Enhancing PHY-Security of FD-Enabled NOMA Systems Using Jamming and User Selection: Performance Analysis and DNN Evaluation

Kyusung Shim, *Student Member, IEEE,* Tri Nhu Do, *Member, IEEE,* Toan-Van Nguyen, *Student Member, IEEE,* Daniel Benevides da Costa, *Senior Member, IEEE,* and Beongku An, *Member, IEEE,*

***Abstract*—In this paper, we study the physical layer security (PHY-security) improvement method for a downlink non-orthogonal multiple access (NOMA) system in the presence of an active eavesdropper. To this end, we propose a full-duplex (FD)-enabled NOMA system and a promising scheme, called minimal transmitter selection (MTS) scheme, to support secure transmission. Specifically, the cell-center and cell-edge users act simultaneously as both receivers and jammers to degrade the eavesdropper channel condition. Additionally, the proposed MTS scheme opportunistically selects the transmitter to minimize the maximum eavesdropper channel capacity. To estimate the secrecy performance of the proposed methods, we derive an approximated closed-form expression for secrecy outage probability (SOP) and build a deep neural network (DNN) model for SOP evaluation. Numerical results reveal that the proposed NOMA system and MTS scheme improve not only the SOP but also the secrecy sum throughput. Furthermore, the estimated SOP through the DNN model is shown to be tightly close to other approaches, i.e., Monte-Carlo method and analytical expressions. The advantages and drawbacks of the proposed transmitter selection scheme are highlighted, along with insightful discussions.**

***Index Terms*—Artificial noise, deep neural network, full-duplex, non-orthogonal multiple access, physical layer security.**

I. Introduction

Power-domain non-orthogonal multiple access (PD-NOMA) is one of the latest multiple access technologies. In the downlink scenario, NOMA can communicate with multiple users by allocating different transmit power levels simultaneously. At the receiver side, most receivers eliminate the other users' message from the received signal using successive interference cancellation (SIC) [1], while the one with the weakest channel condition directly decodes its message from the received signal by treating the other users' signals as interference [2]. Thus, NOMA can significantly improve spectral efficiency because multiple users are served within a single resource block (e.g., time-slot, frequency, spreading sequence, etc) [3].

In fifth-generation (5G) and beyond networks, a massive number of connections among internet-of-things (IoT) devices are envisaged. NOMA arises as one the promising techniques to support machine-to-machine (M2M) communications due to its feature of serving multiple users simultaneously within a single resource block [4]. However, IoT devices may transmit sensitive information such as medical information, banking information, and personal information through radio-frequency (RF) signals [5]. Thus, security becomes as important as spectral efficiency in 5G networks. In particular, physical layer security (PHY-security) has been considered as one of the efficient solutions to protect the message from wiretapping attacks since it utilizes the characteristic of wireless medium to shield signal information [6]. In PHY-security context, secure transmission means that the channel capacity of the main channel (between two legitimate users) is higher than that of the eavesdropper channel [7]. Additionally, when the difference between the channel capacity of the main channel and eavesdropper channel increases, the system becomes more robust from information-theoretic security perspective. In addition, an opportunistic user (antenna) selection can be employed to protect the message by choosing the most robust user (antenna) against the eavesdropper. Recently, as the technology evolves, the trend of eavesdropping has changed from passive eavesdropping to active one using full-duplex (FD) terminals, in which this latter overhears and interrupts transmission between legitimate users at the same time. Furthermore, active eavesdropping is more challenging in a NOMA context since multiple users are served concurrently with a single resource block and may harm the quality-of-service (QoS) of legitimate users.

In FD literature, recent advances in antenna and transceiver design have shown a great potential to eliminate the self-interference (SI) channel up to the receiver noise floor [8]. The SI channel can suppress passive cancellation by using the physical separation/isolation between transmitter and receiver. Active suppression eliminates SI signal from the received signal, which can be further categorized into two stages: analog-domain cancellation and digital-domain cancellation [9]. In analog-domain cancellation, the SI channel is to cancel before

This work was supported in part by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (2019R1A2C1083996), in part by the Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2020R1A6A3A13072303).

K. Shim and T.-V. Nguyen are with the Department of Electronics and Computer Engineering in Graduate School, Hongik University, 30016, Republic of Korea (emails: shimkyusung@outlook.kr, vannguyentoan@gmail.com).

T. N. Do is with the Department of Electrical Engineering, ÉTS, University of Québec, Montreal, QC, Canada (email: trinhu.do@ieee.org).

D. B. da Costa is with the Future Technology Research Center, National Yunlin University of Science and Technology, Douliu, Yunlin 64002, Taiwan, R.O.C., and with the Department of Computer Engineering, Federal University of Ceará, Sobral 62010-560, CE, Brazil (email: danielbcosta@ieee.org).

B. An is with the Department of Software and Communications Engineering, Hongik University, 30016, Republic of Korea (email: beongku@hongik.ac.kr).

analog-to-digital conversion (ADC) by subtracting a predicted copy of the SI channel. In the digital-domain cancellation, the SI channel is canceled after ADC as the last line of defense [9]. After different stages of mitigation [10], [11], the residual self-interference (RSI) component can be decreased up to noise level [8], [9]. It is noteworthy that FD devices can be utilized in wireless transmission to improve the transmission efficiency [3] or protect message against eavesdropping attacks [12].

However, technology advances and/or system requirement increments cause the mathematical model derivation to be more challenging due to the inherently complicated mathematical model. On the other hand, instead of using model-based approach, a data-driven analysis can be carried out by collecting abundant data through a single experiment [13]. To this end, artificial intelligence is the key technique since it can capture the relation between network parameters and system performance without the need to derive closed-form expressions for the performance metrics. Additionally, deep neural network (DNN) model can reduce the computational execution time since it is utilized as a compact mapping function.

A. Related Works and Motivations

One of the solutions to enhance the PHY-security is the user (antenna) selection scheme. It can select the best user (antenna) based on the channel condition. The authors in [14] proposed a transmit antenna selection (TAS) scheme to enhance the PHY-security in multiple-input single-output (MISO)-NOMA system, in which the selected transmit antenna is that one which maximizes the cell-center user's secrecy capacity or cell-center's and cell-edge user's main channel capacity when the passive eavesdropper wiretaps the message. The authors in [15] proposed the max-min-based TAS scheme to improve the secrecy performance in multiple-input multiple-output (MIMO)-NOMA systems, Feng *et al.* in [16] proposed the relay selection scheme to enhance the PHY-security in cooperative NOMA systems in the presence of multiple passive eavesdroppers. Considering MIMO-NOMA systems, two TAS schemes were proposed in [17] to enhance the system secrecy outage probability (SOP) in the presence of a single passive eavesdropper with the aim of finding the best channel condition between the source and the cell-center user, and between the source and the cell-edge user, respectively. In [18], the authors studied the secrecy performance in the two-user NOMA system under reliability outage probability (ROP) constraints. The authors in [19] investigated the impact of imperfect SIC on the secrecy performance with the randomly located eavesdropper. The authors in [20] proposed a jammer selection scheme to protect the confidential information in the uplink NOMA system, while Lv *et al.* in [21] proposed an adaptive cooperative jamming scheme to minimize information leakage in uplink and downlink NOMA with an untrusted relay. All these works have considered a passive eavesdropping attack. On the other hand, assuming the active eavesdropping attack, the authors in [22] proposed a three-stage Stackelberg game to protect messages against active eavesdropping in a cooperative communication system. The authors in [23] addressed the impact of active eavesdropping on secure transmission, in which the transmitter decided whether to transmit data or not based on the receiver's feedback to protect the message against active eavesdropping. In [24], the authors addressed the PHY-security in massive NOMA with a relay acting both as a relaying node and as jammer.

Similar to the active eavesdropper, legitimate users also utilize the artificial noise to protect the legitimate users' transmission against eavesdroppers. The authors in [25] studied the impact of the artificial noise on the NOMA system's secrecy performance. Assuming a base station with multiple antennas, the selected antenna transmits information to receivers, while the other antennas radiate the artificial noise to reduce the eavesdropper channel condition. In [26], the authors exploited PHY-security in a two-way relay NOMA system, where the eavesdropper can overhear the transmission. Though the relay is operated in a FD mode to support two-way relaying, the eavesdropper employed a half-duplex (HD) mode to wiretap the users' signal. In [27], the authors carried out a performance optimization in unmanned aerial vehicle (UAV)-aided NOMA systems. To optimize the throughput, in the first phase, the received power at each receiver is maximized and, in the second phase, the power-splitting ratio and the precoding vectors are jointly optimized to maximize the throughput. However, the works in [25]–[27] assumed a passive eavesdropper.

The aforementioned works [14]–[17] only focused on the user selection scheme to improve PHY-security in the NOMA system against passive eavesdropper. Meanwhile, the researches [22]–[24] studied PHY-security in the presence of active eavesdropper under various network models, while the authors in [25]–[27] addressed the artificial noise to protect the secure message against passive eavesdropping attacks.

Recently, the research of the DNN-based system performance evaluation has been started to replace the model-based approach. The authors in [28] utilized the DNN model to predict the coverage probability in random wireless networks. It is noted that the DNN model overcomes the mathematical approach that can be valid for oversimplified network scenarios. In [29], the authors utilized the DNN model to evaluate secrecy outage performance of ground-to-air communication in the presence of multiple aerial eavesdroppers. From the execution time comparison among Monte Carlo simulations, analytical approaches, and DNN analysis, this latter one significantly reduces the execution time while the performance evaluation's accuracy is maintained. The authors in [30] proposed a DNN-based relay selection scheme in which a DNN model was utilized to predict the system throughput. From the related works [28]–[30], when the system performance analysis becomes intricate from a model-based approach perspective, the DNN-based approach arises as an efficient tool to investigate the performance analysis by providing accurate results and significantly reducing the execution time. Furthermore, some common features of DNN-based analysis are: (i) it does not change the computational cost when the network size is changed; (ii) when the network size is increased, the execution time for throughput evaluation does not much increase while the other scheme significantly increases the execution time.

Based on above, three fundamental questions arise which will be addressed in this paper: (i) In a DL NOMA transmission, how to protect the legitimate transmission from active eavesdropping attacks; (ii) Is it possible to propose a robust PHY-security scheme?; and (iii) Can data-driven method-based performance evaluation replace the role of conventional performance analysis?

B. Contributions and Organization

In this paper, we consider a downlink scenario of a two-user NOMA system in the presence of active eavesdropping attacks. More specifically, the cell-center and cell-edge users act as receiver and jammer at the same time, which means that they not only decode their messages from the received signal but also generate artificial noise (AN) signals to degrade the eavesdropper channel quality. Additionally, we propose a transmitter selection scheme that selects the transmitter which minimizes the maximum eavesdropper capacity for supporting IoT services[1]. The main contributions of this paper can be summarized as follows:

- We propose a novel FD-enabled NOMA system to support secure transmission against active eavesdropping attack. The cell-center and cell-edge users act as receiver and AN-based jammer at the same time to overcome the active eavesdropping attacks. Additionally, we consider the practical scenario, in which imperfect SIC occurs due to the fact that cell-edge user's message is not perfectly eliminated from the received signal at the cell-center user.
- We propose a transmitter selection scheme to support secure transmission against active eavesdropping on FD-enabled NOMA systems. More specifically, the proposed transmitter selection scheme, called the minimal transmitter selection (MTS) scheme, can select the best transmitter that minimizes the maximum eavesdropper channel capacity. The proposed MTS scheme requires low computational complexity while achieving secrecy performance maintains against active eavesdropping attack.
- Different from previous works, the proposed FD-enabled NOMA system considers two kinds of artificial noise to reduce and to confuse the cell-center and cell-edge users' decoding. Additionally, we build a DNN model for SOP evaluation. It arises as an efficient evaluation tool when closed-form expressions for the performance metrics are hard to attain through analytical approaches. Though the DNN approach requires a huge number of sample datasets for DNN model training, it can estimate the complicated system performance by reducing the performance complexity from high non-linear functions.
- It is shown that the proposed FD-enabled NOMA network and MTS scheme improve the secrecy performance compared to that of conventional NOMA system and the random transmitter selection (RTS) scheme, respectively, against the active eavesdropping attack. Although the proposed MTS scheme provides sub-optimal secrecy performance, it requires low-complexity compared to that of the optimal transmitter selection (OTS) scheme since it only uses the eavesdropper channel information to select the transmitter. Besides, we provide the brute-force searching algorithm to optimize the system secrecy performance, which relies on the optimal points of transmit power and power allocation coefficient. It is noted that to provide a reproducible research, our simulation code has been made available at https://github.com/trinhudo/PHY_Security_NOMA_FD_DNN.

[1]The authors in [31] proposed the method how to achieve the eavesdropper channel information. More specifically, the network employs the torch nodes, which place the eavesdropper near and feedback the channel information instead of the eavesdropper's one. Thus, the legitimate users can estimate the eavesdropper channel information through the torch node's channel information.

The rest of the paper is organized as follows: In Section II, we describe the proposed NOMA system model and transmitter selection scheme. Section III derives a tight approximated closed-form expression for SOP, while the DNN model to estimate SOP is introduced in Section IV. Section V presents representative numerical results based on the derived analytical results as well as the DNN model predictions. Finally, this paper is concluded in Section VI.

Notations: $\mathbb{E}[\cdot]$ denotes the expectation; $F_X(x)$ and $f_X(x)$ represent the cumulative distribution function (CDF) and the probability density function (PDF) of the random variable X, respectively; $\Pr(\mathrm{A})$ means the probability that the event A occurs; $\mathcal{CN}(0, \sigma^2)$ denotes a circular symmetric complex Gaussian random variable with zero-mean with variance σ^2.

II. System Model

A. System and Channel Descriptions

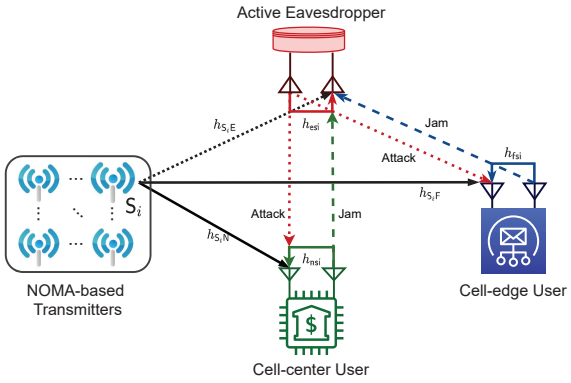


Fig. 1. Schematic illustration of NOMA system with FD receivers and one active eavesdropper.

We consider a downlink scenario of a FD-enabled two-user NOMA system, as depicted in Fig. 1, where a set of K single-antenna transmitters, $\mathcal{S} = \{\mathsf{S}_i \mid i = 1, 2, \ldots, K\}$, transmits message to a cell-center user, denoted by User N, and a cell-edge user, denoted by User F. Meanwhile, an eavesdropper overhears the transmitter's legitimate transmissions to the pair of cell-center and cell-edge users. We assume that the transmitter operates in HD mode, while the cell-center, cell-edge users, and eavesdropper operate in FD mode.

The operation in each coherent time block is divided into two processes, called transmitter selection and data transmission processes, and can be summarized as follows:

- ***Transmitter selection process*:** It is executed before data transmission, in which each channel coefficient is estimated through the signaling and control message exchange to adaptively select the transmitter to overcome against the eavesdropper wiretapping attempts.
- ***Data transmission process*:** The selected user equipment (UE) simultaneously transmits the messages of User N and User F using superposition coding. The operation of two kinds of UEs, namely legitimate users and eavesdropper, are, respectively, explained as follows:
  ***i) At the legitimate users*:** Because the legitimate receivers are FD nodes, they concurrently act as receiver and AN-based jamming node to degrade the eavesdropper channel condition.
  ***ii) At the eavesdropper*:** Due to active eavesdropper, the eavesdropper wiretaps and interferes with the legitimate user's transmission simultaneously. Because the eavesdropper has a strong performance ability to detect [25], the eavesdropper perfectly separates each message from the overheard observations.

Let the channel from X to Y, where $\mathsf{X} \in \mathcal{S} \cup \{\mathsf{N}, \mathsf{F}, \mathsf{E}\}$, and $\mathsf{Y} \in \{\mathsf{N}, \mathsf{F}, \mathsf{E}\}$, contains the small-scale fading ($\tilde{h}_{\mathsf{XY}}$) and large-scale path-loss effect (G_{XY}) [32]. We assume that all wireless channels, except for the SI channel whose distribution is unknown [33], [34], exhibit Rayleigh flat block fading. Since the small-scale fading magnitude, $|\tilde{h}_{\mathsf{XY}}|$, follows Rayleigh distribution, the corresponding fading gain, $|\tilde{h}_{\mathsf{XY}}|^2$, follows Exponential distribution, whose CDF, $F_{|\tilde{h}_{\mathsf{XY}}|^2}(h)$, and PDF, $f_{|\tilde{h}_{\mathsf{XY}}|^2}(h)$, can be described as $F_{|\tilde{h}_{\mathsf{XY}}|^2}(h) = 1 - e^{-\frac{h}{\tilde{\lambda}_{\mathsf{XY}}}}$, $f_{|\tilde{h}_{\mathsf{XY}}|^2}(h) = \frac{1}{\tilde{\lambda}_{\mathsf{XY}}} e^{-\frac{h}{\tilde{\lambda}_{\mathsf{XY}}}}$, respectively, where $\tilde{\lambda}_{\mathsf{XY}}$ denotes the average of $|\tilde{h}_{\mathsf{XY}}|^2$ [3]. On the other hand, the large-scale path-loss effect can be described as $G_{\mathsf{XY}} = (d_{\mathsf{XY}}/d_0)^{-\epsilon}\mathcal{L}$ [3], where d_{XY} indicates Euclidean distance between X and Y, d_0 denotes the reference distance, $\mathcal{L}$ means the power attenuation at d_0 (dB unit), and ϵ stands for the path-loss exponent. Furthermore, the received signal at Y, which is transmitted from X, can be expressed as

$$y_{\mathsf{Y}} = \sqrt{P_{\mathsf{X}} G_{\mathsf{XY}}}\tilde{h}_{\mathsf{XY}} x_{\mathsf{X}} + n_{\mathsf{Y}}, \tag{1}$$

where P_{X} presents the transmit power of X, x_{X} stands for the transmit signal, and n_{Y} indicates the additive white Gaussian noise (AWGN) at Y. In this paper, to alleviate notation, let $h_{\mathsf{XY}} \triangleq G_{\mathsf{XY}}\tilde{h}_{\mathsf{XY}}$. Consequently, the channel models are considered both small-scale fading and large-scale path-loss effect, respectively. Thus, the CDF, $F_{|h_{\mathsf{XY}}|^2}(h)$, and PDF, $f_{|h_{\mathsf{XY}}|^2}(h)$, of $|h_{\mathsf{XY}}|^2$ can be obtained as $F_{|h_{\mathsf{XY}}|^2}(h) = 1 - e^{-\frac{h}{\lambda_{\mathsf{XY}}}}$, $f_{|h_{\mathsf{XY}}|^2}(h) = \frac{1}{\lambda_{\mathsf{XY}}} e^{-\frac{h}{\lambda_{\mathsf{XY}}}}$, respectively, where λ_{XY} is the mean of $|h_{\mathsf{XY}}|^2$.

B. Data Transmission Process

1) NOMA Transmission at S_i: According to NOMA principle, S_i transmits a superimposed signal, i.e., $\sqrt{\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{\theta_{\mathsf{F}}}x_{\mathsf{F}}$, where x_{N} and x_{F} indicate the normalized signal for User N and User F, and θ_{N} and θ_{F} denote the power allocation coefficients of User N and User F, respectively. It is assumed that $|h_{\mathsf{S}_i\mathsf{N}}|^2 > |h_{\mathsf{S}_i\mathsf{F}}|^2$, $\theta_{\mathsf{N}} < \theta_{\mathsf{F}}$, $\theta_{\mathsf{N}} + \theta_{\mathsf{F}} = 1$ [25].

2) At User N: The received observation at User N, $y_{\mathsf{S}_i\mathsf{N}}$, can be expressed as

$$\begin{aligned} y_{\mathsf{S}_i\mathsf{N}} = &\underbrace{(\sqrt{P_i\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{P_i\theta_{\mathsf{F}}}x_{\mathsf{F}})h_{\mathsf{S}_i\mathsf{N}}}_{\text{desired part}} \\ &+ \underbrace{\sqrt{P_{\mathsf{E}}}s_{\mathsf{E}}h_{\mathsf{EN}}}_{\text{interference}} + \underbrace{\sqrt{P_{\mathsf{N}}}s_{\mathsf{N}}h_{\mathsf{nsi}}}_{\text{self-interference}} + n_{\mathsf{N}}, \end{aligned} \tag{2}$$

where P_i represents the transmit power at S_i, P_{N} indicates the transmit power at User N to confuse the eavesdropper, P_{E} means the transmit power at User E to radiate the artificial noise, and $n_{\mathsf{N}} \sim \mathcal{CN}(0, \sigma_{\mathsf{N}}^2)$.

After different stages of mitigation [11], the received observation with the RSI component at User N, $y_{\mathsf{S}_i\mathsf{N}}^{\mathsf{re}}$, can be expressed as

$$y_{\mathsf{S}_i\mathsf{N}}^{\mathsf{re}} = (\sqrt{P_i\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{P_i\theta_{\mathsf{F}}}x_{\mathsf{F}})h_{\mathsf{S}_i\mathsf{N}} + \sqrt{P_{\mathsf{E}}}s_{\mathsf{E}}h_{\mathsf{EN}} + n_{\mathsf{nsi}} + n_{\mathsf{N}}, \tag{3}$$

where the superscript "re" stands for the RSI component, and $n_{\mathsf{nsi}} \sim \mathcal{CN}(0, \sigma_{\mathsf{nsi}})$. Thus, the signal-to-interference-plus-noise ratio (SINR) at User N to decode x_{F}, $\gamma_{\mathsf{S}_i\mathsf{N},x_{\mathsf{F}}}$, can be expressed as

$$\gamma_{\mathsf{S}_i\mathsf{N},x_{\mathsf{F}}} = \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}. \tag{4}$$

After imperfect SIC process, the SINR at User N to decode x_{F}, $\gamma_{\mathsf{S}_i,\mathsf{N},x_{\mathsf{N}}}$, can be expressed as

$$\gamma_{\mathsf{S}_i\mathsf{N},x_{\mathsf{N}}} = \frac{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\beta\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}, \tag{5}$$

where β, $0 \le \beta \le 1$, is the level of residual interference caused by imperfect SIC [35]. As a particular case, $\beta = 0$ and $\beta = 1$ represent the perfect SIC and imperfect SIC, respectively.

3) At User F: Since User F operates in FD mode, the received signal at User F, $y_{\mathsf{S}_i\mathsf{F}}$, can be expressed as

$$\begin{aligned} y_{\mathsf{S}_i\mathsf{F}} = &(\sqrt{P_i\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{P_i\theta_{\mathsf{F}}}x_{\mathsf{F}})h_{\mathsf{S}_i\mathsf{F}} \\ &+ \sqrt{P_{\mathsf{E}}}s_{\mathsf{E}}h_{\mathsf{EF}} + \sqrt{P_{\mathsf{F}}}s_{\mathsf{F}}h_{\mathsf{fsi}} + n_{\mathsf{F}}, \end{aligned} \tag{6}$$

where P_{F} represents the transmit power of User F to degrade the channel capacity of eavesdropper link, and $n_{\mathsf{F}} \sim \mathcal{CN}(0, \sigma_{\mathsf{F}}^2)$. User F also employs different stages of mitigation to degrade the SI channel from the received observation. Thus, after mitigation stages, the received observation with the RSI component at User F, $y_{\mathsf{S}_i\mathsf{F}}^{\mathsf{re}}$, can be expressed as

$$y_{\mathsf{S}_i\mathsf{F}}^{\mathsf{re}} = (\sqrt{P_i\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{P_i\theta_{\mathsf{F}}}x_{\mathsf{F}})h_{\mathsf{S}_i\mathsf{F}} + \sqrt{P_{\mathsf{E}}}s_{\mathsf{E}}h_{\mathsf{EF}} + n_{\mathsf{fsi}} + n_{\mathsf{F}}, \tag{7}$$

where $n_{\mathsf{fsi}} \sim \mathcal{CN}(0, \sigma_{\mathsf{fsi}}^2)$. Different from User N, since for the cell-edge user's message is allocated higher transmit power than the cell-center user's message, User F directly decodes its own message from (7). Thus, the SINR at User F to decode x_{F}, $\gamma_{\mathsf{S}_i\mathsf{F},x_{\mathsf{F}}}$, can be expressed as

$$\gamma_{\mathsf{S}_i\mathsf{F},x_{\mathsf{F}}} = \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{F}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{F}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EF}}|^2 + \sigma_{\mathsf{fsi}}^2 + \sigma_{\mathsf{F}}^2}. \tag{8}$$

4) At User E*:* The eavesdropper tries to overhear the legitimate users' transmission. Thus, the wiretapped signal at eavesdropper can be expressed as

$$\begin{aligned} y_{\mathsf{S}_i\mathsf{E}} = (\sqrt{P_i\theta_{\mathsf{N}}}x_{\mathsf{N}} + \sqrt{P_i\theta_{\mathsf{F}}}x_{\mathsf{F}})h_{\mathsf{S}_i\mathsf{E}} \\ + \sqrt{P_{\mathsf{N}}}s_{\mathsf{N}}h_{\mathsf{NE}} + \sqrt{P_{\mathsf{F}}}s_{\mathsf{F}}h_{\mathsf{FE}} + \sqrt{P_{\mathsf{E}}}s_{\mathsf{E}}h_{\mathsf{esi}} + n_{\mathsf{E}}, \end{aligned} \tag{9}$$

where $n_{\mathsf{E}} \sim \mathcal{CN}(0, \sigma_{\mathsf{E}}^2)$. In order to consider one of the worst scenarios, even though the eavesdropper can not null out the artificial noise from the received signal, we assume that the eavesdropper has strong detection and performance capabilities to correctly distinguish each user's message from the wiretapped signal [25]. Thus, after different stages of mitigation, the SINRs of cell-center user message, x_{N}, and cell-edge user message, x_{F}, at User E can be, respectively, expressed as

$$\gamma_{\mathsf{S}_i\mathsf{E},x_m} = \frac{P_i\theta_m|h_{\mathsf{S}_i\mathsf{E}}|^2}{P_{\mathsf{N}}|h_{\mathsf{NE}}|^2 + P_{\mathsf{F}}|h_{\mathsf{FE}}|^2 + \sigma_{\mathsf{esi}}^2 + \sigma_{\mathsf{E}}^2}, \tag{10}$$

where $m \in \{\mathsf{N}, \mathsf{F}\}$,

In order to analyze the secrecy performance of the considered networks, the main channel capacity of cell-center user's message, x_{N}, and cell-edge user's message, x_{F}, at User N can be, respectively, expressed as

$$\begin{aligned} C_{\mathsf{N},x_{\mathsf{N}}} &= \log_2(1 + \gamma_{\mathsf{S}_i\mathsf{N},x_{\mathsf{N}}}) \\ &= \log_2\left(1 + \frac{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\beta\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}\right), \end{aligned} \tag{11}$$

$$\begin{aligned} C_{\mathsf{N},x_{\mathsf{F}}} &= \log_2(1 + \gamma_{\mathsf{S}_i\mathsf{N},x_{\mathsf{F}}}) \\ &= \log_2\left(1 + \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}\right). \end{aligned} \tag{12}$$

By its turn, the main channel capacity of cell-edge user's message, x_{F}, at User F can be expressed as

$$\begin{aligned} C_{\mathsf{F},x_{\mathsf{F}}} &= \log_2(1 + \gamma_{\mathsf{S}_i\mathsf{F},x_{\mathsf{F}}}) \\ &= \log_2\left(1 + \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{F}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{F}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EF}}|^2 + \sigma_{\mathsf{fsi}}^2 + \sigma_{\mathsf{F}}^2}\right). \end{aligned} \tag{13}$$

Finally, the eavesdropper channel capacity of cell-center user's message, x_{N}, and cell-edge user's message, x_{F}, at User E can be, respectively, expressed as

$$\begin{aligned} C_{\mathsf{E},x_m} &= \log_2(1 + \gamma_{\mathsf{S}_i\mathsf{E},x_m}) \\ &= \log_2\left(1 + \frac{P_i\theta_m|h_{\mathsf{S}_i\mathsf{E}}|^2}{P_{\mathsf{N}}|h_{\mathsf{NE}}|^2 + P_{\mathsf{F}}|h_{\mathsf{FE}}|^2 + \sigma_{\mathsf{esi}}^2 + \sigma_{\mathsf{E}}^2}\right), \end{aligned} \tag{14}$$

where $m \in \{\mathsf{N}, \mathsf{F}\}$. Thus, the secrecy capacity of cell-center user's message and cell-edge user's message can be, respectively, expressed as

$$C_{s,m} = [C_{m,x_m} - C_{\mathsf{E},x_m}]^+ = \left[\log_2\left(\frac{1 + \gamma_{\mathsf{S}_i m,x_m}}{1 + \gamma_{\mathsf{S}_i\mathsf{E},x_m}}\right)\right]^+, \tag{15}$$

where $m \in \{\mathsf{N}, \mathsf{F}\}$ and $\left[x\right]^+ \triangleq \max\left[x, 0\right]$. As in [7], [36], it is assumed that the transmitter perfectly knows the eavesdropper channel for carrying out transmitter selection. In this case, the eavesdropper channel condition is evaluated through the torch nodes' channel feedback.

C. The Proposed Transmitter Selection Schemes

As aforementioned, the transmitter selection process is conducted before data transmission through the signaling and channel state information estimation/calculation system. It is considered that channel state information of the respective links are available. Let S_b denote the selected transmitter; thus, the considered transmitter selection schemes are described as follows.

1) Random Transmitter Selection (RTS) Scheme: The RTS scheme is considered as baseline scheme for comparing the proposed scheme's performance. The RTS scheme randomly selects a single transmitter. Thus, the SINRs of cell-center user's message and cell-edge user's message at User N can be, respectively, expressed as

$$\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{N},x_{\mathsf{N}}} = \frac{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\beta\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}, \tag{16}$$

$$\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{N},x_{\mathsf{F}}} = \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{N}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}. \tag{17}$$

Similar to User N, the instantaneous SINR at User F to decode x_{F}, $\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{F},x_{\mathsf{F}}}$, can be expressed as

$$\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{F},x_{\mathsf{F}}} = \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{F}}|^2}{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{F}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EF}}|^2 + \sigma_{\mathsf{fsi}}^2 + \sigma_{\mathsf{F}}^2}. \tag{18}$$

The eavesdropper channel SINRs to overhear x_{N} and x_{F}, $\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{E},x_{\mathsf{N}}}$ and $\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{E},x_{\mathsf{F}}}$, are mathematically expressed as

$$\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{E},x_{\mathsf{N}}} = \frac{P_i\theta_{\mathsf{N}}|h_{\mathsf{S}_i\mathsf{E}}|^2}{P_{\mathsf{N}}|h_{\mathsf{NE}}|^2 + P_{\mathsf{F}}|h_{\mathsf{FE}}|^2 + \sigma_{\mathsf{esi}}^2 + \sigma_{\mathsf{E}}^2}, \tag{19}$$

$$\gamma^{\mathsf{RTS}}_{\mathsf{S}_b\mathsf{E},x_{\mathsf{F}}} = \frac{P_i\theta_{\mathsf{F}}|h_{\mathsf{S}_i\mathsf{E}}|^2}{P_{\mathsf{N}}|h_{\mathsf{NE}}|^2 + P_{\mathsf{F}}|h_{\mathsf{FE}}|^2 + \sigma_{\mathsf{esi}}^2 + \sigma_{\mathsf{E}}^2}. \tag{20}$$

It is noted that the RTS scheme selects a transmitter without channel information feedback [37]. Therefore, as shown in (16) − (20), the SINR with the RTS scheme has the same meaning as the conventional scheduling scheme, such as round-robin, so that it does not require the channel conditions [37].

2) Minimal Transmitter Selection (MTS) Scheme: It selects the transmitter which minimizes the maximum eavesdropper channel capacity among the cluster of transmitters. Thus, the selected criterion of the MTS scheme can be mathematically expressed as

$$\begin{aligned} \mathsf{S}_b &= \arg\min_{1\le i\le K}\left\{\max\{C_{\mathsf{E},x_{\mathsf{N}}},\ C_{\mathsf{E},x_{\mathsf{F}}}\}\right\} \\ &= \arg\min_{1\le i\le K}\left\{\max\{\log_2(1+\gamma_{\mathsf{S}_i\mathsf{E},x_{\mathsf{N}}}),\ \log_2(1+\gamma_{\mathsf{S}_i\mathsf{E},x_{\mathsf{F}}})\}\right\}. \end{aligned} \tag{21}$$

In the MTS scheme, the instantaneous SINRs to decode x_{N} and x_{F} at User N, $\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_{\mathsf{F}}}$ and $\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_{\mathsf{N}}}$, can be, respectively, expressed as

$$\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_{\mathsf{N}}} = \frac{P_b\theta_{\mathsf{N}}|h_{\mathsf{S}_b\mathsf{N}}|^2}{P_b\beta\theta_{\mathsf{F}}|h_{\mathsf{S}_b\mathsf{N}}|^2 + P_{\mathsf{E}}|h_{\mathsf{EN}}|^2 + \sigma_{\mathsf{nsi}}^2 + \sigma_{\mathsf{N}}^2}, \tag{22}$$

$$\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}} = \frac{P_b\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{N}}|^2}{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{N}}|^2 + P_\mathsf{E}|h_{\mathsf{EN}}|^2 + \sigma^2_{\mathsf{nsi}} + \sigma^2_\mathsf{N}}. \quad (23)$$

Similar to User N, the SINR to decode x_F at User F, $\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}}$, can be expressed as

$$\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{F},x_\mathsf{F}} = \frac{P_b\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{F}}|^2}{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{F}}|^2 + P_\mathsf{E}|h_{\mathsf{EF}}|^2 + \sigma^2_{\mathsf{fsi}} + \sigma^2_\mathsf{F}}. \quad (24)$$

The instantaneous SINRs at eavesdropper to overhear x_N and x_F, $\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}}$ and $\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}}$, can be expressed as

$$\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}} = \frac{\min_{i\in\mathcal{S}}\{P_i\theta_\mathsf{N}|h_{\mathsf{S}_i\mathsf{E}}|^2\}}{P_\mathsf{N}|h_{\mathsf{NE}}|^2 + P_\mathsf{F}|h_{\mathsf{FE}}|^2 + \sigma^2_{\mathsf{esi}} + \sigma^2_\mathsf{E}}, \quad (25)$$

$$\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{F}} = \frac{\min_{i\in\mathcal{S}}\{P_i\theta_\mathsf{F}|h_{\mathsf{S}_i\mathsf{E}}|^2\}}{P_\mathsf{N}|h_{\mathsf{NE}}|^2 + P_\mathsf{F}|h_{\mathsf{FE}}|^2 + \sigma^2_{\mathsf{esi}} + \sigma^2_\mathsf{E}}. \quad (26)$$

The difference between the RTS and MTS scheme relies on the fact that the MTS scheme improves the secrecy performance since it selects the transmitter to avoid the vulnerable transmitter against active eavesdropping attack. This channel information can be reported to the transmitter through the signaling and channel feedback process [3].

3) Optimal Transmitter Selection (OTS) Scheme: The OTS scheme is used as the benchmark scheme. It selects the transmitter which maximizes the sum secrecy capacity that can be mathematically written as

$$\begin{aligned}\mathsf{S}_b &= \arg\max_{1\le i\le K}\left\{C_{S,x_\mathsf{N}} + C_{S,x_\mathsf{F}}\right\}\\ &= \arg\max_{1\le i\le K}\left\{\log_2\left(\frac{(1+\gamma_{\mathsf{S}_i\mathsf{N},x_\mathsf{N}})}{(1+\gamma_{\mathsf{S}_i\mathsf{E},x_\mathsf{N}})}\right)\right.\\ &\qquad\left.+\log_2\left(\frac{(1+\gamma_{\mathsf{S}_i\mathsf{F},x_\mathsf{F}})}{(1+\gamma_{\mathsf{S}_i\mathsf{E},x_\mathsf{F}})}\right)\right\}.\end{aligned} \quad (27)$$

Relying on the property of logarithm, (27) can be further simplified as

$$\mathsf{S}_b = \arg\max_{1\le i\le K}\left\{\log_2\left(\frac{(1+\gamma_{\mathsf{S}_i\mathsf{N},x_\mathsf{N}})(1+\gamma_{\mathsf{S}_i\mathsf{F},x_\mathsf{F}})}{(1+\gamma_{\mathsf{S}_i\mathsf{E},x_\mathsf{N}})(1+\gamma_{\mathsf{S}_i\mathsf{E},x_\mathsf{F}})}\right)\right\}. \quad (28)$$

The instantaneous SINRs to decode x_N and x_F at User N, $\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{N}}$ and $\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}}$, can be expressed as

$$\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{N}} = \frac{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{N}}|^2}{P_b\beta\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{N}}|^2 + P_\mathsf{E}|h_{\mathsf{EN}}|^2 + \sigma^2_{\mathsf{nsi}} + \sigma^2_\mathsf{N}}, \quad (29)$$

$$\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}} = \frac{P_b\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{N}}|^2}{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{N}}|^2 + P_\mathsf{E}|h_{\mathsf{EN}}|^2 + \sigma^2_{\mathsf{nsi}} + \sigma^2_\mathsf{N}}. \quad (30)$$

Similarly, the instantaneous SINRs to decode x_F at User F, $\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}}$, can be expressed as

$$\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{F},x_\mathsf{F}} = \frac{P_b\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{F}}|^2}{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{F}}|^2 + P_\mathsf{E}|h_{\mathsf{EF}}|^2 + \sigma^2_{\mathsf{fsi}} + \sigma^2_\mathsf{F}}. \quad (31)$$

In addition, the instantaneous SINRs to decode x_N and x_F at User E, $\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}}$ and $\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{F}}$, can be expressed as

$$\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}} = \frac{P_b\theta_\mathsf{N}|h_{\mathsf{S}_b\mathsf{E}}|^2}{P_\mathsf{N}|h_{\mathsf{NE}}|^2 + P_\mathsf{F}|h_{\mathsf{FE}}|^2 + \sigma^2_{\mathsf{esi}} + \sigma^2_\mathsf{E}}, \quad (32)$$

$$\gamma^{\mathsf{OTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{F}} = \frac{P_b\theta_\mathsf{F}|h_{\mathsf{S}_b\mathsf{E}}|^2}{P_\mathsf{N}|h_{\mathsf{NE}}|^2 + P_\mathsf{F}|h_{\mathsf{FE}}|^2 + \sigma^2_{\mathsf{esi}} + \sigma^2_\mathsf{E}}. \quad (33)$$

As can be seen from (28), the OTS scheme requires a high computational complexity when the transmitter selects. Therefore, the main purpose of the MTS scheme is to reduce the computational complexity, while the our scheme still providing secure transmission.

III. Secrecy Outage Performance Analysis

In PHY-security context, the secrecy outage probability (SOP) is utilized as one of the performance evaluation metrics. It is given by the probability that the difference between main and eavesdropper channels' capacities is below a predefined threshold, called secrecy target data rate (bps/Hz) [25]. It has practical appeal to examine scenarios where User N fails to perfectly eliminate the cell-edge user's message from the received signal. According to total probability theorem [38], the SOP of the cell-center user's message at User N, $P_{\mathtt{out},\mathsf{N}}$, can be mathematically formulated as [39]

$$\begin{aligned}&P_{\mathtt{out},\mathsf{N}}\\ &= \underbrace{\Pr\left[C_{s,\mathsf{N}} < R_{\mathtt{th},x_\mathsf{N}} | C_{\mathsf{N},x_\mathsf{F}} \ge R_{\mathtt{d},x_\mathsf{F}}\right]}_{A_1}\underbrace{\Pr\left[C_{\mathsf{N},x_\mathsf{F}} \ge R_{\mathtt{d},x_\mathsf{F}}\right]}_{A_2}\\ &+ \underbrace{\Pr\left[C_{s,\mathsf{N}} < R_{\mathtt{th},x_\mathsf{N}} | C_{\mathsf{N},x_\mathsf{F}} < R_{\mathtt{d},x_\mathsf{F}}\right]}_{B_1}\underbrace{\Pr\left[C_{\mathsf{N},x_\mathsf{F}} < R_{\mathtt{d},x_\mathsf{F}}\right]}_{B_2},\end{aligned} \quad (34)$$

where $R_{\mathtt{th},x_\mathsf{N}}$ (bps/Hz) and $R_{\mathtt{d},x_\mathsf{F}}$ stand for, respectively, the secrecy target data rate of cell-center user's message and the codeword rate for decoding cell-edge user's message at User N [2], A_1 denotes the probability that the secrecy capacity of the cell-center user's message is smaller than that of the predefined target data rate conditioned on User N successively decodes the cell-edge user's message, x_F, A_2 means the probability that the cell-center user perfectly decodes the message of cell-edge user at User N, B_1 represents the probability that the secrecy capacity of cell-center user's message, x_N, is below the secrecy target data rate conditioned on User N fails to decode the cell-edge user's message, x_F, and B_2 represents the probability that the cell-center user fails to decode cell-edge user's message, x_F. In this case, User N can not decode the cell-center user's message, x_N; thus, the probability of B_1 is equal to one [39]. Relying on the definition of conditional probability [38], $P_{\mathtt{out},\mathsf{N}}$ can be simplified as

$$\begin{aligned}P_{\mathtt{out},\mathsf{N}} &= \Pr\left[C_{s,\mathsf{N}} < R_{\mathtt{th},x_\mathsf{N}}, C_{\mathsf{N},x_\mathsf{F}} \ge R_{\mathtt{d},x_\mathsf{F}}\right]\\ &\quad+\Pr\left[C_{\mathsf{N},x_\mathsf{F}} < R_{\mathtt{d},x_\mathsf{F}}\right].\end{aligned} \quad (35)$$

Different from the case of cell-center user's message at User F, since the power allocation coefficient of User F is higher than that of User N [40], the cell-edge user's message can be directly decoded from the received observation. Thus, the SOP of cell-edge user's message at User F can be mathematically expressed as [39]

$$P_{\mathtt{out},\mathsf{F}} = \Pr\left[C_{s,x_\mathsf{F}} < R_{\mathtt{th},x_\mathsf{F}}\right]. \quad (36)$$

In this paper, without loss of generality, we assume that both the RSI component and channel noise at each user is equal,

i.e., $\sigma^2_{\mathsf{nsi}} = \sigma^2_{\mathsf{fsi}} = \sigma^2_{\mathsf{esi}} = \sigma^2$ and $\sigma^2_{\mathsf{N}} = \sigma^2_{\mathsf{F}} = \sigma^2_{\mathsf{E}} = \sigma^2$, respectively. We further assume that the transmit power of each transmitter is equal, i.e., $P_1 = P_2 = \cdots = P_K = P_{\mathsf{S}}$, and $R_{\mathtt{th},x_{\mathsf{F}}} = R_{\mathtt{d},x_{\mathsf{F}}}$. In addition, for the sake of simplicity, let $X_i \triangleq |h_{\mathsf{S}_i\mathsf{N}}|^2$, $Y_i \triangleq |h_{\mathsf{S}_i\mathsf{F}}|^2$, $Z_i \triangleq |h_{\mathsf{S}_i\mathsf{E}}|^2$, $T \triangleq |h_{\mathsf{NE}}|^2$, $U \triangleq |h_{\mathsf{RE}}|^2$, $V \triangleq |h_{\mathsf{EN}}|^2$, and $W \triangleq |h_{\mathsf{EF}}|^2$. The defined constants are presented in Table I and next it follows self-defined functions (37) - (40) which will be used along the analysis.

TABLE I
SELF-DEFINED CONSTANTS

$\bar{\gamma}_{\mathsf{S}} = P_{\mathsf{S}}/\sigma^2$	$\bar{\gamma}_{\mathsf{N}} = P_{\mathsf{N}}/\sigma^2$
$\bar{\gamma}_{\mathsf{F}} = P_{\mathsf{F}}/\sigma^2$	$\bar{\gamma}_{\mathsf{E}} = P_{\mathsf{E}}/\sigma^2$
$\alpha_1 = \gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}\lambda_{\mathsf{SE}}$	$\alpha_2 = \gamma_{\mathtt{th},x_{\mathsf{F}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{F}}\lambda_{\mathsf{SE}}$
$\alpha_3 = \gamma_{\mathsf{N}}\lambda_{\mathsf{NE}}$	$\alpha_4 = \gamma_{\mathsf{F}}\lambda_{\mathsf{FE}}$
$\alpha_5 = K\gamma_{\mathsf{N}}\lambda_{\mathsf{NE}}$	$\alpha_6 = K\gamma_{\mathsf{F}}\lambda_{\mathsf{FE}}$

$$\Lambda(a,b,x) = \frac{a}{bx+a}, \tag{37}$$

$$\Lambda(a,b,c,x) = \frac{a}{(bx+a)(cx+a)}, \tag{38}$$

$$\Lambda(a,b,c,K,x) = \frac{ab}{bx+a} + \frac{ac}{cx+a} + 2K, \tag{39}$$

$$\mathcal{F}(a,b,c,d,x) = \frac{\bar{\gamma}_{\mathsf{S}}(a-bx)c}{\bar{\gamma}_{\mathsf{E}}xd + \bar{\gamma}_{\mathsf{S}}(a-bx)c}e^{-\frac{2x}{\bar{\gamma}_{\mathsf{S}}(a-bx)c}}. \tag{40}$$

A. RTS scheme

1) User N*:* The next Lemma will help to obtain a closed-form expression for SOP of User N under the RTS scheme.

Lemma 1. *The CDF and PDF of* $S_1 \triangleq \frac{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}Z_i}{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2}$ *can be, respectively, derived as*

$$F_{S_1}(s) = 1 - \Lambda(\alpha_1,\alpha_3,s)\Lambda(\alpha_1,\alpha_4,s)e^{-\frac{2}{\alpha_1}s}, \tag{41}$$

$$f_{S_1}(s) = \Lambda(\alpha_1,\alpha_3,\alpha_4,1,s)\Lambda(\alpha_1,\alpha_3,\alpha_4,s)e^{-\frac{2}{\alpha_1}s}. \tag{42}$$

Proof: The CDF of S_1 can be given by

$$\begin{aligned} F_{S_1}(s) &= \Pr\left[\frac{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}Z_i}{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2} < s\right] \\ &= \Pr\left[Z_i < \frac{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2}{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}}s\right], \end{aligned} \tag{43}$$

where $\gamma_{\mathtt{th},x_{\mathsf{N}}} \triangleq 2^{R_{\mathtt{th},x_{\mathsf{N}}}}$. $F_{S_1}(s)$ can be further expressed as

$$F_{S_1}(s) = \int_0^\infty \underbrace{\int_0^\infty F_{Z_i}\left(\frac{\bar{\gamma}_{\mathsf{N}}t+\bar{\gamma}_{\mathsf{F}}u+2}{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}}s\right)f_T(t)dt}_{\Xi_1} f_U(u)du. \tag{44}$$

By relying on [41, Eq. 3.310], the integral in Ξ_1 can be further expressed as

$$\Xi_1 = 1 - \frac{\alpha_1}{\alpha_3 s + \alpha_1}e^{-\frac{(\bar{\gamma}_{\mathsf{F}}u+2)s}{\alpha_1}}. \tag{45}$$

By plugging (45) into (44), the CDF of S_1 can be written as

$$\begin{aligned} F_{S_1}(s) =& \frac{1}{\lambda_{\mathsf{FE}}}\int_0^\infty e^{-\frac{1}{\lambda_{\mathsf{FE}}}u}du \\ &- \frac{1}{\lambda_{\mathsf{FE}}}\frac{\alpha_1}{\alpha_3 s+\alpha_1}e^{-\frac{2s}{\alpha_1}}\int_0^\infty e^{-(\frac{\bar{\gamma}_{\mathsf{F}}s}{\alpha_1}+\frac{1}{\lambda_{\mathsf{FE}}})u}du. \end{aligned} \tag{46}$$

By making use of [41, Eq. 3.310], the CDF of S_1 can be obtained as (41). After some algebraic manipulations, one can also obtain the PDF of S_1 as (42), which completes the proof of Lemma 1. ∎

Theorem 1. *A tight approximated closed-form expression for SOP of User* N *under RTS scheme can be derived as*

$$\begin{aligned} P^{\mathsf{RTS}}_{\mathtt{out},\mathsf{N}} \approx 1 - &\sum_{r=1}^{R}\frac{\Omega_1\pi}{2R}\sqrt{1-s_r^2} \\ &\times \mathcal{F}(\theta_{\mathsf{N}},\beta\theta_{\mathsf{F}},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\omega_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)) \\ &\times \Lambda(\alpha_1,\alpha_3,\alpha_4,1,\omega_1)\Lambda(\alpha_1,\alpha_3,\alpha_4,\omega_1)e^{-\frac{2}{\alpha_1}\omega_1}, \end{aligned} \tag{47}$$

where $\Omega_1 \triangleq \frac{\theta_{\mathsf{N}}}{\beta\theta_{\mathsf{F}}} - (\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)$, $s_r = \cos\left(\frac{2r-1}{R}\pi\right)$ *and* $\omega_1 \triangleq \frac{\Omega_1 s_r+\Omega_1}{2}$.

Proof: Please, see Appendix A. ∎

2) User F*:* The next Lemma will help to obtain a closed-form expression for SOP of User F under RTS scheme.

Lemma 2. *The CDF and PDF of* $S_2 \triangleq \frac{\gamma_{\mathtt{th},x_{\mathsf{F}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{F}}Z_i}{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2}$ *can be, respectively, obtained as*

$$F_{S_2}(s) = 1 - \Lambda(\alpha_2,\alpha_3,s)\Lambda(\alpha_2,\alpha_4,s)e^{-\frac{2}{\alpha_2}s}, \tag{48}$$

$$f_{S_2}(s) = \Lambda(\alpha_2,\alpha_3,\alpha_4,1,s)\Lambda(\alpha_2,\alpha_3,\alpha_4,s)e^{-\frac{2}{\alpha_2}s}. \tag{49}$$

Proof: Similar to Lemma 1, the CDF and PDF of S_2 can be obtained as (48) and (49), respectively. ∎

Theorem 2. *A tight approximated closed-form expression for SOP of User* F *under RTS scheme can be derived as*

$$\begin{aligned} P^{\mathsf{RTS}}_{\mathtt{out},\mathsf{F}} \approx 1 - &\sum_{r=1}^{R}\frac{\Omega_2\pi}{2R}\sqrt{1-s_r^2} \\ &\times \mathcal{F}(\theta_{\mathsf{F}},\theta_{\mathsf{N}},\lambda_{\mathsf{SF}},\lambda_{\mathsf{EF}},\omega_2+(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)) \\ &\times \Lambda(\alpha_2,\alpha_3,\alpha_4,1,\omega_2)\Lambda(\alpha_2,\alpha_3,\alpha_4,\omega_2)e^{-\frac{2}{\alpha_2}\omega_2}, \end{aligned} \tag{50}$$

where $\gamma_{\mathtt{th},x_{\mathsf{F}}} \triangleq 2^{R_{\mathtt{th},x_{\mathsf{F}}}}$, $\Omega_2 \triangleq \frac{\theta_{\mathsf{F}}}{\theta_{\mathsf{N}}} - (\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)$ *and* $\omega_2 \triangleq \frac{\Omega_2 s_r+\Omega_2}{2}$. s_r *is defined as* (47).

Proof: Please, see in Appendix B. ∎

B. MTS scheme

1) User N*:* The next Lemma will help to obtain the tight approximated closed-form expression for SOP of User N with the MTS scheme.

Lemma 3. *The CDF and PDF of* $S_3 \triangleq \frac{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}Z_b}{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2}$ *can be, respectively, expressed as*

$$F_{S_3}(s) = 1 - \Lambda(\alpha_1,\alpha_5,s)\Lambda(\alpha_1,\alpha_5,s)e^{-\frac{2K}{\alpha_1}s}, \tag{51}$$

$$f_{S_3}(s) = \Lambda(\alpha_1,\alpha_5,\alpha_6,K,s)\Lambda(\alpha_1,\alpha_5,\alpha_6,s)e^{-\frac{2K}{\alpha_1}s}. \tag{52}$$

Proof: The CDF of S_3 can be re-written as

$$F_{S_3}(s) = \Pr\left[Z_b < \frac{(\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2)s}{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}}\right]. \tag{53}$$

Since the CDF of Z_b is expressed as $F_{Z_b}(z) = 1 - e^{-\frac{K}{\lambda_{\mathsf{SE}}}z}$ [7], [36], $F_{S_3}(s)$ can be further expressed as

$$F_{S_3}(s) = \int_0^\infty \underbrace{\int_0^\infty \left[1 - e^{-\frac{K(\bar{\gamma}_{\mathsf{N}} t + \bar{\gamma}_{\mathsf{F}} u + 2)s}{\gamma_{\mathtt{th},x_{\mathsf{N}}} \bar{\gamma}_{\mathsf{S}} \theta_{\mathsf{N}} \lambda_{\mathsf{SE}}}}\right] f_T(t) dt}_{\Xi_2} f_U(u) du. \tag{54}$$

By making use of [41, Eq. 3.310], Ξ_2 in (54) can be expressed as

$$\Xi_2 = 1 - \frac{\alpha_1}{\alpha_5 s + \alpha_1} e^{-\frac{K(\bar{\gamma}_{\mathsf{F}} u + 2)s}{\alpha_1}}. \tag{55}$$

Thus, by plugging (55) into (54) and relying on [41, Eq. 3.310], the CDF of S_3 can be obtained as in (51) and, further basic mathematical steps, the PDF of S_3 can also be obtained as in (52). ∎

Theorem 3. *A tight approximated closed-form expression for SOP of User* F *under MTS scheme can be derived as*

$$\begin{aligned} P_{\mathtt{out},\mathsf{N}}^{\mathsf{MTS}} \approx 1 - \sum_{r=1}^{R} \frac{\Omega_1 \pi}{2R} \sqrt{1 - s_r^2} \\ \times \mathcal{F}(\theta_{\mathsf{N}}, \beta\theta_{\mathsf{F}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \times \Lambda(\alpha_2, \alpha_5, \alpha_6, K, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \times \Lambda(\alpha_2, \alpha_5, \alpha_6, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) e^{-\frac{2K}{\alpha_2}\omega_1}, \end{aligned} \tag{56}$$

where Ω_1, ω_1 *and* s_r *are defined as in* (47).

Proof: Please, see in Appendix C. ∎

2) User F*:* The next Lemma will help to obtain the closed-form expression for SOP of User F with the MTS scheme.

Lemma 4. *The CDF and PDF of* $S_4 \triangleq \frac{\gamma_{\mathtt{th},x_{\mathsf{F}}} \bar{\gamma}_{\mathsf{S}} \theta_{\mathsf{F}} Z_b}{\bar{\gamma}_{\mathsf{N}} T + \bar{\gamma}_{\mathsf{F}} U + 2}$ *can be, respectively, derived as*

$$F_{S_4}(s) = 1 - \Lambda(\alpha_2, \alpha_5, s)\Lambda(\alpha_2, \alpha_6, s) e^{-\frac{2K}{\alpha_2}s}, \tag{57}$$

$$f_{S_4}(s) = \Lambda(\alpha_2, \alpha_5, \alpha_6, K, s)\Lambda(\alpha_2, \alpha_5, \alpha_6, s) e^{-\frac{2K}{\alpha_2}s}. \tag{58}$$

Proof: The CDF of S_4 can be expressed as

$$\begin{aligned} F_{S_4}(s) &= \Pr\left[\frac{\gamma_{\mathtt{th},x_{\mathsf{F}}} \bar{\gamma}_{\mathsf{S}} \theta_{\mathsf{F}} Z_b}{\bar{\gamma}_{\mathsf{N}} T + \bar{\gamma}_{\mathsf{F}} U + 2} < s\right] \\ &= \Pr\left[Z_b < \frac{(\bar{\gamma}_{\mathsf{N}} T + \bar{\gamma}_{\mathsf{F}} U + 2)s}{\gamma_{\mathtt{th},x_{\mathsf{F}}} \bar{\gamma}_{\mathsf{S}} \theta_{\mathsf{F}}}\right]. \end{aligned} \tag{59}$$

$F_{S_4}(s)$ can be further expressed as

$$F_{S_4}(s) = \int_0^\infty \underbrace{\int_0^\infty F_{Z_b}\left(\frac{(\bar{\gamma}_{\mathsf{N}} t + \bar{\gamma}_{\mathsf{F}} u + 2)s}{\gamma_{\mathtt{th},x_{\mathsf{F}}} \bar{\gamma}_{\mathsf{S}} \theta_{\mathsf{F}}}\right) f_T(t) dt}_{\Xi_3} f_U(u) du. \tag{60}$$

In order to further express the integral in (60), by relying on [41, eq. (3.310)], Ξ_3 can be further obtained as

$$\Xi_3 = 1 - \frac{\alpha_2}{\alpha_5 s + \alpha_2} e^{-\frac{K(\bar{\gamma}_{\mathsf{F}} u + 2)s}{\alpha_2}}. \tag{61}$$

Thus, by plugging (61) into (60) and making use of [41, eq. 3.310], $F_{S_4}(s)$ can be obtained as in (57). After some algebraic steps, the PDF of S_4 can be obtained as in (58), which concludes the proof. ∎

Theorem 4. *A tight approximated closed-form expression for SOP of User* F *under MTS scheme can be derived as*

$$\begin{aligned} P_{\mathtt{out},\mathsf{F}}^{\mathsf{MTS}} \approx 1 - \sum_{r=1}^{R} \frac{\Omega_2 \pi}{2R} \sqrt{1 - s_r^2} \\ \times \mathcal{F}(\theta_{\mathsf{F}}, \theta_{\mathsf{N}}, \lambda_{\mathsf{SF}}, \lambda_{\mathsf{EF}}, \omega_2 + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)) \\ \times \Lambda(\alpha_2, \alpha_5, \alpha_6, K, \omega_2)\Lambda(\alpha_2, \alpha_5, \alpha_6, \omega_2) e^{-\frac{2K}{\alpha_2}\omega_2}, \end{aligned} \tag{62}$$

where s_r *is defined as* (47). Ω_2, ω_2 *are defined as in* (56).

Proof: Please, see in Appendix D. ∎

IV. DNN-BASED SOP EVALUATION

In this section, we design a DNN model to evaluate SOP. The DNN model, as a data-driven approach, becomes an alternative solution when the system model is complex which makes difficult to apply the mathematical derivation approach. In this paper, since the OTS scheme is too intricate for investigating the system performance through closed-form expression, the DNN model will be employed to find the relation between network parameters and the secrecy performance by using a compact mapping function as well as the reducing execution time.

A. Training Data Preparation

The DNN model requires the training step to find the optimal weights and biases of each connection for accurate SOP evaluation. Thus, the model training step needs the trainable datasets, called sample datasets, which consists of input data (networks parameters) and output data (corresponding SOP). The contained networks parameters are the number of transmit users, transmit power of transmitter, User N, User F, and eavesdropper, the distance between transmitter and User N/User F/eavesdropper, power allocation coefficient of User N, secrecy target data rate of User N and User F. Thus, the input data vector ($\mathtt{v} \triangleq D_{in,\mathsf{N}}$ (or $D_{in,\mathsf{F}}$)) contains the following parameters:

$$\mathtt{v} \triangleq [K, P_{\mathsf{S}}, P_{\mathsf{N}}, P_{\mathsf{F}}, P_{\mathsf{E}}, d_{\mathsf{SN}}, d_{\mathsf{SE}}, d_{\mathsf{NE}}, d_{\mathsf{FE}}, \theta_{\mathsf{N}}, R_{\mathtt{th},x_{\mathsf{N}}}, R_{\mathtt{th},x_{\mathsf{F}}}].$$

The values of input data to train the DNN model can be summarized as Table II.

TABLE II
INPUTS PARAMETERS FOR DNN TRAINING AND TESTING

Inputs	Values	Inputs	Values
M	4	P_{S}	[-20: 5: 60] (dB)
P_{N}	[5, 10] (dB)	P_{F}	[5, 10] (dB)
P_{E}	[5, 10] (dB)	d_{SN}	[0.2, 0.4]
d_{SE}	[0.5, 1]	d_{NE}	[0.5, 1]
d_{FE}	[0.5, 1]	θ_{N}	[0.2, 0.4]
$R_{\mathtt{th},x_{\mathsf{N}}}$	[0.1, 0.2] (bps/Hz)	$R_{\mathtt{th},x_{\mathsf{F}}}$	[0.1, 0.2] (bps/Hz)

The n-th output data ($D_{out,\mathsf{N}}[n]$ and $D_{out,\mathsf{F}}[n]$) for User N and User F with the considered networks are, respectively, obtained by using (35) and (36). Consequently, n-th sample

datasets ($D_{Sample,\mathsf{N}}[n]$ and $D_{Sample,\mathsf{F}}[n]$) to train the DNN model contains the following parameters:

$$D_{Sample,\mathsf{N}}[n] = \big[D_{in,\mathsf{N}}[n], D_{out,\mathsf{N}}[n]\big], n \in N,$$

$$D_{Sample,\mathsf{F}}[n] = \big[D_{in,\mathsf{F}}[n], D_{out,\mathsf{F}}[n]\big], n \in N,$$

where N indicates the number of sample datasets.

B. The DNN Model Training

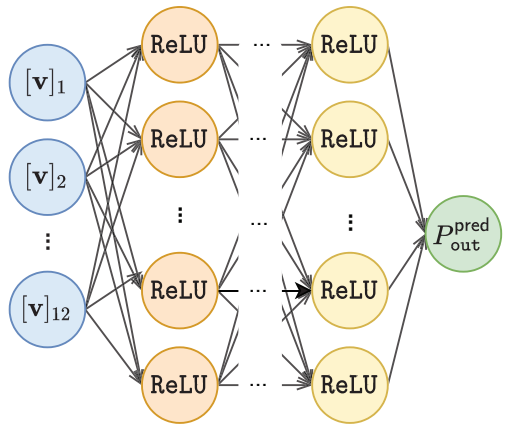


Fig. 2. The construction of a DNN model for SOP prediction.

1) DNN Model Architecture: The DNN model is constructed as three layers, which are input layer, multiple hidden layer, and output layer, as depicted in Fig. 2. The role of each layer to train the DNN model using the sample datasets can be summarized as follows:

- **Input layer:** The input layer receives input data so that the DNN model can find the relation between system parameters and corresponding SOP. Thus, the input layer neurons do not have an activation function, and the number of neurons is identical to the number of network parameters.
- **Hidden layer:** Multiple hidden layers mainly calculates the relation between input data and output data. Thus, each connection in each hidden neuron has different weights and biases to properly calculate the relation. Additionally, each hidden neuron has a non-linear activation function to maximize computational efficiency.
- **Output layer:** The output layer predicts the secrecy performance by synthesizing the results of multiple hidden layers. Therefore, the output layer consists of a single neuron. Similar to the input layer, the output layer's neuron does not have an activation function.

It is noted that the DNN model needs to iteratively update the process of the optimal weights and biases finding at each connection. In the next subsubsection, we explain how to update the weights and biases to find the optimal weights and biases through the sample datasets in detail.

2) The DNN Training: The DNN model calculates the relation between input data and output data using the sample datasets. Using the input data, the DNN model can calculate the connection between j-th neuron of i-th hidden layer and i-th neuron of (l-1)-th layer in n-th sample datasets, $\delta_j^l[n]$, can be expressed as

$$\delta_j^l[n] = g\big(\sum_{i\in N}(w_{ij}^l[n]\delta_i^{l-1}[n] + u_j^l[n])\big), \tag{63}$$

where $g(\cdot)$ represents the activation function. $w_{ij}^l[n]$ and $u_j^l[n]$ indicate the weight between j-th neuron of l-th layer and i-th neuron of (l-1)-th layer and bias in j-th neuron in l-th layer, respectively. The DNN model compares the difference between the DNN model's results ($y[n]$) and the output data of the training datasets ($t[n] \triangleq D_{out}[n]$) by using the loss function and iteratively update the weight and biases. When the DNN model training completes, the DNN model can predict the SOP accurately. It is noted that the DNN model training is operated offline. It means that the DNN model is trained at the network planning step. We only utilize the trained DNN model to evaluate the system performance in a certain time block.

C. Real-Time Prediction

When the offline training is completed, the DNN model has the optimal weights and biases, which can be represented as a compact mapping function, $\mathfrak{F}(\cdot)$. When the new network information is arranged as a new vector ($\mathtt{x}_{\mathtt{new}}$), the result of the DNN model can be written as

$$P_{\mathtt{out}}^{\mathtt{pred}} = \mathfrak{F}(\mathtt{x}_{\mathtt{new}}). \tag{64}$$

From (64), the secrecy outage performance can be predicted by the DNN model in a short execution time. Since the DNN model performance can be improved by adding more hidden layers or hidden neurons, the architecture of DNN is adaptively designed by the performance requirements. For example, the DNN model will need to re-train with a new appropriate training data setting (new learning rate, adjust the number of hidden layers or hidden neurons, new training datasets) until the value of loss function in (64) is smaller than the error threshold.

D. Performance of DNN Model for SOP Prediction

We investigate the accuracy of the DNN model for evaluating SOP. The sample data is generated over $10,000$, where 80% for training, 10% for validation, and the remainder for testing. More specifically, the designed DNN model is equipped with 5 hidden layers, and each hidden layer has 128 hidden neurons, where the hidden neurons adopt the rectified linear unit (ReLU) as the non-linear activation function, which is mathematically defined as [42]

$$g(x) = \max\{x, 0\}. \tag{65}$$

The mean-square-error (MSE) is utilized as the loss function to calculate the estimation accuracy of the DNN model, which is mathematically expressed as

$$\mathrm{MSE}(t[n], y[n]) = \frac{1}{\widetilde{N}}\sum_{n=1}^{\widetilde{N}}(y[n] - t[n])^2, \tag{66}$$

where $\widetilde{N}$ is the number of training samples. Adam optimizer [43] is used to find each connection's optimal weights and biases. Additionally, a callback method is used for the DNN model to adjust the learning rate schedule over time. The setup of the callback is as follows. Initial learning rate is 10^{-2}, minimum learning rate is 10^{-10}, factor is 0.8, patient is 1, batch size is 200, and epoch is 30. The specifications of the system setting for the DNN model training are i7-7700 (CPU), 32GB (RAM), and GeForce GTX 1060 6GB (GPU).

To evaluate the estimation performance of the proposed DNN model, the root-mean-square error (RMSE) is used to measure the accuracy between the predicted SOP and the output data of the test set ($z[n]$). The RMSE can be mathematically written as

$$\begin{aligned}\mathrm{RMSE}(z[n], y[n]) &= \sqrt{\mathrm{MSE}(z[n], y[n])} \\ &= \sqrt{\frac{1}{N_t}\sum_{n=1}^{N_t}(z[n]-y[n])^2},\end{aligned} \tag{67}$$

where N_t represents the number of test set among the sample datasets. When the RMSE is smaller, the predicted SOP and observation are more tightly matched.

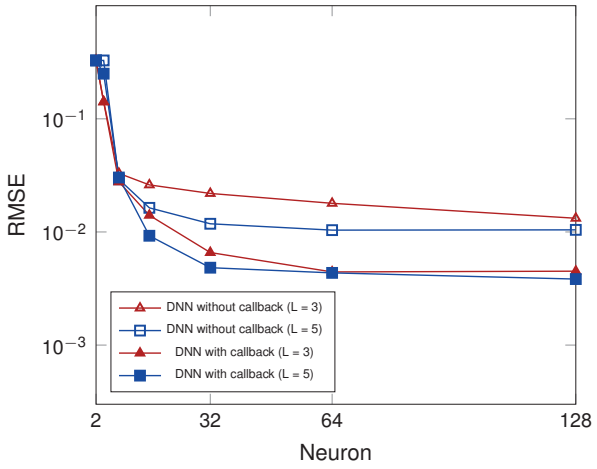


Fig. 3. RMSE of the DNN model with different number of hidden layers and number of neurons.

Fig. 3 presents the impact of the number of hidden neurons on the RMSE by setting different number of hidden layers. As can be seen, more hidden neurons imply in lower RMSE between the predicted SOP and test data. It means that the estimated SOP is tightly close to the test data when the number of hidden neurons increases. This phenomenon can be explained by the fact that, when the number of hidden neurons is increased, the designed DNN model can capture the pattern from the input-output pairs accurately. Similar to the impact of the number of hidden neurons, when the number of the hidden layers is increased, the RMSE is reduced. Besides, when the callback is used, the RMSE is less than without a callback. From Fig. 3, the DNN model can reasonably estimate the secrecy performance of the proposed NOMA system from the new network parameters when the number of hidden layers is increased, and the callback is used.

TABLE III
THE EXECUTION TIME OF THE MTS SCHEME WHEN THE NUMBER OF TRANSMITTERS IS 4.

Approaches	Monte-Carlo	Mathematical	DNN model
Execution time	310.3 s	1.2 s	0.36 s

Next, we compare the execution time of the system performance evaluation with different approaches. The execution time in Table III is defined as the time spent to evaluate the secrecy outage performance. As can be seen, the proposed DNN model spends the shortest execution time among the three approaches. Monte-Carlo approach only requires the network parameters to estimate the secrecy performance, but it consumes a huge execution time to be implemented. On the other hand, the mathematical method employs complicated calculations to estimate secrecy performance, although (if successful) one can easily investigate which network parameters impact the secrecy performance. In contrast, the DNN model can reduce the execution time since it utilizes the mapping function as shown in (64). From Table III, the proposed DNN arises as a well-suited method for real-time system performance evaluation.

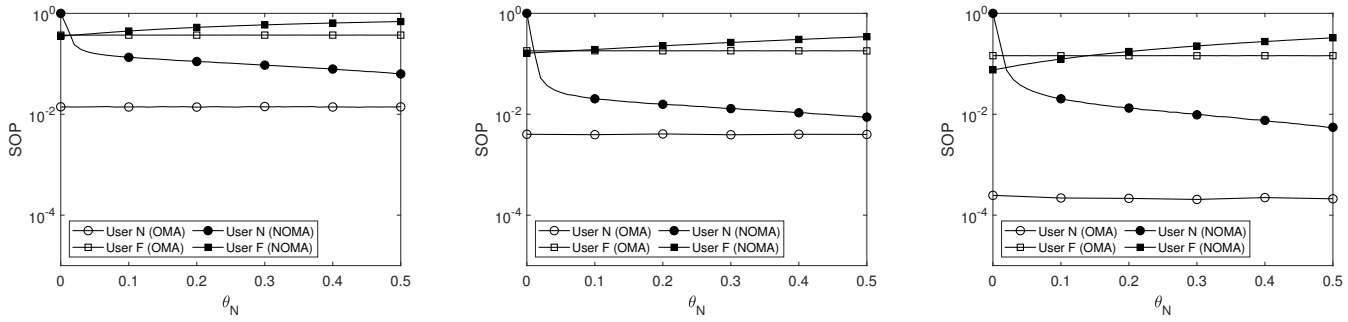
V. NUMERICAL RESULTS

We present representative numerical results to evaluate secrecy performance of the proposed transmitter selection schemes in terms of SOP and secrecy throughput. Insightful discussions related to the proper design of the transmit SNR at transmitter ($\bar{\gamma}_{\mathsf{S}}$), power allocation coefficient of User N (θ_{N}), the transmit SNR at E ($\bar{\gamma}_{\mathsf{E}}$), imperfect SIC coefficient (β), number of transmitters (K), and secrecy target data rate ($R_{\mathtt{th},x_{\mathsf{N}}}$ and $R_{\mathtt{th},x_{\mathsf{F}}}$) will be presented. Unless otherwise stated, the simulation parameters are presented in Table IV.

TABLE IV
SIMULATION PARAMETERS

Parameters	Value
The distance between S and User N (d_{SN})	0.2
The distance between S and User F (d_{SF})	1
The distance between S and User E (d_{SE})	1
The distance between User N and E (d_{NE})	0.5
The distance between User F and E (d_{FE})	0.5
Path-loss exponent (ϵ)	2.7
Path-loss at reference distance ($\mathcal{L}$ at d_0 = 1 m)	-30 dB
Imperfect SIC coefficient (β)	0.1
Target secrecy data rate of User N ($R_{\mathtt{th},\mathsf{N}}$)	0.2 bps/Hz
Target secrecy data rate of User F ($R_{\mathtt{th},\mathsf{F}}$)	0.2 bps/Hz

In Fig. 4, we compare the secrecy performance between orthogonal multiple access (OMA) and NOMA with various transmitter selection schemes. As can be seen, cell-center and cell-edge users' secrecy performance with OMA does not affect the power allocation coefficients since it divides the timeblock to serve multiple users. In contrast, the secrecy performance of cell-center and cell-edge users with NOMA affects the power allocation coefficients since it allocates



(a) RTS scheme (b) MTS scheme (c) OTS scheme

Fig. 4. The comparison between NOMA and OMA with different transmitter selection schemes.

different transmit power to serve multiple users simultaneously. Specifically, the secrecy performance of the cell-center user's with NOMA is more robust when θ_{N} increases. It can be explained by the fact that the transmitter allocates more transmit power for the cell-center user message as (5). Thus, when θ_{N} increases, the interference of User N is reduced, which leads to cell-center user's secrecy performance enhancement. The secrecy performance of User F with NOMA is vulnerable compared to that of User F with OMA. The reason is that the cell-edge user directly decodes its message from the received message, which occurs the interference when User F with NOMA decodes its message. In addition, the secrecy outage event of User F is more vulnerable when θ_{N} increases. The reason is that when θ_{N} increases, the power allocation coefficient of User F is reduced. Thus, the strength of the cell-center user's message at User F is reduced, and interference of User F increases due to the principle of NOMA. In addition, the OTS scheme has the best secrecy performance among the transmitter selection schemes because it considers both channel informations (main channel and eavesdropper channel of User N and User F) to select the transmitter aiming to protect the confidential information from the active eavesdropper.

Different from OMA that allocates to each user a different resource block, NOMA allocates the same resource block to multiple users. Thus, for the exploiting system secrecy performance of NOMA, we consider the system SOP, $P_{\mathtt{sys}}$, which is mathematically defined as [7]

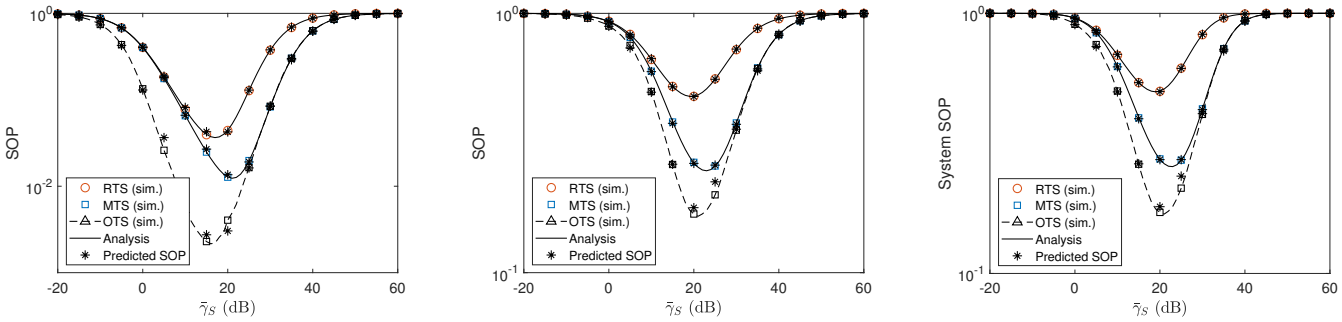
$$P_{\mathtt{sys}} = 1 - (1 - P_{\mathtt{out},\mathsf{N}})(1 - P_{\mathtt{out},\mathsf{N}}). \tag{68}$$

The SOP of User N and User F as well as the system SOP are plotted as a function of transmit SNR ($\bar{\gamma}_{\mathsf{S}}$) in Fig. 5. The OTS scheme shows the most robust secrecy performance compared to that of other schemes. This can be explained as follows. The RTS scheme does not utilize the channel condition to select the best transmitter, while the MTS scheme utilizes the eavesdropper channel capacity to select the best transmitter. However, the OTS scheme requires both the secrecy capacity of cell-center and cell-edge users, yielding consequently in a more robust secrecy performance. Additionally, the results show that as $\bar{\gamma}_{\mathsf{S}}$ increases, the SOP decreases. However, as $\bar{\gamma}_{\mathsf{S}}$ continues to decrease, the SOP reaches its minimum at $\bar{\gamma}_{\mathsf{S}}$, called $\bar{\gamma}_{\mathsf{S}}^*$. As $\bar{\gamma}_{\mathsf{S}}$ goes beyond $\bar{\gamma}_{\mathsf{S}}^*$, the SOP degrades. This occurs because when $\bar{\gamma}_{\mathsf{S}}$ increases, the interference of cell-center and cell-edge users increases due to the imperfect SIC coefficient in (5) and cell-center user's components in (8), respectively. It is noteworthy that, although the MTS scheme requires the knowledge of the eavesdropper channel capacity to select the best transmitter, the MTS and OTS schemes perform close at high SNR regime, e.g., $\bar{\gamma}_{\mathsf{S}} > 25$ (dB). Note also that the predicted SOP through the DNN model is in tightly agreement with Monte-Carlo and the mathematical analysis which allows us to state that the data-driven approach is an acceptable method to estimate the system performance that is too complex to express through the closed-form expression.

Algorithm 1 Brute-Force Search to Find Optimal $\bar{\gamma}_S$ and θ_{N}

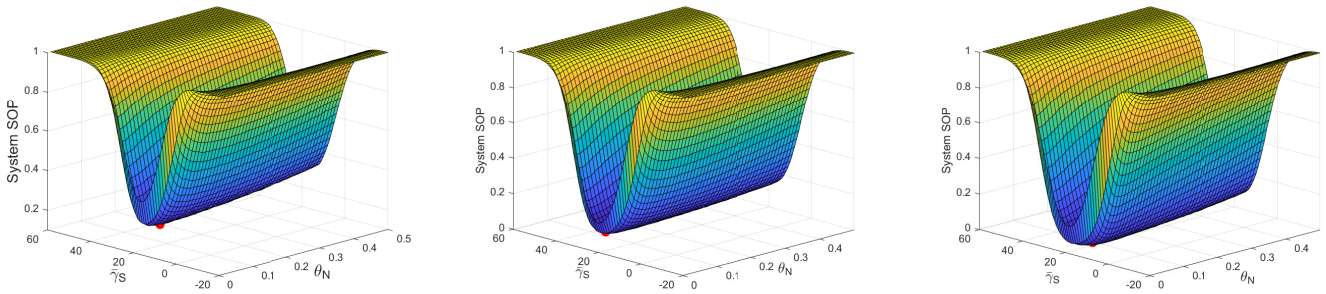
Input: System parameters such as K, $\bar{\gamma}_{\mathsf{S}}$, $\bar{\gamma}_{\mathsf{N}}$, $\bar{\gamma}_{\mathsf{F}}$, $\bar{\gamma}_{\mathsf{E}}$, λ_{SN}, λ_{SF}, λ_{SE}, λ_{NE}, λ_{FE}, λ_{EN}, λ_{EF}, θ_{N}, θ_{F}, β, $R_{\mathtt{th},x_{\mathsf{N}}}$ and $R_{\mathtt{th},x_{\mathsf{F}}}$.
Output: $P_{\min}(\bar{\gamma}_{\mathsf{S}}^*, \theta_{\mathsf{N}}^*)$
Initialization : $P_{\min}(\bar{\gamma}_{\mathsf{S}}, \theta_{\mathsf{N}}) \leftarrow \infty$, $\bar{\gamma}_{\mathsf{S}_i}$, θ_{N_j}
for $i \leftarrow 1$ to $\bar{\gamma}_{\mathsf{S}_{\max}}$ **do**
  for $j \leftarrow 1$ to $\theta_{\mathsf{N}_{\max}}$ **do**
    $P_{\mathtt{sys}}(\bar{\gamma}_{\mathsf{S}_i}, \theta_{\mathsf{N}_j}) \leftarrow$
    $1 - (1 - P_{\mathtt{out},x_{\mathsf{N}}}(\bar{\gamma}_{\mathsf{S}_i}, \theta_{\mathsf{N}_j}))(1 - P_{\mathtt{out},x_{\mathsf{F}}}(\bar{\gamma}_{\mathsf{S}_i}, \theta_{\mathsf{N}_j}))$
    if $P_{\mathtt{sys}}(\bar{\gamma}_{\mathsf{S}_i}, \theta_{\mathsf{N}_j}) < P_{\min}(\bar{\gamma}_{\mathsf{S}}, \theta_{\mathsf{N}})$ **then**
      $P_{\min}(\bar{\gamma}_{\mathsf{S}}, \theta_{\mathsf{N}}) \leftarrow P_{\mathtt{sys}}(\bar{\gamma}_{\mathsf{S}_i}, \theta_{\mathsf{N}_j})$,
      $\bar{\gamma}_{\mathsf{S}}^* \leftarrow \bar{\gamma}_{\mathsf{S}_i}$, $\theta_{\mathsf{N}}^* \leftarrow \theta_{\mathsf{N}_j}$
    end if
  end for
end for
return $(\bar{\gamma}_{\mathsf{S}}^*, \theta_{\mathsf{N}}^*)$

In Fig. 6, the system SOP versus transmit SNR ($\bar{\gamma}_{\mathsf{S}}$) and power allocation coefficient (θ_{N}) is plotted for different transmitter selection schemes. Let $\theta_{\mathsf{F}} = 1 - \theta_{\mathsf{N}}$. Note that the system SOP with OTS scheme outperforms the other two transmitter selection schemes. The reason is that the OTS scheme considers the secrecy capacity of User N and User F at the same time. In addition, as $\bar{\gamma}_{\mathsf{S}}$ and θ_{N} increase, the system SOP exhibits a concave pattern. The first reason is that when $\bar{\gamma}_{\mathsf{S}}$ increase, the interference of the main channel also increase as well as the strength of the received signal. The second



(a) User N (b) User F (c) System

Fig. 5. The effect of transmit SNR at S ($\bar{\gamma}_S$) on the system SOP with different transmitter selection schemes.



(a) RTS scheme (b) MTS scheme (c) OTS scheme

Fig. 6. Effect of $\bar{\gamma}_S$ and θ_N on system outage performance with different transmitter selection schemes.

reason is that when θ_N increases, the interference of User N increases due to imperfect SIC, and User F increases the interference because of the principle of NOMA as (5) and (8). Due to this feature, we can utilize the brute-force search (BFS) algorithm [44] to find the optimal points ($\bar{\gamma}_S^*$, θ_N^*). In order to adopt the BFS algorithm, the searching interval of $\bar{\gamma}_S$ and θ_N is set as 1 (dB) and 0.03, respectively. It is noted that the BFS algorithm has been adopted to find the optimal system SOP from Figs. 7 to 11.

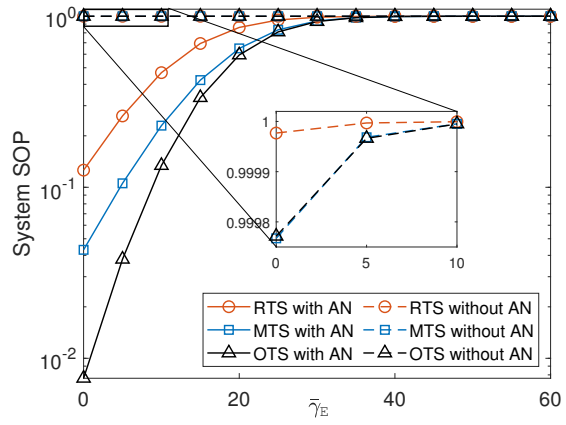


Fig. 7. The effect of the transmit SNR at E ($\bar{\gamma}_E$) on system SOP with different transmitter selection schemes.

In Fig. 7, the system SOP is plotted as a function of $\bar{\gamma}_E$. To compare the proposed NOMA system's secrecy performance, we provide the conventional NOMA system, called without AN, which does not generate AN signals at User N and User F to confuse the active eavesdropper. The proposed NOMA system significantly improves the secrecy performance compared to that of the conventional one. The reason is that User N and User F of the proposed NOMA system act as AN-based jammers to interfere with the active eavesdropper as well as receivers. Thus, the proposed NOMA system can neutralize or overcome the active eavesdropping attacks, differently from the conventional NOMA system that operates in HD mode. Besides, as $\bar{\gamma}_E$ increases, the system SOPs of both transmitter selection schemes increase. One can also see from Fig. 7 that the OTS scheme achieves better secrecy performance compared to that of other schemes.

The impact of the imperfect SIC coefficient (β) on the system SOP is depicted in Fig. 8. The proposed scheme achieves better secrecy performance compared to that of the conventional one. One possible reason is that User N and User F operate in FD mode in the proposed NOMA system different from the conventional one. Thus, User N and User F generate AN signals to prevent the active eavesdropping attack when they receive information signals. Additionally, the system SOP with RTS and MTS schemes increases when the β increases because User N cannot eliminate the cell-edge user's message from the received signal. Different from the RTS and MTS schemes, the OTS scheme shows that as β increases, the system SOP improves. However, as β increases,

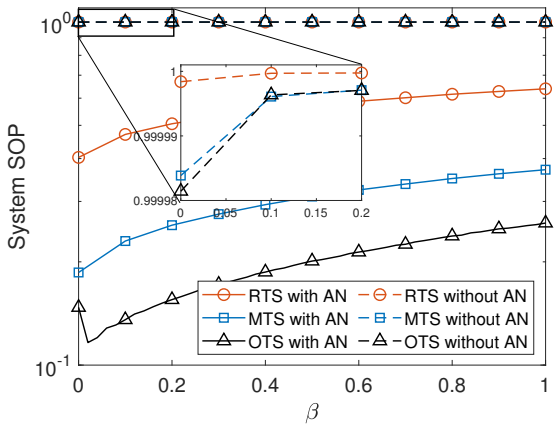


Fig. 8. The effect of imperfect SIC coefficient (β) on system SOP with different transmitter selection schemes.

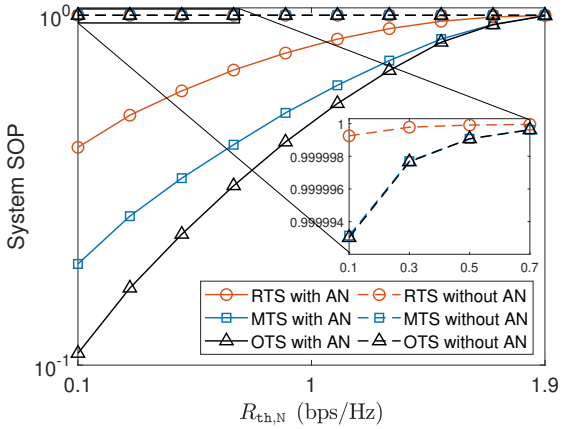


Fig. 10. The effect of $R_{\mathtt{th},x_\mathsf{N}}$ ($R_{\mathtt{th},x_\mathsf{F}}$) on system SOP with different transmitter selection schemes.

the system SOP reaches its minimum at the appropriate value, called β^*. When β goes beyond β^*, the system SOP increases. Note that appropriately selected imperfect SIC coefficient in the OTS scheme plays an important role in network planning to enhance the system secrecy performance.

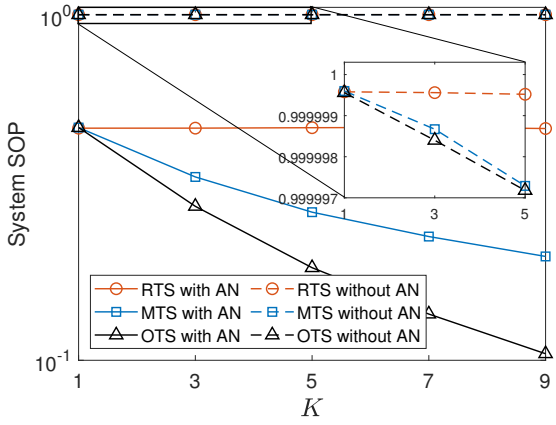


Fig. 9. The effect of K on system SOP with different transmitter selection schemes.

In Fig. 9, the system SOP is plotted as a function of the number of transmitters. The proposed NOMA system achieves better secrecy performance compared to that of the conventional NOMA system. It can be explained by the following reason. The User N and User F in the proposed NOMA system generate AN signals to degrade the active eavesdropper channel condition as well as receiving information signal. However, User N and User F in the conventional NOMA system receive information signal because they operate in HD mode. In addition, the RTS scheme is not affected by the number of transmitters since it randomly selects the transmitter. Different from the RTS scheme, the system SOP with MTS and OTS schemes improves when the number of transmitters increases because these latter schemes utilize the channel condition information to select the best transmitter.

The impact of secrecy target rate on the system SOP is illustrated in Fig. 10. As expected, the proposed NOMA system with three transmitter selection schemes shows better secrecy outage performance than the conventional NOMA system. It can be explained that User N and User F operate in FD mode to receive information signal and generate AN signals to degrade the eavesdropper channel condition. Besides, the system SOP increases as the secrecy target rate increases. Since a high secrecy target data means that the system requires a more robust secrecy level, the system outage performance frequently occurs when the secrecy target data rate increases. The most robust secrecy performance among the three transmitter selection schemes is the OTS scheme, which requires both the secrecy capacity of cell-center and cell-edge users. Also, the performance difference gap between the conventional NOMA system's SOP with MTS and OTS schemes is summarized in Table V. In the conventional NOMA system, the OTS scheme shows better secrecy performance than the MTS scheme since the OTS scheme requires more various channel information to select the best transmitter. However, as can be seen, the secrecy performance difference between the MTS and OTS scheme is too small. Thus, the curves of MTS and OTS schemes is tightly close.

TABLE V
THE PERFORMANCE GAP BETWEEN THE SYSTEM SOP WITH MTS AND OTS SCHEMES ON THE CONVENTIONAL NOMA IN FIG. 10.

$R_{\mathtt{th},x_\mathsf{N}}$ ($R_{\mathtt{th},x_\mathsf{F}}$)	0.1	0.3	0.5
MTS scheme	0.99999314	0.99999770	0.99999907
OTS scheme	0.99999302	0.99999766	0.99999907
Performance gap	0.00000012	0.00000004	0

Next, we investigate the impact of the proposed NOMA and the proposed transmitter selection schemes on the secrecy throughput of User N and User F, and secrecy sum throughput. The secrecy throughput of User N and User F can be, respectively, defined as [7]

$$\mathcal{T}_m = (1 - P_{\mathtt{out},m}) R_{\mathtt{th},m}, \tag{69}$$

where $m \in \{\mathsf{N}, \mathsf{F}\}$. The secrecy sum throughput is mathemat-

ically expressed as

$$\begin{aligned}\mathcal{T}_{\mathtt{sys}} =&\mathcal{T}_{\mathsf{N}} + \mathcal{T}_{\mathsf{F}} \\ =&(1 - P_{\mathtt{out},\mathsf{N}})R_{\mathtt{th},\mathsf{N}} + (1 - P_{\mathtt{out},\mathsf{F}})R_{\mathtt{th},\mathsf{F}}.\end{aligned} \tag{70}$$

The impact of the transmit SNR ($\bar{\gamma}_{\mathsf{S}}$) on the secrecy throughput of User N and User F, and secrecy sum throughput is illustrated in Fig. 11. The proposed NOMA system significantly improves the spectral efficiency compared to the conventional NOMA system. As can be seen, the throughput of cell-center and cell-edge users with the proposed NOMA system shows concave function when $\bar{\gamma}_{\mathsf{S}}$ increases. The reason is that when $\bar{\gamma}_{\mathsf{S}}$ increases, the interference of cell-center and cell-edge users increases because of the imperfect SIC coefficient as (5) and cell-center user's message as (8), respectively. In addition, the secrecy sum throughput with the proposed one also shows a convex pattern when $\bar{\gamma}_{\mathsf{S}}$ increases for the same reason explained earlier. More specifically, the OTS scheme shows the best spectral efficiency among the three transmitter selection schemes.

TABLE VI
THE COMPARISON OF COMPLEXITY ORDER IN THE TRANSMITTER SELECTION SCHEMES

Scheme	RTS scheme	MTS scheme	OTS scheme
Complexity Order	2	K + 3	$3K$ + 6

We now turn our attention to the complexity order of each transmitter selection scheme, as shown in Table VI. Complexity order represents the required channel estimation to select the user and transmit channel information [7]. The amount of channel information of the RTS scheme is the smallest one among the proposed user selection schemes. The reason is that the RTS scheme does not need to channel information to select the user. It needs channel information for data transmission. Therefore, the required channel information of the RTS scheme is 2. Differently, as can be seen in (21), the MTS scheme selects the best user that minimizes the eavesdropper channel capacity. Thus, the complexity order of the MTS scheme is K + 3. Optimally, since the OTS scheme requires the secrecy sum capacity to select the transmitter as in (28), the OTS scheme's complexity is $3K$ + 6. From Table VI, each transmitter selection scheme has a specific advantage and drawback. More specifically, the MTS scheme shows an adequate amount of the required channel information and secrecy performance. However, the OTS scheme requires a considerable amount of channel information, while secrecy performance is not much improved than the MTS scheme. Thus, in the network planning perspective, each scheme can be cleverly applied in different scenarios to achieve a good trade-off between secrecy performance and complexity.

VI. CONCLUSIONS

In this paper, we exploited the secrecy performance for a downlink NOMA system in the presence of an active eavesdropper. In particular, to protect confidential information, we proposed a new FD-enabled NOMA system and a transmitter selection scheme, namely the MTS scheme. The cell-center and cell-edge users in the proposed NOMA system acted as both receiver and AN-based jammer by operating in FD mode. The MTS scheme opportunistically chose the best transmitter, which minimized the maximum eavesdropper channel capacity. We derived the closed-form expressions for SOP of cell-center and cell-edge users to evaluate the proposed NOMA system and transmitter selection schemes. In order to evaluate the secrecy performance in real-time and overcome the limitation of the mathematical approach, we built the DNN model for SOP evaluation. From the numerical results, the proposed NOMA system and the MTS scheme enhanced the secrecy outage performance compared to that of the conventional NOMA system and the RTS scheme, respectively, against the active eavesdropping attack. Additionally, the MTS scheme reduced the complexity in order to select the best transmitter while the secrecy performance was acceptably maintained by comparing the OTS scheme. Finally, a DNN model was built to predict the secrecy performance and it showed to be an efficient tool when model-based approaches are hard to be employed due to the intricacy behind the mathematical derivations.

APPENDIX A
THE PROOF OF THEOREM 1

From (35), the SOP of cell-center user with the RTS scheme can be expressed as

$$\begin{aligned}P_{\mathtt{out},\mathsf{N}}^{\mathsf{RTS}} = &\underbrace{\Pr\left[C_{s,x_{\mathsf{N}}}^{\mathsf{RTS}} < R_{\mathtt{th},x_{\mathsf{N}}}, C_{\mathsf{N},x_{\mathsf{F}}}^{\mathsf{RTS}} \geq R_{\mathtt{th},x_{\mathsf{F}}}\right]}_{\Psi_A} \\ &+ \underbrace{\Pr\left[C_{\mathsf{N},x_{\mathsf{F}}}^{\mathsf{RTS}} < R_{\mathtt{th},x_{\mathsf{F}}}\right]}_{\Psi_B}.\end{aligned} \tag{71}$$

By plugging (16), (17), and (19) into Ψ_A, using the property of probability [45], i.e., $\Pr\left[a < x < b\right] = \Pr[x < b] - \Pr[x < a]$, and conditioning $V = v$, Ψ_A in (71) can be further written as (72), as shown at the top of next page.

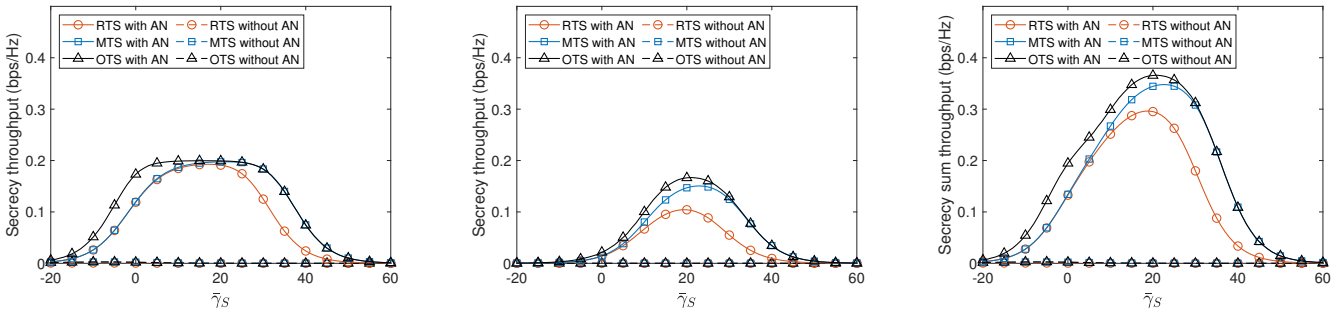
Ψ_{A1} in (72) can be re-written as

$$\begin{aligned}\Psi_{A1} = \int_0^{\infty} &\underbrace{\Pr\left[X_i < \frac{(S_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1))(\bar{\gamma}_{\mathsf{E}} v + 2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}} - \beta\theta_{\mathsf{F}}(S_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)))}\right]}_{\Psi_{A1a}} \\ &\times f_V(v)dv.\end{aligned} \tag{73}$$

Ψ_{A1a} can be further expressed as

$$\begin{aligned}\Psi_{A1a} = 1 - \int_0^{\Omega_1} &e^{-\frac{(s+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1))(\bar{\gamma}_{\mathsf{E}} v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}} - \beta\theta_{\mathsf{F}}(s+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)))\lambda_{\mathsf{SN}}}} \\ &\times \Lambda(\alpha_1, \alpha_3, \alpha_4, 1, s)\Lambda(\alpha_1, \alpha_3, \alpha_4, s)e^{-\frac{2}{\alpha_1}s}ds.\end{aligned} \tag{74}$$

To the best of authors' knowledge, it is very difficult to obtain an exact closed-form expression to (74). By using



(a) User N (b) User F (c) System

Fig. 11. Effect of $\bar{\gamma}_{\mathsf{S}}$ on secrecy throughput of User N and User F and secrecy sum throughput with different transmitter selection schemes.

$$\Psi_A = \Pr\left[\frac{\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}X_i}{\bar{\gamma}_{\mathsf{S}}\beta\theta_{\mathsf{F}}X_i+\bar{\gamma}_{\mathsf{E}}V+2} < (\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)+\frac{\gamma_{\mathtt{th},x_{\mathsf{N}}}\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}Z_i}{\bar{\gamma}_{\mathsf{N}}T+\bar{\gamma}_{\mathsf{F}}U+2}, \frac{\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{F}}X_i}{\bar{\gamma}_{\mathsf{S}}\theta_{\mathsf{N}}X_i+\bar{\gamma}_{\mathsf{E}}V+2} \geq (\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)\right]$$
$$= \underbrace{\int_0^\infty \Pr\left[X_i < \frac{(S_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1))(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}}-\beta\theta_{\mathsf{F}}(S_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)))}\right] f_V(v)dv}_{\Psi_{A1}} - \underbrace{\int_0^\infty \Pr\left[X_i < \frac{(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1))}\right] f_V(v)dv}_{\Psi_{A2}}, \quad (72)$$

Gaussian-Chebyshev quadrature [46, Eq. (25.4.38)], (74) can be approximated as

$$\Psi_{A1a} = 1-\sum_{r=1}^{R}\frac{\Omega_1\pi}{2R}\sqrt{1-s_r^2}e^{-\frac{(\omega_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1))(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}}-\beta\theta_{\mathsf{F}}(\omega_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)))\lambda_{\mathsf{SN}}}} \times \Lambda(\alpha_1,\alpha_3,\alpha_4,1,\omega_1)\Lambda(\alpha_1,\alpha_3,\alpha_4,\omega_1)e^{-\frac{2}{\alpha_1}\omega_1}, \quad (75)$$

By plugging (75) into (73) and relying on [41, Eq. (3.310)], Ψ_{A1} in (72) can be further calculated as

$$\Psi_{A1} = 1-\sum_{r=1}^{R}\frac{\Omega_1\pi}{2R}\sqrt{1-s_r^2} \times \mathcal{F}(\theta_{\mathsf{N}},\beta\theta_{\mathsf{F}},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\omega_1+(\gamma_{\mathtt{th},x_{\mathsf{N}}}-1)) \times \Lambda(\alpha_1,\alpha_3,\alpha_4,1,\omega_1)\Lambda(\alpha_1,\alpha_3,\alpha_4,\omega_1)e^{-\frac{2}{\alpha_1}\omega_1}, \quad (76)$$

Since the random variable X_i is the non-negative random variable, $\frac{(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1))}$ should be larger than zero, i.e., $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, otherwise , Ψ_{A2} = 0 will be always held. Thus, when $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, Ψ_{A2} in (72) can be expressed as

$$\Psi_{A2} = \int_0^\infty \left[1-e^{-\frac{(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1))\lambda_{\mathsf{SN}}}}\right]\frac{1}{\lambda_{\mathsf{EN}}}e^{-\frac{1}{\lambda_{\mathsf{EN}}}v}dv, \quad (77)$$

By making use of [41, Eq. (3.310)], if $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, Ψ_{A2} can be further expressed as

$$\Psi_{A2} = 1-\mathcal{F}(\theta_{\mathsf{F}},\theta_{\mathsf{N}},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\gamma_{\mathtt{th},x_{\mathsf{F}}}-1), \quad (78)$$

otherwise, Ψ_{A2} = 0. By plugging (76) and (78) into (72), Ψ_A in (72) can be written as (79), as shown at the top of next page.

Ψ_B in (71) can be further expressed as

$$\Psi_B = \Pr\left[X_i < \frac{(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)(\bar{\gamma}_{\mathsf{E}}V+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1))}\right], \quad (80)$$

Since X_i is non-negative random variable, $\frac{(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)(\bar{\gamma}_{\mathsf{E}}V+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1))}$ should be larger than zero, i.e., $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, otherwise, Ψ_B = 0 will be always held. Thus, when $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, Ψ_B can be further expressed as

$$\Psi_B = \int_0^\infty \left[1-e^{-\frac{1}{\lambda_{\mathsf{SN}}}\left(\frac{(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1)(\bar{\gamma}_{\mathsf{E}}v+2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}}-\theta_{\mathsf{N}}(\gamma_{\mathtt{th},x_{\mathsf{F}}}-1))}\right)}\right]\frac{1}{\lambda_{\mathsf{EN}}}e^{-\frac{1}{\lambda_{\mathsf{EN}}}v}dv. \quad (81)$$

By relying on [41, Eq. (3.310)] and after some mathematical steps, if $\frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1$, Ψ_B can be obtained as

$$\Psi_B = 1-\mathcal{F}(\theta_{\mathsf{F}},\theta_{\mathsf{N}},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\gamma_{\mathtt{th},x_{\mathsf{F}}}-1), \quad (82)$$

otherwise, Ψ_B = 0. Consequently, by combining Ψ_{A1} and Ψ_B, the closed-form expression for SOP of User N with the RTS scheme, $P_{\mathtt{out},\mathsf{N}}^{\mathsf{RTS}}$, can be easily obtained as (47). The proof of Theorem 1 is concluded.

Appendix B
The Proof of Theorem 2

From (36), the SOP of cell-center user with the RTS scheme, $P_{\mathtt{out},\mathsf{F}}^{\mathsf{RTS}}$, can be further written as

$$\Psi_A = \Psi_{A1} - \Psi_{A2} = \begin{cases} \mathcal{F}(\theta_{\mathsf{F}}, \theta_{\mathsf{N}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \gamma_{\mathtt{th},x_{\mathsf{F}}} - 1) \\ -\sum_{r=1}^{R} \frac{\Omega_1 \pi}{2R} \sqrt{1-s_r^2} \mathcal{F}(\theta_{\mathsf{N}}, \beta\theta_{\mathsf{F}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \quad \times \Lambda(\alpha_1, \alpha_3, \alpha_4, 1, \omega_1) \Lambda(\alpha_1, \alpha_3, \alpha_4, \omega_1) e^{-\frac{2}{\alpha_1}\omega_1} & \text{, if } \frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1 \\ 1 - \sum_{r=1}^{R} \frac{\Omega_1 \pi}{2R} \sqrt{1-s_r^2} \mathcal{F}(\theta_{\mathsf{N}}, \beta\theta_{\mathsf{F}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \quad \times \Lambda(\alpha_1, \alpha_3, \alpha_4, 1, \omega_1) \Lambda(\alpha_1, \alpha_3, \alpha_4, \omega_1) e^{-\frac{2}{\alpha_1}\omega_1} & \text{, otherwise} \end{cases} \tag{79}$$

$$\begin{aligned} P_{\mathtt{out},\mathsf{F}}^{\mathsf{RTS}} &= \Pr\left[Y_i < \frac{(S_2 + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))(\bar{\gamma}_{\mathsf{E}} W + 2)}{\bar{\gamma}_{\mathsf{S}}\big(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))\big)} \right] \\ &= \int_0^{\infty} \int_0^{\infty} F_{Y_i}\left(\frac{(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))(\bar{\gamma}_{\mathsf{E}} w + 2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)))} \right) \\ &\quad \times f_W(w) dw f_{S_2}(s) ds. \end{aligned} \tag{83}$$

Since the random variable Y_i is non-negative random variable, $\frac{(S_2 + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))(\bar{\gamma}_{\mathsf{E}} W + 2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(S_2 + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)))}$ is larger than zero, i.e., $\Omega_2 > S_2$. Thus, the integral in (83) can be further expressed as

$$\begin{aligned} &P_{\mathtt{out},\mathsf{F}}^{\mathsf{RTS}} \\ &= \int_0^{\Omega_2} \underbrace{\int_0^{\infty} F_{Y_i}\left(\frac{(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))(\bar{\gamma}_{\mathsf{E}} w + 2)}{\bar{\gamma}_{\mathsf{S}}\big(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))\big)} \right) f_W(w) dw}_{\Phi_1} \\ &\quad \times f_{S_2}(s) ds + \int_{\Omega_2}^{\infty} \int_0^{\infty} f_W(w) dw f_{S_2}(s) ds. \end{aligned} \tag{84}$$

In order to further express (84), Φ_1 in (84) can be further expressed as

$$\begin{aligned} \Phi_1 =& \frac{1}{\lambda_{\mathsf{EF}}} \int_0^{\infty} e^{-\frac{1}{\lambda_{\mathsf{EF}}} w} dw - \frac{1}{\lambda_{\mathsf{EF}}} e^{-\frac{2(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)))\lambda_{\mathsf{SF}}}} \\ &\times \int_0^{\infty} e^{-\left(\frac{\bar{\gamma}_{\mathsf{E}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1))}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{F}} - \theta_{\mathsf{N}}(s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)))\lambda_{\mathsf{SF}}} + \frac{1}{\lambda_{\mathsf{EF}}}\right) w} dw. \end{aligned} \tag{85}$$

By making use of [41, Eq. (3.310)], Φ_1 can be expressed as

$$\Phi_1 = 1 - \mathcal{F}(\theta_{\mathsf{F}}, \theta_{\mathsf{N}}, \lambda_{\mathsf{SF}}, \lambda_{\mathsf{EF}}, s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)). \tag{86}$$

By plugging (86) and (49) into (84) and after some algebraic steps, $P_{\mathtt{out},\mathsf{F}}^{\mathsf{RTS}}$ can be re-written as

$$\begin{aligned} P_{\mathtt{out},\mathsf{F}}^{\mathsf{RTS}} =& 1 - \int_0^{\Omega_2} \mathcal{F}(\theta_{\mathsf{F}}, \theta_{\mathsf{N}}, \lambda_{\mathsf{SF}}, \lambda_{\mathsf{EF}}, s + (\gamma_{\mathtt{th},x_{\mathsf{F}}} - 1)) \\ &\times \Lambda(\alpha_2, \alpha_3, \alpha_4, 1, s) \Lambda(\alpha_2, \alpha_3, \alpha_4, s) e^{-\frac{2}{\alpha_2} s} ds. \end{aligned} \tag{87}$$

To the best of authors' knowledge, it is very difficult to obtain an exact closed-form expression to (87). By using Gaussian-Chebyshev quadrature [46, Eq. (25.4.38)], (87) can be approximated as (50). The proof of Theorem 2 is concluded.

Appendix C
The proof of Theorem 3

From (35), the SOP of cell-center user with the MTS scheme, $P_{\mathtt{out},\mathsf{F}}^{\mathsf{MTS}}$, can be expressed as

$$\begin{aligned} P_{\mathtt{out},\mathsf{N}}^{\mathsf{MTS}} =& \underbrace{\Pr\left[C_{s,x_{\mathsf{N}}}^{\mathsf{MTS}} < R_{\mathtt{th},x_{\mathsf{N}}}, C_{\mathsf{N},x_{\mathsf{F}}}^{\mathsf{MTS}} \geq R_{\mathtt{th},x_{\mathsf{F}}} \right]}_{\Delta_A} \\ &+ \underbrace{\Pr\left[C_{\mathsf{N},x_{\mathsf{F}}}^{\mathsf{MTS}} < R_{\mathtt{th},x_{\mathsf{F}}} \right]}_{\Delta_B}. \end{aligned} \tag{88}$$

By conditioning $V = v$ and using the property of probability, i.e., $\Pr[a < x < b] = \Pr[x < b] - \Pr[x < a]$, Δ_A in (88) can be further expressed as (89), as show at the top of next page.

Since the random variable, X_b, is non-negative random variable, $\frac{(S_3 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1))(\bar{\gamma}_{\mathsf{E}} v + 2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}} - \beta\theta_{\mathsf{F}}(S_3 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)))}$ is larger than zero, i.e., $\Omega_1 > S_3$ and the CDF of X_b can be obtained as $1 - e^{-\frac{1}{\lambda_{\mathsf{SN}}} x}$ [7], [36], if $1 > \beta\theta_{\mathsf{F}}\gamma_{\mathtt{th},x_{\mathsf{N}}}$, Δ_{A1} in (89) can be further expressed as

$$\begin{aligned} \Delta_{A1} =& \int_0^{\infty} \int_0^{\infty} f_{S_3}(s) ds f_V(v) dv \\ &- \int_0^{\infty} \int_0^{\Omega_1} e^{-\frac{(s + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1))(\bar{\gamma}_{\mathsf{E}} V + 2)}{\bar{\gamma}_{\mathsf{S}}(\theta_{\mathsf{N}} - \beta\theta_{\mathsf{F}}(S_3 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)))\lambda_{\mathsf{SN}}}} f_{S_3}(s) ds f_V(v) dv, \end{aligned} \tag{90}$$

otherwise, $\Delta_{A1} = 0$, where Ω_1 is defined as (47). By plugging (52) into Δ_{A1} in (90), and relying on the property of PDF, i.e., $\int_0^{\infty} f_{S_3}(s) ds = 1$, and [41, Eq. (3.310)], Δ_{A1} in (90) can be further expressed as

$$\begin{aligned} \Delta_{A1} =& 1 - \int_0^{\infty} \int_0^{\Omega_1} e^{-\frac{(s + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1))(\bar{\gamma}_{\mathsf{E}} v + 2)}{\bar{\gamma}_b(\theta_{\mathsf{N}} - \beta\theta_{\mathsf{F}}(S_3 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)))\lambda_{\mathsf{SN}}}} \\ &\times \Lambda(\alpha_1, \alpha_5, \alpha_6, K, s) \Lambda(\alpha_1, \alpha_5, \alpha_6, s) e^{-\frac{2K}{\alpha_1} s} ds f_V(v) dv, \end{aligned} \tag{91}$$

To the best of authors' knowledge, it is very difficult to obtain an exact closed-form expression to (91). Relying on [46, Eq. (25.4.38)] and [41, Eq. (3.310)], (91) can be approximated as

$$\Delta_A = \Pr\left[\log_2\left(\frac{1+\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{N}}}{1+\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{E},x_\mathsf{N}}}\right) < R_{\mathtt{th},x_\mathsf{N}}, \log_2(1+\gamma^{\mathsf{MTS}}_{\mathsf{S}_b\mathsf{N},x_\mathsf{F}}) \geq R_{\mathtt{th},x_\mathsf{F}}\right]$$
$$= \underbrace{\int_0^\infty \Pr\left[X_b < \frac{(S_3+(\gamma_{\mathtt{th},x_\mathsf{N}}-1))(\bar{\gamma}_\mathsf{E}v+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{N}-\epsilon\theta_\mathsf{F}(S_3+(\gamma_{\mathtt{th},x_\mathsf{N}}-1)))}\right] f_V(v)dv}_{\Delta_{A1}} - \underbrace{\int_0^\infty \Pr\left[X_b < \frac{(\gamma_{\mathtt{th},x_\mathsf{F}}-1)(\bar{\gamma}_\mathsf{E}v+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(\gamma_{\mathtt{th},x_\mathsf{N}}-1))}\right] F_V(v)dv}_{\Delta_{A2}} \quad (89)$$

$$\Delta_{A1} = 1 - \sum_{r=1}^{R} \frac{\Omega_1\pi}{2R}\sqrt{1-s_r^2} \times \mathcal{F}(\theta_\mathsf{N}, \beta\theta_\mathsf{F}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1+\gamma_{\mathtt{th},x_\mathsf{N}}-1)) \times \Lambda(\alpha_1,\alpha_5,\alpha_6,K,\omega_1)\Lambda(\alpha_1,\alpha_5,\alpha_6,\omega_1)e^{-\frac{2K}{\alpha_1}\omega_1}. \quad (92)$$

Next, Δ_{A2} in (89) can be further expressed as

$$\Delta_{A2} = \Pr\left[X_b < \frac{(\gamma_{\mathtt{th},x_\mathsf{F}}-1)(\bar{\gamma}_\mathsf{E}V+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(\gamma_{\mathtt{th},x_\mathsf{F}}-1))}\right] \quad (93)$$

Since the random variables, X_b, is non-negative, the probability is satisfied when $\frac{(\gamma_{\mathtt{th},x_\mathsf{F}}-1)(\bar{\gamma}_\mathsf{E}V+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(\gamma_{\mathtt{th},x_\mathsf{F}}-1))}$ is larger than zero, i.e., $\frac{1}{\theta_\mathsf{N}} > \gamma_{\mathtt{th},x_\mathsf{F}}$, and relying on the fact, $\int_0^\infty e^{-\frac{1}{p}x}dx = \frac{1}{p}$ [41, Eq. (3.310)], if $\frac{1}{\theta_\mathsf{N}} > \gamma_{\mathtt{th},x_\mathsf{F}}$, Δ_{A2} can be further obtained as

$$\Delta_{A2} = \int_0^\infty \left[1 - e^{-\frac{(\gamma_{\mathtt{th},x_\mathsf{F}}-1)(\bar{\gamma}_\mathsf{E}v+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(\gamma_{\mathtt{th},x_\mathsf{F}}-1))}}\right]\frac{1}{\lambda_{\mathsf{EN}}}e^{-\frac{1}{\lambda_{\mathsf{EN}}}v}dv = 1 - \mathcal{F}(\theta_\mathsf{F},\theta_\mathsf{N},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\gamma_{\mathtt{th},x_\mathsf{F}}-1), \quad (94)$$

otherwise, $\Delta_{A2} = 1$. Consequently, by plugging (92) and (94) into (89), Δ_A can be obtained as (95), as shown at top of next page.

Next, Δ_B in (88) can be further expressed as

$$\Delta_B = \Pr\left[X_b < \frac{(\gamma_{\mathtt{th},x_\mathsf{F}}-1)(\bar{\gamma}_\mathsf{E}V+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(\gamma_{\mathtt{th},x_\mathsf{F}}-1))}\right]. \quad (96)$$

Similar to the mathematical steps of Δ_{A2}, if $1 > \gamma_{\mathtt{th},x_\mathsf{F}}\theta_\mathsf{N}$, Δ_B can be easily obtained as

$$\Delta_B = 1 - \mathcal{F}(\theta_\mathsf{F},\theta_\mathsf{N},\lambda_{\mathsf{SN}},\lambda_{\mathsf{EN}},\gamma_{\mathtt{th},x_\mathsf{F}}-1), \quad (97)$$

otherwise $\Delta_B = 0$. In the sequel, by substituting (95) and (97) into (88), $P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{N}}$ can be written as (56). The proof of Theorem 3 is concluded.

Appendix D
The proof of Theorem 4

From (36), $P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}}$ can be further expressed as

$$P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}} = \Pr\left[Y_b < \frac{(S_4+(\gamma_{\mathtt{th},x_\mathsf{F}}-1))(\bar{\gamma}_\mathsf{E}W+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(S_4+(\gamma_{\mathtt{th},x_\mathsf{F}}-1)))}\right]. \quad (98)$$

Because Y_b is non-negative random variable, $\frac{(S_4+(\gamma_{\mathtt{th},x_\mathsf{F}}-1))(\bar{\gamma}_\mathsf{E}W+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(S_4+(\gamma_{\mathtt{th},x_\mathsf{F}}-1)))}$ is larger than zero, i.e., $\Omega_2 > S_4$. The CDF of Y_b is expressed as $1-e^{-\frac{1}{\lambda_{\mathsf{SF}}}y}$ [7], [36]. Thus, $P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}}$ can be re-expressed as

$$P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}} = \int_0^{\Omega_2} \underbrace{\int_0^\infty \left[1 - e^{-\frac{(s+(\gamma_{\mathtt{th},x_\mathsf{F}}-1))(\bar{\gamma}_\mathsf{E}w+2)}{\bar{\gamma}_\mathsf{S}(\theta_\mathsf{F}-\theta_\mathsf{N}(s+(\gamma_{\mathtt{th},x_\mathsf{F}}-1)))\lambda_{\mathsf{SF}}}}\right] f_W(w)dw}_{\Gamma_1} \times f_{S_4}(s)ds + \int_{\Omega_2}^\infty \int_0^\infty f_W(w)dw F_{S_4}(s)ds. \quad (99)$$

By relying on [41, Eq. (3.310)], Γ_1 in (99) can be further obtained as

$$\Gamma_1 = 1 - \mathcal{F}(\theta_\mathsf{F},\theta_\mathsf{N},\lambda_{\mathsf{SF}},\lambda_{\mathsf{EF}},s+(\gamma_{\mathtt{th},x_\mathsf{F}}-1)). \quad (100)$$

Again, plugging (58) and (100) into (99), $P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}}$ can be further written as

$$P^{\mathsf{MTS}}_{\mathtt{out},\mathsf{F}} = 1 - \int_0^{\Omega_2} \mathcal{F}(\theta_\mathsf{F},\theta_\mathsf{N},\lambda_{\mathsf{SF}},\lambda_{\mathsf{EF}},s+(\gamma_{\mathtt{th},x_\mathsf{F}}-1)) \times \Lambda(\alpha_2,\alpha_5,\alpha_6,K,s)\Lambda(\alpha_2,\alpha_5,\alpha_6,s)e^{-\frac{2K}{\alpha_2}s}ds \quad (101)$$

To best author's knowledge, it is difficult to calculate the integral in (101). Thus, by using the Gaussian-Chevbyshev quadrature [46, Eq. (25.4.38)], The integral in (101) can be approximated as (62), as shown at the top of next page. The proof of Theorem 4 is concluded.

References

[1] L. Luo, Q. Li, and J. Cheng, "Performance Analysis of Overlay Cognitive NOMA Systems With Imperfect Successive Interference Cancellation," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4709–4722, May 2020.

[2] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA Transmission With Artificial Noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[3] T.-N. Do, D. B. da Costa, T. Q. Duong, and B.An, "Improving the Performance of Cell-Edge Users in NOMA Systems Using Cooperative Relaying," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 1883–1901, May 2018.

[4] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive Non-Orthogonal Multiple Access for Cellular IoT: Potentials and Limitations," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[5] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Jul. 2019.

[6] F. Shu, T. Shen, L. Xu, Y. Qin, S. Wan, S. Jin, X. You, and J. Wang, "Directional Modulation: A Physical-Layer Security Solution to B5G and Future Wireless Networks," *IEEE Netw.*, vol. 34, no. 2, pp. 210–216, Sep. 2020.

$$\Delta_A = \Delta_{A1} - \Delta_{A2} = \begin{cases} \mathcal{F}(\theta_{\mathsf{F}}, \theta_{\mathsf{N}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \gamma_{\mathtt{th},x_{\mathsf{F}}} - 1) \\ -\sum_{r=1}^{R} \frac{\Omega_1 \pi}{2R} \sqrt{1-s_r^2} \mathcal{F}(\theta_{\mathsf{N}}, \beta\theta_{\mathsf{F}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \quad \times \Lambda(\alpha_2, \alpha_5, \alpha_6, K, \omega_1) \Lambda(\alpha_2, \alpha_5, \alpha_6, \omega_1) e^{-\frac{2K}{\alpha_2}\omega_1} & \text{, if } \frac{1}{\theta_{\mathsf{N}}\gamma_{\mathtt{th},x_{\mathsf{F}}}} > 1 \\ 1 - \sum_{r=1}^{R} \frac{\Omega_1 \pi}{2R} \sqrt{1-s_r^2} \mathcal{F}(\theta_{\mathsf{N}}, \beta\theta_{\mathsf{F}}, \lambda_{\mathsf{SN}}, \lambda_{\mathsf{EN}}, \omega_1 + (\gamma_{\mathtt{th},x_{\mathsf{N}}} - 1)) \\ \quad \times \Lambda(\alpha_2, \alpha_5, \alpha_6, K, \omega_1) \Lambda(\alpha_2, \alpha_5, \alpha_6, \omega_1) e^{-\frac{2K}{\alpha_2}\omega_1} & \text{, otherwise} \end{cases} \tag{95}$$

[7] K. Shim, T. Nguyen, and B. An, "Exploiting Opportunistic Scheduling Schemes to Improve Physical-Layer Security in MU-MISO NOMA Systems," *IEEE Access*, vol. 7, pp. 180 867–180 886, Dec. 2019.

[8] M. Mohammadi, X. Shi, B. K. Chalise, Z. Ding, H. A. Suraweera, C. Zhong, and J. S. Thompson, "Full-Duplex Non-Orthogonal Multiple Access for Next Generation Wireless Systems," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 110–116, May 2019.

[9] X. Chen, G. Liu, Z. Ma, X. Zhang, P. Fan, S. Chen, and F. R. Yu, "When Full Duplex Wireless Meets Non-Orthogonal Multiple Access: Opportunities and Challenges," *IEEE Wirel. Commun.*, vol. 26, no. 4, pp. 148–155, Aug. 2019.

[10] T. K. Baranwal, D. S. Michalopoulos, and R. Schober, "Outage Analysis of Multihop Full Duplex Relaying," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 63–66, Jan. 2013.

[11] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-Complexity End-to-End Performance Optimization in MIMO Full-Duplex Relay Systems," *IEEE Trans. Wirel. Commun.*, vol. 13, no. 2, pp. 913–927, Feb. 2014.

[12] J. Kim, J. Kim, J. Lee, and J. P. Choi, "Physical-Layer Security Against Smart Eavesdroppers: Exploiting Full-Duplex Receivers," *IEEE Access*, vol. 6, pp. 32 945–32 957, Jun. 2018.

[13] F. J. Montáns, F. Chinesta, R. Gómez-Bombarelli, and J. N. Kutz, "Data-driven modeling and learning in science and engineering," *Comptes Rendus Mécanique*, vol. 347, no. 11, pp. 845–855, Nov. 2019.

[14] H. Lei, J. Zhang, K. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. Alouini, "On Secure NOMA Systems With Transmit Antenna Selection Schemes," *IEEE Access*, vol. 5, pp. 17 450–17 464, Aug. 2017.

[15] H. Lei, J. Zhang, K. Park, P. Xu, Z. Zhang, G. Pan, and M. Alouini, "Secrecy Outage of Max–Min TAS Scheme in MIMO-NOMA Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Apr. 2018.

[16] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-Stage Relay Selection for Enhancing Physical Layer Security in Non-Orthogonal Multiple Access," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1670–1683, Nov. 2019.

[17] D. Tran, H. Tran, D. Ha, and G. Kaddoum, "Secure Transmit Antenna Selection Protocol for MIMO NOMA Networks Over Nakagami-m Channels," *IEEE Syst. J.*, vol. 14, no. 1, pp. 253–264, Mar. 2020.

[18] H. Lei, R. Gao, K. H. Park, I. S. Ansari, K. J. Kim, and M. S. Alouini, "On Secure Downlink NOMA Systems With Outage Constraint," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7824–7836, Dec. 2020.

[19] H. Lei, R. Gao, Z. Ren, K. H. Park, G. Pan, and M. S. Alouini, "The Meta Distributions of Secrecy Rate for the Downlink NOMA Systems," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 291–295, Feb. 2021.

[20] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the Security Enhancement of Uplink NOMA Systems With Jammer Selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.

[21] L. Lv, H. Jiang, Z. Ding, L. Yang, and J. Chen, "Secrecy-Enhancing Design for Cooperative Downlink and Uplink NOMA With an Untrusted Relay," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1698–1715, Mar. 2020.

[22] H. Fang, L. Xu, Y. Zou, X. Wang, and K. R. Choo, "Three-Stage Stackelberg Game for Defending Against Full-Duplex Active Eavesdropping Attacks in Cooperative Communication," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 788–10 799, Sep. 2018.

[23] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy Performance of an Artificial Noise Assisted Transmission Scheme With Active Eavesdropper," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 971–975, Jan. 2020.

[24] P. Singh and A. Trivedi, "NOMA and massive MIMO assisted physical layer security using artificial noise precoding," *Phys. Commun.*, vol. 39, p. 100977, Apr. 2020.

[25] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[26] M. K. Shukla, H. H. Nguyen, and O. J. Pandey, "Secrecy Performance Analysis of Two-Way Relay Non-Orthogonal Multiple Access Systems," *IEEE Access*, vol. 8, pp. 39 502–39 512, Feb. 2020.

[27] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint Precoding Optimization for Secure SWIPT in UAV-Aided NOMA Networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[28] H. E. Hammouti, M. Ghogho, and S. A. Raza Zaidi, "A Machine Learning Approach to Predicting Coverage in Random Wireless Networks," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, UAE, Feb. 2018, pp. 1–6.

[29] T. Bao, J. Zhu, H. C. Yang, and M. O. Hasna, "Secrecy Outage Performance of Ground-to-Air Communications With Multiple Aerial Eavesdroppers and Its Deep Learning Evaluation," *IEEE Wireless Commun. Lett.*, vol. 9, no. 9, pp. 1351–1355, Sep. 2020.

[30] T. V. Nguyen, T. N. Tran, K. Shim, T. Huynh-The, and B. An, "A Deep Neural Network-based Relay Selection Scheme in Wireless-Powered Cognitive IoT Networks," *IEEE Internet Things J.*, to be published. DOI: 10.1109/JIOT.2020.3038907.

[31] Y. Choi and D. Kim, "Performance analysis with and without torch node in secure communications," in *2015 International Conference on Advanced Technologies for Communications (ATC)*, Beijing, China, Aug. 2015, pp. 84–87.

[32] B. Sklar, "Rayleigh fading channels in mobile digital communication systems .I. Characterization," *IEEE Commun. Mag.*, vol. 35, no. 7, pp. 90–100, Jul. 1997.

[33] M. F. Kader, S. Y. Shin, and V. C. M. Leung, "Full-Duplex Non-Orthogonal Multiple Access in Cooperative Relay Sharing for 5G Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5831–5840, Jul. 2018.

[34] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. S. Evans, "Physical-Layer Security in Full-Duplex Multi-Hop Multi-User Wireless Network With Relay Selection," *IEEE Trans. Wirel. Commun.*, vol. 18, no. 2, pp. 1216–1232, Feb. 2019.

[35] I. Abu Mahady, E. Bedeer, S. Ikki, and H. Yanikomeroglu, "Sum-Rate Maximization of NOMA Systems Under Imperfect Successive Interference Cancellation," *IEEE Commun. Lett.*, vol. 23, no. 3, Mar. 2019.

[36] K. Shim, T.-V. Nguyen, and B. An, "Exploiting Opportunistic Scheduling Schemes and WPT-Based Multi-Hop Transmissions to Improve Physical Layer Security in Wireless Sensor Networks," *Sensors*, vol. 19, no. 24, p. 5456, Dec. 2019.

[37] R. H. Y. Louie, M. R. McKay, and I. B. Collings, "Sum Capacity of Opportunistic Scheduling for Multiuser MIMO Systems with Linear Receivers," in *2008 IEEE GLOBECOM*, New Orleans, LA, USA, Nov. 2008, pp. 1–5.

[38] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[39] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M. Alouini, "Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[40] N. T. Do, D. B. da Costa, T. Q. Duong, and B. An, "A BNBF User Selection Scheme for NOMA-Based Cooperative Relaying Systems With SWIPT," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 664–667, Mar. 2017.

[41] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products (7th ed.)*. Academic Press is an imprint of Elsevier, 2007.

[42] R. H. Hahnioser, R. Sarapeshkar, M. A. Mahowald, R. J. Douglas, and H. S. Seung, "Digital selection and analogue amplification coexist in a cortex-inspired silicon circuit," *Nature*, vol. 405, pp. 947 – 951, Jun. 2000.

[43] D. P. Kingma and J. L. Ba, "Adam: A method for stochastic optimization," in *2015Proc. Int. Conf. Learn. Represent.*, San Diego, CA, USA, May 2015, pp. 1–15.

[44] T. V. Nguyen, V. D. Nguyen, D. B. da Costa, and B. An, "Hybrid User Pairing for Spectral and Energy Efficiencies in Multiuser MISO-NOMA Networks With SWIPT," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4874–4890, May 2020.

[45] L.-G. Alberto, *Probability, Statistics, and Random Processes for Electrical Engineering (3rd ed.)*. Pearson Prentice Hall, 2008, vol. 55.

[46] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1964.