan, J. Huang, R. Schober, and R. K. Mallik, “Secure transmission with antenna selection in MIMO Nakagami-m fading channels,” IEEE Trans. Wireless Commun., vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
TELEX M. N. NGATCHED (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics from the University of Yaoundé, Cameroon, in 1992 and 1993, respectively, the M.Sc.Eng. degree (cum laude) in electronic engineering from the University of Natal, Durban, South Africa, in 2002, and the Ph.D. degree in electronic engineering from the University of KwaZulu-Natal, Durban, South Africa, in 2006. From July 2006 to December 2007, he was a Postdoctoral Fellow with the University of KwaZulu-Natal. From 2008 to 2012, he was a Research Associate with the Department of Electrical and Computer Engineering, University of Manitoba, Canada. He joined Memorial University, in August 2012, where he is currently an Associate Professor and a Co-ordinator of the Engineering One Program at Grenfell Campus. His research interests include 5G enabling technologies, visible light communications, power-line communications, optical communications, and underwater communications. He was a recipient of the Best Paper Award at the IEEE Wireless Communications and Networking Conference (WCNC) in 2019. He was a Technical Program Committee (TPC) Member and a Session Chair of many prominent IEEE conferences, including IEEE GLOBECOM, IEEE ICC, IEEE WCNC, IEEE VTC, and IEEE PIMRC. He was the Publication Chair of the IEEE CWIT 2015. He serves as the Managing Editor for the IEEE Communications Letters and as an Associate Editor for the IEEE Open Journal of the Communications Society. He was an Associate Editor of the IEEE Communications Letters from 2015 to 2019. He is a Professional Engineer (P.Eng.) registered with the Professional Engineers and Geoscientists of Newfoundland and Labrador, St. John’s, NL, Canada.

MOHAMED H. AHMED (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Carleton University, Ottawa, ON, Canada, in 2001. From 2001 to 2003, he worked as a Senior Research Associate with Carleton University. In 2003, he joined the Faculty of Engineering and Applied Science, Memorial University, where he worked as a Full Professor, until December 2019, and as an Adjunct Professor, since January 2020. He is currently an LTA Professor at the University of Ottawa. He has published more than 155 papers in international journals and conferences. His research interests include radio resource management in wireless networks, multi-hop relaying, cooperative communication, vehicular ad-hoc networks, cognitive radio networks, and wireless sensor networks. His research is sponsored by NSERC, CFI, QNRF, Bell/Aliant, and other governmental and industrial agencies. He won the Ontario Graduate Scholarship for Science and Technology in 1997, the Ontario Graduate Scholarship in 1998, 1999, and 2000, and the Communication and Information Technology Ontario (CITO) Graduate Award in 2000. He served as a Co-Chair for the Signal Processing Track in ISSPIT 2014, and served as a Co-Chair for the Transmission Technologies Track in VTC 2010-Fall and the Multimedia and Signal Processing Symposium in CCECE 2009. He served as an Editor for IEEE Communications Surveys and Tutorials, from 2007 to 2018, as a Guest Editor of a Special Issue on Fairness of Radio Resource Allocation, EURASIP JWCN, in 2009, and as a Guest Editor of a Special Issue on Radio Resource Management in Wireless Internet, Wireless Communications and Mobile Computing (Wiley) journal, in 2003. He is a Registered Professional Engineer (P.Eng.) in the province of NL, Canada.