Exploiting Secrecy Performance of Uplink NOMA in Cellular Networks

MINH-SANG VAN NGUYEN, DINH-THUAN DO (Senior Member, IEEE), FATEMEH AFGHAH (Senior Member, IEEE), S. M. RIAZUL ISLAM (Member, IEEE), AND ANH-TU LE (Senior Member, IEEE)

1Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City 700000, Vietnam
2Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan
3School of Informatics, Computing, and Cyber Systems, Northern Arizona University, Flagstaff, AZ 86011, USA
4Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
5Faculty of Information Technology, Van Lang University, Ho Chi Minh City 700000, Vietnam

Corresponding author: Anh-Tu Le (tule.iuh@gmail.com)

This work was supported in part by the Air Force Office of Scientific Research under Award FA9550-20-1-0090, and in part by the National Science Foundation under Grant CNS-2034218.

ABSTRACT We study the secrecy transmission of uplink non-orthogonal multiple access (NOMA) with single antenna and multi-antenna users in presence of an eavesdropper. Two phases are required for communications during each time frame between the users and the base station in cellular networks. We study the case where an eavesdropper overhears the relay and direct links from the users to the base stations. In terms of the secure performance analysis, we focus on two main metrics including secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC) with the assumption that the eavesdropper is able to detect the signals. Analytical closed-form expressions for the SOP and SPSC are derived to evaluate the system secure performance achieved by the proposed schemes. Furthermore, the asymptotic analysis is presented to gain further insights. The analytical and numerical results indicate that the proposed schemes can realize better secrecy performance once we improve the channel condition and signal-to-noise ratio (SNR) at the base station. Our results confirms that the secrecy performance gaps exist among the two users since different power allocation factors are assigned to these users.

INDEX TERMS Physical layer security, non-orthogonal multiple access, secrecy outage probability, strictly positive secrecy capacity.

I. INTRODUCTION

Due to superior spectral efficiency offeblack by NOMA, such promising multiple access technique is proposed for 5G networks [1]–[5]. Enabling superimposing multiple users in the power domain at the transmitter and requiring successive interference cancellation (SIC) at the receiver, differentiate NOMA from conventional orthogonal multiple access (OMA) technique was reported [6]. The multiple users can be served at the same time and frequency in the context of NOMA [7]. Based on the channel condition in NOMA system, the users are divided into different kinds of kinds such as the far users and the near users. However, the reliability of the far user depends on the existence of the near user [8]. In particular, to ensure user fairness the far user with poor channel condition is assigned with a higher power level compablack with the near user which has a good channel condition. It is beneficial in term of spectrum efficiency by employing multiple-input-multiple-output (MIMO) technologies in cooperative NOMA, as well as the interplay between cognitive radio and NOMA [8]. Especially, to achieve a balance between the performance of two users, cooperative NOMA techniques have been widely studied in recent work [9]–[16] along with various scenarios and system performance analysis. In cooperative NOMA schemes, the users located close to the base station (BS) can act as a relay to assist the far users. Particularly, the work in [10] explored a cooperative device-to-device (D2D) system with NOMA to allow the BS to simultaneously communicate with all users to satisfy the full information transmission.
requirement. They derived expressions in terms of the ergodic sum-rate (SR), outage probability and ergodic capacity. Meanwhile, the study in [12] indicated the remarkable outage performance gains of the scheme that combines the relay with the cooperative NOMA. The benefits of relay-assisted NOMA system can be reported if it is compared with the existing OMA schemes. In addition, the authors in [13] considered two modes of full-duplex (FD) and half-duplex (HD) to allow multiple relay nodes and a cell-center D2D device to support the transmission of a cell-edge D2D device. The authors calculated the closed-form expressions of the outage probabilities for both D2D users in different scenarios where the BS sends the signals to the far D2D user either through a near D2D user or multiple decode-and-forward (DF) relay nodes. In research of [14], the performance of a secondary network is determined in the system model which is enabled by a cognitive radio network with a NOMA scheme (namely CR-NOMA system) to serve many destination users. In particular, a D2D approach is implemented in the secondary network to further provide the signal transmission at a close distance of NOMA users in downlink. The performance of the NOMA users is studied under the interference received from the primary network.

The 5G and beyond wireless networks improve the performance of cellular users in term of security by introducing physical layer security (PLS) approaches [17]. Wyner in [18] first proposed PLS without exchanging secret keys where channel coding is regarded as the protection of information against eavesdropping signals. The PLS can benefit low-power devices (e.g. sensor networks) where traditional security methods do not work effectively. In fact, to enhance the overall system security, PLS techniques have been deployed in a wide range of RF applications to complement existing cryptography-based security approaches [19]. By leveraging features of the surrounding environments via sophisticated encoding schemes at the physical layer, the potential of PLS can be seen in recent work [20]. In [21], the authors explored secure downlink transmission in orthogonal frequency division multiplexing (OFDM)-assisted cognitive radio networks by allocating the power of the primary base station and cognitive base station (CBS) across different OFDM subcarriers in the presence of a multi-antenna eavesdropper. In [22], the authors studied a practical energy harvesting (EH) model by applying the secure transmit design for a downlink cognitive radio network using multiple-input-single-output (MISO). The authors in [23] considered a secure dual-hop mixed radio frequency-free space optical (RF-FO) downlink by conducting energy harvesting protocol. The authors examined the secrecy outage probability (SOP) in the scenario such that the FSO link and all RF links follow Gamma-Gamma, independent, and identical Nakagami-\(m\) fading. In [24], the authors focused on heterogeneous networks and point-to-point systems to exhibit a comprehensive review on various multiple-antenna techniques in PLS together with transmit beamforming designs for multiple antenna nodes.

A. RELATED WORK

In [25], the authors presented exact analytic expressions to indicate secure performance such as SOP, average secrecy capacity (ASC), and probability of SPSC along with their insightful asymptotic computations. In addition, a particular case of mixed fading channels (Nakagami-\(m\)/Nakagami-\(m\)) is studied corresponding to formulas of ASC, SOP and SPSC. In [26], a hybrid free-space optical/radio frequency (FSO/RF) communication system is examined in terms of the secrecy performance. Since the eavesdropper tries to overhear the RF link between the legitimate transmitter and receiver of the hybrid system, secure performance need be analysed. Reference [27] introduced the secrecy measurements by deriving closed-form mathematical formulas of secure metrics such as SOP, ASC and SPSC. Reference [28] derived the exact SOP and the probability of SPSC expressions for two transmit antenna selection (TAS) mechanisms.

Despite various advantages of NOMA, it should be strengthen secure information for users accessing to the BS. Due to the broadcast characteristics of radio communications, NOMA users make the confidential information vulnerable to eavesdropping users. To this end, security provisioning of NOMA-aided systems is of critical importance, that calls for the application of PLS techniques to NOMA transmission. Considering PLS in NOMA systems [29-33], the authors in [29] studied the impact of PLS on the performance of a unified non-orthogonal multiple access (NOMA) framework by evaluating both external and internal eavesdroppers. The stochastic geometry approach is deployed for spatial distributions of eavesdroppers and legitimate users. The authors in [4] considered the multiple-antenna system for further enhancing the security of a beamforming-aided system where artificial noise is generated at the base station. The authors proved new exact formulas of the security outage probability for both single-antenna and multiple-antenna cases to evaluate the secrecy performance. The work in [30] focused on the PLS for massive MIMO systems with internal eavesdroppers. A new concept called secrecy area has been defined when near user was eavesdropped by the far user. The authors in [31] examined the sum achievable secrecy rate in a cellular downlink MISO-NOMA system. They considered a secure beamforming and power allocation design to achieve to maximal secure performance metric. The authors in [33] proposed reliable and secure communications with two optimal relay section schemes. In particular, they derived exact formulas of SOP and SPSC.

However, there are still only few works considering uplink NOMA system, in which the BS is under security threat when it processes the signals from massive users. In addition, the work on uplink cooperative NOMA in the aforementioned studies usually assume that there are direct links between the BS and the uplink users. In practice, the uplink users cannot transmit signals directly to the BS for some typical circumstances of small cells networks. To the best of the authors’ knowledge, there are not much studies regarding the
uplink secure NOMA systems without direct links between the BS and the users, which motivates us to conduct this paper. However, in the scope of our study, we only consider particular circumstance in practice.

B. OUR CONTRIBUTIONS
NOMA is applicable in both uplink and downlink transmission systems since benefits of NOMA scheme are well proved. As discussed in aforementioned studies, most of the secure performance of NOMA networks are comprehensively analysed to raise performance gap among destinations. However, spectrum efficiency improvement in uplink is also crucial for 5G networks, which inspired this research. Further, motivated by the above observations [4], [29]–[33], we study in this paper a framework of a group of two NOMA users with respect to examine the security perspective of uplink NOMA transmissions in the presence of an eavesdropper. We further compare with similar studies to highlight our important contributions, shown in Table 1. In particular, the major contributions of this paper can be summarized as follows.

- This is one of few work considering the secure performance of uplink NOMA system with single antenna and multiple antennas at users when the direct and relay links from the user to the base station are enabled. In this regard, an eavesdropper is able to overhear information from both NOMA users.
- Corresponding to signal processing procedures at these phases, we compute the signal to interference plus noise ratio (SINR) to further achieve secure performance metrics, i.e. SOP and SPSC. The expressions of SOP and SPSC are derived in the closed-form. It can be found that the power allocation factors and the transmit SNR at the base station are main controlling coefficients that impact the secure performance as expected. We also consider a practical situation in which the relay cannot deploy SIC perfectly, the counterparts including the similar uplink NOMA with jammer selection and OMA schemes. To provide more insights, we obtain the approximate expressions of SOP to exhibit lower bounds of SOP for two users.
- By exploiting numerical simulations, our secure uplink NOMA schemes can guarantee the perfect security by adjusting the power allocation factors and limiting the impact of eavesdropper’s signal, thus making our schemes very attractive for secure uplink NOMA transmissions in the deployment of NOMA in practice.

The remaining parts of this paper are organized as follows. Section II introduces the framework of secure cooperative uplink NOMA scenario by exploiting a single antenna two-user model. Section III and Section IV present the corresponding closed-form expressions and analyze the secrecy performance of SOP and SPSC respectively. Section V presents multi-antenna user case along performance analysis. Section VI provides numerical simulations and discussions. The paper is finally concluded in Section VII.

![FIGURE 1. System model of secure uplink NOMA.](image)

II. SECURE UPLINK NOMA WITH SINGLE ANTENNA: SYSTEM MODEL
The system model for the NOMA system is depicted in Fig. 1. This system contains the base station (BS), two users $D_1$ and $D_2$ employing the principle of NOMA in the uplink. Since $D_2$ is located at far cell-edge area, it needs assistance of a relay ($R$) to communicate with the BS (denoted as BS), user $D_1$ sends its signal directly to the BS. In the security perspective, an eavesdropper is able to overhear signals from nearby users including $D_1$, $D_2$ and relay $R$. Two phases of signal processing are adopted. The relay is required to decode the signal before communicating toward the base station. The system further requires a synchronous procedure to enable the two users to send their signals to the base station simultaneously. The wireless channels in such NOMA are subjected to Rayleigh flat fading plus additive white Gaussian noise. It is noted that the main parameters are shown in Table 2.

A. PHASE 1
Considering uplink NOMA [40], [41], the destinations $D_1$ and $D_2$ are able to communicate in the same time to the BS. The corresponding signals for two users are $x_1$ and $x_2$ which are allocated power portion as $\alpha_1 P$ and $\alpha_2 P$, respectively. It is noted simple allocation scheme is adopted due to simplicity in implementation of NOMA in practice, i.e. $\alpha_i P$, $(i = 1, 2)$ are the power allocation coefficients satisfying $\alpha_1 + \alpha_2 = 1$.\(^1\) In the uplink manner, the transmit power levels at users are either a controlled transmit power or maximum power [40]. For many practical circumstance, the total transmit power requirement is crucial obeyed [41].

\(^1\)Normally, the fixed power allocation approach is adopted to analyse the secure performance of various models regarding NOMA. Therefore, for implementation of an uplink secure NOMA transmission and to reduce overhead, such power allocation as well as channel state information (CSI) are still meaningful to study a performance analysis as presented in this study. The dynamic power allocation scheme is beyond the scope of this paper.
TABLE 1. Comparison of the proposed scheme with similar ideas.

| | Our Scheme | [28] | [35] | [36] | [37] | [58] | [39] | [48] |
|---|---|---|---|---|---|---|---|---|
| NOMA | x | x | x | x | x | x | x | x |
| Uplink NOMA | x | x | x | x | x | x | x | x |
| The security of uplink NOMA | x | x | x | x | x | x | x | x |
| The uplink with assistance of a relay | x | x | x | x | x | x | x | x |
| Imperfect SIC | x | x | x | x | x | x | x | x |
| Interference from user to relay | x | x | x | x | x | x | x | x |
| Multiple antennas at user | x | x | x | x | x | x | x | x |
| Multiple users for uplink | x | x | x | x | x | x | x | x |
| SOP | x | x | x | x | x | x | x | x |
| Asymptotic of SOP | x | x | x | x | x | x | x | x |
| SPSC | x | x | x | x | x | x | x | x |

TABLE 2. Main notations.

| Symbol | Description |
|---|---|
| $\mathcal{F}()$ | Probability |
| $\mathcal{F}_Z()$ | The cumulative distribution function (CDF) of a random variable $Z$ |
| $f_Z()$ | The probability density function (PDF) of a random variable $Z$ |
| $\text{Bi}()$ | The exponential integral function |
| $P$ | The total transmit power |
| $\omega_i, (i = 1, 2, 3)$ | The level of residual interference due to imperfect SIC at $R$ from $D_i$, at BS from $D_1$ and at BS from $R$ with $(0 < \omega_i < 1)$, such that $\omega = \omega_1 = \omega_2 = \omega_3$ |
| $R_{D_1}$ | The target data rate for user $D_1$ |
| $\sigma_S$ | Additive white Gaussian noise (AWGN) noise variance at BS with $\sigma_S \sim \text{CN}(0, \varphi_2^2)$ |
| $\sigma_R$ | AWGN noise variance at $R$ with $\sigma_R \sim \text{CN}(0, \varphi_2^2)$ |
| $\sigma_E$ | AWGN noise variance at $E$ with $\sigma_E \sim \text{CN}(0, \varphi_E^2)$ |
| $\phi$ | The transmit SNR with $\phi = \frac{\mathcal{P}}{\sigma}$ |
| $h_{D1S}$ | The complex channel coefficient for the link $D_1 \rightarrow$ BS with $|h_{D1S}|^2 \sim \text{CN}(0, \lambda_1)$ |
| $h_{D1R}$ | The complex channel coefficient for the link $D_1 \rightarrow R$ with $|h_{D1R}|^2 \sim \text{CN}(0, \lambda_1)$ |
| $h_{D2R}$ | The complex channel coefficient for the link $D_2 \rightarrow R$ with $|h_{D2R}|^2 \sim \text{CN}(0, \lambda_2)$ |
| $h_{RS}$ | The complex channel coefficient for the link $R \rightarrow S$ with $|h_{RS}|^2 \sim \text{CN}(0, \lambda_R)$ |
| $h_{D1E}$ | The complex channel coefficient for the link $D_1 \rightarrow E$ with $|h_{D1E}|^2 \sim \text{CN}(0, \lambda_1)$ |
| $h_{D2E}$ | The complex channel coefficient for the link $D_2 \rightarrow E$ with $|h_{D2E}|^2 \sim \text{CN}(0, \lambda_2)$ |
| $h_{RE}$ | The complex channel coefficient for the link $R \rightarrow E$ with $|h_{RE}|^2 \sim \text{CN}(0, \lambda_R)$ |

In this model, the received signal at the BS from $D_1$ in the first phase is given by [42]

$$y_{D1-S}^{(p1)} = h_{D1S} \sqrt{\varphi_1} P x_1 + \sigma_S.$$ (1)

The signal to interference plus noise ratio (SINR) at the BS to receive signal from user $D_1$ is given by [42]

$$\gamma_{D1-S}^{(p1)} = \frac{\alpha_1 \varphi |h_{D1S}|^2}{\sigma_S}.$$ (2)

On the other hand, the relay is able to receive signals from both two users $D_i$ simultaneously under the assumption of perfect time synchronization between $D_1$ and $D_2$.

The relay can proceed signals in the first phase as [42]

$$y_{R}^{(p1)} = h_{D2R} \sqrt{\alpha_2} P x_2 + h_{D1R} \sqrt{\alpha_1} P x_1 + \sigma_R.$$ (3)

There are two possibilities to the relay to decode the symbol $x_2$ of $D_2$, i.e. namely $G_1$ and $G_2$ cases. It is worth noting that in the uplink NOMA, the decoding order gives higher priority for the user having better channel condition compared to the user having worse channel condition.

Case 1 ($G_1$): depending how strong two channels are. For the case $G_1$, condition on $h_{D1R} > h_{D2R}$, by treating the other user symbol (i.e. $x_2$) subject to the inferior link quality as noise, the relay $R$ first decodes the user symbol ($x_1$) subject to the better link quality [42]. It is noted that $G_1$-$D_1$ refers to user $D_1$ with condition $G_1$. In this context, we can calculate the SINR of $R$ as

$$\gamma_{R,1}^{(p1)} = \frac{\alpha_2 \varphi |h_{D2R}|^2}{\alpha_1 \varphi |h_{D1R}|^2 + 1}.$$ (4)

where $\tilde{h}_{D1R} \sim \text{CN}(0, \omega_1 \lambda_{p1})$. As a special case, $\omega_1 = 0$ denotes perfect SIC, whereas $\omega_1 = 1$ means that no SIC is performed at $R$.

Case 2: By contrast, $h_{D1R} < h_{D2R}$ corresponds to the condition $G_2$. In this circumstance, $R$ has higher priority to decode signal $x_2$ for the better link quality and signal $x_1$ is treated as the inferior link or noise [42]. In particular, we examine the SINR at the relay $R$ as

$$\gamma_{R,2}^{(p1)} = \frac{\alpha_2 \varphi |h_{D2R}|^2}{\alpha_1 \varphi |h_{D1R}|^2 + 1}.$$ (5)

The received signal at $E$ from $D_i$ ($i = 1, 2$) in the first phase is given by [43]

$$y_E^{(p)} = h_{D1E} \sqrt{\alpha_1} P x_1 + h_{D2E} \sqrt{\alpha_2} P x_2 + \sigma_E.$$ (6)

In this study, we suppose that the eavesdropper has a multi-user detection capability. In particular, a parallel interference cancellation (PIC) technique is employed at the eavesdropper to decode the superposed signal of $D_i$. Hence, the received SINR at eavesdropper to detect $D_i$’s message can be written as [43]

$$\gamma_{D_i-E}^{(p1)} = \frac{\alpha_i \varphi_E |h_{D_iE}|^2}{\sigma_E}.$$ (7)

where $\varphi_E = \frac{P}{\sigma_E}$.

We consider the secure scenario of the uplink NOMA in practical situation, such that a group of two users along with the existence an eavesdropper, in which the eavesdroppers are assumed to have enough detection capabilities to distinguish data stream processed in the same group [4], [5]. It is also assumed that the received signal from other group is too small that the data stream cannot be distinguished.
In second phase, as main role of the relay $R$, it re-transmits the decoded symbol $x_2$ with power $\beta_2 P$ while $D_1$ processes $\tilde{y}_2$. Note that $\beta_1 + \beta_2 = 1$, where $\beta_1$ are the power allocation factors. The received signal at BS in the second phase is given by

$$y_2^{(p2)} = h_{D1S} \sqrt{\beta_1 P_1} + h_{RS} \sqrt{\beta_2 P_2} + \sigma_s. \quad (8)$$

**Case 1:** In the case when $h_{D1R} > h_{RS}$, the BS treats signal $x_2$ as noise to first decode $y_1$. It is noted that SIC is required to decode $y_1$. We compute SINRs at the BS to decode signals $y_1, x_2$ respectively by [42]

$$y_1^{(p2)} = \frac{\beta_1 P h_{D1S}^2}{\beta_2 P h_{RS}^2 + 1}, \quad (9)$$
$$y_2^{(p2)} = \frac{\beta_2 P h_{RS}^2}{\beta_1 P h_{D1S}^2 + 1}. \quad (10)$$

where $\tilde{h}_{D1S} \sim \text{CN} (0, \omega_2 \lambda_{ip2})$.

**Case 2:** By considering the case such that $h_{D1R} < h_{RS}$, the BS treats $y_1$ as noise to decode $x_2$. Similarly, we can obtain SINRs at the BS corresponding to decode $x_2, y_1$ respectively as

$$y_2^{(p2)} = h_{D1E} \sqrt{\beta_1 P_1} + h_{RE} \sqrt{\beta_2 P_2} + \sigma_e. \quad (13)$$

After PIC, the received SINR at the eavesdropper to detect $D_1$’s message can be written as

$$y_{\bar{D}_1}^{(p2)} = \beta P h_{\bar{D}_1S}^2, \quad (14)$$

where $X = \{ \bar{D}_1E, \bar{D}_1E \}$.

The sum achievable secrecy rates of $D_1$ is written as [42]–[44]

$$C_{D1} = \frac{1}{2} \log_2 \left( 1 + \frac{y_{D1L}^{(p1)}}{y_{D1L}^{(p2)}} \right), \quad (16)$$

where $\beta_1 = \frac{1}{2} 1 + y_{D1L}^{(p2)} \bigg) \right], \quad (17)$

be further examined by using results in (4), (5), (7) and (10) as

$$C_{D1}^{(2)} = \frac{1}{2} \log_2 \left( 1 + \frac{y_{R1}^{(p1)}}{1 + y_{D2L}^{(p2)}} \right). \quad (18)$$

**III. ANALYSIS OF SOP**

To evaluate the security performance of the considered uplink system, we expect to compute expressions of SOP. However, before achieving SOP we need distributions of related channels. SOP is can be defined as the probability that the secrecy capacity is less than a given target rate.

It is noted that all channels follow the Rayleigh distribution with CDF and PDF can be expressed respectively by [42]

$$F_U(u) = 1 - \exp \left( -\frac{u}{\bar{V}} \right), \quad (19)$$

where $U \in \{ h_{D1S}, h_{D1R}, h_{D1E}, h_{D2R}, h_{RS}, h_{RS}, h_{D1E}, h_{D2E}, h_{RE} \}$ and $V \in \{ \lambda_{iS}, \omega_2 \lambda_{ip2}, \lambda_{iR}, \omega_1 \lambda_{ip1}, \lambda_{iR}, \lambda_{RS}, \omega_3 \lambda_{ip3}, \lambda_{iE}, \lambda_{iE}, \lambda_{RE} \}$.

**A. SOP OF $D_1$**

In uplink NOMA systems, we refer to the ability to decode $D_1$’s signal at the BS. The secure outage can be determined by considering possibility such that $C_{D1}^{(p1)}$ or $C_{D1}^{(p2)}$ falls below their own target rates. In particular, the SOP at the BS for decoding $D_1$’s signal is given by [43]

$$SOP_{D1} = \text{Pr} \left( C_{D1}^{(p1)} < R_{D1} \text{ or } C_{D1}^{(p2)} < R_{D1} \right) = 1 - \text{Pr} \left[ \frac{1 + y_{D1L}^{(p1)}}{1 + y_{D1L}^{(p2)}} \geq \mu_1, \frac{1 + y_{D1L}^{(p2)}}{1 + y_{D1L}^{(p1)}} < \mu_1 \right]. \quad (20)$$

**Proposition 1:** The closed-form expression of SOP for $D_1$ can be expressed by

$$SOP_{D1} = 1 + \frac{\phi \lambda_{iS}}{\mu_1 \phi \lambda_{iE} + \phi \lambda_{iS} + \mu_1 \phi P_2 \lambda_{iE} \lambda_{RS}} \times \exp \left( \lambda \theta - \beta \mu_1 \lambda_{iS} - \beta \phi \lambda_{iE} \right) \text{Ei} \left( -\lambda \theta \right), \quad (21)$$

where $\theta = \mu_1 \phi \lambda_{iE} + \phi \lambda_{iS}, \mu_i = \gamma^{2R_{Di}}, \bar{\mu} = \mu_i - 1, i \in 1, 2, \lambda = \frac{\lambda_{iS}}{\lambda_{iE}} + \frac{\lambda_{iS}}{\lambda_{RS}}$.

**Proof:** See Appendix A.

**B. SOP OF $D_2$**

By treating two conditions $G1$ and $G2$, we need to compute the SOP of $D_2$’s signal in the closed-form.
1) SOP OF $D_2$: CASE G1

From (16), the SOP of user $D_2$ can be expressed as

$$SOP^{(G1)}_{D_2} = \Pr \left[ C_{D_2}^{(G1)} < R_{D_2} \right]$$

$$= 1 - \Pr \left[ \min \left( \frac{1 + y_{R_1}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}}, \frac{1 + y_{R_2}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \right) \geq \mu_2 \right]$$

$$= 1 - \Pr \left[ \frac{1 + y_{R_1}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \geq \mu_2 \right] \Pr \left[ \frac{1 + y_{R_2}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \geq \mu_2 \right]. \quad (22)$$

**Proposition 2**: The closed-form expression of SOP for $D_2$ corresponding to case G1 can be expressed by

$$SOP^{(G1)}_{D_2} = 1 - \frac{\lambda_{2R}}{\mu_2 \alpha_1 \phi_E \alpha_1 \lambda_{ip1} \lambda_{2E} \mu_2 \beta_1 \phi_E \alpha_2 \lambda_{ip2} \lambda_{RE}} \times \exp \left( \psi_1 \delta_1 - \frac{\mu_2}{\lambda_{2R}} + \psi_2 \delta_2 - \frac{\mu_2}{\beta_2 \phi_L \lambda_{RS}} \right) \times \exp \left( -\psi_1 \delta_1 \right) \exp \left( -\psi_2 \delta_2 \right). \quad (23)$$

where $\psi_1 = \frac{\mu_2 \lambda_{ip2} + \lambda_{ip1}}{\mu_2 \alpha_1 \phi_L \lambda_{ip1} \lambda_{2E} \mu_2 \beta_1 \phi_L \alpha_2 \lambda_{ip2} \lambda_{RE}}$, $\psi_2 = \frac{\mu_2 \lambda_{ip2} + \lambda_{ip1}}{\mu_2 \beta_1 \phi_L \lambda_{ip1} \lambda_{2E} \mu_2 \alpha_1 \phi_L \alpha_2 \lambda_{ip2} \lambda_{RE}}$, $\delta_1 = \frac{\mu_2}{\lambda_{2R}} + \frac{1}{\alpha_1 \lambda_{ip1}}$, $\delta_2 = \frac{\mu_2}{\beta_2 \phi_L \lambda_{RS}} + \frac{1}{\alpha_2 \lambda_{ip2}}$.

**Proof**: See Appendix B.

2) SOP OF $D_2$: CASE G2

From (17), the SOP of $D_2$ can be expressed as

$$SOP^{(G2)}_{D_2} = \Pr \left[ C_{D_2}^{(G2)} < R_{D_2} \right]$$

$$= 1 - \Pr \left[ \min \left( \frac{1 + y_{R_1}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}}, \frac{1 + y_{R_2}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \right) \geq \mu_2 \right]$$

$$= 1 - \Pr \left[ \frac{1 + y_{R_1}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \geq \mu_2 \right] \Pr \left[ \frac{1 + y_{R_2}^{(p_1)}}{1 + y_{D_2E}^{(p_2)}} \geq \mu_2 \right]. \quad (24)$$

**Proposition 3**: The closed-form expression of SOP for $D_2$ corresponding to case G2 can be formulated by

$$SOP^{(G2)}_{D_2} = 1 - \frac{\lambda_{2R}}{\mu_2 \alpha_1 \phi_E \lambda_{1R} \lambda_{2E} \mu_2 \beta_1 \phi_E \alpha_2 \lambda_{ip2} \lambda_{RE}} \times \exp \left( \psi_1 \chi - \frac{\mu_2}{\lambda_{2R}} + \psi_2 \delta_2 - \frac{\mu_2}{\beta_2 \phi_L \lambda_{RS}} \right) \times \exp \left( -\psi_1 \chi \right) \exp \left( -\psi_2 \delta_2 \right). \quad (25)$$

where $\chi = \frac{\phi_E}{\phi_L}$.  

**Proof**: From (24), $C_1$ can be calculated as (26), where the CDF of $|h_{D2E}|^2$, the PDF of $|h_{D2E}|^2$ and $|h_{D1R}|^2$ base on (18) and (19), shown at the bottom of the next page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $C_1$ is written by

$$C_1 = -\frac{\lambda_{2R}}{\mu_2 \alpha_1 \phi_E \lambda_{1R} \lambda_{2E}} \exp \left( -\frac{\mu_2}{\beta_2 \phi_L \lambda_{RS}} \right) \times \exp (\psi_1 \chi) \exp (-\psi_1 \chi). \quad (27)$$

Substituting (27) into (24), (25) can be obtained.

The proof is completed.

To further analyse system performance, we can see that two conditions of successful decoding signal corresponding to the two phases lead to the variations of SOP performance. The target rates appear in expressions of SOP, for example (20), and therefore such target rates will limit improvement of secure performance. Although the ergodic secrecy rate is also important, but the SOP is at a higher priority to examine the secure performance of such kind of uplink NOMA.

**Remark 1**: Since expressions of SOP are so complicated, we examine the main factors affecting the SOP performance. For example, (25) contains the parameters $\phi$, $\phi_L$ and the channel gains, and hence the secure performance metrics depend mainly on these parameters. As a result, it can be concluded which parameters can be improved to obtain the best security behavior. The reason for the imbalance in the performance of two users is the power allocation factors which appear in coefficient $\chi$. Further, we should note that the SOP performance can be improved when $\phi$ increases.

C. ASYMPTOTIC OF SOP

When $\phi \to \infty$ and based on (A.1)-(A.3), the asymptotic SOP of $D_1$ is given by

$$SOP^{asymp}_{D_1} = 1 - \frac{1}{\lambda_{RS}} \int_0^\infty \exp \left( -\frac{1}{\psi_1 (\phi_L)} \right) dy = 1 - \frac{1}{\beta_1 \lambda_{1S}}. \quad (28)$$

Similarly, from (28), (B.1) and (B.3), when $\phi \to \infty$, the asymptotic SOP of $D_2$ for the case G1 is given by

$$SOP^{(G1,asym)}_{D_2} = 1 - \frac{1}{\alpha_1 \lambda_{ip1} \alpha_2 \lambda_{ip2}} \times \int_0^\infty \exp \left( -\frac{1}{\psi_2 \phi_L \lambda_{RS}} \right) \times \int_0^\infty \exp \left( -\frac{1}{\psi_2 \phi_L \lambda_{RS}} \right) dy = 1 - \frac{1}{\beta_2 \lambda_{RS}}. \quad (29)$$

Next, from (26) and (B.3), when $\phi \to \infty$, the asymptotic SOP of $D_2$ for the case G2 is computed by

$$SOP^{(G2,asym)}_{D_2} = 1 - \frac{1}{\lambda_{1R} \alpha_2 \lambda_{ip2}} \times \int_0^\infty \exp \left( -\frac{1}{\psi_2 \phi_L \lambda_{RS}} \right) \times \int_0^\infty \exp \left( -\frac{1}{\psi_2 \phi_L \lambda_{RS}} \right) dy = 1 - \frac{1}{\beta_2 \lambda_{RS}}. \quad (30)$$
Remark 2: In order to gain more insights, such system’s asymptotic behavior obtained in this section is necessary when the transmit SNR at destinations are sufficiently large. In particular, when $\phi \to \infty$, the expressions of asymptotic SOP in (28), (29), and (30) mainly depend on system parameters such as target rates, channel gains and power allocation factors. Therefore, we predict that such SOP is likely saturated at high region of $\phi$.

IV. SPSC ANALYSIS

A. SPSC OF $D_1$

Another main performance metric is SPSC, which is the fundamental benchmark for secrecy performance and denotes the probability of existence of the secrecy capacity [43]. Thus, the SPSC of $D_1$ is readily given by

$$
SPSC_{D1} = \Pr \left( C_{D1}^{(p1)} > 0, C_{D1}^{(p2)} > 0 \right) = \Pr \left( \gamma_{D1}^{(p1)} > \gamma_{D1}^{(p2)} \right) \Pr \left( \gamma_{D1}^{(p2)} > \gamma_{D1}^{(p2)} \right).
$$

\hspace{1.5cm} (31)

**Proposition 4:** The closed-form expression of SPSC for $D_1$ can be expressed by

$$
SPSC_{D1} = \frac{\phi \lambda_{1S}}{\phi E \lambda_{1E} + \phi \lambda_{1S} \beta_2 \phi E \lambda_{1E} \lambda_{RS}} \times \exp \left( \Phi_1 \right) Ei \left( -\Phi_1 \right).
$$

where $\Phi_1 = \frac{\phi E \lambda_{1E} + \phi \lambda_{1S} \beta_2 \phi E \lambda_{1E} \lambda_{RS}}{\phi E \lambda_{1E} + \phi \lambda_{1S} \beta_2 \phi E \lambda_{1E} \lambda_{RS}}$.

Proof: See Appendix C.

B. SPSC OF $D_2$

Case 1: The SPSC for $G_1 - D_2$ can be expressed as

$$
SPSC_{D2}^{(G1)} = \Pr \left[ C_{D2}^{(p1)} > 0 \right] = \Pr \left[ \gamma_{R,1}^{(p1)} > \gamma_{D2}^{(p1)} \right] \Pr \left[ \gamma_{D2}^{(p2)} > \gamma_{D2}^{(p2)} \right].
$$

\hspace{1.5cm} (33)

**Proposition 5:** The closed-form expression of SPSC for $G_1 - D_2$ can be expressed by

$$
SPSC_{D2}^{(G1)} = \frac{\lambda_{RS}}{\lambda_{RS}} \times \exp \left( \Phi_2 \right) Ei \left( -\Phi_2 \right),
$$

\hspace{1.5cm} (34)

where $\Phi_2 = \frac{\phi \lambda_{2E} + \phi \lambda_{2R} \beta_1 \phi \lambda_{2E} \lambda_{RS} \gamma_{D2}}{\phi \lambda_{2E} + \phi \lambda_{2R} \beta_1 \phi \lambda_{2E} \lambda_{RS} \gamma_{D2}}$.

Proof: See Appendix C.

Case 2: Similar to $G_1 - D_2$, the SPSC for $G_2 - D_2$ case can be expressed as

$$
SPSC_{D2}^{(G2)} = \Pr \left[ C_{D2}^{(p2)} > 0 \right] = \Pr \left[ \gamma_{R,2}^{(p1)} > \gamma_{D2}^{(p1)} \right] \Pr \left[ \gamma_{D2}^{(p2)} > \gamma_{D2}^{(p2)} \right].
$$

\hspace{1.5cm} (35)

**Proposition 6:** The closed-form expression of SPSC for $G_2 - D_2$ can be expressed by

$$
SPSC_{D2}^{(G2)} = \frac{\lambda_{RS}}{\lambda_{RS}} \times \exp \left( \Phi_3 \right) Ei \left( -\Phi_3 \right),
$$

\hspace{1.5cm} (36)

where $\Phi_3 = \frac{\phi \lambda_{2E} + \phi \lambda_{2R} \beta_1 \phi \lambda_{2E} \lambda_{RS} \gamma_{D2}}{\phi \lambda_{2E} + \phi \lambda_{2R} \beta_1 \phi \lambda_{2E} \lambda_{RS} \gamma_{D2}}$.

Proof: From (35), $\Phi_1$ can be calculated as (37), where the CDF of $|h_{D2R}|^2$, the PDF of $|h_{D2E}|^2$ and $|h_{D1R}|^2$ base on (18) and (19), shown at the bottom of the next page.

Substituting (37) into (35), (36) can be obtained and the proof is completed.

Remark 3: Similarly, since the same parameters lead to the enhancement of SOP, this section presents the expressions of SPSC performance which relate to the similar system parameters reported for SOP metric. For example, we examine the main factors affecting the SPSC performance in (36) which are $\phi$, $\phi_E$ and the related channel gains, and hence secure performance metrics depend mainly on these parameters. As a result, by controlling these values, an improvement in the SOP and SPSC indicators can be achieved.
V. EXTENSION TO MULTIPLE ANTENNAS AT USERS

In Fig. 2, two users may benefit by multi-antenna design. It is assumed that users $D_1, D_2$ are equipped with $N$ and $M$ antennas respectively [47]. For simplicity, the system treats its nodes in a half-duplex mode. The transmit antenna selection approach is adopted to reduce cost of multi-antenna users. Once the $n$-th antenna at user $D_1$ is selected, the channel for link $D_1$-BS is characterized by distribution $h_{D1S,n} \sim CN (0, \lambda_{1S,n})$ (with $n=1, \ldots, N$). Similarly, we characterize the channel for the link $D_2$ to $R$ ($m$-th antenna at user $D_2$ is decided to be transmitted) as $h_{D2R,m} \sim CN (0, \lambda_{2R,m})$ (with $m=1, \ldots, M$), for link $D_1$-$R$, the channel distribution is $h_{D1R,n} \sim CN (0, \lambda_{1R,n})$. For links associated with eavesdropper, links $D_1$-$E$, $D_2$ to $E$ (the $n$-th antenna is selected at user $D_1$, the $m$-th antenna at user $D_2$) experience $h_{D1E,n} \sim CN (0, \lambda_{1E,n})$, $h_{D2E,m} \sim CN (0, \lambda_{2E,m})$, respectively.

The SINR at the BS to receive signal from multi-antenna user $D_1$ is given by

$$\gamma_{D1,n-S}^{(p1)} = \frac{\alpha_1 |h_{D1S,n}|^2}{\alpha_1 |h_{D1R,n}|^2 + 1}. \quad (39)$$

The received signal at $R$ in the first phase is given by

$$\gamma_{R,nm}^{(p1)} = h_{D2R,m} \sqrt{\alpha_2} |x_2| + h_{D1R,n} \sqrt{\alpha_1} |x_1| + \sigma_R. \quad (40)$$

For multi-antenna user case, we only emphasize on the first case when $h_{D1R,n} > h_{D2R,m}$. $R$ first decodes $x_1$ corresponding SINR as below [42]

$$\gamma_{R,nn}^{(p1)} = \frac{\alpha_2 |h_{D2R,m}|^2}{\alpha_1 |h_{D1R,n}|^2 + 1}. \quad (41)$$

where $h_{D1R,n} \sim CN (0, \alpha_1 \lambda_{1p1,n})$.

**Case 2:** If $h_{D1R,n} < h_{D2R,m}$ in the case $G_2$, $R$ decodes the user symbol (i.e. $x_2$) subject to the better link quality by treating the user symbol (i.e. $x_1$) subject to the inferior link quality as noise [42]. The SINR of $R$ is given by

$$\gamma_{R,nn}^{(p1)} = \frac{\alpha_2 |h_{D2R,m}|^2}{\alpha_1 |h_{D1R,n}|^2 + 1}. \quad (42)$$

The received signal at $E$ from multi-antenna users $D_1$ in the first phase is given by

$$\gamma_{E,nn}^{(p1)} = h_{D1E,n} \sqrt{\alpha_1} |x_1| + h_{D2E,m} \sqrt{\alpha_2} |x_2| + \sigma_E. \quad (43)$$

After PIC, the received SINR at eavesdropper to detect $D_i$’s signals can be written as

$$\gamma_{Di,E-z}^{(p1)} = \alpha_i |h_{DiE,z}|^2, \quad (44)$$

where $z = \{n; m\}$.

\[ \Theta_1 = \text{Pr} \left[ |h_{D2R}|^2 > \frac{\phi_E |h_{D2E}|^2 (\alpha_1 |h_{D1R}|^2 + 1)}{\phi} \right] \]

\[ = \frac{1}{\lambda_2 \lambda_1} \int_0^{\infty} \int_0^{\infty} \left( 1 - F_{|h_{D2R}|^2} \right) \left( \frac{\phi_E (\alpha_1 |y| + 1)}{\phi} \right) f_{|h_{D2E}|^2} (x) f_{|h_{D1R}|^2} (y) dxdy \]

\[ = \frac{1}{\lambda_2 \lambda_1} \int_0^{\infty} \exp \left( - \frac{\phi_E (\alpha_1 |y| + 1)}{\phi \lambda_2} \right) \exp \left( - \frac{y}{\lambda_1} \right) dy \]

\[ = \frac{1}{\lambda_2 \lambda_1} \exp \left( \Phi_4 \right) \text{Ei} (-\Phi_4). \quad (37) \]
**B. PHASE 2**

Similar (8), the received signal at BS from $D_1$ and $R$ in the second phase is given by

$$y_{S,n}^{(p2)} = h_{D1S,n} \sqrt{\beta_1} y_1 + h_{RS} \sqrt{\beta_2} x_2 + \sigma_s. \quad (45)$$

Similar (9), we just consider details for the first case corresponding to $h_{D1R,n} > h_{RS}$, the BS first decodes $y_1$ and then $x_2$ using SIC. In particular, we examine the expressions of SINR for signals $y_1, x_2$ respectively as [42]

$$\gamma_{y_1,n}^{(p2)} = \frac{\beta_1 \phi_{[h_{D1S,n}]}^2}{\beta_2 \phi_{[h_{RS}]}^2 + 1}, \quad (46)$$

$$\gamma_{x_2,n}^{(p2)} = \frac{\beta_2 \phi_{[h_{RS}]}^2}{\beta_1 \phi_{h_{D1S,n}}^2 + 1}, \quad (47)$$

where $\tilde{h}_{D1S,n} \sim CN(0, \omega_s \lambda_{ip2,n})$.

The received signal at $E$ from $R$ and $D_1$ with multi-antenna

$$y_{E,n}^{(p2)} = h_{D1E,n} \sqrt{\beta_1} y_1 + h_{RE} \sqrt{\beta_2} x_2 + \sigma_E. \quad (48)$$

After PIC, the received SINR at the eavesdropper to detect $D_1$’s message can be written as

$$\gamma_{D1i,E-Z-E}^{(p2)} = \beta_i \phi_E |h_U|^2, \quad (49)$$

where $U = \{D1E, n; RE\}$.

The selected antenna can be achieved to strengthen uplink transmission from the user $D_1 \rightarrow BS$ and $D_2 \rightarrow R$ as [44]

$$n^* = \arg \max_{n=1,..,N} \left( |h_{D1S,n}|^2 \right), \quad (50)$$

$$m^* = \arg \max_{m=1,..,M} \left( |h_{D2R,m}|^2 \right). \quad (51)$$

The channel regarding selected antenna of $D_1$ and $D_2$ have PDF, and CDF respectively as [48]

$$f_{|h_{1r}|^2}(x) = 1 - \sum_{z=1}^{Z} \left( \frac{Z}{z} \right) (-1)^{z-1} \exp \left( \frac{-zx}{\lambda Q} \right), \quad (52)$$

$$f_{|h_{2r}|^2}(x) = \sum_{z=1}^{Z} \left( \frac{Z}{z} \right) (-1)^{z-1} \frac{z}{\lambda Q} \exp \left( \frac{-zx}{\lambda Q} \right). \quad (53)$$

where $T = \{D1S, n^*; D2R, m^*\}, Q = \{1S, n; 2R, m\}, Z = \{N; M\}$, $z = \{n; m\}$.

**C. ANALYSIS OF SOP**

It is worth pointing out that selecting the optimal transmit antenna based on mentioned criteria lead to similar way in computing performance between user $D_1$ and user $D_2$, which expects that SOP performance depends on the number of antennas equipped at destinations $D_1, D_2$.

1) SOP OF $D_1$

**Proposition 7:** The closed-form expression of SOP for multi-antenna user $D_1$ can be expressed by

$$SOP_{D1}^{(\alpha)} = 1 + \sum_{n=1}^{N} \sum_{r=1}^{N} \sum_{l=1}^{N} \sum_{i=1}^{N} \left( \frac{N}{n} \right) \left( \frac{N}{r} \right) \left( \frac{N}{l} \right)$$

$$\times (-1)^{n+r+l+i-4} \frac{r \phi \lambda_{1S,n}}{n \phi \lambda_{1E,n} + r \phi \lambda_{1S,n}} \frac{t \lambda_{1S,n}}{\theta_n} \exp \left( \frac{\lambda_{1S,n}}{\theta_n} \right), \quad (54)$$

where $\lambda_{n} = \frac{\mu \phi \lambda_{1S,n}}{\theta_n} + 1, \theta_n = \frac{\mu \phi \lambda_{1S,n}}{\theta_n}.$

**Proof:** See Appendix E.

2) SOP OF $D_2$

We just focus on $G1$ case here. We omit another case since the case $G2$ can be proved in similar way. Then, the following proposition is provided to highlight benefits of multiple antennas design at users.

**Proposition 8:** The closed-form expression of SOP for $G1 - D2$ with $M$ antennas can be expressed by

$$SOP_{D2}^{(G1, \alpha)} = 1 - \sum_{m=1}^{M} \sum_{r=1}^{M} \sum_{l=1}^{M} \sum_{i=1}^{M} \left( \frac{M}{m} \right) \left( \frac{M}{r} \right) \left( \frac{M}{l} \right)$$

$$\times (-1)^{m+r+l+i-4} \frac{r \lambda_{2R,m}}{\mu \phi \lambda_{1S,n} + \phi \lambda_{2R,m}} \frac{t \lambda_{RS}}{\phi \lambda_{1E,n} + \phi \lambda_{2R,m}}$$

$$\times \exp \left( \frac{\psi_1, m \delta_1, n - \frac{\mu z}{\sigma \phi \lambda_{2R,m}} + \psi_2 \delta_2, m - \frac{\mu z}{\beta_2 \phi \lambda_{RS}}}{} \right)$$

$$\times \exp \left( \frac{-\psi_1, m \delta_1, n}{\phi \lambda_{2R,m}} \right) \left( \frac{t \lambda_{RS}}{\phi \lambda_{1E,n} + \phi \lambda_{2R,m}} \right), \quad (55)$$

where $\psi_1, m = \frac{\mu v \phi \lambda_{2R,m}}{\mu \phi \lambda_{1E,n} + \phi \lambda_{2R,m}}$, $\delta_1, m = \frac{\mu \phi \lambda_{1S,n}}{\sigma \phi \lambda_{2R,m}} + \frac{1}{\omega_1 \phi \lambda_{1S,n}}.$

**Proof:** See Appendix F.

**D. ANALYSIS OF SPSC**

1) SPSC OF $D_1$

**Proposition 9:** The closed-form expression of SPSC for $D_1$ with $N$ antennas can be expressed by

$$SPSC_{D1}^{(\alpha)} = \sum_{n=1}^{N} \sum_{r=1}^{N} \sum_{l=1}^{N} \sum_{i=1}^{N} \left( \frac{N}{n} \right) \left( \frac{N}{r} \right) \left( \frac{N}{l} \right)$$

$$\times (-1)^{n+r+l+i-4} \frac{r \phi \lambda_{1S,n}}{n \phi \lambda_{1E,n} + r \phi \lambda_{1S,n}} \frac{t \lambda_{1S,n}}{\phi \lambda_{1S,n} \lambda_{RS}} \times \exp \left( \phi_{1,n} \right), \quad (56)$$

where $\Phi_{1,n} = \frac{\mu \phi \lambda_{1S,n} + \phi \lambda_{1S,n}}{\mu \phi \lambda_{1S,n} + \phi \lambda_{2R,m} \lambda_{RS}}.$

**Proof:** See Appendix G.
By contrast, multi-antenna users exhibit improved SOP and depends on power allocation factors, and channel gains. Experience different SOP as well as SPSC which mainly

![FIGURE 3. SOP vs transmit SNR with different $\alpha_1 = \beta_1$ [51]

$(R_D1 = R_D2 = 0.2$ (bps/Hz), $\lambda_1 = \lambda_8 = \lambda_9 = \lambda_2 = 1$ [43], $\lambda_{ip1} = \lambda_{ip2} = 1$, $\lambda_1E = \lambda_2E = \lambda_{RE} = 0.01$, $\omega = \omega_1 = \omega_2 = 0.2$ [52], $\phi_E = 1$ (dB)).

2) SPSC OF $D_2$

Proposition 10: The closed-form expression of SPSC for multi-antenna user $D_2$ (case $G1$ only) can be formulated by

$$SPSC_{D_2}^{(G1,m*)} = \sum_{m=1}^{M} \sum_{r=1}^{M} \sum_{N} \sum_{N} \left( \begin{array}{c} M \\ m \end{array} \right) \left( \begin{array}{c} M \\ r \end{array} \right) \left( \begin{array}{c} N \\ \lambda_{2R,m} \end{array} \right) \left( \begin{array}{c} N \\ \lambda_{RS} \end{array} \right) \frac{r\lambda_{2R,m}}{m! \lambda_{1E,m} \lambda_{ip1,n} \beta_1 \lambda_{RE,0} \lambda_{ip2,n}} \times \exp \left( \Phi_{2,m} + \Phi_{3,m} \right) \exp \left( \Phi_{2,m} \right) \exp \left( \Phi_{3,m} \right),$$

where $\Phi_{2,m} = \frac{\lambda_{1E,m} + \lambda_{ip1,n}}{m! \lambda_{1E,m} \lambda_{ip1,n}}$, $\Phi_{3,m} = \frac{\lambda_{RE,0} + \lambda_{ip2,n}}{\beta_1 \lambda_{RE,0} \lambda_{ip2,n}}$.

Proof: See Appendix H.

Remark 3: As discussed earlier, two single antenna users experience different SOP as well as SPSC which mainly depends on power allocation factors, and channel gains. By contrast, multi-antenna users exhibit improved SOP and SPSC performance as expected, shown in (54), (54), (56) and (57). The uplink communication tasks in the context of NOMA strategy shows more complicated expressions of secure performance. However, even though similar setup of end-to-end SINR and target transmission rate, and the selection criterion is indeed a combination of the best transmit antennas at two multi-antenna users to produce an improvement. Unfortunately, a challenging issue may arise: how could the antenna can be jointly selected so that the optimal performance of such system is enhanced? To tackle this problem, we develop numerical experiment to evaluate antenna parameters $N$, $M$ to secure performance.

VI. SIMULATION RESULTS

In this section, we conduct numerical simulation by run $10^6$ iterations for Monte-Carlo simulation. Main parameters are provided in each figure.

In Fig. 3, we first analyze the SOP secrecy performance versus the transmit SNR $\phi$ at the BS over different power allocation factors when $\alpha_1 = \beta_1$, in which the asymptotic lines are included to show the lower bound of these SOP curves. As can be observed from the curves and the corresponding markers, the Monte-Carlo results are matched tightly with the analytical results and such good agreement validates the accuracy of our analytical results. As for the comparison of the SOPs, the simulation results exhibit the best case for user $D_1$ since the high power factor is allocated to it. We observe that the SOP is a monotonically decreasing function of $\phi$, since the SINRs depend on $\phi$. It’s obvious that the change in $\alpha_1 = \beta_1$ from 0.9 to 0.7 leads to deduction of SOP performance. Thus, the secrecy performance can be improved at the cost of reliable performance by controlling $\alpha_1$ and $\beta_1$.

Fig. 4 shows the similar trends of SOP performance of two users by changing the target rates, $R_{D1}$, $R_{D2}$. Since formulas of SOP depend on these values of $R_{D1}, R_{D2}$, the lower required black target rates result in a better SOP performance.
It is confirmed that the lower bound of SOP is matched with the exact SOP values at high SNR regime, i.e. $\phi = 40$ (dB).

The impact of the level of imperfect SIC at user $D_2$ can be seen clearly as Fig. 5. Once we set $\omega = 0.8$, it causes a significant reduction in the SOP. Further, the channel conditions reported in cases $G_1$ and $G_2$ also show performance gaps for consideration on performance of user $D_2$. Since formulas of SOP depend on the transmit SNR, and hence high SNR leads to significant improvement on SOP performance.

As observed from expressions of SOP metric in Fig. 6, for example (25) reports that the SOP performance will become worse if the SNR of the eavesdropper increases. We can confirm such result as seen in Fig. 6. The impact of transmit SNR at the base station also contribute to improving performance in this circumstance. Further, $\phi_E$ in the range from 15 (dB) to 25 (dB) results in significant variations of SOP.

In Fig. 7, as further observation from expressions of SOP metric, for example (25) indicates that the target rates are main parameter to limit the performance of SOP. The curves of SOP approach to 1 when the target rates $R_{D1} = R_{D2} = 0.2$ (bps/Hz), $\lambda_{1E} = \lambda_{RE} = \lambda_{1R} = \lambda_{2R} = 1$ [43], $\lambda_{ip1} = \lambda_{ip2} = 1$, $\lambda_{2E} = \lambda_{RE} = 0.01$, $\omega = \omega_1 = \omega_2 = 0.2$ [52]. $\phi_E = 10$ (dB)).

In this circumstance. Further, $\phi_E$ in the range from 15 (dB) to 25 (dB) results in significant variations of SOP.

In Fig. 7, as further observation from expressions of SOP metric, for example (25) indicates that the target rates are main parameter to limit the performance of SOP. The curves of SOP approach to 1 when the target rates $R_{D1} = R_{D2} = 0.2$ (bps/Hz), $\lambda_{1E} = \lambda_{RE} = \lambda_{1R} = \lambda_{2R} = 1$ [43], $\lambda_{ip1} = \lambda_{ip2} = 1$, $\lambda_{2E} = \lambda_{RE} = 0.01$, $\omega = \omega_1 = \omega_2 = 0.2$ [52]. $\phi_E = 10$ (dB)).
performance of user $D_1$ just slightly relies on the antenna configuration. The main reason is that decoding signal procedure at the BS for user $D_1$ is more complicated since it belongs to processing at both transmission hops. On the other hand, the SOP performance has also floor at high SNR region which indicates that more antennas at users only contribute to improvement at low SNR region which more system parameters with higher weight compared to $\phi$.

Then, Fig. 10 shows the increase in the SPSC performance when the SNR at the BS increases $\phi$. The performance gap between the two users is still observable in this figure. We provide more comparisons on OMA as well. In this case, $D_1$ is reported as best case except for OMA case. It is obvious that $\phi_D$ results in the deduction of SPSC in Fig. 11. We also know from the calculated expression that SPSC is a monotonically increasing function of $\phi$. Similarly, as shown in Fig. 12, the impact of power allocation factors is small if we compare the two cases of $\alpha_1 = \beta_1 = 0.8$ and $\alpha_1 = \beta_1 = 0.2$.

Furthermore, the impact of imperfect SIC on SPSC can be seen clearly in Fig. 13. When $\phi_D$ changes from 35 to 40, the SPSC performance of user $D_2$ is affected significantly. Other trends of such secure performance metric are similar as previous figures. Similarly, Fig. 14 compares SPSC for two cases of antenna configuration, $N = M = 1$ and $N = M = 3$.

VII. CONCLUSION

In this paper, we studied the secrecy performance of an uplink NOMA for single antenna and multiple antennas users cases. We consider the uplink transmission scenario where users are...
classified based on their locations around the serving base station in the presence of an eavesdropper. We also analyzed the PLS performances in terms of SOP and SPSC. Such uplink NOMA transmission proves reliability since there are two kinds of links from user ends to the base station. A group of two NOMA users is adopted to have a tractable analysis since the interference from other groups is neglected. Based on the proposed model, the closed-form expressions of SOP and SPSC are derived for characterizing the systems' reliability performance and secrecy performance. Additionally, we provide the main parameters which explicitly capture the reliability performance and secrecy performance of the network. It’s proved that the performance gaps of two users in terms of SOP and SPSC can be improved by varying power allocation factors and channel conditions. It is worth mentioning that the results in this study are primarily theoretically oriented and offer a useful theoretical guidelines for uplink NOMA transmission in cellular systems.

**APPENDIX A**

**PROOF OF PROPOSITION 1**

From (20), the SOP of $D_1$ can be written by

$$SOP_{D_1} = 1 - Pr\left[\frac{1 + \gamma_{D_1-S}^{(p1)}}{1 + \gamma_{D_1-E}^{(p1)}} \geq \mu_1\right] \times Pr\left[\frac{1 + \gamma_{S1}^{(p2)}}{1 + \gamma_{D_1-E}^{(p2)}} < \mu_1\right]. \quad (A.1)$$

From (A.1), $A_1$ can be calculated as

$$A_1 = Pr\left[\gamma_{D_1-S}^{(p1)} \geq \mu_1 \gamma_{D_1-E}^{(p1)}\right] \times Pr\left[\gamma_{S1}^{(p2)} < \mu_1\right].$$

From (A.1), $A_2$ can be calculated as (A.3), shown at the bottom of the next page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $A_2$ is given by

$$A_2 = -\frac{\lambda_{1S}}{\mu_1 \phi E \beta_2 \lambda_{1E} \lambda_{RS}} \exp \left(\frac{\lambda \theta - \frac{\mu_1}{\beta_1 \phi \lambda_{1S}}}{}\right) Ei\left(-\frac{x \lambda \theta}{\lambda_{1E}}\right), \quad (A.4)$$

where $\lambda = \frac{\gamma \mu \beta_2}{\beta_1 \phi \lambda_{1S}} + \frac{1}{\lambda_{RS}}, \theta = \frac{\mu_1 \phi \lambda_{1E} + \phi_{1S}}{\mu_1 \phi \beta_2 \lambda_{1E}}$.

Substituting (A.2) and (A.4) into (A.1), we can obtain (21). The proof is completed.

**APPENDIX B**

**PROOF OF PROPOSITION 2**

From (22), $B_1$ can be calculated as (B.1), shown at the bottom of the next page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $B_1$ is given by

$$B_1 = -\frac{\lambda_{2R}}{\mu_2 \alpha_1 \phi \lambda_{2E} \lambda_{PE}} \exp \left(\psi_1 \delta_1 - \frac{\mu_2}{\alpha_2 \phi \lambda_{2R}}\right) \times Ei\left(-\frac{\psi_1 \delta_1}{\lambda_{2E}}\right), \quad (B.2)$$

where $\psi_1 = \frac{\mu_2 \phi \lambda_{2E} + \phi_{2R}}{\mu_2 \alpha_2 \phi \lambda_{2E}}$, $\delta_1 = \frac{\mu_2 \delta_1}{\alpha_2 \lambda_{2E}} + \frac{1}{\alpha_2 \lambda_{2E}}$.

Next, $B_2$ can be calculated as (B.3), shown at the bottom of the next page.

Similar $B_1$, based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $B_2$ is given by

$$B_2 = -\frac{\lambda_{RS}}{\mu_2 \beta_1 \phi \lambda_{2E} \lambda_{RE}} \exp \left(\psi_2 \delta_2 - \frac{\mu_2}{\beta_2 \phi \lambda_{RS}}\right) \times Ei\left(-\frac{\psi_2 \delta_2}{\lambda_{RE}}\right), \quad (B.4)$$

where $\psi_2 = \frac{\mu_2 \phi \lambda_{RE} + \phi_{RS}}{\mu_2 \beta_2 \phi \lambda_{RE}}$, $\delta_2 = \frac{\mu_2 \delta_2}{\beta_2 \lambda_{RE}} + \frac{1}{\beta_2 \lambda_{RE}}$.

Substituting (B.2) and (B.4) into (22), we can obtain (23). The proof is completed.

**APPENDIX C**

**PROOF OF PROPOSITION 3**

From (31), we can express $Q_1$ as

$$Q_1 = Pr\left[|h_{D11}|^2 > \frac{\phi E|h_{D1E}|^2}{\phi}\right] = \frac{1}{\lambda_{1E}} \int_0^\infty \exp\left(-\left(\frac{\phi E}{\phi \lambda_{1S}} + \frac{1}{\lambda_{1E}}\right) x\right) dx = \frac{\phi \lambda_{1S}}{\phi \lambda_{1E} + \phi \lambda_{1S}}. \quad (C.1)$$

Further, $Q_2$ can be calculated as

$$Q_2 = Pr\left[|h_{D12}|^2 > \frac{\phi E|h_{D1E}|^2}{\phi}\left(\beta_2 \phi \lambda_{RS} + 1\right)\right] = \int_0^\infty \int_0^\infty \left(1 - F_{|h_{D12}|^2}\left(\frac{\phi E \left(\beta_2 \phi \lambda_{RE} + 1\right)}{\phi}\right)\right) \times f_{|h_{D12}|^2} (x) f_{|h_{RE}|^2} (y) dx dy = \int_0^\infty \int_0^\infty \exp\left(-\frac{\phi E \left(\beta_2 \phi \lambda_{RS} + 1\right)}{\phi \lambda_{1S}}\right) \frac{1}{\lambda_{1E}} \exp\left(-\frac{x}{\lambda_{1E}}\right) dx dy.$$
\[
\begin{align*}
\times \frac{1}{\lambda_{RS}} \exp \left( -\frac{y}{\lambda_{RS}} \right) dxdy & = \frac{1}{\lambda_{1E}} \frac{1}{\lambda_{RS}} \int_0^\infty \int_0^\infty \exp \left( -\frac{\phi_E (\beta_2 \phi y + 1)}{\phi_{1_{E}}} + \frac{1}{\lambda_{1E}} \right) x \right) \\
& \times \exp \left( -\frac{y}{\lambda_{RS}} \right) dxdy \\
& = \frac{1}{\lambda_{RS}} \int_0^\infty \phi_{1_{E}} \phi_{2_{RS}} \phi_{1_{E}} + \phi_1 \phi_{1_{E}} + \phi_{1_{E}} \exp \left( -\frac{y}{\lambda_{RS}} \right) dy. \\
(C.2)
\end{align*}
\]

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, \( Q_2 \) is written as
\[
Q_2 = -\frac{\lambda_{1S}}{\beta_2 \phi_{E} \lambda_{1E} \lambda_{RS}} \exp (\Phi_1) \text{Ei} (-\Phi_1),
\]
where \( \Phi_1 = \frac{\phi_{1_{E}} \lambda_{1E} + \phi_{2_{RS}}}{\beta_2 \phi_{E} \lambda_{1E} \lambda_{RS}}. \)

The expected result can be obtained as plugging (C.1) and (C.3) into (31).

It is the end of the proof.

\[
\begin{align*}
A_2 &= \text{Pr} \left[ y_1^{(p_2)} \geq \frac{\mu_1 + \mu_1 y_{D1-E}}{\beta_1 \phi_{hD1}} \right] \\
&= \text{Pr} \left[ \frac{\mu_1 \beta_1 \phi_{hD1}^2}{\beta_2 \phi_{hD1}^2} \geq \frac{\mu_1 + \mu_1 \beta_1 \phi_{hD1}}{\beta_1 \phi_{hD1}^2} \right] \\
&= \text{Pr} \left[ \phi_{hD1}^2 \geq \frac{(\mu_1 + \mu_1 \beta_1 \phi_{hD1}^2) (\beta_2 \phi_{hD1}^2 + 1)}{\beta_1 \phi_{hD1}^2} \right] \\
&= \int_0^\infty \int_0^\infty \left( 1 - F_{\phi_{hD1}^2} \left( \frac{\mu_1 + \mu_1 \beta_1 \phi_{hD1}^2} \beta_1 \phi_{hD1}^2 \right) (\beta_2 \phi_{hD1}^2 + 1) \right) \phi_{hD1}^2 (x) f_{\phi_{hD1}^2} (y) dxdy \\
& = \frac{1}{\lambda_{1E} \lambda_{RS}} \exp \left( -\frac{\lambda_{1E}}{\beta_1 \phi_{1_{E}}} \right) \frac{\mu_1 \phi_{1_{E}} \phi_{2_{RS}} \phi_{1_{E}} + \mu_1 \phi_1 \phi_{1_{E}} + \phi_{1_{E}} \exp \left( -\frac{\lambda_{1E}}{\lambda_{RS}} \right) y dxdy. \\
(A.3)
\end{align*}
\]

\[
\begin{align*}
B_1 &= \text{Pr} \left[ y_{R1}^{(p_1)} \geq \frac{\mu_2 + \mu_2 y_{D2-E}}{\alpha_2 \phi} \right] \\
&= \text{Pr} \left[ \phi_{D2}^2 \geq \frac{(\mu_2 + \mu_2 \alpha_2 \phi_{E} \phi_{D2-E}^2) (\alpha_2 \phi_{hD1}^2 + 1)}{\alpha_2 \phi_{hD1}^2} \right] \\
&= \int_0^\infty \int_0^\infty \left( 1 - F_{\phi_{D2}^2} \left( \frac{\mu_2 + \mu_2 \alpha_2 \phi_{E} \phi_{D2-E}^2} \alpha_2 \phi_{E} \phi_{D2-E}^2 \right) (\alpha_2 \phi_{hD1}^2 + 1) \right) \phi_{D2}^2 (x) f_{\phi_{D2}^2} (y) dxdy \\
& = \frac{1}{\lambda_{2E} \lambda_{RS}} \exp \left( -\frac{\lambda_{2E}}{\omega_1 \lambda_{ip1}} \right) \frac{\mu_2 \alpha_2 \phi_{E} \phi_{2_{RS}} \phi_{E} \phi_{D2-E} + \mu_2 \phi_2 \phi_{E} \phi_{2_{RS}} + \phi_{2_{RS}} \exp \left( -\frac{\lambda_{2E}}{\omega_1 \lambda_{ip1}} \right) y dxdy. \\
(B.1)
\end{align*}
\]

\[
\begin{align*}
B_2 &= \text{Pr} \left[ y_{R2}^{(p_2)} \geq \frac{\mu_2 + \mu_2 y_{D2-E}}{\beta_2 \phi} \right] \\
&= \text{Pr} \left[ \phi_{RS}^2 \geq \frac{(\mu_2 + \mu_2 \beta_2 \phi_{E} \phi_{RS}^2) (\beta_2 \phi_{hD1}^2 + 1)}{\beta_2 \phi_{hD1}^2} \right] \\
&= \int_0^\infty \int_0^\infty \left( 1 - F_{\phi_{RS}^2} \left( \frac{\mu_2 + \mu_2 \beta_2 \phi_{E} \phi_{RS}^2} \beta_2 \phi_{E} \phi_{RS}^2 \right) (\beta_2 \phi_{hD1}^2 + 1) \right) \phi_{RS}^2 (x) f_{\phi_{RS}^2} (y) dxdy \\
& = \frac{1}{\lambda_{RE} \lambda_{ip2}} \exp \left( -\frac{\lambda_{RE}}{\omega_2 \lambda_{ip2}} \right) \frac{\mu_2 \beta_2 \phi_{E} \phi_{RE} \phi_{RS} + \mu_2 \phi_2 \phi_{E} \phi_{RE} + \phi_{RS} \exp \left( -\frac{\lambda_{RE}}{\omega_2 \lambda_{ip2}} \right) y dxdy. \\
(B.3)
\end{align*}
\]

95148 VOLUME 9, 2021
PROOF OF PROPOSITION 4

With the help of (33), $W_1$ is given as

$$W_1 = \Pr \left[ \frac{\phi_2}{|h_{D2R}|^2} > \frac{\phi_2}{\phi h_{D2E}} \right]$$

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $W_1$ is written by

$$W_1 = \frac{\lambda_{RS}}{\alpha \phi_2} \exp (\Phi_2) \exp (-\Phi_2), \quad (D.2)$$

where $\Phi_2 = \frac{\phi_2 \lambda_{RS} + \phi \lambda_{2R}}{\alpha \phi_2}$.

Next, $W_2$ can be calculated as

$$W_2 = \Pr \left[ \frac{\phi_2}{|h_{RE}|^2} > \frac{\phi_2}{\phi h_{RE}} \right]$$

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $W_2$ is given by

$$W_2 = \frac{\lambda_{RS}}{\beta \phi h_{RE} \phi_2 \lambda_{ip2}} \exp (\Phi_3) \exp (-\Phi_3), \quad (D.4)$$

where $\Phi_3 = \frac{\phi_2 \lambda_{RS} + \phi \lambda_{2R}}{\alpha \phi_2}$. Substituting (D.2) and (D.4) into (33), we can obtain (29). It is the end of the proof.

PROOF OF PROPOSITION 7

Similar to (20), the SOP of $D_1$ with $N$ antennas can be expressed as

$$SOP^{(n)}_{D_1} = 1 - \Pr \left[ \frac{1 + \gamma_{D_1}^{(p1)} \phi \lambda_{RS}}{1 + \gamma_{D_1}^{(p1)} \phi \lambda_{RS}} \geq \mu_1 \right]$$

Next, $A_{2,n^*}$ can be calculated as (E.2), shown at the bottom of the next page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $A_{2,n^*}$ is written by

$$A_{2,n^*} = -\sum_{l=1}^{N} \sum_{l=1}^{N} \left( \begin{array}{c} N \\ i \end{array} \right) \left( \begin{array}{c} N \\ i \end{array} \right) (-1)^{i+l-2} \frac{t\lambda_{1S,n}}{\mu_1 \lambda_{1S,n} \lambda_{RS}}$$

where $\lambda_n = \frac{\mu_1 \lambda_{1S,n}}{\mu_1 \lambda_{1S,n} + 1}$, $\theta_n = \frac{\mu_2 \lambda_{1S,n} + \lambda_{RS}}{\mu_2 \lambda_{1S,n} + \lambda_{RS}}$.

Substituting (E.2) and (E.3) into (E.1), we can obtain (54). The proof is completed.

PROOF OF PROPOSITION 8

Similar to (22), the SOP of $G_1 - D_2$ with $M$ antennas can be expressed as

$$SOP^{(G_1,m^*)}_{D_2} = 1 - \Pr \left[ \frac{1 + \gamma_{G_1}^{(p1)} \phi \lambda_{RS}}{1 + \gamma_{G_2}^{(p1)} \phi \lambda_{RS}} \geq \mu_2 \right]$$

where $\Phi_3 = \frac{\phi_2 \lambda_{RS} + \phi \lambda_{2R}}{\alpha \phi_2}$. Substituting (D.2) and (D.4) into (33), we can obtain (29). It is the end of the proof.

$$SOP^{(G_1,m^*)}_{D_2} = 1 - \Pr \left[ \frac{1 + \gamma_{G_1}^{(p1)} \phi \lambda_{RS}}{1 + \gamma_{G_2}^{(p1)} \phi \lambda_{RS}} \geq \mu_2 \right]$$

where $\Phi_3 = \frac{\phi_2 \lambda_{RS} + \phi \lambda_{2R}}{\alpha \phi_2}$. Substituting (D.2) and (D.4) into (33), we can obtain (29). It is the end of the proof.
Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $B_{1,m^*}$ is written by

$$
B_{1,m^*} = - \sum_{m=1}^{M} \sum_{r=1}^{M} \sum_{l=1}^{N} \left( \frac{M}{r} \right) \left( \frac{N}{l} \right) (-1)^{m+r+l-3} \sum_{m=1}^{M} \sum_{r=1}^{M} \sum_{l=1}^{N} \left( \frac{M}{r} \right) \left( \frac{N}{l} \right) (-1)^{m+r+l-3}
$$

Next, $B_{2,m^*}$ can be calculated as (F.4), shown at the middle of the next page.

\[ A_{1,n^*} = \text{Pr} \left[ Y_{D1,n^*} \geq \mu_{1} + \mu_{1} Y_{D1,n^*} \right] \]

\[ A_{2,n^*} = \text{Pr} \left[ Y_{D1,n^*} \geq \mu_{1} + \mu_{1} Y_{D1,n^*} \right] \]

\[ B_{1,m^*} = \text{Pr} \left[ Y_{R1,m^*} \geq \mu_{2} + \mu_{2} Y_{D2,m^*} \right] \]

\[ B_{2,m^*} = \text{Pr} \left[ Y_{R1,m^*} \geq \mu_{2} + \mu_{2} Y_{D2,m^*} \right] \]

\[ \text{exp} \left( \psi_{1,m^*} - \frac{m \mu_{2} \lambda_{2,R,m}}{\alpha_{2} \phi_{\lambda_{2,R,m}}} \right) \]

Next, $B_{2,m^*}$ can be calculated as (F.4), shown at the middle of the next page.
Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $B_{2,m^*}$ is written by

$$B_{2,m^*} = - \sum_{i=1}^{N} \binom{N}{i} (-1)^{i-1} \frac{t \lambda_{RS}}{\mu_2 \beta_1 \phi_{RE} \omega \lambda_{ip2,n} \lambda_{RE}} \times \exp \left( \psi_2 \delta_{2,m} - \frac{\mu_2}{\beta_2 \phi_{RS}} \right) \text{Ei} \left( -\psi_2 \delta_{2,m} \right), \quad (F.5)$$

where $\delta_{2,m} = \frac{\mu_2}{\beta_2 \phi_{RS}} + \frac{t}{\omega \lambda_{ip2,n}}$.

Substituting (F.3) and (F.5) into (F.1), we can obtain (55). The proof is completed.

**APPENDIX G
PROOF OF PROPOSITION 9**

Similar (31), the SPSC of $D_1$ with $N$ antennas can be expressed as

$$SPSC_{D1} (n^*) = \Pr \left[ y_{D_1,n^*}^{(p1)} > y_{D_1,n^*}^{(p1)} \right] \times \Pr \left[ y_{D_1,n^*}^{(p2)} > y_{D_1,n^*}^{(p2)} \right]. \quad (G.1)$$

From (G.1), $Q_{1,n^*}$ can be calculated as

$$Q_{1,n^*} = \Pr \left[ |h_{D1,n^*}|^2 \geq \frac{\phi_E |h_{D1,n^*}|^2}{\phi} \right]$$

$$= \int_0^\infty \left( 1 - F_{|h_{D1,n^*}|^2} \right) \left( \frac{\phi_E}{\phi} \right) |h_{D1,n^*}|^2 (x) \, dx$$

$$= \sum_{n=1}^{N} \sum_{r=1}^{N} \binom{N}{n} \binom{N}{r} (-1)^{n+r-2} \frac{r}{\lambda_{1,E,n}}$$

Next, $Q_{2,n^*}$ can be calculated as (G.3), shown at the bottom of the next page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, $Q_{2,n^*}$ is written by

$$Q_{2,n^*} = - \sum_{i=1}^{N} \sum_{i=1}^{N} \binom{N}{i} \binom{N}{i} (-1)^{i+j-2} \times \frac{t \lambda_{1,n^*}}{\mu_2 \beta_2 \phi_{E1,n^*} \lambda_{RS}} \exp \left( \Phi_{1,n} \right) \text{Ei} \left( -\Phi_{1,n} \right). \quad (G.4)$$

where $\Phi_{1,n} = \frac{\lambda_1 \phi_{E1,n} + \lambda \phi_{RS}}{\lambda_1 \phi_{E1,n} + \lambda}$. Substituting (G.2) and (G.4) into (G.1), we can obtain (56). The proof is completed.

**APPENDIX H
PROOF OF PROPOSITION 10**

Similar (33), the SPSC of $G_1 - D_1$ with $M$ antennas can be expressed as

$$SPSC_{D2}^{(G_1,m^*)} = \Pr \left[ y_{D_1,m^*}^{(p1)} > y_{D_1,m^*}^{(p1)} \right] \times \Pr \left[ y_{D_1,m^*}^{(p2)} > y_{D_1,m^*}^{(p2)} \right]. \quad (H.1)$$

From (H.1), $W_{1,m^*}$ can be calculated as (H.2), shown at the bottom of the next page.
Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, \( W_{1,m^*} \) is written by

\[
W_{1,m^*} = -\sum_{m=1}^{\infty} \sum_{r=1}^{l-1} \sum_{l=1}^{N} (M_m) (M_r) (N_l) (-1)^{m+r+l-3} \times \frac{r l \lambda_{2,m}}{m \alpha_1 \phi E \lambda_{2,E,m} \omega_1 \lambda_{ip1,n}} \exp \left( j \Phi_{2,m} \right) E \left( -j \Phi_{2,m} \right),
\]

where \( \Phi_{2,m} = \frac{\ln \mu E \lambda_{2,E,m} + l \phi \lambda_{2,m}}{m \alpha_1 \phi E \lambda_{2,E,m} \omega_1 \lambda_{ip1,n}} \).

From (H.1), \( W_{2,m^*} \) can be calculated as (H.4), shown at the bottom of the page.

Based on [45, Eq. (3.352.4)] and applying some polynomial expansion manipulations, \( W_{2,m^*} \) is written by

\[
W_{2,m^*} = -\sum_{l=1}^{N} \langle N \rangle (-1)^{l-1} \frac{t \lambda_{RS}}{\beta_1 \phi E \lambda_{RE} \omega_2 \lambda_{ip2,n}} \times \exp \left( j \Phi_{3,m} \right) E \left( -j \Phi_{3,m} \right),
\]

where \( \Phi_{3,m} = \frac{i \phi \lambda_{RE} + l \phi \lambda_{RS}}{\beta_1 \phi E \lambda_{RE} \omega_2 \lambda_{ip2,n}} \).

Substituting (H.3) and (H.5) into (H.1), we can obtain (57).

The proof is completed.
MINH-SANG VAN NGUYEN was born in Bentre, Vietnam. He is currently pursuing the master’s degree in wireless communications. He worked with the Industrial University of Ho Chi Minh City, Vietnam. His research interests include electronic design, signal processing in wireless communications networks, non-orthogonal multiple access, and physical layer security.

DINH-THUAN DO (Senior Member, IEEE) received the B.S., M.Eng., and Ph.D. degrees from Vietnam National University (VNU-HCM) in 2003, 2007, and 2013, respectively, all in Communications Engineering. From 2003 to 2009, he was a Senior Engineer with VinaPhone Mobile Network. From 2009 to 2010, he was a Visiting Ph.D. Student with the Communications Engineering Institute, National Tsing Hua University, Taiwan. He published more than 85 SCI/SCIE journal articles. His research interests include signal processing in wireless communications networks, reconfigurable intelligent surfaces, non-orthogonal multiple access, full-duplex transmission, and energy harvesting. In 2015, he was recipient of the Golden Globe Award from the Vietnam Ministry of Science and Technology (Top ten excellent young scientists nationwide). He is currently serving as an Associate Editor for EURASIP Journal on Wireless Communications and Networking, Computer Communications (Elsevier), and KSII Transactions on Internet and Information Systems.

FATEMEH AFGHAH (Senior Member, IEEE) was an Assistant Professor with the Electrical and Computer Engineering Department, North Carolina Agricultural and Technical State University, Greensboro, NC, USA, from 2013 to 2015. She is currently an Associate Professor with the School of Informatics, Computing and Cyber Systems, Northern Arizona University (NAU), Flagstaff, AZ, USA, where she is the Director of the Wireless Networking and Information Processing (WiNIP) Laboratory. Her research interests include wireless communication networks, decision making in multi-agent systems, radio spectrum management, hardware-based security, and artificial intelligence in healthcare. She was a recipient of several awards, including the NSF CRII Award, in 2017, the Air Force Office of Scientific Research Young Investigator Award, in 2019, and the National Science Foundation (NSF) CAREER Award, in 2020.

S. M. RIAZUL ISLAM (Member, IEEE) was affiliated with the Memorial University, Canada as a Postdoctoral Fellow. Before that, he was with the University of Dhaka, Bangladesh, as an Assistant Professor and a Lecturer with the Department of Electrical and Electronic Engineering. He worked as a Chief Engineer with Samsung R&D Institute Bangladesh, Department of Solution Laboratory for advanced research. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, South Korea. Prior to joining Sejong, he worked as a Postdoctoral Fellow with the Wireless Communications Research Center, Inha University, South Korea. His research interests include wireless communications, the Internet of Things, and applied artificial intelligence.

ANH-TU LE was born in Lam Dong, Vietnam, in 1997. He is currently pursuing the master’s degree in communications and information system, with a focus on wireless communications. He is a Research Assistant with the WICOM Laboratory led by Dr. Thuan. His research interests include wireless channel modeling, NOMA, cognitive radio, and MIMO.