Physical Layer Security of Partial-NOMA and NOMA in Poisson Networks

Konpal Shaukat Ali*, *Member, IEEE*, Arafat Al-Dweik†, *Senior Member, IEEE*, Ekram Hossain+, *Fellow, IEEE*, and Marwa Chafii*, *Member, IEEE*

***Abstract*—Security is an issue in non-orthogonal multiple access (NOMA) and partial-NOMA because a user may decode the message of its paired-user with which it shares a resource element (RE). Three scenarios are studied where, of the paired-users, the eavesdropper is: 1) an actively malicious strong-user, 2) a passive strong-user, 3) an actively malicious weak-user. We define the event of secure-communication in each scenario and derive the corresponding secrecy probabilities for partial-NOMA and NOMA. Our results highlight that with careful selection of the RE's overlap α, partial-NOMA can significantly outperform NOMA in terms of secrecy probability. Further, careless selection of α can cause partial-NOMA to perform worse than NOMA. We show the non-trivial impact of incorporating the impact of intercell interference on secrecy. Our results shed light on parameter-selection if knowledge of the eavesdropper type is available highlighting that security can be improved without traditional techniques such as jamming that increase power consumption and interference. While NOMA decoding uses successive-interference-cancellation (SIC), partial-NOMA decoding employs receive-filtering followed by flexible-SIC (FSIC). We show that not employing receive-filtering or using SIC instead of FSIC can have a drastic negative impact on secrecy, highlighting the role of the partial-NOMA decoding approach in enhancing secure-communication.**

Index Terms: Non-orthogonal multiple access (NOMA), partial-NOMA, physical layer security, stochastic geometry.

I. Introduction

A. Background

Non-orthogonal multiple access (NOMA) was proposed as technique to improve spectrum efficiency over the more traditional orthogonal multiple access (OMA) by having user equipments (UEs) share a resource element (RE). While this improves throughput in NOMA, it introduces additional interference which deteriorates coverage. In light of this trade off, a number of studies have been conducted that investigate the average performance of hybrid systems that employ NOMA in some REs and OMA in others (cf. Fig. 1c). These hybrid systems have been referred to as partial-NOMA in [1]–[6] ; such studies have also been conducted under other names [7]–[9] which reflect the hybrid nature of the setup. In [1], it is shown that for certain ratios of the bandwidth (BW) occupied by NOMA to the total available BW, the hybrid scheme is superior, in terms of total throughput, to using NOMA in all of the frequency channels. In [2], it is shown that the hybrid scheme is also superior in terms of UE fairness. In [3], an algorithm is proposed for the joint allocation of power and BW ratio to maximize the total throughput subject to fairness constraints. In [4], double power allocation is proposed to achieve the same rate for the near and far user in the hybrid system. In an attempt to improve fairness again, a scheme where the OMA bands are reserved for the far UE only while the NOMA bands are shared by both the near and far UEs is proposed in [5]. In [6], NOMA is integrated into the LTE-U and Wi-Fi coexisting networks. The hybrid system is based on having stronger UEs and WiFi stations share the channel via NOMA, while weaker UEs have their own channel, i.e., OMA. In [7], an algorithm is proposed to solve an optimization problem that accounts for the rate and costs of NOMA and OMA. It is shown that the hybrid setup outperforms both OMA and NOMA.

All of the aforementioned works involve studying the average performance, over multiple REs, of a hybrid setup which has NOMA in some of the REs and OMA in the others. Different from these, partial-NOMA in [10], [11] is introduced as a flexible technique between the two extremes of OMA and NOMA by having the UEs share only a fraction α of *one* RE (cf. Fig. 1a). Such a setup allows some spectrum reuse while limiting the intracell interference encountered by UEs, resulting in better throughput than OMA and better coverage than NOMA. This is what we refer to as partial-NOMA in our work. In [10], [11], partial sharing of a RE is accomplished by having the two signals overlap only with a fraction of each other in the frequency domain while having complete access to the entire time slot. The partial overlap in the frequency domain allows using matched filtering at the receiver side, referred to as receive-filtering, to further suppress the interference encountered by the UEs. The receive-filtering also enabled devising a new decoding technique referred to as flexible successive interference cancellation (FSIC). It was shown that receive-filtering in conjunction with FSIC allows partial-NOMA to outperform traditional NOMA in terms of throughput [10] and in terms of the meta distribution [11].

* The authors are with the the Department of Electrical and Computer Engineering, New York University (NYU) Abu Dhabi, UAE (email: {konpal.ali, marwa.chafii}@nyu.edu). M. Chafii is also with NYU WIRELESS, NYU Tandon School of Engineering, New York.

† The author is with the the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE (email: arafat.dweik@ku.ac.ae). A. Al-Dweik is also with the Department of Electrical and Computer Engineering, Western University, London, ON, Canada (email: dweik@fulbrightmail.org).

+ The author is with the Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, Canada (email: ekram.hossain@umanitoba.ca).

B. Motivation

While technologies such as NOMA and partial-NOMA improve spectral efficiency and performance, they also give rise to issues such as increasing the vulnerability of the system to eavesdropping. In particular, NOMA and partial-NOMA are more susceptible to eavesdropping for two main reasons:

- They involve multiple UEs sharing a RE, which grants access that UEs would not have in OMA.
- Using successive interference cancellation (SIC) for NOMA and FSIC for partial-NOMA may require a user to decode a message not intended for it.

A number of works have focused on exploiting the physical nature of the wireless network to enhance security [12]–[17]. This is often based on exploiting the random fluctuations of the received power at the legitimate receiver and eavesdropper that give rise to opportunities for secure information transmission.

C. State of the Art

Due to the susceptibility to eavesdropping and the growing interest in physical layer security, a number of works have studied secure communication for NOMA in various contexts [18]–[28]. The work in [18] studies a two-user NOMA system where a trusted user is paired with an untrusted user. The work investigates the feasibility of achieving outage-optimal performance for the pair under a secrecy outage probability constraint for the trusted user. In [19], a multi-user NOMA setup is studied where the base station (BS) superposes the messages of M legitimate users in a single RE. It is assumed that one eavesdropper is also present. A power allocation strategy is derived that maximizes the secrecy sum rate constrained to a quality of service for each legitimate user. A multiple-input single-output (MISO) NOMA system is studied in [20]. The work proposes a secrecy beamforming scheme that efficiently exploits artificial noise to improve the secrecy of two legitimate users and only degrades the eavesdropper's channel. In [21], jamming is used to improve the secrecy performance of legitimate NOMA users. A multi-antenna full-duplex relay is used to forward information and generate artificial jamming to deteriorate the eavesdropper's performance, while precoding vectors are designed to zero-force the jamming signal at the legitimate receivers. In [22], the focus is on exploiting interference to enhance secure communication; using both intentionally generated interference such as jamming or artificial noise as well as the intracell interference of NOMA is proposed. Scenarios where the eavesdropper is one of the NOMA UEs as well as external eavesdroppers are discussed.

The works in [18]–[22] focus on single cell networks and do not take into account the impact of intercell interference in their analysis. As real networks are becoming more and more dense, taking into account the impact of intercell interference coming from the entire network is becoming crucial. It was shown in [29] that not taking intercell interference into account can significantly overestimate NOMA performance as well as lead to incorrect resource allocation (RA) that has devastating impacts on performance. Similarly, [28] emphasized that not taking into account intercell interference accurately hinders the ability to analyze key system parameters that directly impact NOMA secrecy performance in dense networks such as IoT. Stochastic geometry has succeeded to provide a unified mathematical paradigm for modeling large wireless cellular networks and characterizing their operation while taking intercell interference into account [30]–[33]. The works in [23]–[28] use stochastic geometry tools for studying physical layer security of NOMA.

In [23] and [24], a network with a single BS at the center of a disk with UEs distributed in the inner disk and outer ring is considered. In [23], security for NOMA in a single antenna and multi-antenna scenario in the presence of external eavesdroppers is studied. An exclusion area is adopted around the BS to improve secrecy performance and in the multi-antenna scenario artificial noise is generated by the BS for further improving the security of a beamforming-aided system. In [24], the scenario with external eavesdroppers as well as with internal eavesdroppers, where one of the paired NOMA UEs is the eavesdropper, is considered. The secrecy of an uplink NOMA system with a single BS and external eavesdroppers is studied in [25]. The eavesdroppers are distributed according to a PPP but an eavesdropper exclusion region around the transmitter is considered to enhance security. In [26], secure communication in a hybrid NOMA/power division multiplexing (PDM) IoT system is studied in the presence of external eavesdroppers. In [27], a NOMA assisted millimeter wave simultaneous wireless in simultaneous wireless information and power transfer (SWIPT) unmanned aerial vehicle (UAV) network is considered. Secure communication in the presence of external eavesdroppers is studied. Directional modulation is used to improve security. While the works in [23]–[27] use stochastic geometry tools for modeling the locations of some of the nodes, they do not take into account intercell interference. The secrecy of uplink NOMA in the cellular internet of things (IoT) in the presence of external eavesdroppers is investigated in [28]. This work considers intercell interference. The BS emits jamming signals at all times to deteriorate eavesdropper performance.

D. Contributions

Different from the works in [18]–[22] that focus on single cell networks and the works in [23]–[27], which consider large networks but do not take into account intercell interference, this work, like [28], considers a large network taking into account intercell interference. Unlike [28], however, our focus is on secure communication in the downlink. The aforementioned works study the scenario of external eavesdroppers or internal eavesdropper that are known [18], [22], [24]. In such situations, techniques such as jamming and artificial noise are proposed to improve secure communication. Unlike these works, in our setup, the BS may not have knowledge of the internal eavesdropper. Due to this, unlike the previous works, techniques such as jamming are not considered. Instead, our focus is on 1) the deterioration that can be caused under different eavesdropping scenarios and 2) shedding light on parameter selection to improve secure communication in such circumstances without increasing power consumption and

creating additional network interference that the traditional techniques require. Further, while all of the aforementioned works study secrecy in networks employing NOMA, this work studies secure communication for partial-NOMA networks where NOMA is a special case when the UEs have a full overlap of the RE. As required by the FSIC protocol for partial-NOMA, which becomes SIC for NOMA, decoding messages that require prior decoding and removing of stronger messages is also taken into account as a joint event in this work. This allows us to accurately measure the probabilities of secure communication events.

This work studies a partial-NOMA setup and focuses on scenarios where one of the two paired users attempts to eavesdrop the message of the other user. Partial-NOMA is interesting to study in the context of secure communication as the nature of the technology can provide additional physical layer security, particularly over traditional NOMA setups. This is because partial-NOMA UEs only share a part of the RE making the rest of the information inaccessible, compared to NOMA where information from the entire RE is accessible to all UEs. Additionally, receive-filtering in partial-NOMA further suppresses the message not intended for a receiver, making decoding harder for an eavesdropper. While the strong UE always decodes the message of the weaker UE in NOMA, in partial-NOMA with FSIC this is not always the case, thereby improving the security of the weaker UE. These factors make investigating the physical layer security achievable in a partial-NOMA setup and comparing to that for traditional NOMA interesting. It also helps highlight the impact of network parameters on physical layer security as well as identify regions where partial-NOMA is superior to NOMA. To the best of our knowledge, this is the first work to: 1) study physical layer security of partial-NOMA networks, where NOMA is a special case, 2) study physical layer security of NOMA (and partial-NOMA) in a large downlink network taking into account the impact of intercell interference on secure communication. The main contributions of this work can be summarized as follows:

- We study the physical layer security achievable in a partial-NOMA or NOMA setup for three eavesdropping scenarios:
  - The strong UE is a malicious eavesdropper and prioritizes decoding the weak UE's message.
  - The strong UE is a passive eavesdropper and only decodes the weak UE's message when FSIC/SIC requires it for decoding its own message.
  - The weak UE is a malicious eavesdropper and prioritizes decoding the strong UE's message.
- We define the event of secure communication in each of the three eavesdropping scenarios. The mathematical analysis for the secrecy probability of each scenario is derived for partial-NOMA and for traditional NOMA.
- We show the non-trivial impact on secure communication of taking into account intercell interference. We find that the impact of intercell interference is not always negative; in fact, at larger α (including NOMA), intercell interference improves secure communication significantly. Further, we show that without intercell interference, the impact of network parameters such as α on secure communication trends is completely misleading.
- For each eavesdropping scenario in partial-NOMA, we compute the secrecy probability for a decoding strategy where: (I) receive-filtering is followed by SIC instead of FSIC, (II) FSIC is used without receive-filtering.
- We find that not employing FSIC or receive-filtering for partial-NOMA can have a drastic negative impact on secrecy. For instance, without FSIC, secure communication is not possible at lower α values. This emphasizes the significance of the partial-NOMA decoding approach on not just coverage but also secure communication.
- We show that partial-NOMA can achieve much higher secrecy than NOMA. Gains of upto 3166%, 1198% and 356% are seen in the malicious strong, passive strong and malicious weak eavesdropper cases, respectively. However, we also find that partial-NOMA with certain overlap values can perform worse than NOMA. These results highlight: 1) that secure communication does not necessarily decrease monotonically with α, 2) the significant impact of a carefully chosen overlap on secrecy performance, 3) the ability to improve secure communication from that in NOMA without using traditional techniques such as jamming that increase power consumption and create additional network interference.

The rest of the paper is organized as follows. The system model is described in Section II. In Section III, the analysis for physical layer security is provided. The results are presented in Section IV and the paper is concluded in Section V.

Notation: We denote vectors using bold text, $\|\mathbf{z}\|$ is used to denote the Euclidean norm of the vector $\mathbf{z}$ and $b(\mathbf{z}, R)$ denotes a ball centered at $\mathbf{z}$ with radius R. The ordinary hypergeometric function is denoted by ${}_2F_1$. The Laplace transform (LT) of the PDF of the RV X is denoted by $\mathcal{L}_X(s) = \mathbb{E}[e^{-sX}]$ where $\mathbb{E}[\cdot]$ is the statistical expectation. The probability is denoted as $\mathbb{P}$. The indicator function, denoted as $\mathbb{1}_A$ has value 1 when event A occurs and is 0 otherwise. We use $\mathrm{Sinc}(x) = \sin(\pi x)/(\pi x)$ when $x \neq 0$, and $\psi(x) = 1$ when $x = 0$.

II. System Model and Assumptions

A. Network Model

This work considers a downlink cellular network where BSs are distributed according to a homogeneous Poisson point process (PPP) Φ with intensity λ. We assume an interference-limited regime. A BS serves two UEs in each RE via partial-NOMA using a total power budget of $P = 1$. We study the performance of one such RE in this work. To the network we add a BS at the origin $\mathbf{o}$, which under expectation over Φ, becomes the typical BS serving UEs in the typical cell. In the remainder of this work, we study the typical cell. Since Φ does not include the BS at $\mathbf{o}$, the set of interfering BSs for the UEs in the typical cell is denoted by Φ. The distance between the typical BS at $\mathbf{o}$ and its nearest neighboring BS is denoted by ρ. Since Φ is a PPP, the PDF of ρ is

$$f_\rho(x) = 2\pi\lambda x e^{-\pi\lambda x^2}, \quad x \geq 0. \tag{1}$$

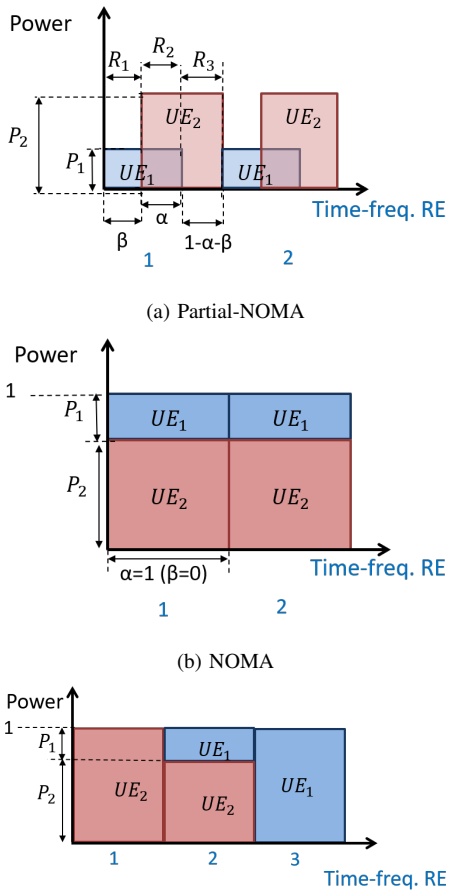
Consider a disk around the BS at $\mathbf{o}$ with radius $\rho/2$, i.e., $b(\mathbf{o}, \rho/2)$; this is referred to as the in-disk [10], [34], [35]. The in-disk is the largest disk centered at a BS that fits inside its Voronoi cell. We study a model where the two partial-NOMA UEs are distributed uniformly and independently at random in the in-disk $b(\mathbf{o}, \rho/2)$ of the BS at $\mathbf{o}$. The rationale behind using a model like this one, where UEs are not too far from the serving BS, in setups where each UE does not have an individual dedicated RE was shown in [35]. In this work we assume that one of the partial-NOMA UEs sharing a RE eavesdrops the message of the other UE. We assume that the eavesdropper has the capability to demodulate and decode the message not intended for it. The specific eavesdropping scenarios studied in this work are detailed in Section III.

We assume a Rayleigh fading environment such that the fading coefficients are independent and identically distributed (i.i.d.) with a unit mean exponential distribution. A power-law path-loss model is considered where the signal decays at the rate $r^{-\eta}$ with distance r, $\eta > 2$ denotes the path-loss exponent and $\delta = \frac{2}{\eta}$. Fixed rate transmissions are used by the BSs where the transmission rate of each UE can be different. Such transmissions result in effective rates, referred to as the throughput of the UEs, that are lower than the transmission rate because of outage.

B. Partial-NOMA Model

A BS serves two UEs in each RE via partial-NOMA by multiplexing the signals for each UE with different power levels using the total power budget. While in traditional NOMA, the two UEs have complete access to the full RE, i.e., the entire time slot and the whole frequency channel, each UE in partial-NOMA has access only to a part of the RE as shown in Fig. 1a. This makes it different from hybrid setups where some REs employ NOMA while others employ OMA (cf. Fig. 1c) and the average performance over multiple REs is studied [1]–[9]. In our work two UEs share a RE, overlapping over only a fraction of the RE and we study the performance of one such RE.

In our partial-NOMA setup, the RE is split into three regions, R_1, R_2 and R_3 as shown in Fig. 1. The fraction of the RE in region R_2 that the two UEs share is denoted by α. In particular, the UEs have full access to the time slot while they share an overlap α of the frequency channel. It should be noted that another way to achieve an overlap α of the RE is by having full access to the frequency channel for each UE and only an overlap α of the time slot. Such an overlap scenario is not studied in this work. We refer to the fraction of the RE in region R_1, accessible to only UE_1, by β, where $0 \leq \beta \leq 1-\alpha$. Thus, the fraction of the bandwidth available to UE_1 is $\text{BW}_1 = \alpha + \beta$. The remaining fraction of the bandwidth, $1-\alpha-\beta$, in region R_3, is available solely to UE_2. The total fraction of the bandwidth thus available to UE_2 is $\text{BW}_2 = 1-\beta$. With a slight abuse of notation, in the remainder of the manuscript, we will refer to the overlap α in the frequency channel of the RE simply as an overlap α of the RE. As the entire time slot is available to both UEs, we will disregard this aspect when referring to the partial overlap



(a) Partial-NOMA

(b) NOMA

(c) A hybrid setup that employs NOMA in some REs and OMA in other REs.

Fig. 1: A contrast between partial-NOMA with overlap $0 \leq \alpha \leq 1$, traditional NOMA with $\alpha = 1$ and a hybrid setup.

of a RE. Additionally, as shown in Fig. 1, in the special case of $\alpha = 1$, partial-NOMA becomes traditional NOMA as the UEs overlap over the complete RE. Thus, traditional NOMA is, loosely speaking, a subset of partial-NOMA.

An overlap in the frequency domain allows implementing filtering at the receiver side to further suppress interference. A matched filter that has a Fourier transform equal to the complex conjugate of the Fourier transform of the transmitted signal is used [10], [36], [37]. In this work, we assume that square pulses are used for transmissions of both UEs. Receive-filtering results in any message that has only an α-overlap with the message of the UE of interest to be scaled by an effective interference factor $0 \leq \mathcal{I}(\alpha, \beta) \leq 1$[1]. From [10], the effective interference factor as a function of β and the overlap α is calculated as

$$\mathcal{I}(\alpha,\beta) = \left(\int_{\beta}^{\beta+\alpha} \frac{1}{E_1 E_2} \text{Sinc}\left(\frac{2(f-f_a)}{\text{BW}_1}\right) \text{Sinc}\left(\frac{2(f-f_b)}{\text{BW}_2}\right) df \right)^2, \tag{2}$$

[1]Note that messages that overlap completely with the message of interest (like in the case of traditional NOMA), even after receive-filtering, are not suppressed as the effective interference factor in this case is 1.

where the center frequency of UE_1's message is $f_a = \frac{\alpha+\beta}{2}$ and UE_2's message is $f_b = \frac{1+\beta}{2}$. The factors E_i for $i \in \{1,2\}$ are used to scale the energy to 1 and are calculated as $E_i^2 = \int_{-\text{BW}_i/2}^{\text{BW}_i/2} \text{Sinc}^2\left(\frac{2f}{\text{BW}_i}\right) df$. Note that $\mathcal{I}(\alpha,\beta)$ is 0 when $\alpha = 0$, is 1 when $\alpha = 1$, and increases monotonically with α [10, Fig. 2]. As $0 \leq \mathcal{I}(\alpha,\beta) \leq 1$, receive-filtering suppresses the intracell interference from the other UE partially sharing the RE. Since any message that has an α-overlap with the UE of interest is scaled by $\mathcal{I}(\alpha,\beta)$, not only does receive-filtering suppress intracell interference, but also reduces intercell interference.

Similar to NOMA, partial-NOMA requires ordering UEs based on some measure of channel strength. This is required for both RA and decoding. In this work, we order the UEs based on the link distance, R, between the typical BS at $\mathbf{o}$ and its UEs uniformly distributed in the in-disk with radius ρ; the link distance is thus conditioned on ρ. Ordering UEs based on increasing link distance is equivalent to ordering based on the decreasing received mean signal power, i.e., $R^{-\eta}$. From hereon, we refer to the strong (weak) UE, with the shorter (longer) link distance, as UE_1 (UE_2). As the order of the UEs is known at the BS, we use ordered statistics for the PDF of R_i, the ordered link distance of UE_i, where $i \in \{1,2\}$. Using the theory of order statistics [38], in the typical cell

$$f_{R_i|\rho}(r \mid \rho) = \frac{16r}{\rho^2}\left(\frac{4r^2}{\rho^2}\right)^{i-1}\left(1-\frac{4r^2}{\rho^2}\right)^{2-i} \quad 0 \leq r \leq \frac{\rho}{2}. \quad (3)$$

While traditional NOMA uses SIC for decoding, FSIC was introduced in [10] to decode partial-NOMA UEs. In conventional SIC, a strong UE decodes and removes the message of the weak UE before decoding its own message. After matched filtering in partial-NOMA, however, the message of the weak UE scaled by $\mathcal{I}(\alpha,\beta)$ may be too weak for the strong UE to decode. FSIC was introduced to combat this problem and improve performance. In particular, the strong UE, i.e., UE_1 using FSIC can decode its own message in either of two ways: 1) Similar to conventional SIC, the message of UE_2 is first decoded, treating the message of UE_1 as noise, and removed, followed by decoding of the message of UE_1, or 2) the message of UE_1 is decoded while treating the interference from the message of UE_2 as noise. Decoding for UE_2 in FSIC, as in SIC, involves simply decoding its own message while treating the message of UE_1 as noise. Again, note that, loosely speaking, SIC is a subset of FSIC.

The power allocated to UE_i is denoted by P_i where $i \in \{1,2\}$. Since fixed rate transmission is used in this work, the transmission rate corresponding to the message of UE_i is $\log(1+\theta_i)$. Accordingly, a UE can only decode the message of UE_i if its signal-to-interference ratio (SIR) exceeds θ_i. While SIC requires the message of UE_2 to be decoded by both UEs all the time, FSIC requires the message of UE_2 to be decoded by both UEs some of the time. Thus, as in the case of SIC, FSIC allocates resources so that the message of UE_2 is easier to decode by allocating it higher power and/or lower transmission rate. While the two UEs only have an α overlap in the RE, since the power allocated to a UE in a RE is fixed over the RE and as the sum power of the two UEs can never exceed the power budget of $P = 1$, we have $P_1 + P_2 = 1$. Thus, in the non-overlap areas of the RE, the power being used will be less than the power budget as shown in Fig. 1. The throughput of UE_i, $i \in \{1,2\}$ is defined as $\mathcal{T}_i = \text{BW}_i\, \mathbb{P}(C_i)\, \log(1+\theta_i)$, where C_i is the event that UE_i is in coverage. The cell sum throughput of the typical cell is thus $\mathcal{T}_1 + \mathcal{T}_2$. As BW_i is a function of both α and β, the resources to be allocated in a partial-NOMA setup for a given α are $P_1 = (1-P_2)$, θ_1, θ_2 and β.

C. SIRs Associated with Partial-NOMA and Coverage Events

Since partial-NOMA uses FSIC decoding, there are multiple SIRs of interest. For the two-user downlink partial-NOMA setup we require SIR_j^i, the SIR for decoding the j^{th} message at UE_i where $i \leq j$ and the messages of all UEs weaker than UE_j have been removed while the messages of all UEs stronger than UE_j are treated as noise. In particular, these are

$$\text{SIR}_2^2 = \frac{h_2 R_2^{-\eta} P_2}{h_2 R_2^{-\eta} P_1 \mathcal{I}(\alpha,\beta) + \tilde{I}_2^{\phi}} \quad (4)$$

$$\text{SIR}_2^1 = \frac{h_1 R_1^{-\eta} P_2 \mathcal{I}(\alpha,\beta)}{h_1 R_1^{-\eta} P_1 + \tilde{I}_1^{\phi}} \quad (5)$$

$$\text{SIR}_1^1 = \frac{h_1 R_1^{-\eta} P_1}{\tilde{I}_1^{\phi}}. \quad (6)$$

For $i \in \{1,2\}$, $\tilde{I}_i^{\phi}$ is the inter-cell interference experienced at UE_i, $\tilde{I}_i^{\phi} = (P_i + (1-P_i)\mathcal{I}(\alpha,\beta)) \sum_{\mathbf{x}\in\Phi} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta}$, where $\mathbf{y}_i = \mathbf{x} - \mathbf{u}_i$ and $\mathbf{u}_i$ is the location of UE_i. The fading coefficient from the serving BS (interfering BS) located at $\mathbf{o}$ ($\mathbf{x}$) to UE_i is h_i ($g_{\mathbf{y}_i}$). For notational convenience, the intercell interference scaled to unit transmission power by each interferer is defined as I_i^{ϕ}; hence, $\tilde{I}_i^{\phi} = (P_i + (1-P_i)\mathcal{I}(\alpha,\beta))\, I_i^{\phi}$. Note that since $(P_i + (1-P_i)\mathcal{I}(\alpha,\beta)) \leq 1$, intercell interference in the partial-NOMA setup is lower than in OMA and NOMA. Additionally, since the network model conditions an interferer to exist at a distance ρ from the typical BS at $\mathbf{o}$, we can rewrite I_i^{ϕ} as

$$I_i^{\phi} = \sum_{\substack{\mathbf{x}\in\Phi \\ \|\mathbf{x}\|>\rho}} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta} + \sum_{\substack{\mathbf{x}\in\Phi \\ \|\mathbf{x}\|=\rho}} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta}. \quad (7)$$

Note that as there is no interfering BS inside $b(\mathbf{o},\rho)$, the nearest interfering BS from UE_i is at least $\rho - R_i$ away. As $\rho - R_i > R_i$, the in-disk model offers a larger guard zone than the usual guard zone of link distance for UEs in a downlink Poisson network [34].

While SIR_1^1 is the SIR associated with UE_1 decoding its message after the message of UE_2 has been decoded and removed, FSIC also allows UE_1 to decode its own message while treating the message of UE_2 as noise. The SIR associated with UE_1 for decoding its own message when the message of UE_2 has not been removed is

$$\widetilde{\text{SIR}}_1^1 = \frac{h_1 R_1^{-\eta} P_1}{h_1 R_1^{-\eta} P_2 \mathcal{I}(\alpha,\beta) + \tilde{I}_1^{\phi}}. \quad (8)$$

As FSIC decoding for UE_2 involves decoding its own message while treating the interference from the message of UE_1 as noise, the event of successful decoding at UE_2 is defined as

$$C_2 = \left\{\text{SIR}_2^2 > \theta_2\right\} = \left\{h_2 > R_2^{\eta} \tilde{I}_2^{\phi} \bar{M}_2\right\}, \quad (9)$$

where

$$\bar{M}_2 = \frac{\theta_2}{P_2 - \theta_2 P_1 \mathcal{I}(\alpha,\beta)}. \tag{10}$$

FSIC decoding for UE_1, on the other hand, is the joint event as described in Section II-B. The event of successful decoding at UE_1 is thus defined as

$$\begin{aligned} C_1 &= \left\{ \left(\mathrm{SIR}_2^1 > \theta_2 \bigcap \mathrm{SIR}_1^1 > \theta_1 \right) \bigcup \widetilde{\mathrm{SIR}}_1^1 > \theta_1 \right\} \\ &= \left\{ h_1 > R_1^{\eta} \tilde{I}_1^{\phi} M_1 \bigcup h_1 > R_1^{\eta} \tilde{I}_1^{\phi} M_0 \right\} \\ &= \left\{ h_1 > R_1^{\eta} \tilde{I}_1^{\phi} \bar{M}_1 \right\}, \end{aligned} \tag{11}$$

where

$$\begin{aligned} \bar{M}_1 &= \min\{M_0, M_1\} \mathbb{1}_{\tilde{P}_1>0} \mathbb{1}_{\tilde{P}_2^1>0} \mathbb{1}_{P_1>0} + \\ & M_0 \mathbb{1}_{\tilde{P}_1>0} \mathbb{1}_{\tilde{P}_2^1 \le 0 \cup P_1 \le 0} + M_1 \mathbb{1}_{\tilde{P}_1 \le 0} \mathbb{1}_{\tilde{P}_2^1>0} \mathbb{1}_{P_1>0} \end{aligned} \tag{12}$$

using $\tilde{P}_1 = P_1 - \theta_1 P_2 \mathcal{I}(\alpha,\beta)$, $\tilde{P}_2^1 = P_2 \mathcal{I}(\alpha,\beta) - \theta_2 P_1$, $M_0 = \frac{\theta_1}{\tilde{P}_1}$ and $M_1 = \max\left\{ \frac{\theta_2}{\tilde{P}_2^1}, \frac{\theta_1}{P_1} \right\}$.

The event of successful decoding at UE_i is thus of the form $C_i = \left\{ h_i > R_i^{\eta} \tilde{I}_i^{\phi} \bar{M}_i \right\}$. Using $\tilde{I}_i^{\phi} = (P_i + (1-P_i)\mathcal{I}(\alpha,\beta)) I_i^{\phi}$ and $\tilde{M}_i = (P_i + (1-P_i)\mathcal{I}(\alpha,\beta))\bar{M}_i$, we can rewrite C_i as

$$C_i = \left\{ h_i > R_i^{\eta} I_i^{\phi} \tilde{M}_i \right\}. \tag{13}$$

Note that if either $\bar{M}_1 < 0$ or $\bar{M}_2 < 0$, we have guaranteed outage because of the choice of RA and parameter selection (θ_1, θ_2, P_1, α, β) [10]. In such a scenario there is no transmission, and therefore, no secure communication.

III. Analysis for Physical Layer Security

In this section, we focus on physical layer security which is based on exploiting the nature of the wireless network to enhance security. As has been mentioned, this involves exploiting random fluctuations in the power at the intended receiver and eavesdropper. In particular, in instances when the eavesdropper receives a deteriorated version of the signal while the legitimate receiver receives a strong signal, the transmitter can send the message of interest at a transmission rate higher than the capacity of the eavesdropper link. This will lead to the event of opportunistic secure spectrum access (OSSA) defined in [17] where the eavesdropper cannot decode the message while the legitimate receiver can. In this work, we define the *secrecy probability* as the probability of OSSA and use this as the metric for measuring the physical layer security our setup can achieve.

Partial-NOMA and NOMA are susceptible to eavesdropping for two main reasons: 1) the overlap α of the RE shared by the two UEs, 2) the use of FSIC (SIC) in partial-NOMA (NOMA) which at times (always) requires UE_1 to decode the message of UE_2. In this work, we study the following three scenarios:

- UE_1 is an active malicious eavesdropper that prioritizes decoding the message of UE_2, the legitimate receiver. We refer to this as the *malicious eavesdropping UE*$_1$.
- UE_1 is a passive or 'lazy' eavesdropper and it does not prioritize eavesdropping. It therefore only decodes the message of UE_2, the legitimate receiver, when it is required for decoding its own message.We refer to this as the *innocent eavesdropping UE*$_1$.
- UE_2 is an active eavesdropper and prioritizes decoding the message of UE_1, the legitimate receiver. We refer to this as the *malicious eavesdropping UE*$_2$.

To be explicit, we formally define the secrecy probability in our setup below.

Definition 1: Secrecy probability *- denoted by $\mathbb{P}_{\mathrm{sec}}$, is the probability of the event that the legitimate UE is able to decode its own message and that the eavesdropping UE is unable to decode the message of the legitimate UE.*

Remark 1: We do not study the scenario where UE_2 is a passive eavesdropper as UE_2 does not decode the message of UE_1 in this case (cf. (9)).

Before delving into the secrecy probabilities, we introduce the LT of the intercell interference encountered by the UEs. The LT of I_i^{ϕ}, the intercell interference at the typical UE_i scaled to unit transmission power, conditioned on R_i and ρ was approximated in [34, Lemma 1], [10] as

$$\begin{aligned} \mathcal{L}_{I_i^{\phi}|R_i,\rho}(s) \approx & \exp\left(\frac{-2\pi\lambda s/(\eta-2)}{(\rho - R_i)^{\eta-2}} {}_2F_1\left(1, 1-\delta; 2-\delta; \frac{-s}{\rho - {R_i}^{\eta}}\right)\right) \\ & \times \frac{1}{1+s\rho^{-\eta}} \end{aligned} \tag{14}$$

$$\overset{\eta=4}{=} e^{-\pi\lambda\sqrt{s}\tan^{-1}\left(\frac{\sqrt{s}}{(\rho-R_i)^2}\right)} \frac{1}{1+s\rho^{-4}}. \tag{15}$$

Consequently, $\mathcal{L}_{\tilde{I}_i^{\phi}|R_i,\rho}(s) = \mathcal{L}_{I_i^{\phi}|R_i,\rho}\left(\widehat{P}_i\ s\right)$, where $\widehat{P}_i = (P_i + (1-P_i)\mathcal{I}(\alpha,\beta))$.

A. Malicious Eavesdropping UE$_1$

In the case of a malicious eavesdropping UE_1 in partial-NOMA, secure communication is achieved when UE_2 is in coverage (i.e., the event C_2 occurs) and UE_1 is in one of the following situations:

i) UE_1 can only decode its own message while treating the message of UE_2 as noise and also cannot extract the message of UE_2 after (and therefore also before) decoding its own message.
ii) UE_1 is unable to decode its own message and also cannot extract the message of UE_2.

Note that as UE_1 is malicious, we consider the possibility of UE_1 decoding UE_2's message even if it cannot decode its own message after removing the message of UE_2. Based on these, we can write the secrecy probability in the presence of a malicious UE_1 in partial-NOMA as

$$\begin{aligned} \mathbb{P}_{\mathrm{sec}} = \mathbb{P}\Bigg(C_2 \bigcap \Bigg(& \left(\widetilde{\mathrm{SIR}}_1^1 > \theta_1 \bigcap h_1 < \frac{R_1^{\eta} \tilde{I}_1^{\phi} \theta_2}{P_2 \mathcal{I}(\alpha,\beta)} \right) \\ & \bigcup \left(\mathbb{1}_{\bar{M}_1>0} \left(h_1 < R_1^{\eta} \tilde{I}_1^{\phi} \bar{M}_1 \right) \bigcap \mathrm{SIR}_2^1 < \theta_2 \right) \Bigg) \Bigg). \end{aligned} \tag{16}$$

Theorem 1: The secrecy probability when UE_1 is a malicious eavesdropper in a partial-NOMA network is

$$\mathbb{P}_{\mathrm{sec}} = \mathbb{E}_{\rho}\left[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^{\phi}|R_2,\rho}\left(\frac{\widehat{P}_2 \bar{M}_2}{R_2^{-\eta}} \right) \right] \left(\mathbb{E}_{R_1|\rho}\left[\mathbb{1}_{\tilde{P}_1>0} \right. \right. \right.$$

$$\mathbb{1}_{\frac{\theta_2}{P_2\mathcal{I}(\alpha,\beta)}>M_0}\left(\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\frac{\widehat{P}_1 M_0}{R_1^{-\eta}}\right)-\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\frac{\widehat{P}_1 R_1^{\eta}\theta_2}{P_2\mathcal{I}(\alpha,\beta)}\right)\right)\mathbb{1}_{\bar{M}_1>0}\left(1-\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\widehat{P}_1 R_1^{\eta}\bar{M}_1\right)\right)\Bigg]\Bigg)\Bigg], \tag{20}$$

$$+\mathbb{1}_{\bar{M}_1>0}\Bigg(1-\mathbb{1}_{\tilde{P}_2^1>0}\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\widehat{P}_1 R_1^{\eta}\min\left(\bar{M}_1,\frac{\theta_2}{\tilde{P}_2^1}\right)\right)-\mathbb{1}_{\tilde{P}_2^1\leq 0}\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\widehat{P}_1 R_1^{\eta}\bar{M}_1\right)\Bigg)\Bigg]\Bigg)\Bigg], \tag{17}$$

where $\mathcal{L}_{I_i^{\mathrm{e}}|R_i,\rho}(s)$ for $i\in\{1,2\}$ is given in (14).

Proof: See **Appendix A**. □

Corollary 1: The secrecy probability when UE_1 is a malicious eavesdropper in a NOMA network is

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\theta_2 R_2^{\eta}}{P_2-\theta_2 P_1}\right)\right]\Bigg(\mathbb{E}_{R_1|\rho}\Bigg[\mathbb{1}_{M_1>0}\Bigg(1-\mathbb{1}_{P_2>\theta_2 P_1}\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(R_1^{\eta}\min\left(M_1,\frac{\theta_2}{P_2-\theta_2 P_1}\right)\right)-\mathbb{1}_{P_2\leq\theta_2 P_1}\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(R_1^{\eta}M_1\right)\Bigg)\Bigg]\Bigg)\Bigg]. \tag{18}$$

Proof: Along the lines of the proof of Theorem 1 and since UE_1 in NOMA cannot decode its own message while treating the message of UE_2 as noise, the contribution to secure communication from $A_{\mathrm{mal}}^{\mathrm{UE}_1}=0$. Thus we have $B_{\mathrm{mal}}^{\mathrm{UE}_1}$ when $\alpha=1$ ($\because\mathcal{I}(\alpha,\beta)=1$) and SIC is used instead of FSIC. □

B. Innocent Eavesdropping UE$_1$

In the case of a rather innocent eavesdropping UE_1 in partial-NOMA, secure communication is achieved when UE_2 is in coverage (i.e., the event C_2 occurs) and UE_1 is in one of the following situations:

i) UE_1 can only decode its own message while treating the message of UE_2 as noise.
ii) UE_1 can decode both messages and it can also decode its own message while treating the message of UE_2 as noise. However, the latter is chosen as it is easier for UE_1.
iii) UE_1 is unable to decode its own message, i.e., it is in outage.

Based on these, we can write the secrecy probability in the presence of an innocent UE_1 in partial-NOMA as

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{P}\Bigg(C_2\bigcap\Bigg(\left(\widetilde{\mathrm{SIR}}_1^1>\theta_1\bigcap\left(\mathrm{SIR}_2^1<\theta_2\bigcup\mathrm{SIR}_1^1<\theta_1\right)\right)\bigcup\left(\widetilde{\mathrm{SIR}}_1^1>\theta_1\bigcap\left(\mathbb{1}_{M_0<M_1}\left(\mathrm{SIR}_2^1>\theta_2\bigcap\mathrm{SIR}_1^1>\theta_1\right)\right)\right)\bigcup\left(\mathbb{1}_{\bar{M}_1>0}\left(h_1<R_1^{\eta}\tilde{I}_1^{\mathrm{e}}\bar{M}_1\right)\right)\Bigg)\Bigg). \tag{19}$$

Theorem 2: The secrecy probability when UE_1 is an innocent eavesdropper in a partial-NOMA network is

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\widehat{P}_2\bar{M}_2}{R_2^{-\eta}}\right)\right]\Bigg(\mathbb{E}_{R_1|\rho}\Bigg[\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\frac{\widehat{P}_1 M_0}{R_1^{-\eta}}\right)\times\left(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1\leq 0\cup P_1\leq 0}+\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\right)+\mathbb{1}_{\bar{M}_1>0}\left(1-\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\widehat{P}_1 R_1^{\eta}\bar{M}_1\right)\right)\Bigg]\Bigg)\Bigg], \tag{20}$$

where $\mathcal{L}_{I_i^{\mathrm{e}}|R_i,\rho}(s)$ for $i\in\{1,2\}$ is given in (14).

Proof: See **Appendix B**. □

Corollary 2: The secrecy probability when UE_1 is an innocent eavesdropper in a NOMA network is

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\theta_2 R_2^{\eta}}{P_2-\theta_2 P_1}\right)\right]\Bigg(\mathbb{E}_{R_1|\rho}\Bigg[\mathbb{1}_{M_1>0}\times\left(1-\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(R_1^{\eta}M_1\right)\right)\Bigg]\Bigg)\Bigg], \tag{21}$$

Proof: Along the lines of the proof of Theorem 2 and since UE_1 in NOMA cannot decode its own message while treating the message of UE_2 as noise, the contribution to secure communication from $A_{\mathrm{inn}}^{\mathrm{UE}_1}=0$. Thus we have $B_{\mathrm{inn}}^{\mathrm{UE}_1}$ when $\alpha=1$ ($\because\mathcal{I}(\alpha,\beta)=1$) and SIC is used instead of FSIC. □

C. Malicious Eavesdropping UE$_2$

In the case of a malicious eavesdropping UE_2, secure communication is achieved when UE_1 is in coverage (i.e., the event C_1 occurs) and UE_2 is in one of the following situations:

i) UE_2 can decode its own message while treating the message of UE_1 as noise and also cannot extract the message of UE_1 after (and therefore also before) decoding its own message.
ii) UE_2 is unable to decode its own message and also cannot extract the message of UE_1.

Note that while UE_2 does not decode the message of UE_1 in FSIC or SIC, since UE_2 is malicious in this scenario, we consider the possibility of UE_2 decoding UE_1's message. Based on these, we can write the secrecy probability in the presence of a malicious UE_2 as

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{P}\Bigg(C_1\bigcap\Bigg(\left(\mathrm{SIR}_2^2>\theta_2\bigcap h_2<\frac{R_2^{\eta}\tilde{I}_2^{\mathrm{e}}\theta_1}{P_1\mathcal{I}(\alpha,\beta)}\right)\bigcup\Bigg(\left(\mathrm{SIR}_2^2<\theta_2\right)\times\mathbb{1}_{\bar{M}_2>0}\bigcap\left(\mathbb{1}_{P_1\leq\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\bigcup\mathbb{1}_{P_1>\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\frac{h_2 R_2^{-\eta}P_1\mathcal{I}(\alpha,\beta)}{h_2 R_2^{-\eta}P_2+\tilde{I}_2^{\mathrm{e}}}<\theta_1\right)\Bigg)\Bigg)\Bigg). \tag{22}$$

Theorem 3: The secrecy probability when UE_2 is a malicious eavesdropper in a partial-NOMA network is

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\frac{\widehat{P}_1\bar{M}_1}{R_1^{-\eta}}\right)\right]\Bigg(\mathbb{E}_{R_2|\rho}\Bigg[\mathbb{1}_{0<\bar{M}_2<\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)}}\times\left(\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\widehat{P}_2\bar{M}_2}{R_2^{-\eta}}\right)-\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\widehat{P}_2 R_2^{\eta}\theta_1}{P_1\mathcal{I}(\alpha,\beta)}\right)\right)+\mathbb{1}_{\bar{M}_2>0}\times\left(\mathbb{1}_{P_1\leq\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\left(1-\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\widehat{P}_2\bar{M}_2}{R_2^{-\eta}}\right)\right)+\mathbb{1}_{P_1>\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\times\left(1-\mathcal{L}_{I_2^{\mathrm{e}}|R_2,\rho}\left(\frac{\widehat{P}_2}{R_2^{-\eta}}\min\left(\bar{M}_2,\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)-P_2\theta_1}\right)\right)\right)\right)\Bigg]\Bigg)\Bigg], \tag{23}$$

where $\mathcal{L}_{I_i^{\mathrm{e}}|R_i,\rho}(s)$ for $i\in\{1,2\}$ is given in (14).

Proof: See **Appendix C**. □

Corollary 3: The secrecy probability when UE_2 is a malicious eavesdropper in a NOMA network is

$$\mathbb{P}_{\mathrm{sec}}=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^{\mathrm{e}}|R_1,\rho}\left(\frac{M_1}{R_1^{-\eta}}\right)\right]\Bigg(\mathbb{E}_{R_2|\rho}\Bigg[\mathbb{1}_{0<\frac{\theta_2}{P_2-\theta_2 P_1}<\frac{\theta_1}{P_1}}\times$$

$$\left(\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)-\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_1}{P_1}\right)\right)+\mathbb{1}_{\frac{\theta_2}{P_2-\theta_2P_1}>0}\times\left(\mathbb{1}_{P_1\le P_2\theta_1}\left(1-\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)\right)+\mathbb{1}_{P_1>P_2\theta_1}\times\left(1-\mathcal{L}_{I_2^o|R_2,\rho}\left(R_2^\eta\min\left(\frac{\theta_2}{P_2-\theta_2P_1},\frac{\theta_1}{P_1-P_2\theta_1}\right)\right)\right)\right)\right]\Bigg]. \quad (24)$$

Proof: Along the lines of the proof of Theorem 3, using $\alpha = 1$ ($\because \mathcal{I}(\alpha,\beta) = 1$) and SIC instead of FSIC, (24) is obtained. □

D. Impact of Receive-Filtering and FSIC

In addition to studying the secrecy probability for partial-NOMA that employs receive-filtering and FSIC, it is also necessary to highlight the impact that receive-filtering and FSIC have on secrecy of partial-NOMA. We thus study the following two cases for each of the three eavesdropping scenarios in a partial-NOMA network:

(I) When SIC is used by UE_1 instead of FSIC, i.e., UE_1 always decodes and removes the message of UE_2 before decoding its own message.

(II) When receive-filtering is not employed prior to the FSIC decoding. In this scenario, $\mathcal{I}(\alpha,\beta)$ takes on the value 1 for all values of α and β.

Corollary 4: The secrecy probability in the presence of a malicious UE_1 in a partial-NOMA network employing (I) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^o|R_2,\rho}\left(\widehat{P}_2R_2^\eta\bar{M}_2\right)\right]\mathbb{1}_{M_1>0}\mathbb{E}_{R_1|\rho}\Bigg[1-\mathbb{1}_{\tilde{P}_2^1>0}\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{\widehat{P}_1\min\left(M_1,\frac{\theta_2}{\tilde{P}_2^1}\right)}{R_1^{-\eta}}\right)-\mathbb{1}_{\tilde{P}_2^1\le0}\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{\widehat{P}_1M_1}{R_1^{-\eta}}\right)\Bigg]\Bigg]. \quad (25)$$

Proof: With SIC the terms in (17) from $A_{\text{mal}}^{\text{UE}_1}$ become 0. Additionally, as SIC does not allow UE_1 to decode its own message while treating the message of UE_2 as noise, $\bar{M}_1 = M_1$. □

Corollary 5: The secrecy probability in the presence of an innocent UE_1 in a partial-NOMA network employing (I) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^o|R_2,\rho}\left(\widehat{P}_2R_2^\eta\bar{M}_2\right)\right]\mathbb{1}_{M_1>0}\times\left(1-\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^o|R_1,\rho}\left(\widehat{P}_1R_1^\eta M_1\right)\right]\right)\Bigg]. \quad (26)$$

Proof: Following the proof of Corollary 4, the terms in (20) from $A_{\text{inn}}^{\text{UE}_1}$ become 0 and $\bar{M}_1 = M_1$. □

Corollary 6: The secrecy probability in the presence of a malicious UE_2 in a partial-NOMA network employing (I) is $\mathbb{P}_{\text{sec}}\Big|_{\bar{M}_1=M_1}$ in (23).

Proof: As FSIC never requires UE_2 (unlike UE_1) to decode the message of the other UE, when SIC is deployed instead, $A_{\text{mal}}^{\text{UE}_2}$ does not become 0. The only impact of employing (I) is $\bar{M}_1 \to M_1$. We do not write the full equation for brevity. □

Corollary 7: The secrecy probability in the presence of a malicious UE_1 in a partial-NOMA network employing (II) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)\right]\Bigg(\mathbb{E}_{R_1|\rho}\Big[\mathbb{1}_{P_1>\theta_1P_2}\times\mathbb{1}_{\frac{\theta_2}{P_2-\theta_2P_1}>\frac{\theta_1}{P_1-\theta_1P_2}}\left(\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{R_1^\eta\theta_1}{P_1-\theta_1P_2}\right)-\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{R_1^\eta\theta_2}{P_2}\right)\right)+\mathbb{1}_{\bar{M}_1^1>0}\Big(1-\mathbb{1}_{P_2>\theta_2P_1}\mathcal{L}_{I_1^o|R_1,\rho}\left(R_1^\eta\min\left(\bar{M}_1^1,\frac{\theta_2}{P_2-\theta_2P_1}\right)\right)-\mathbb{1}_{P_2\le\theta_2P_1}\mathcal{L}_{I_1^o|R_1,\rho}\left(R_1^\eta\bar{M}_1^1\right)\Big)\Big]\Bigg)\Bigg]. \quad (27)$$

Proof: Along the lines of Theorem 1 and using $\mathcal{I}(\alpha,\beta) = 1$, $\widehat{P}_i|_{\mathcal{I}(\alpha,\beta)=1} = P_i + (1-P_i) = 1$, (27) is obtained where $M_1^1 = M_1\Big|_{\mathcal{I}(\alpha,\beta)=1}$ and $\bar{M}_1^1 = \bar{M}_1\Big|_{\mathcal{I}(\alpha,\beta)=1}$ are used for brevity. □

Corollary 8: The secrecy probability in the presence of an innocent UE_1 in a partial-NOMA network employing (II) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)\right]\Bigg(\mathbb{E}_{R_1|\rho}\Big[\Big(\mathbb{1}_{P_1>\theta_1P_2}\times\mathbb{1}_{P_2\le\theta_2P_1\cup P_1\le0}+\mathbb{1}_{P_1>\theta_1P_2}\mathbb{1}_{P_2>\theta_2P_1}\mathbb{1}_{P_1>0}\mathbb{1}_{\frac{\theta_1}{P_1-\theta_1P_2}<M_1^1}\Big)\times\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{\theta_1R_1^\eta}{P_1-\theta_1P_2}\right)+\mathbb{1}_{\bar{M}_1^1>0}\left(1-\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{\bar{M}_1^1}{R_1^{-\eta}}\right)\right)\Big]\Bigg)\Bigg]. \quad (28)$$

Proof: Along the lines of Theorem 2 and using $\mathcal{I}(\alpha,\beta) = 1$, $\widehat{P}_i|_{\mathcal{I}(\alpha,\beta)=1} = 1$, (28) is obtained where $M_1^1 = M_1\Big|_{\mathcal{I}(\alpha,\beta)=1}$ and $\bar{M}_1^1 = \bar{M}_1\Big|_{\mathcal{I}(\alpha,\beta)=1}$ are used for brevity. □

Corollary 9: The secrecy probability in the presence of a malicious UE_2 in a partial-NOMA network employing (II) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^o|R_1,\rho}\left(\frac{\bar{M}_1^1}{R_1^{-\eta}}\right)\right]\Bigg(\mathbb{E}_{R_2|\rho}\Big[\mathbb{1}_{0<\frac{\theta_2}{P_2-\theta_2P_1}<\frac{\theta_1}{P_1}}\times\left(\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)-\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_1}{P_1}\right)\right)+\mathbb{1}_{\frac{\theta_2}{P_2-\theta_2P_1}>0}\times\left(\mathbb{1}_{P_1\le P_2\theta_1}\left(1-\mathcal{L}_{I_2^o|R_2,\rho}\left(\frac{R_2^\eta\theta_2}{P_2-\theta_2P_1}\right)\right)+\mathbb{1}_{P_1>P_2\theta_1}\times\left(1-\mathcal{L}_{I_2^o|R_2,\rho}\left(R_2^\eta\min\left(\frac{\theta_2}{P_2-\theta_2P_1},\frac{\theta_1}{P_1-P_2\theta_1}\right)\right)\right)\right)\Big]\Bigg)\Bigg]. \quad (29)$$

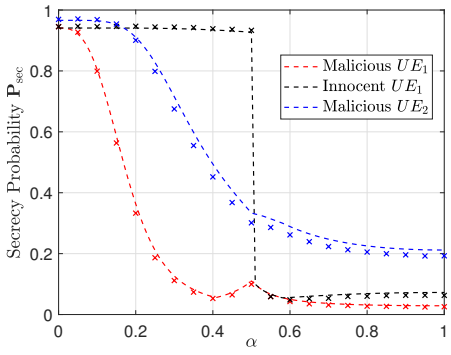
Proof: Following the proof of Corollary 3 but the fact that FSIC is still used. For brevity we use $\bar{M}_1^1 = \bar{M}_1\Big|_{\mathcal{I}(\alpha,\beta)=1}$. □

IV. Results and Discussion

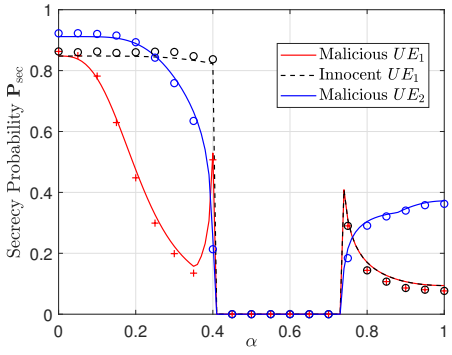
In this section, we consider BS intensity $\lambda = 10$ and $\eta = 4$. Simulations are repeated 10^5 times. As the power budget is $P = 1$, $P_2 = 1 - P_1$. Fixed RA is used in some of the figures while the other figures use the optimum RA associated with a problem that aims to maximize cell sum throughput while constrained to a threshold minimum throughput (TMT) according to [10, Algorithm 1]. Note that solving such a problem results in RA such that the minimum required resources are spent on UE_2 to attain throughput equal to the TMT and the remaining resources are given to UE_1 to maximize its throughput with.

A. Analytical Verification, Impact of Intercell Interference and Secrecy Probability Components

Fig. 2 is a plot of the secrecy probability vs. α for the three eavesdropping scenarios studied in this work using different RA. The figure validates our analysis in Section III as the



(a) $P_1 = 1/3$, $\theta_1 = 0$ dB, $\theta_2 = -3$ dB



(b) $P_1 = 1/3$, $\theta_1 = 5$ dB, $\theta_2 = 2$ dB

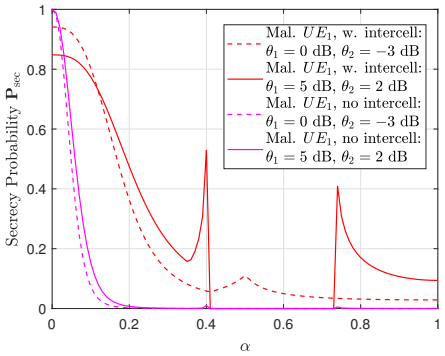
Fig. 2: Secrecy probability versus α for the scenarios of the malicious UE_1, innocent UE_1 and malicious UE_2 using different values of P_1, θ_1, θ_2 and $\beta = (1-\alpha)/2$. Simulations are represented using markers.

simulations are a tight match. We observe that for each eavesdropping scenario, the secrecy probability is high at low α. This happens due to the intrinsic physical layer security provided by the nature of partial-NOMA which makes it difficult to decode the message of the other UE at low α due to low $\mathcal{I}(\alpha, \beta)$. As α increases, a steep drop in secrecy probability is observed for all three cases. The drop in secrecy probability occurs at lower α for the malicious UE_1 and UE_2 cases than for the innocent UE_1, highlighting the increased susceptibility to eavesdropping in the case of the malicious UEs. Further, we observe that for the innocent UE_1 case, this drop, while at higher α, occurs abruptly; for the malicious UE_1 and UE_2 cases the drop is more gradual. The drop in secrecy depends on α where $\mathcal{I}(\alpha, \beta)$ becomes large enough to make the message being eavesdropped sufficiently strong to be decoded by the eavesdropper. In the malicious cases, there is a larger effort to eavesdrop, thus the drop in secrecy occurs at a lower α value; however, it is gradual because $\mathcal{I}(\alpha, \beta)$ is not necessarily large enough for the eavesdropper to be able to decode the message of the other UE most of the time. As anticipated, a malicious UE_1, being the stronger UE, is in general more detrimental to secrecy than a malicious UE_2. Note that in Fig. 2b, with the choice of RA, the secrecy probability becomes 0 for the mid-range α values for all three eavesdropping scenarios. This happens due to the choice of the RA (i.e., P_1, θ_1, θ_2) and α in this range resulting in guaranteed outage (independent of eavesdropping) for partial-NOMA as $\bar{M}_1$ or $\bar{M}_2$ is < 0, thus there is no transmission and therefore no secure communication. After this range of α, transmissions resume and the secrecy probability becomes non-zero again. The figure also highlights that using partial-NOMA with carefully selected α, a significantly higher secrecy probability can be attained than in the case of NOMA ($\alpha = 1$) and without carefully selected α we can end up with no secure communication. The details of the trends of the individual eavesdropper scenarios are explained in Fig.4.

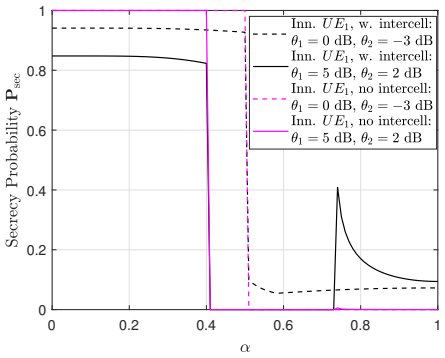
We observe in Fig. 2 that when $\alpha = 0$, while there is zero overlap, implying any eavesdropper is unable to decode the message of the legitimate receiver it is paired with, the secrecy probability is not 1. This stems from the fact that secrecy in our partial-NOMA or NOMA setup, where one of the paired users is eavesdropping the others message, is defined to be the event when the eavesdropper is unable to decode the legitimate receiver's message and the legitimate receiver is able to decode its own message. Thus, at $\alpha = 0$, the secrecy probability becomes the coverage probability of the legitimate receiver.

Fig. 3 is a plot of the secrecy probability vs. α for the three eavesdropping scenarios when the impact of intercell interference is taken into account (as done in this work) and when it is not. In this work we assume an interference-limited regime which is accurate since intercell interference is coming from the large network and noise does not impact the performance.[2] In the scenario without intercell interference, we take into account noise power $\sigma^2 = 10^{-12}$; this is necessary to compute performance for the scenario when there is no intracell interference and no intercell interference. Fig. 3 highlights the non-trivial impact of taking into account inter-cell interference on secrecy performance compared to the scenario where intercell interference is not considered. We firstly observe that accounting for intercell interference does not lead to a simple performance degradation, which is a common mis-assumption, but a change in the trends of performance. The presence of intercell interference helps obtain non-zero secrecy probability at higher α values for all the eavesdropping scenarios; this highlights the role of intercell interference in protecting the network against eavesdropping. Interestingly, we observe that at lower α values, taking into account intercell interference results in a degradation in secrecy but at larger α values (including the case of NOMA, i.e., $\alpha = 1$), it results in an improvement in secure communication. At lower α, it is difficult for the eavesdropper to decode the message not intended for it due to the smaller overlap. Introducing intercell interference has a more significant and negative impact on the legitimate receiver in this scenario, resulting in a decrease in secrecy probability. At higher α, however, the eavesdropper is better able to decode the message not intended for it. The presence of intercell interference here helps improve secure communication by having a significant deteriorating impact on the eavesdroppers channel. We also observe that while secrecy probability falls with α at lower α values, in the absence of intercell interference, this happens much faster for the malicious eavesdropper cases. This highlights the protection

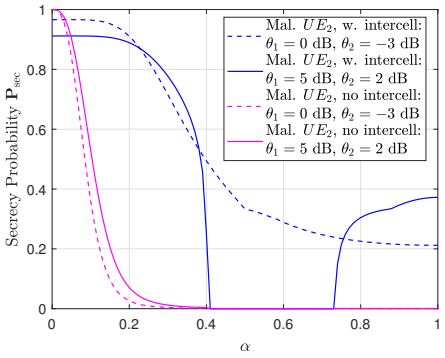
[2]Using the SIR instead of the SINR to compute secrecy probabilities in this interference-limited regime also helps avoid the equations becoming much longer without impacting the performance.



(a) Malicious UE_1

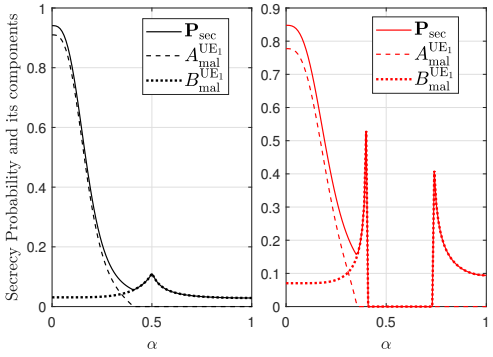


(b) Innocent UE_1

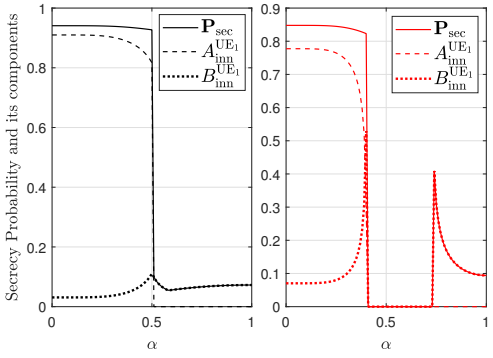


(c) Malicious UE_2

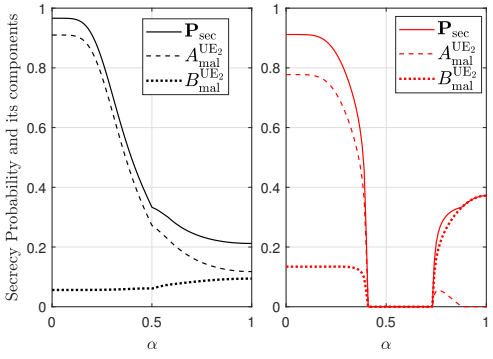
Fig. 3: Secrecy probability versus α for the three eavesdropping scenarios using $P_1 = 1/3$, $\beta = (1-\alpha)/2$ and different θ_1 and θ_2. The probabilities for both the scenario with intercell interference and without it (in magenta) are plotted.



(a) Malicious UE_1



(b) Innocent UE_1



(c) Malicious UE_2

Fig. 4: Secrecy probability and its components vs. α using $P_1 = 1/3$ and $\beta = (1-\alpha)/2$ for the three eavesdropping scenarios. Black (red) lines use $\theta_1 = 0$ dB and $\theta_2 = -3$ dB ($\theta_1 = 5$ dB and $\theta_2 = 2$ dB) .

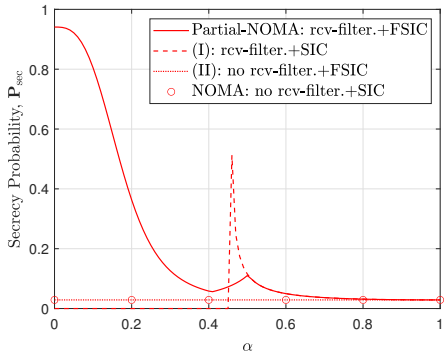
against eavesdropping that the network interference provides even at lower α. The figure highlights the importance of taking into account intercell interference coming from a large network on the performance of secure communication in NOMA and partial-NOMA. In the remainder of the results we do not show the scenario without intercell interference.

Fig. 4 is a plot of the secrecy probability and its components for the three eavesdropping scenarios using $\{\theta_1, \theta_2\} = \{0, -3\}$ dB and $\{5, 2\}$ dB. The components $A_{\text{mal}}^{\text{UE}_1}$ and $A_{\text{inn}}^{\text{UE}_1}$ capture the probability of UE_1 decoding its own message while being unable to decode UE_2's message for the malicious and innocent UE_1 cases, respectively. Similarly, $A_{\text{mal}}^{\text{UE}_2}$ captures the probability of a malicious eavesdropping UE_2 decoding its own message without being able to decode UE_1's message. As the ability to eavesdrop generally increases with α, $A_{\text{mal}}^{\text{UE}_1}$, $A_{\text{inn}}^{\text{UE}_1}$ and $A_{\text{mal}}^{\text{UE}_2}$ decrease monotonically with α in all of the cases except that of $\{\theta_1, \theta_2\} = \{5, 2\}$ dB for the malicious UE_2. Here, due to the choice of parameters and RA, after the guaranteed outage range, the probability becomes non-zero again and then decreases monotonically with α. Since FSIC requires UE_1 to decode and remove the message of UE_2 before decoding its own message, we observe that at higher α $A_{\text{mal}}^{\text{UE}_1} \to 0$ and $A_{\text{inn}}^{\text{UE}_1} \to 0$. Note that $A_{\text{mal}}^{\text{UE}_1} \to 0$ more quickly due to its malicious nature. On the other hand, since FSIC never requires UE_2 to decode UE_1's message, $A_{\text{mal}}^{\text{UE}_2}$ does not go to 0 for $\{\theta_1, \theta_2\} = \{0, -3\}$ dB as the malicious UE_2 is not guaranteed to decode UE_1's message even at high α.

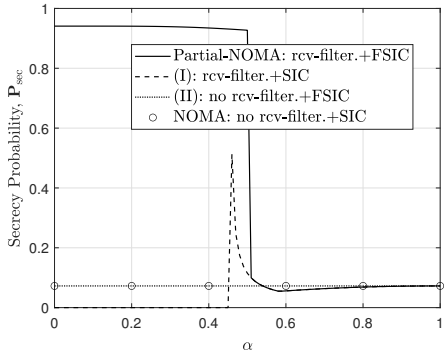
The components $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ capture the probability of UE_1 being unable to decode both its own message as well as the message of UE_2 for the malicious and innocent UE_1 cases, respectively. Similarly, $B_{\text{mal}}^{\text{UE}_2}$ captures the probability of a malicious UE_2 being unable to decode both its own as well as UE_1's message. We observe in Fig. 4 that for $\{\theta_1, \theta_2\} = \{0, -3\}$ dB, $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ have a maxima at $\alpha = 0.5$. Prior to this, FSIC does not require UE_1 to decode and remove the message of UE_2 before decoding its own message. Thus, when $\alpha \leq 0.5$, increasing α increases the interference from the message of UE_2, increasing outage of UE_1 and therefore $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$. Note that in this regime, α is not large enough for the malicious UE_1 to decode UE_2's message without removing its own first, thus $B_{\text{mal}}^{\text{UE}_1}$ is identical to $B_{\text{inn}}^{\text{UE}_1}$ when $\alpha \leq 0.5$. After the optimum, between $0.5 < \alpha \leq 0.58$, both $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ decrease with α. This happens because FSIC requires UE_1 to decode UE_2's message first in this regime; since increasing α makes this easier, a decrease is seen in both $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$. However, when $\alpha > 0.58$, $B_{\text{mal}}^{\text{UE}_1}$ continues decreasing with α while $B_{\text{inn}}^{\text{UE}_1}$ slowly increases with α. When $\alpha > 0.58$, the bottleneck of UE_1's coverage is not decoding UE_2's message anymore but becomes decoding its own message after UE_2's message has been decoded and removed. The innocent UE_1's outage thus increases with α as the intercell interference increases with α, making decoding its own message harder. While in outage, the innocent UE_1, due to its non-malicious nature, does not decode the message of UE_2 either and the secrecy probability component $B_{\text{inn}}^{\text{UE}_1}$ slowly increases with α in this regime. However, the malicious UE_1 can decode the message of UE_2 even when it cannot decode its own message. As this becomes easier with increasing α, the secrecy probability component $B_{\text{mal}}^{\text{UE}_1}$ continues to decrease. Similar trends are observed for $\{\theta_1, \theta_2\} = \{5, 2\}$ dB but the maxima of $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ is hidden in the guaranteed outage region. Thus, we see growth with α before the guaranteed outage and then a decrease with α after this. Note that for $B_{\text{inn}}^{\text{UE}_1}$, due to the choice of RA we never see it slowly increase with α at higher α. For the case of the malicious UE_2, we observe that $B_{\text{mal}}^{\text{UE}_2}$ for $\{\theta_1, \theta_2\} = \{0, -3\}$ dB increases monotonically with α. Until $\alpha = 0.5$, the increase is very slow as decoding its own message becomes harder for UE_2 with increasing interference but at the same time the growing α makes decoding the message of UE_1 easier. These two factors almost counterbalance one another but the decrease in probability of decoding its own message dominates slightly, and we observe a slow increase in $B_{\text{mal}}^{\text{UE}_2}$. After $\alpha = 0.5$, the growing interference when decoding its own message dominates even more, and $B_{\text{mal}}^{\text{UE}_2}$ grows at a faster pace with α. Similar trends are observed for $\{\theta_1, \theta_2\} = \{5, 2\}$ dB but the guaranteed outage region hides the growth occurring gradually with α.

B. Impact of FSIC, Receive-Filtering and RA

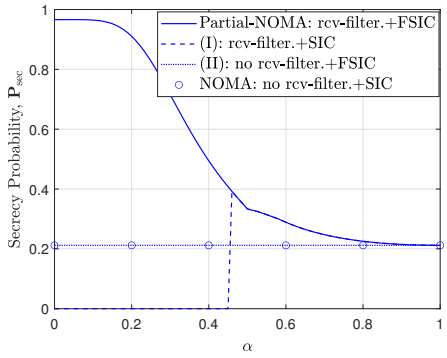
Fig. 5 plots the secrecy probability vs. α and compares the partial-NOMA decoding approach, i.e., receive-filtering and FSIC, with: (I) where receive-filtering is followed by SIC instead of FSIC, (II) where there is no receive-filtering but FSIC is used, and traditional NOMA. We observe that the secrecy probability in (II) is the same as that in traditional NOMA for all three eavesdropping scenarios. This happens because not having receive-filtering results in $\mathcal{I}(\alpha, \beta) = 1$ and as UE_1 is unable to treat the interference from the message of UE_2 as noise when $\mathcal{I}(\alpha, \beta)$ is this high; thus, FSIC→SIC. Consequently, the performance is equivalent to that of a traditional NOMA setup. For (I) the secrecy probability is zero for all three eavesdropping scenarios when $\alpha < 0.46$. In this range of low α, $\tilde{P}_2^1 < 0$ and consequently it is not possible for UE_1 to decode UE_2's message before decoding its own. Since (I) uses SIC and thus requires UE_1 to decode UE_2's message before decoding its own, transmission does not take



(a) Malicious UE_1



(b) Innocent UE_1



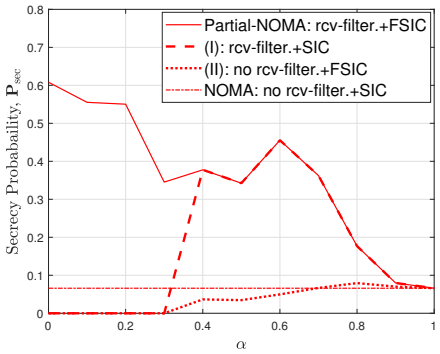
(c) Malicious UE_2

Fig. 5: Secrecy probability for a partial-NOMA setup, partial-NOMA using (I), partial-NOMA using (II) and a traditional NOMA setup versus α using $P_1 = 1/3$, $\beta = (1-\alpha)/2$, $\theta_1 = 0$ dB, $\theta_2 = -3$ dB for the three eavesdropping scenarios.

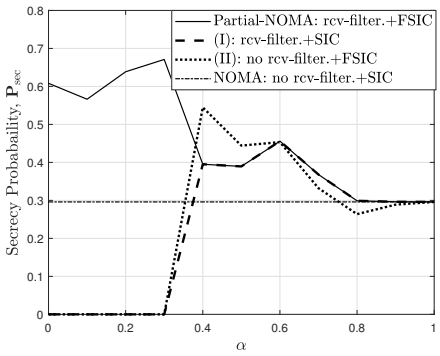
place in this regime of low α and the probability of secure transmission (and any transmission) is zero.

In Fig. 5, once $\alpha \geq 0.46$, $\tilde{P}_2^1 \geq 0$ and we see a jump in secrecy probability of (I) for all three scenarios. Note that since (I) uses SIC instead of FSIC, UE_1 must always decode UE_2's message to decode its own; thus, secure communication in (I) for the innocent and malicious UE_1 scenarios can only be achieved when UE_1 is in outage. Consequently, the contribution to secrecy probability in (I) for the malicious (innocent) UE_1 from $A_{\text{mal}}^{\text{UE}_1}$ ($A_{\text{inn}}^{\text{UE}_1}$) is 0. This is not the case for the malicious UE_2 which is not required to decode UE_1's message for decoding its own even in SIC; thus, we observe that the secrecy probability in the presence of a malicious UE_2 in (I) is identical to the decoding approach for partial-NOMA when $\alpha > 0.46$. While the contribution from $A_{\text{mal}}^{\text{UE}_1}$ ($A_{\text{inn}}^{\text{UE}_1}$) is 0 for the malicious (innocent) UE_1 case, the secrecy probability of (I) is much larger than $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ in Fig. 4 when $0.46 \leq \alpha \leq 0.5$. This happens because although $\tilde{P}_2^1 \geq 0$ when $0.46 \leq \alpha \leq 0.5$ and thus UE_1 can decode the message of UE_2, FSIC (in the partial-NOMA decoding approach) is used in Fig. 4 which opts for UE_1 to treat the message of UE_2 as noise as this is the superior approach in this range of α values. As the partial-NOMA decoding approach decodes UE_1 using a superior technique, it has lower outage, consequently $B_{\text{mal}}^{\text{UE}_1}$ and $B_{\text{inn}}^{\text{UE}_1}$ (which require UE_1 to be in outage for secure communication) in Fig. 4 are lower than the secrecy probability in (I) where UE_1 using the suboptimum SIC in this range of α is more susceptible to being in outage, thereby increasing secrecy probability. We also observe in Fig. 5 that in the range of $0.46 \leq \alpha \leq 0.5$ the secrecy of (I) is superior to the decoding approach of partial-NOMA in the case of the malicious UE_1, while the partial-NOMA approach is superior in case of the innocent UE_1. This happens because in the malicious case, $A_{\text{mal}}^{\text{UE}_1} = 0$ in this range of α (cf. Fig. 4), thus, secrecy probability is $B_{\text{mal}}^{\text{UE}_1}$ which is lower in the partial-NOMA decoding approach than (I). On the other hand, in the innocent case, $A_{\text{mal}}^{\text{UE}_1}$ has a significant contribution to the secrecy probability in the partial-NOMA decoding approach for this range of α, thus although the secrecy probability of (I) in this range of α is larger than $B_{\text{mal}}^{\text{UE}_1}$, it is still less than the secrecy probability of the partial-NOMA decoding approach. When $\alpha > 0.5$, the secrecy probability of the partial-NOMA decoding approach and (I) overlap for the malicious (innocent) UE_1 case as $\mathbb{P}_{\text{sec}} \to B_{\text{mal}}^{\text{UE}_1}$ ($\mathbb{P}_{\text{sec}} \to B_{\text{inn}}^{\text{UE}_1}$) for both approaches in this regime.

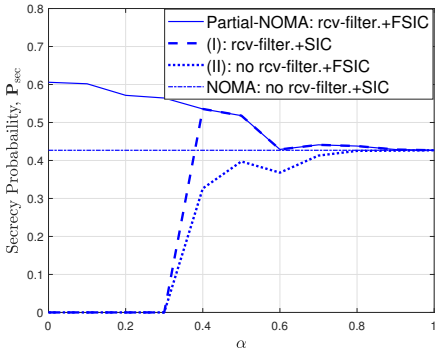
We observe from Fig. 5 that the partial-NOMA decoding approach allows us to attain significant improvement in secure communication compared to a traditional NOMA setup. In particular, by carefully choosing α, gains of as much as 3166%, 1198% and 356% over traditional NOMA can be obtained for the malicious UE_1, innocent UE_1 and and malicious UE_2 cases, respectively. It ought to be mentioned that while these gains are very appealing from a secure communication stand point, the price paid for this is reduced spectral efficiency associated with the lower values of α. Further, these results highlight the significance of FSIC without which secure communication is not possible at low α values. Similarly, without receive-filtering the secrecy probability for all α values drops



(a) Malicious UE_1



(b) Innocent UE_1



(c) Malicious UE_2

Fig. 6: Secrecy probability for a partial-NOMA setup, partial-NOMA using (I), partial-NOMA using (II) and a traditional NOMA setup versus α. Optimum RA for TMT $= 0.25$ in Table I is used.

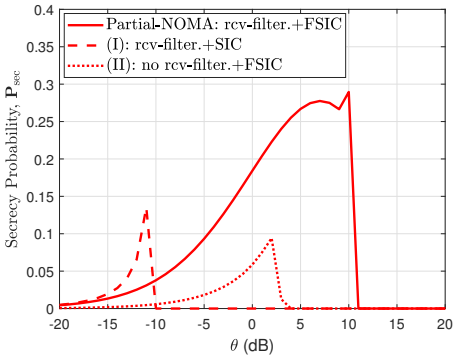
to that of a traditional NOMA network. These observations emphasize the significance of the decoding procedure (i.e., receive-filtering followed by FSIC) used in this work for secure communication. We also observe that careful choice of network parameters such as α is crucial; for instance, operating at $\alpha = 0.6$ in the presence of an innocent UE_1 is slightly inferior to traditional NOMA in terms of secrecy probability, while using $\alpha < 0.5$ results in much superior secrecy.

TABLE I: Optimum RA for each α associated with a TMT$= 0.25$ obtained from [10, Algorithm 1].

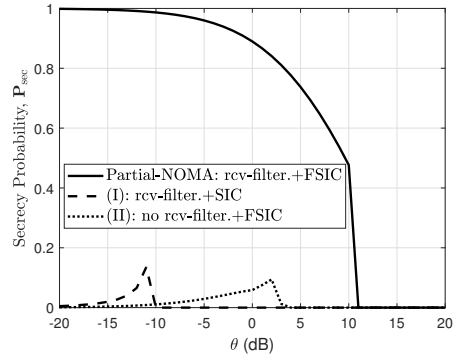
α	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
β	0.8	0.81	0.72	0.7	0.6	0.4	0.4	0.27	0.2	0.1	0
P_1	0.99	0.93	0.92	0.75	0.14	0.36	0.44	0.58	0.61	0.62	0.64
θ_1 (dB)	16	16	15.5	12	14.5	15	17.5	16	15	15	15]
θ_2 (dB)	8.5	9	4.5	3.5	0	-2.5	-2	-3	-3	-3.5	-4

Fig. 6 is a plot of the secrecy probabilities vs. α using the optimum RA associated with each α for a TMT of 0.25 given in Table I. Partial-NOMA outperforms traditional NOMA (i.e., $\alpha = 1$) in terms of secrecy probability for all α values for each of the three eavesdropping scenarios. Similar to Fig. 5, the curves for (I) (i.e., using SIC instead of FSIC) coincide with the partial-NOMA decoding approach (i.e., receive-filtering followed by FSIC) at higher α values ($\alpha \geq 0.4$ in this scenario) as in this regime UE_1 employing FSIC also always decodes and removes the message of UE_2, as in the case of SIC. Prior to this, for $\alpha < 0.4$, the secrecy probability using (I) is zero for all three eavesdropping scenarios as $\tilde{P}_2^1 < 0$, i.e., $M_1 = 0$, and thus transmission does not occur. In contrast to Fig. 5, we observe that the secrecy probability in the case of (II), where there is no receive-filtering, does not coincide with that of traditional NOMA. This occurs because optimum RA has been used in Fig. 6 which is different for each α unlike the previous figure where fixed RA is used. With no receive-filtering in (II), i.e., $\mathcal{I}(\alpha, \beta) = 1$, at low α, $\tilde{P}_2^1 < 0$ and $\tilde{P}_2 - \theta_2 P_1 \mathcal{I}(\alpha, \beta) < 0$; thus, the RA is not sufficient for transmission and secrecy is 0. Due to $\mathcal{I}(\alpha, \beta) = 1$, $\bar{M}_1$ is never M_0, i.e., UE_1 can never decode its own message without decoding UE_2's message. For the malicious UE_1 scenario, secrecy therefore comes from UE_1 being in outage and unable to decode UE_2's message, while in the case of the innocent UE_1, by UE_1 simply being in outage. The high $\mathcal{I}(\alpha, \beta) = 1$ makes the bottleneck of UE_1's outage decoding its own message as decoding the message of UE_2 is easy due to the high $\mathcal{I}(\alpha, \beta)$. Thus, the secrecy probability for the case of the malicious UE_1 in (II) is much lower than the innocent UE_1 case as decoding the message of UE_2 is easy for the malicious UE_1 even when it cannot decode its own message. Similarly, for the case of the malicious eavesdropping UE_2, due to high $\mathcal{I}(\alpha, \beta)$, decoding the message of UE_1 is easy and we observe that the secrecy probability is low. In particular, for the malicious UE_1 and malicious UE_2 scenarios, we observe that without receive-filtering (i.e., (II)) the achievable secrecy probability is almost always lower than that of traditional NOMA, highlighting the significance of receive-filtering in improving secure communication in the presence of a malicious eavesdropper.

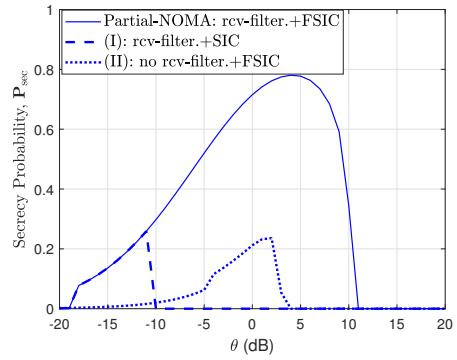
Fig. 7 is a plot of secrecy probability vs. θ, where $\theta = \theta_1 = \theta_2$, for $\alpha = 0.3$. We compare the performance of the partial-NOMA decoding approach with (I) and (II). We observe that for each eavesdropping scenario, the partial-NOMA decoding approach provides secure communication for a significantly broader range of θ than both (I) and (II). Further, the innocent eavesdropping UE_1 allows secure communication for a much broader range of θ than both the malicious UE_1 and malicious UE_2 eavesdropper scenarios, while the malicious eavesdropping UE_1 scenario is the most detrimental in terms of achievable secrecy from all three scenarios. This highlights the harm a strong malicious user can cause and the significance of careful parameter selection and RA in such a scenario to achieve the desired levels of secure communication. We also observe that (I) allows secure communication for a lower range of transmission rates and corresponding θ, while (II) allows this for higher range.



(a) Malicious UE_1



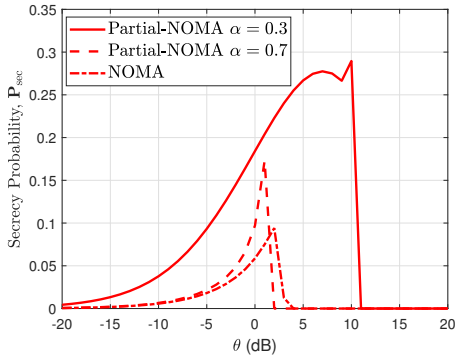
(b) Innocent UE_1



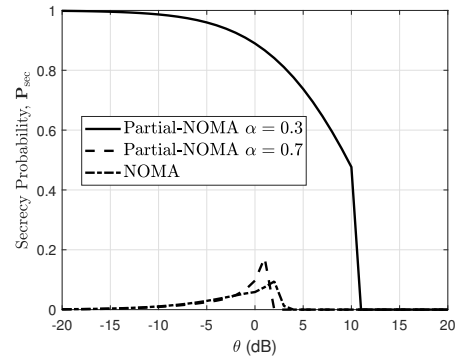
(c) Malicious UE_2

Fig. 7: Secrecy probability for a partial-NOMA setup, partial-NOMA using (I) and partial-NOMA using (II) versus θ, where $\theta = \theta_1 = \theta_2$. We plot the results for $\alpha = 0.3$, $\beta = (1 - \alpha)/2$ and $P_1 = 1/3$ for the three eavesdropping scenarios.

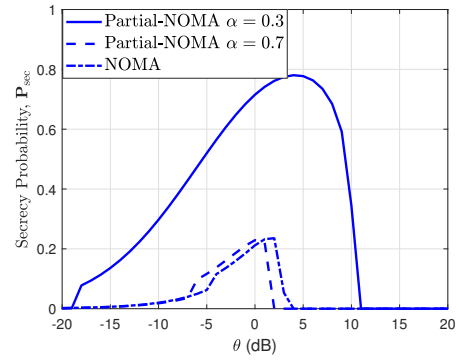
Fig. 8 is a plot of secrecy probability vs. θ, where $\theta = \theta_1 = \theta_2$. We compare the secrecy probability achievable for $\alpha = 0.3$, $\alpha = 0.7$ and $\alpha = 1$ (NOMA). The results reflect the significance of careful choice of α as we observe that the secrecy probability with $\alpha = 0.7$ is much lower than that for $\alpha = 0.3$ for all three eavesdropping scenarios. Further, in the presence of a malicious UE_2, NOMA can outperform $\alpha = 0.7$. This occurs because at these high α values (0.7 and 1), FSIC requires UE_1 to decode and remove the message of UE_2 before decoding its own. Increasing α from 0.7 to 1 improves the ability to do this and therefore legitimate UE's ability to decode its own message, thereby increasing secrecy probability. This also again highlights that secure communica-



(a) Malicious UE_1



(b) Innocent UE_1



(c) Malicious UE_2

Fig. 8: Secrecy probability versus θ, where $\theta = \theta_1 = \theta_2$. We plot the results for $\alpha = 0.3$, $\alpha = 0.7$ and $\alpha = 1$ (NOMA) using $P_1 = 1/3$ and $\beta = (1-\alpha)/2$ for the three eavesdropping scenarios.

tion performance does not necessarily decrease monotonously with α. Note that at higher θ the secrecy probability goes to 0 because of guaranteed outage with the choice of RA and parameter selection. For $\alpha = 0.7$, guaranteed outage occurs at a lower θ than it does for $\alpha = 1$. We also observe that the impact of α on secure communication, while significant in all three scenarios, is most pronounced in the case of an innocent eavesdropping UE_1, reflecting that with careful parameter selection valuable gains in secure communication can be attained.

V. Conclusion

This work studied the physical layer security achievable in a network employing partial-NOMA or NOMA where one of the paired UEs eavesdrops the message of the other. We focused on the scenarios where: 1) a malicious eavesdropping UE_1 prioritizes decoding UE_2's message, 2) an innocent eavesdropping UE_1 only decodes UE_2's message when it is required for decoding its own message, 3) a malicious eavesdropping UE_2 prioritizes decoding UE_1's message. The secure communication event for each eavesdropping scenario was defined and the secrecy probability was derived for partial-NOMA and NOMA in each scenario. The obtained results showed the significant superiority of partial-NOMA with a smaller overlap over traditional NOMA ($\alpha = 1$), highlighting the intrinsic physical layer security provided by the nature of partial-NOMA. In particular, with partial-NOMA gains of upto 3166%, 1198% and 356% were seen over NOMA for the three eavesdropping scenarios, respectively, emphasizing that with carefully selected α we can protect the network from severe degradation to secrecy without the use of traditional techniques such as jamming that increase power consumption and network interference. While partial-NOMA has the potential to provide stellar gains, it was shown that secure communication does not necessarily decrease monotonically with α and that without careful parameter selection, there is a risk of performing worse than NOMA. Further, a careful choice of α also allows secure communication for a wider range of target rates. We showed the non-trivial impact of taking into account intercell interference on secure communication. Without intercell interference, the trends of secrecy probability are very misleading. We also showed that at larger α, intercell interference helps improve secrecy probability significantly by having a greater impact on the eavesdropper than the legitimate receiver. We also studied the impact of decoding for partial-NOMA where: (I) receive-filtering was followed by SIC instead of FSIC, and (II) FSIC was used without receive-filtering. We found that both (I) and (II) can have a drastic negative impact on secrecy performance. (I) can result in no secure communication at low α and (II) can result in the secrecy probability falling to that of traditional NOMA for all α. These observations highlight the significance of the partial-NOMA decoding approach on secure communication. We also found that while a malicious UE_1 is the most detrimental eavesdropper, secrecy in the presence of an innocent UE_1 is most impacted by varying α, highlighting the different but significant impact of careful parameter selection in all eavesdropping scenarios. Such knowledge sheds light on selection of α if the network operator has knowledge of the type of eavesdropper that may be present.

An extension of this work would be to the multi-antenna scenario which we leave for future work. Further, due to space constraints, we did not incorporate the impact of imperfections in FSIC and SIC but plan to include this in future work. Optimizing RA for secrecy constrained problems or for optimizing secrecy is also a direction we intend to explore. Studying secure communication in multi-user NOMA/partial-NOMA scenarios is also an interesting and challenging future direction.

APPENDIX A
PROOF OF THEOREM 1

Based on (16), we can rewrite the secrecy probability as

$$\mathbb{P}_{\text{sec}} = \underbrace{\mathbb{P}\left(C_2 \bigcap \left(\widetilde{\text{SIR}}_1^1 > \theta_1 \bigcap h_1 < \frac{R_1^\eta \tilde{I}_1^\phi \theta_2}{P_2 \mathcal{I}(\alpha,\beta)}\right)\right)}_{A_{\text{mal}}^{\text{UE}_1}} + \underbrace{\mathbb{P}\left(C_2 \bigcap \left(\mathbb{1}_{\bar{M}_1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi \bar{M}_1\right) \bigcap \text{SIR}_2^1 < \theta_2\right)\right)}_{B_{\text{mal}}^{\text{UE}_1}}.$$

Here

$$A_{\text{mal}}^{\text{UE}_1} = \mathbb{P}\Bigg(h_2 > R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \bigcap \mathbb{1}_{\tilde{P}_1>0}\left(h_1 > R_1^\eta \tilde{I}_1^\phi M_0\right) \bigcap \mathbb{1}_{\frac{\theta_2}{P_2\mathcal{I}(\alpha,\beta)}>M_0}\left(h_1 \le R_1^\eta \tilde{I}_1^\phi \frac{\theta_2}{P_2\mathcal{I}(\alpha,\beta)}\right)\Bigg)$$

$$\overset{(a)}{=} \mathbb{E}\left[e^{-R_2^\eta \tilde{I}_2^\phi \bar{M}_2} \mathbb{1}_{\tilde{P}_1>0} \mathbb{1}_{\frac{\theta_2}{P_2\mathcal{I}(\alpha,\beta)}>M_0}\left(e^{-R_1^\eta \tilde{I}_1^\phi M_0} - e^{-\frac{R_1^\eta \tilde{I}_1^\phi \theta_2}{P_2\mathcal{I}(\alpha,\beta)}}\right)\right]$$

$$\overset{(b)}{=} \mathbb{E}_\rho\left[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^\phi|R_2,\rho}\left(\frac{\widehat{P}_2\bar{M}_2}{R_2^{-\eta}}\right)\right]\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\frac{\theta_2}{P_2\mathcal{I}(\alpha,\beta)}>M_0} \mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^\phi|R_1,\rho}\left(\frac{\widehat{P}_1 M_0}{R_1^{-\eta}}\right) - \mathcal{L}_{I_1^\phi|R_1,\rho}\left(\frac{\widehat{P}_1\theta_2 R_1^\eta}{P_2\mathcal{I}(\alpha,\beta)}\right)\right]\right],$$

where (a) is obtained using the CDF of $h_i \sim \exp(1)$, $i \in \{1,2\}$. Using the LT of I_i^ϕ conditioned on R_i and ρ, we arrive at (b). Similarly,

$$B_{\text{mal}}^{\text{UE}_1} = \mathbb{P}\Bigg(h_2 > R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \bigcap \mathbb{1}_{\bar{M}_1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi \bar{M}_1\right) \bigcap \left(\mathbb{1}_{\tilde{P}_2^1\le 0} \bigcup \mathbb{1}_{\tilde{P}_2^1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi \frac{\theta_2}{\tilde{P}_2^1}\right)\right)\Bigg)$$

$$= \mathbb{P}\Bigg(h_2 > \tilde{I}_2^\phi \frac{\bar{M}_2}{R_2^{-\eta}} \bigcap \Bigg(\mathbb{1}_{\bar{M}_1>0}\Bigg(\mathbb{1}_{\tilde{P}_2^1\le 0}\left(h_1 < \tilde{I}_1^\phi \frac{\bar{M}_1}{R_1^{-\eta}}\right) \bigcup \mathbb{1}_{\tilde{P}_2^1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi \min\left(\bar{M}_1, \frac{\theta_2}{\tilde{P}_2^1}\right)\right)\Bigg)\Bigg)\Bigg)$$

$$= \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^\phi|R_2,\rho}\left(R_2^\eta \widehat{P}_2 \bar{M}_2\right)\right] \times \mathbb{1}_{\bar{M}_1>0}\Bigg(1 - \mathbb{E}_{R_1|\rho}\Bigg[\mathbb{1}_{\tilde{P}_2^1\le 0}\mathcal{L}_{I_1^\phi|R_1,\rho}\left(R_1^\eta \widehat{P}_1 \bar{M}_1\right) + \mathbb{1}_{\tilde{P}_2^1>0}\mathcal{L}_{I_1^\phi|R_1,\rho}\left(R_1^\eta \widehat{P}_1 \min\left(\bar{M}_1, \frac{\theta_2}{\tilde{P}_2^1}\right)\right)\Bigg]\Bigg)\Bigg].$$

APPENDIX B
PROOF OF THEOREM 2

Based on (19), we can rewrite the secrecy probability as

$$\mathbb{P}_{\text{sec}} = \underbrace{\mathbb{P}\left(C_2 \bigcap \left(\mathbb{1}_{\bar{M}_1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi \bar{M}_1\right)\right)\right)}_{B_{\text{inn}}^{\text{UE}_1}} + \underbrace{\mathbb{P}\left(C_2 \bigcap \left(\widetilde{\text{SIR}}_1^1 > \theta_1 \bigcap \left(\left(\text{SIR}_2^1 < \theta_2 \bigcup \text{SIR}_1^1 < \theta_1\right) \bigcup \left(\mathbb{1}_{M_0<M_1}\left(\text{SIR}_2^1 > \theta_2 \bigcap \text{SIR}_1^1 > \theta_1\right)\right)\right)\right)\right)}_{A_{\text{inn}}^{\text{UE}_1}}.$$

Along the lines of the proof of Theorem 1

$$A_{\text{inn}}^{\text{UE}_1} = \mathbb{P}\Bigg(h_2 > R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \bigcap \Bigg(\left(\mathbb{1}_{\tilde{P}_1>0}\left(h_1 > R_1^\eta \tilde{I}_1^\phi M_0\right) \bigcap \left(\mathbb{1}_{\tilde{P}_2^1\le 0 \cup P_1\le 0} \bigcup \mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\left(h_1 < R_1^\eta \tilde{I}_1^\phi M_1\right)\right)\right) \bigcup \Bigg(\mathbb{1}_{\tilde{P}_1>0} \times \left(h_1 > \frac{\tilde{I}_1^\phi M_0}{R_1^{-\eta}}\right) \bigcap \left(\mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\left(h_1 > \frac{\tilde{I}_1^\phi M_1}{R_1^{-\eta}}\right)\right)\Bigg)\Bigg)\Bigg)$$

$$= \mathbb{P}\Bigg(h_2 > \tilde{I}_2^\phi R_2^\eta \bar{M}_2 \bigcap \Bigg(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1\le 0 \cup P_1\le 0}\left(h_1 > R_1^{-\eta}\tilde{I}_1^\phi M_0\right) \bigcup \left(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\left(R_1^\eta \tilde{I}_1^\phi M_0 < h_1 < R_1^\eta \tilde{I}_1^\phi M_1\right)\right) \bigcup \left(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\left(h_1 > R_1^\eta \tilde{I}_1^\phi \max\{M_0, M_1\}\right)\right)\Bigg)\Bigg)$$

$$= \mathbb{E}\Big[e^{-R_2^\eta \tilde{I}_2^\phi \bar{M}_2}\Big(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1\le 0 \cup P_1\le 0}e^{-R_1^\eta \tilde{I}_1^\phi M_0} + \mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1>0} \times \mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\left(e^{-R_1^\eta \tilde{I}_1^\phi M_0} - e^{-R_1^\eta \tilde{I}_1^\phi M_1} + e^{-R_1^\eta \tilde{I}_1^\phi M_1}\right)\Big)\Big]$$

$$= \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^\phi|R_2,\rho}\left(R_2^\eta \widehat{P}_2 \bar{M}_2\right)\right] \mathbb{E}_{R_1|\rho}\Bigg[\mathcal{L}_{I_1^\phi|R_1,\rho}\left(R_1^\eta \widehat{P}_1 M_0\right) \times \left(\mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1\le 0 \cup P_1\le 0} + \mathbb{1}_{\tilde{P}_1>0}\mathbb{1}_{\tilde{P}_2^1>0}\mathbb{1}_{P_1>0}\mathbb{1}_{M_0<M_1}\right)\Bigg]\Bigg]$$

and

$$B_{\text{inn}}^{\text{UE}_1} = \mathbb{E}\left[\exp\left(-R_2^\eta \tilde{I}_2^\phi \bar{M}_2\right)\mathbb{1}_{\bar{M}_1>0}\left(1 - \exp\left(-R_1^\eta \tilde{I}_1^\phi \bar{M}_1\right)\right)\right]$$

$$= \mathbb{E}_\rho\Bigg[\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^\phi|R_2,\rho}\left(\widehat{P}_2 R_2^\eta \bar{M}_2\right)\right] \times \mathbb{1}_{\bar{M}_1>0}\left(1 - \mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^\phi|R_1,\rho}\left(\widehat{P}_1 R_1^\eta \bar{M}_1\right)\right]\right)\Bigg].$$

APPENDIX C
PROOF OF THEOREM 3

Based on (22), we can rewrite the secrecy probability as

$$\mathbb{P}_{\text{sec}} = \underbrace{\mathbb{P}\left(C_1 \bigcap \left(\text{SIR}_2^2 > \theta_2 \bigcap h_2 < \frac{R_2^\eta \tilde{I}_2^\phi \theta_1}{P_1\mathcal{I}(\alpha,\beta)}\right)\right)}_{A_{\text{mal}}^{\text{UE}_2}} + \underbrace{\mathbb{P}\left(C_1 \bigcap \left(\mathbb{1}_{\bar{M}_2>0}\left(\text{SIR}_2^2 < \theta_2\right) \bigcap \left(\mathbb{1}_{P_1\mathcal{I}(\alpha,\beta)\le P_2\theta_1} \bigcup \mathbb{1}_{P_1\mathcal{I}(\alpha,\beta)>P_2\theta_1}\left(h_2 < \frac{R_2^\eta \tilde{I}_2^\phi \theta_1}{P_1\mathcal{I}(\alpha,\beta) - P_2\theta_1}\right)\right)\right)\right)}_{B_{\text{mal}}^{\text{UE}_2}}.$$

Along the lines of the proof of Theorem 1

$$A_{\text{mal}}^{\text{UE}_2} = \mathbb{P}\left(h_1 > \frac{\tilde{I}_1^\phi \bar{M}_1}{R_1^{-\eta}} \bigcap \mathbb{1}_{\bar{M}_2>0}\left(h_2 > \frac{\tilde{I}_2^\phi \bar{M}_2}{R_2^{-\eta}}\right) \bigcap h_2 \le \frac{R_2^\eta \tilde{I}_2^\phi \theta_1}{P_1\mathcal{I}(\alpha,\beta)}\right)$$

$$= \mathbb{E}\left[e^{-R_1^\eta \tilde{I}_1^\phi \bar{M}_1}\mathbb{1}_{0<\bar{M}_2<\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)}}\left(e^{-R_2^\eta \tilde{I}_2^\phi \bar{M}_2} - e^{-\frac{R_2^\eta \tilde{I}_2^\phi \theta_1}{P_1\mathcal{I}(\alpha,\beta)}}\right)\right]$$

$$= \mathbb{E}_\rho\left[\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^\phi|R_1,\rho}\left(R_1^\eta \widehat{P}_1 \bar{M}_1\right)\right]\mathbb{1}_{0<\bar{M}_2<\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)}} \times\right.$$

$$\mathbb{E}_{R_2|\rho}\left[\mathcal{L}_{I_2^{\phi}|R_2,\rho}\left(R_2^{\eta}\widehat{P}_2\bar{M}_2\right)-\mathcal{L}_{I_2^{\phi}|R_2,\rho}\left(\frac{\widehat{P}_2\theta_1 R_2^{\eta}}{P_1\mathcal{I}(\alpha,\beta)}\right)\right]\Bigg],$$

and

$$B_{\text{mal}}^{\text{UE}_2}=\mathbb{P}\Bigg(h_1>\frac{\tilde{I}_1^{\phi}\bar{M}_1}{R_1^{-\eta}}\bigcap\mathbb{1}_{\bar{M}_2>0}\Bigg(h_2<\frac{\tilde{I}_2^{\phi}\bar{M}_2}{R_2^{-\eta}}\Bigg)\bigcap$$
$$\Bigg(\mathbb{1}_{P_1\leq\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\bigcup\mathbb{1}_{P_1>\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\left(h_2<\frac{R_2^{\eta}\tilde{I}_2^{\phi}\theta_1}{P_1\mathcal{I}(\alpha,\beta)-P_2\theta_1}\right)\Bigg)\Bigg)$$
$$=\mathbb{P}\Bigg(h_1>R_1^{\eta}\tilde{I}_1^{\phi}\bar{M}_1\bigcap\mathbb{1}_{\bar{M}_2>0}\Bigg(\mathbb{1}_{P_1\leq\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\left(h_2<R_2^{\eta}\tilde{I}_2^{\phi}\bar{M}_2\right)\bigcup$$
$$\mathbb{1}_{P_1>\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\left(h_2<R_2^{\eta}\tilde{I}_2^{\phi}\min\left(\bar{M}_2,\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)-P_2\theta_1}\right)\right)\Bigg)\Bigg)$$
$$=\mathbb{E}_{\rho}\Bigg[\mathbb{E}_{R_1|\rho}\left[\mathcal{L}_{I_1^{\phi}|R_1,\rho}\left(\frac{\widehat{P}_1\bar{M}_1}{R_1^{-\eta}}\right)\right]\mathbb{1}_{\bar{M}_2>0}\times$$
$$\mathbb{E}_{R_2|\rho}\Bigg[\mathbb{1}_{P_1\leq\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\left(1-\mathcal{L}_{I_2^{\phi}|R_2,\rho}\left(\frac{\widehat{P}_2\bar{M}_2}{R_2^{-\eta}}\right)\right)+\mathbb{1}_{P_1>\frac{P_2\theta_1}{\mathcal{I}(\alpha,\beta)}}\times$$
$$\left(1-\mathcal{L}_{I_2^{\phi}|R_2,\rho}\left(\frac{\widehat{P}_2}{R_2^{-\eta}}\min\left(\bar{M}_2,\frac{\theta_1}{P_1\mathcal{I}(\alpha,\beta)-P_2\theta_1}\right)\right)\right)\Bigg]\Bigg].$$

REFERENCES

[1] B. Kim, Y. Park, and D. Hong, "Partial non-orthogonal multiple access (P-NOMA)," *IEEE Wireless Comm. Letters*, vol. 8, no. 5, pp. 1377–1380, Oct. 2019.

[2] B. Kim, J. Heo, and D. Hong, "Partial non-orthogonal multiple access (P-NOMA) with respect to user fairness," in *Proc. of IEEE 90th Vehicular Technology Conf. (VTC19)*, 2019, pp. 1–5.

[3] N. W. M. Thet and M. K. Ozdemir, "Joint overlap ratios and power allocation with user fairness in partial non-orthogonal multiple access (P-NOMA)," in *Proc. of 28th Signal Processing and Communications Applications Conference (SIU2020)*, 2020, pp. 1–4.

[4] T. Fuasungnoen, P. Uthansakul, and M. Uthansakul, "Double power allocations for user fairness in P-NOMA system," in *Proc. of 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON21)*, 2021, pp. 504–507.

[5] P. Sharma, A. Kumar, and M. Bansal, "Performance analysis of P-N-NOMA over generalized fading channel," *IEEE Access*, vol. 8, pp. 105 962–105 971, 2020.

[6] H. He, H. Shan, A. Huang, Q. Ye, and W. Zhuang, "Partial NOMA-based resource allocation for fairness in LTE-U system," in *Proc. of IEEE Global Communications Conf. (GLOBECOM19)*, 2019, pp. 1–6.

[7] M. Baghani, S. Parsaeefard, M. Derakhshani, and W. Saad, "Dynamic non-orthogonal multiple access and orthogonal multiple access in 5G wireless networks," *IEEE Trans. Wireless Commun.*, vol. 67, no. 9, pp. 6360–6373, Sep. 2019.

[8] A. S. Marcano and H. L. Christiansen, "Impact of NOMA on network capacity dimensioning for 5G hetnets," *IEEE Access*, vol. 6, pp. 13 587–13 603, 2018.

[9] A. J. Morgado, K. M. S. Huq, J. Rodriguez, C. Politis, and H. Gacanin, "Hybrid resource allocation for millimeter-wave NOMA," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 23–29, Oct 2017.

[10] K. S. Ali, E. Hossain, and M. J. Hossain, "Partial non-orthogonal multiple access (NOMA) in downlink Poisson networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7637–7652, Nov. 2020.

[11] K. S. Ali, A. Al-Dweik, E. Hossain, and M. Chafii, "Meta distribution of partial-NOMA," *IEEE Wireless Comm. Letters*, vol. 11, no. 12, pp. 2695–2699, Dec. 2022.

[12] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[13] A. Mukherjee *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Thirdquarter 2014.

[14] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[15] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 56–69, Feb. 2015.

[16] X. Zhou *et al.*, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[17] K. S. Ali, H. ElSawy, M. Haenggi, and M. Alouini, "The effect of spatial interference correlation and jamming on secrecy in cellular networks," *IEEE Wireless Comm. Letters*, vol. 6, no. 4, pp. 530–533, Aug. 2017.

[18] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *Proc. of IEEE Global Communications Conf. (GLOBECOM18)*, 2018, pp. 1–6.

[19] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Comm. Letters*, vol. 20, no. 5, pp. 930–933, May 2016.

[20] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Vehicular Tech.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[21] D. Li, Y. Cao, Z. Yang, Y. Chen, S. Zhang, N. Zhao, and Z. Ding, "Secrecy analysis in NOMA full-duplex relaying networks with artificial jamming," *IEEE Trans. Vehicular Tech.*, vol. 70, no. 9, pp. 8781–8794, Sep. 2021.

[22] L. Lv, H. Jiang, Z. Ding, Q. Ye, N. Al-Dhahir, and J. Chen, "Secure non-orthogonal multiple access: An interference engineering perspective," *IEEE Network*, vol. 35, no. 4, pp. 278–285, Aug. 2021.

[23] 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.

[24] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure communications in a unified non-orthogonal multiple access framework," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 2163–2178, Mar. 2020.

[25] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70 422–70 435, 2019.

[26] H. Chamkhia, A. Erbad, A. Mohamed, A. R. Hussein, A. Al-Ali, and M. Guizani, "Stochastic geometry-based physical layer security performance analysis of a hybrid NOMA-PDM based IoT system," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[27] X. Sun, W. Yang, and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1884–1897, Mar. 2020.

[28] S. Zhang, X. Xu, H. Wang, J. Peng, D. Zhang, and K. Huang, "Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular internet of things," *IEEE Access*, vol. 6, pp. 58 405–58 417, 2018.

[29] K. S. Ali, H. Elsawy, A. Chaaban, and M. S. Alouini, "Non-orthogonal multiple access for large-scale 5G networks: Interference aware design," *IEEE Access*, vol. 5, pp. 21 204–21 216, 2017.

[30] B. Blaszczyszyn, M. Haenggi, P. Keeler, and S. Mukherjee, *Stochastic Geometry Analysis of Cellular Networks*. Cambridge University Press, 2018.

[31] J. Andrews, F. Baccelli, and R. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

[32] H. ElSawy, A. Sultan-Salem, M. S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys and Tutorials*, vol. 19, no. 1, pp. 167–203, Firstquarter 2017.

[33] W. Lu and M. D. Renzo, "Stochastic geometry modeling of cellular networks: Analysis, simulation and experimental validation," *CoRR*, vol. abs/1506.03857, 2015. [Online]. Available: http://arxiv.org/abs/1506.03857

[34] K. S. Ali, M. Haenggi, H. E. Sawy, A. Chaaban, and M. Alouini, "Downlink non-orthogonal multiple access (NOMA) in Poisson networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1613–1628, Feb. 2019.

[35] K. S. Ali, H. E. Sawy, and M. Alouini, "Meta distribution of downlink non-orthogonal multiple access (NOMA) in Poisson networks," *IEEE Wireless Comm. Letters*, vol. 8, no. 2, pp. 572–575, Apr. 2019.

[36] A. AlAmmouri *et al.*, "In-band α-duplex scheme for cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6797–6812, Oct. 2016.

[37] I. Randrianantenaina, H. Dahrouj, H. Elsawy, and M. Alouini, "Interference management in full-duplex cellular networks with partial spectrum overlap," *IEEE Access*, vol. 5, pp. 7567–7583, 2017.

[38] H. A. David, *Order statistics*. NJ: John Wiley, 1970.