Meta Distribution and Secrecy of Partial Non-Orthogonal Multiple Access (NOMA) in Poisson Networks

Konpal Shaukat Ali, *Member, IEEE* and Arafat Al-Dweik, *Senior Member, IEEE*

Abstract

This work studies the meta distribution in a partial-NOMA network to obtain fine-grained information about the network performance. As the meta distribution is approximated using the beta distribution via moment matching of the first two moments, reduced integral expressions are derived for the first two moments of the meta distribution. Accurate approximate moments are also proposed to further simplify the calculation. Security is an issue in partial-NOMA because the strong user may decode the weak user's message in the process of decoding its own message using flexible successive interference cancellation (FSIC). Therefore, a measure of secrecy is defined in this context and the secrecy probability is derived for the case of: 1) a malicious strong user that prioritizes eavesdropping, 2) an innocent strong user that decodes the weak user's message only when it is required to do so. The obtained results highlight the superiority of partial-NOMA over traditional NOMA in terms of secrecy. They also show that receive filtering and FSIC have a significant positive impact on the secrecy of partial-NOMA. Furthermore, partial-NOMA with a small overlap of the resource-block can secure the network from the additional deterioration a malicious eavesdropper may cause.

Index Terms

non-orthogonal multiple access (NOMA), stochastic geometry, meta distribution, physical layer security.

The authors are with the the Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE. (email: {konpal.shaukat, dweik}@ku.ac.ae).

Arafat Al-Dweik is also with the department of electrical and computer engineering, Western University, London, ON, Canada. (email: dweik@fulbrightmail.org).

I. INTRODUCTION

Orthogonal multiple access (OMA) is used to avoid interference between the users' equipment (UEs) being served by a base station (BS) by allocating each UE orthogonal resources. This is performed by allocating each UE a unique time slot and/or frequency channel. The available time and frequency resources are split into a grid of what are referred to as time-frequency resource-blocks [1]. Each UE in OMA can be exclusively allocated one or more resource-blocks. In contrast to OMA, non-orthogonal multiple access (NOMA) allows multiple UEs to share a resource-block by superposing their messages in the power domain, i.e., NOMA UEs transmit their messages using the same resource-block, but at different power levels. Successive interference cancellation (SIC) is used to decode the messages of NOMA UEs. Sharing a resource-block by multiple UEs in NOMA improves the spectral efficiency at the expense of introduction of interference between the UEs being served by the same BS [2], [3]; the interference in this case is referred to as intracell interference. In NOMA, the resource allocation for each UE is based on some measure of channel strength, such that decoding is easier for UEs with weaker channels. Most of the existing work on NOMA orders the UEs channel quality based on the received signal mean power [4]–[9], the quality of the transmission channel such as the fading coefficient [10]–[13], the fading-to-noise ratio [14], the instantaneous received signal-to-intercell-interference-and-noise ratio [15], and the instantaneous received signal-to-intercell-interference ratio [16]. Such UE ordering and appropriate resource allocation allow using SIC where a UE decodes messages of UEs weaker than itself and treats the messages of UEs stronger than itself as noise. The achievable sum throughput of NOMA is superior to OMA, which has been extensively shown in the literature [5], [7], [8], [12]–[19].

While NOMA is based on the complete sharing of a resource-block by multiple UEs to improve throughput, the introduced intracell interference deteriorates UE coverage. On the contrary, OMA has no intracell interference, which results in superior coverage, but no spectrum reuse can be applied to UEs served by a BS, which results in lower throughput. In [20], partial-NOMA was introduced as a flexible technique between the two extremes of OMA and NOMA to provide better coverage than NOMA while providing better throughput than OMA. In contrast to NOMA, where UEs share the entire resource-block, partial-NOMA UEs share only a fraction α of the resource-block [20, Fig. 1], thus allowing some spectrum reuse while limiting the intracell interference encountered by UEs. Such a setup is general and allows flexibility to control how

much of the resource-block is shared between the UEs, thereby allowing control over both the spectrum reuse and intracell interference encountered. In [20], partial sharing of a resource-block was 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 allowed the use of matched filtering at the receiver side to further suppress the interference encountered by partial-NOMA UEs resulting in improved coverage. Additionally, the receive filtering also enabled devising a new decoding technique referred to as flexible successive interference cancellation (FSIC). It was shown in [20] that using receive filtering in conjunction with FSIC allows partial-NOMA to outperform traditional NOMA in terms of throughput.

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 [21]–[24]. Research on NOMA [7]–[9], [15], [16], [19], [25], [26] and partial-NOMA [20] use stochastic geometry modeling to analyze large networks that encounter both intercell and intracell interference. Stochastic geometry based studies of large networks often focus on the spatial averages of performance metrics, the most frequent being the spatially averaged coverage probability (SCP), which is generally referred to as the coverage probability. The SCP averages performance over all fading, activity, and network realizations; it is thus a measure of the performance of the average/typical link in the network. The actual distribution of the performance of the majority of the links may not necessarily be close to the SCP. For example, certain links could be much better than the SCP and others much worse. Spatial averages thus do not reveal information about the percentile performance of links which the network operators would be interested in as these reveal the quality of service that the network can provide. It is thus pertinent to study the percentile performance of UEs, where the fading and activity change while the network realization is kept constant. The coverage probability given a fixed network realization is defined as the conditional coverage probability (CCP) [27]. The complementary cdf (ccdf) of the CCP, denoted as the meta distribution, reveals the percentile performance across an arbitrary network realization. Works such as [9], [28], [29], have studied the meta distribution for NOMA UEs. On the other hand, only the SCP for partial-NOMA UEs is studied in [20]. Thus, the first part of this work focuses on studying the meta distribution of UEs in a partial-NOMA network to reveal more fine-grained information about the performance of such a setup.

A number of works have focused on exploiting the physical nature of the wireless network

to enhance security [30]–[37]. This is typically based on exploiting the random fluctuations in the interference power at the receiver and eavesdropper that give rise to opportunities for secure information transmission. Techniques such as jamming have also been used to improve physical layer security [37]. Partial-NOMA is interesting to study in this context 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 resource-block making the rest of the information inaccessible, compared to NOMA where information from the entire resource-block is accessible to all UEs. Additionally, receive filtering 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 makes studying the physical layer security achievable in a partial-NOMA setup interesting. It also helps highlight the impact of network parameters on physical layer security. In the second part of this work, we use stochastic geometry to study physical layer security in a large cellular network employing partial-NOMA and compare this with traditional NOMA. Additionally, we study the impact that receive filtering and FSIC have on improving physical layer security.

The main contributions of this paper can be summarized as follows:

- We obtain integral expressions for the moments of the meta distribution for a partial-NOMA setup. For the first two moments, which are required to approximate the meta distribution, we are able to reduce the integrations required.
- We propose accurate approximate moments of the meta distribution to further simplify the integral calculation.
- We study the physical layer security achievable in a partial-NOMA setup for the weak UE as the strong UE may be able to decode its message. We define ‘secrecy’ as an event of secure communication for the case of: 1) a malicious strong UE that tries its best to decode the weak UE’s message, 2) an innocent strong UE that only decodes the weak UE’s message when it is required. We provide the mathematical analysis for the secrecy probability achievable in each case. Such scenarios shed light on the maximum damage that can be done in terms of physical layer security and the ideal situation of innocent users. We find that at small values of the overlap, the malicious eavesdropper is unable to deteriorate secrecy more than its innocent counterpart, highlighting the physical layer security provided by the nature of the partial-NOMA setup to the network.

- We compare the secrecy probability for a partial-NOMA setup employing receive filtering and FSIC with: 1) a setup that always employs traditional SIC, 2) a setup that does not employ receive filtering and 3) traditional NOMA. We find that not employing FSIC or receive filtering has a drastic negative impact on secrecy at lower α values, highlighting their importance on not just coverage but also secure communication. We also observe that partial-NOMA ($\alpha \leq 1$) is able to achieve much higher secrecy than traditional NOMA ($\alpha = 1$).

The rest of the paper is organized as follows. The system model is described in Section II. The signal-to-interference ratio (SIR) analysis for the meta distribution of the coverage probability is studied in Section III. In Section IV, the SIR analysis for physical layer security is studied. The results are presented in Section V and the paper is concluded in Section VI.

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 $\mathbb{1}_A$, to have value 1 when event A occurs and to be 0 otherwise. We use $\text{Sinc}(x) = \sin(\pi x)/(\pi x)$ when $x \neq 0$, and $\text{Sinc}(x) = 1$ when $x = 0$.

II. SYSTEM MODEL

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 . As a large network is being studied in this work, we assume an interference-limited regime. A BS serves two UEs in each resource-block via partial-NOMA using a total power budget of $P = 1$. 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 $f_\rho(x) = 2\pi\lambda x e^{-\pi\lambda x^2}$, $x \geq 0$. 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 [9], [15], [20]. 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

o. The rationale behind using such a model where UEs are not too far from the serving BS in setups where each UE does not have an individual dedicated resource-block was shown in [9].

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 resource-block 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 resource-block, i.e., the entire time slot and the whole frequency channel, each UE in partial-NOMA has access only to a part of the resource-block. The fraction of the resource-block the two UEs share is denoted by α . In particular, in our work, 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 resource-block 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 beyond the scope of this work. We refer to the fraction of the resource-block accessible to only UE₁ by β , where $0 \leq \beta \leq 1 - \alpha$. Thus, the fraction of the bandwidth available to UE₁ is $BW_1 = \alpha + \beta$. The remaining fraction of the bandwidth $1 - \alpha - \beta$ is available solely to UE₂. The total fraction of the bandwidth thus available to UE₂ is $BW_2 = 1 - \beta$. 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 resource-block simply as an overlap α of the resource-block. As the entire time slot is available to both UEs, we will disregard this aspect when referring to the partial overlap of a resource-block.

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 [20], [38], [39]. In this work, we assume that square pulses are used for transmissions of both UEs. Receive filtering results in any message that has an α -overlap with the UE of interest to be scaled by an effective

interference factor $0 \leq \mathcal{I}(\alpha, \beta) \leq 1$. From [20], the effective interference factor as a function of β and the overlap α is calculated as

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

where the center frequency of UE₁'s message is $f_a = \frac{\alpha+\beta}{2}$ and UE₂'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 $E_i^2 = \int_{-\text{BW}_i/2}^{\text{BW}_i/2} \text{Sinc}^2 \left(\frac{2f}{\text{BW}_i} \right) df$. As $0 < \mathcal{I}(\alpha, \beta) < 1$, receive filtering results in suppression of the interference from the other UE partially sharing the resource-block. 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 resource allocation 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 UE₁ (UE₂). 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 [40], in the typical cell

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

While traditional NOMA uses SIC for decoding, FSIC was introduced in [20] 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., UE₁ using FSIC can decode its own message in either of two ways: 1) Similar to conventional SIC, the message of UE₂ is first decoded, treating the message of UE₁ as noise, and removed, followed by decoding of the message of UE₁, or 2) the message of UE₁ is decoded while treating the interference from the message of UE₂ as noise. Decoding for UE₂ in FSIC,

like in SIC, involves simply decoding its own message while treating the message of UE₁ as noise.

Since fixed rate transmission is used in this work, the transmission rate corresponding to the message of UE₁ is $\log(1 + \theta_1)$. Accordingly, to be able to decode the message of UE₁, the SIR needs to exceed θ_1 . Similarly, the transmission rate for the message of UE₂ is $\log(1 + \theta_2)$ and a UE can only decode the message of UE₂ if its SIR exceeds θ_2 . While SIC requires the message of UE₂ to be decoded by both UEs all the time, FSIC also requires the message of UE₂ to be decoded by both UEs at times. Thus, as in the case of SIC, FSIC allocates resources so that the message of UE₂ is easier to decode by allocating it higher power and/or lower transmission rate. It should be noted that while the two UEs only have an α overlap in the resource-block, since the power allocated to a UE in a resource-block is fixed over the resource-block and as the sum power of the two UEs can never exceed the power budget such that $P_1 + P_2 = 1$. Note that in the non-overlap areas of the resource-block, the power being used will be less than the power budget. 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

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

$$\text{SIR}_2^1 = \frac{h_1 R_1^{-\eta} P_2 \mathcal{I}(\alpha, \beta)}{h_1 R_1^{-\eta} P_1 + \tilde{I}_1^\phi} \quad (3)$$

$$\text{SIR}_1^1 = \frac{h_1 R_1^{-\eta} P_1}{\tilde{I}_1^\phi}. \quad (4)$$

For $i \in \{1, 2\}$, $\tilde{I}_i^\phi$ denotes the intercell interference experienced at UE_i defined as $\tilde{I}_i^\phi = (P_i + (1 - P_i)\mathcal{I}(\alpha, \beta)) \sum_{\mathbf{x} \in \Phi} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta}$, 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 its traditional counterparts. 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

$$I_i^\phi = \sum_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x}\| > \rho}} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta} + \sum_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x}\| = \rho}} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta}. \quad (5)$$

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 [15].

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

$$\widetilde{\text{SIR}}_1^1 = \frac{h_1 R_1^{-\eta} P_1}{h_1 R_1^{-\eta} P_2 \mathcal{I}(\alpha, \beta) + \tilde{I}_1^\phi}. \quad (6)$$

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

$$C_2 = \{\text{SIR}_2^2 > \theta_2\} = \left\{h_2 > R_2^\eta \tilde{I}_2^\phi \bar{M}_2\right\}, \quad (7)$$

where

$$\bar{M}_2 = \frac{\theta_2}{P_2 - \theta_2 P_1 \mathcal{I}(\alpha, \beta)}. \quad (8)$$

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

$$\begin{aligned} C_1 &= \left\{ \left(\text{SIR}_2^1 > \theta_2 \cap \text{SIR}_1^1 > \theta_1 \right) \cup \widetilde{\text{SIR}}_1^1 > \theta_1 \right\} = \left\{ h_1 > R_1^\eta \tilde{I}_1^\phi M_1 \cup h_1 > R_1^\eta \tilde{I}_1^\phi M_0 \right\} \\ &= \left\{ h_1 > R_1^\eta \tilde{I}_1^\phi \bar{M}_1 \right\}, \end{aligned} \quad (9)$$

where

$$\bar{M}_1 = \min \{M_0, M_1\} \mathbb{1}_{\tilde{P}_1 > 0} \mathbb{1}_{\tilde{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} + M_0 \mathbb{1}_{\tilde{P}_1 > 0} \mathbb{1}_{\tilde{P}_2^1 \leq 0 \cup P_1 \leq 0} + M_1 \mathbb{1}_{\tilde{P}_1 \leq 0} \mathbb{1}_{\tilde{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \quad (10)$$

using

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

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

$$C_i = \left\{ h_i > R_i^\eta I_i^\phi \tilde{M}_i \right\}, \quad (11)$$

where $\tilde{M}_i = (P_i + (1 - P_i) \mathcal{I}(\alpha, \beta)) \bar{M}_i$.

III. SIR ANALYSIS OF THE META DISTRIBUTION

As mentioned, network operators and vendors are often interested in the percentile performance of UEs, where the fading and activity, if any, change while the network realization is kept constant. In this regard, the CCP was defined as the coverage probability given a fixed network realization [27]. For a fixed, yet arbitrary, realization of the network $\mathcal{P}_{C_i}$, the CCP of UE_i in a partial-NOMA setup, is defined as,

$$\begin{aligned} \mathcal{P}_{C_i} &\triangleq \mathbb{P}(C_i \mid \Phi) \stackrel{(a)}{=} \mathbb{E}_{g_{\mathbf{y}_i}} \left[\exp \left(- R_i^\eta \tilde{M}_i \underbrace{\sum_{\mathbf{x} \in \Phi} g_{\mathbf{y}_i} \|\mathbf{y}_i\|^{-\eta}}_{I_i^\phi} \right) \mid \Phi \right] \\ &\stackrel{(b)}{=} \prod_{\mathbf{x} \in \Phi} \frac{1}{1 + R_i^\eta \tilde{M}_i \|\mathbf{y}_i\|^{-\eta}}, \end{aligned} \quad (12)$$

where (a) follows by using the definition of C_i in (11) and the cdf of $h_i \sim \exp(1)$. Using the MGF of the independent RVs $g_{\mathbf{y}_i} \sim \exp(1)$, (b) is obtained.

The requirement for more fine-grained information on performance leads to the notion of studying the distribution of the CCP. The meta distribution was thus defined as the ccdf of the CCP [27]. The meta distribution for UE_i can be written as

$$\bar{F}_{\mathcal{P}_{C_i}}(\mu) \triangleq \mathbb{P}(\mathcal{P}_{C_i} > \mu), \quad 0 \leq \mu \leq 1.$$

The b^{th} moment of the CCP of UE_i , by definition, can be calculated using (12) as

$$\mathcal{M}_{i,b} = \mathbb{E} [\mathcal{P}_{C_i}^b] = \mathbb{E} \left[\prod_{\mathbf{x} \in \Phi} \left(1 + R_i^\eta \tilde{M}_i \|\mathbf{y}_i\|^{-\eta} \right)^{-b} \right]. \quad (13)$$

Note that by definition, the SCP of UE_i is the first moment of the CCP of UE_i , i.e., $\mathcal{M}_{i,1}$

Calculating the meta distribution is difficult. To combat this, the beta distribution using moment matching was proposed as a very accurate approximation for the meta distribution [27]. This approach only requires the first two moments of the CCP, i.e., $\mathcal{M}_{i,1}$ and $\mathcal{M}_{i,2}$. In particular,

$$\bar{F}_{\mathcal{P}_{C_i}}(\mu) \approx 1 - \mathcal{I}_\mu \left(\frac{\beta_i \mathcal{M}_{i,1}}{1 - \mathcal{M}_{i,1}}, \beta_i \right), \quad (14)$$

where $\beta_i = \frac{(\mathcal{M}_{i,1} - \mathcal{M}_{i,2})(1 - \mathcal{M}_{i,1})}{\mathcal{M}_{i,2} - \mathcal{M}_{i,1}^2}$ and $\mathcal{I}_\mu(a, b) = \int_0^\mu l^{a-1} (1-l)^{b-1} dl$ is the regularized incomplete beta function. The variance of the meta distribution of UE_i is defined as

$$\sigma_i^2 = \mathcal{M}_{i,2} - \mathcal{M}_{i,1}^2. \quad (15)$$

A. Exact Moments of the Meta Distribution

This subsection evaluates the moments of the meta distribution of UE_i .

Lemma 1: The b^{th} moment of the CCP of UE_i is

$$\mathcal{M}_{i,b} \approx \mathbb{E}_{\rho, R_i} \left[\exp \left(- 2\pi\lambda \underbrace{\int_{\rho-R_i}^{\infty} \left(1 - \left(1 + \tilde{M}_i \frac{R_i^\eta}{r^\eta} \right)^{-b} \right) r dr}_{\mathcal{A}_{i,b}} \right) \left(1 + \tilde{M}_i \frac{R_i^\eta}{\rho^\eta} \right)^{-b} \right]. \quad (16)$$

Proof: By writing $\mathcal{M}_{i,b}$ according to the definition in (13) and separating the intercell interference along the lines of (5), we have

$$\mathcal{M}_{i,b} = \mathbb{E} \left[\prod_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x} - \mathbf{x}_0\| > \rho}} \left(1 + \tilde{M}_i \frac{R_i^\eta}{\|\mathbf{y}_i\|^\eta} \right)^{-b} \prod_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x} - \mathbf{x}_0\| = \rho}} \left(1 + \tilde{M}_i \frac{R_i^\eta}{\|\mathbf{y}_i\|^\eta} \right)^{-b} \right].$$

From this, we arrive at the first term of (16) by using the the probability generating functional (PGFL) of the PPP; since the in-disk model allows a larger guard zone, the lower limit on the distance from the nearest interferer, in the inner integral $\mathcal{A}_{i,b}$, is $\rho - R_i$. The average distance between a UE in the in-disk and the interfering BS ρ away from $\mathbf{o}$ is approximated to be ρ , which was validated as a tight approximation [8], [15]. The approximation in (16) comes from the use of this approximation in the denominator of the second term. $\square$

While $\mathcal{M}_{i,b}$ for general b requires a triple integration according to (16), for the cases of $b = 1$ and 2 we are able to reduce the calculation by one integration. In particular, closed-form expressions for $\mathcal{A}_{i,b}$ in (16) can be obtained for $b \in \{1, 2\}$. It should be noted that $\mathcal{M}_{i,1}$ and $\mathcal{M}_{i,2}$ are the two most relevant moments of the CCP of UE_i as they are sufficient to evaluate both the meta distribution and SCP of UE_i .

Corollary 1: The inner integral for calculating the first moment of the CCP, i.e., the SCP, of UE_i , $\mathcal{M}_{i,1}$, is

$$\mathcal{A}_{i,1} = \frac{\tilde{M}_i R_i^\eta}{\eta - 2} (\rho - R_i)^{2-\eta} {}_2F_1 \left(1, 1 - \delta; 2 - \delta; -\tilde{M}_i R_i^\eta (\rho - R_i)^{-\eta} \right). \quad (17)$$

Corollary 2: The inner integral for calculating the second moment of the CCP of UE_i , $\mathcal{M}_{i,2}$, is

$$\begin{aligned} \mathcal{A}_{i,2} = & \frac{\tilde{M}_i R_i^\eta}{\eta} \left(\frac{2(\rho - R_i)^\eta + \tilde{M}_i R_i^\eta}{(\rho - R_i)^\eta + \tilde{M}_i R_i^\eta} (\rho - R_i)^{2-\eta} + \frac{4(\rho - R_i)^{2-\eta}}{(\eta - 2)} {}_2F_1 \left(1, 1 - \delta; 2 - \delta; -\tilde{M}_i R_i^\eta (\rho - R_i)^{-\eta} \right) + \right. \\ & \left. \frac{(\eta - 2)\tilde{M}_i R_i^\eta}{2(1 - \eta)} (\rho - R_i)^{2-2\eta} {}_2F_1 \left(1, 2 - \delta; 3 - \delta; -\tilde{M}_i R_i^\eta (\rho - R_i)^{-\eta} \right) \right). \end{aligned} \quad (18)$$

B. Approximate Moments of the Meta Distribution

Another approach to calculating the moments of the CCP is based on the relative distance process (RDP) [41]. Since the partial-NOMA setup deals with ordered link distances, we will use the ordered RDP. The ordered RDP for UE_i is defined as

$$\mathcal{R}_i = \left\{ x \in \Phi : \frac{R_i}{\|\mathbf{y}_i\|} \right\}. \quad (19)$$

Using the ordered RDP for UE_i , we can rewrite the moments of the CCP of UE_i in (13) as

$$\mathcal{M}_{i,b} = \mathbb{E} \left[\prod_{z \in \mathcal{R}_i} \left(1 + \tilde{M}_i z^\eta \right)^{-b} \right]. \quad (20)$$

As (13) is in terms of the PPP Φ , evaluating $\mathcal{M}_{i,b}$ in (16) required the PGFL of the PPP. Accordingly, as $\mathcal{M}_{i,b}$ in (20) is in terms of the RDP $\mathcal{R}_i$, the PGFL of $\mathcal{R}_i$ is required to evaluate $\mathcal{M}_{i,b}$. Note that the distribution of the ordered link distance R_i and the distribution of the ordered RDP $\mathcal{R}_i$ are conditioned on ρ . Consequently, the PGFL of $\mathcal{R}_i$ is also conditioned on ρ .

Lemma 2: The PGFL of the ordered RDP of UE_i , $\mathcal{R}_i$, conditioned on ρ is

$$\mathcal{G}_{\mathcal{R}_i|\rho}[f] = \mathbb{E}_{R_i} \left[\exp \left(-2\pi\lambda \int_{\rho-R_i}^{\infty} \left(1 - f \left(\frac{R_i}{a} \right) \right) a da \right) \prod_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x} - \mathbf{x}_0\| = \rho}} f \left(\frac{R_i}{\|\mathbf{y}_i\|} \right) \right]. \quad (21)$$

Proof: By definition of the PGFL we have

$$\mathcal{G}_{\mathcal{R}_i|\rho}[f] \triangleq \mathbb{E} \left[\prod_{z \in \mathcal{R}_i} f(z) \right] = \mathbb{E} \left[\prod_{x \in \Phi} f \left(\frac{R_i}{\|\mathbf{y}_i\|} \right) \right] \stackrel{(a)}{=} \mathbb{E} \left[\prod_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x} - \mathbf{x}_0\| > \rho}} f \left(\frac{R_i}{\|\mathbf{y}_i\|} \right) \prod_{\substack{\mathbf{x} \in \Phi \\ \|\mathbf{x} - \mathbf{x}_0\| = \rho}} f \left(\frac{R_i}{\|\mathbf{y}_i\|} \right) \right].$$

Similar to (5), (a) is obtained by separating the interferers into two types, the interferers that are farther than ρ from $\mathbf{o}$ and the interferer conditioned to be a distance ρ away from $\mathbf{o}$. From this, we obtain the first term in (21) using the PGFL of the PPP. $\square$

Unfortunately, it is not possible to obtain closed-form expressions for (21). In this subsection, along the lines of [9], we propose the use of two approximations to relax the constraints and simplify the calculation of the PGFL of the ordered RDP for UE_i . In particular, the two approximations used are:

- **A1:** The guard zone around the UEs is approximated to be of radius R_i although the largest guaranteed guard zone has radius $\rho - R_i$. As $\rho - R_i > R_i$ this approximation overestimates the intercell interference encountered by the UEs.
- **A2:** Deconditioning on the BS located a distance ρ from $\mathbf{o}$. This approximation underestimates the intercell interference experienced by the UEs.

Note that the two approximations have opposing effects on how much intercell interference is accounted for. Using these approximations we can calculate the PGFL of $\mathcal{R}_i$ in closed-form.

Lemma 3: The PGFLs of the ordered RDP for UE_2 and UE_1 , respectively, using approximations **A1** and **A2** are

$$\tilde{\mathcal{G}}_{\mathcal{R}_2|\rho}[f] = \frac{32}{\rho^4} \left(2\pi\lambda \int_1^\infty (1 - f(y^{-1})) y dy \right)^{-2} \left(\Gamma(2) - \Gamma \left(2, \frac{\rho^2}{2} \pi\lambda \int_1^\infty (1 - f(y^{-1})) y dy \right) \right) \quad (22)$$

$$\begin{aligned} \tilde{\mathcal{G}}_{\mathcal{R}_1|\rho}[f] &= \frac{8}{\rho^2} \left(2\pi\lambda \int_1^\infty (1 - f(y^{-1})) y dy \right)^{-1} \left(\Gamma(1) - \Gamma \left(1, \frac{\rho^2}{2} \pi\lambda \int_1^\infty (1 - f(y^{-1})) y dy \right) \right) \\ &\quad - \tilde{\mathcal{G}}_{\mathcal{R}_2|\rho}[f]. \end{aligned} \quad (23)$$

Proof: Along the lines of the proof of Lemma 2, the PGFL of the ordered RDP for UE_i using **A1** and **A2** is

$$\tilde{\mathcal{G}}_{\mathcal{R}_i|\rho}[f] = \mathbb{E}_{R_i} \left[\exp \left(-2\pi\lambda \int_{R_i}^\infty \left(1 - f \left(\frac{R_i}{a} \right) \right) a da \right) \right].$$

Here the second term in (21) has been removed due to **A2**. Additionally, the lower limit of the integral of the first term in (21) is updated to reflect R_i , the radius of the guard zone in **A1**. Using $f_{R_i|\rho}$ in (1) for $i = 2$ and $i = 1$ we obtain (22) and (23), respectively. $\square$

Lemma 4: The b^{th} moments of the CCP for UE₂ and UE₁, respectively, using approximations **A1** and **A2** are

$$\widetilde{\mathcal{M}}_{2,b} = \mathbb{E}_\rho \left[\frac{32}{\rho^4} \left(\pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_2) - 1 \right) \right)^{-2} \left(1 - \Gamma \left(2, \frac{\rho^2}{4} \left(\pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_2) - 1 \right) \right) \right) \right) \right] \quad (24)$$

$$\begin{aligned} \widetilde{\mathcal{M}}_{1,b} = \mathbb{E}_\rho & \left[\frac{8}{\rho^2} \left(\pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_1) - 1 \right) \right)^{-1} \left(1 - \exp \left(-\frac{\rho^2}{4} \pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_1) - 1 \right) \right) \right) \right. \\ & \left. - \frac{32}{\rho^4} \left(\pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_1) - 1 \right) \right)^{-2} \left(1 - \Gamma \left(2, \frac{\rho^2}{4} \left(\pi \lambda \left({}_2F_1(b, -\delta; 1-\delta; -\tilde{M}_1) - 1 \right) \right) \right) \right) \right]. \quad (25) \end{aligned}$$

Proof: Using the definition in (20), we have

$$\widetilde{\mathcal{M}}_{i,b} = \mathbb{E}_\rho \left[\widetilde{\mathcal{G}}_{\mathcal{R}_i|\rho}[f(z)] \Big|_{f(z)=(1+\tilde{M}_i z^\eta)^{-b}} \right].$$

$\widetilde{\mathcal{G}}_{\mathcal{R}_i|\rho}[f(z)]$ in (23) and (22) for UE₁ and UE₂, respectively, are then plugged into the equation above. We arrive at (24) and (25) using

$$\begin{aligned} \int_1^\infty (1 - f(z^{-1})) z dz \Big|_{f(z)=(1+\tilde{M}_i z^\eta)^{-b}} &= \int_1^\infty \left(1 - (1 + \tilde{M}_i z^{-\eta})^{-b} \right) z dz \\ &\stackrel{(a)}{=} \frac{{}_2F_1\left(b, -\delta; 1-\delta, -\tilde{M}_i\right) - 1}{2}, \end{aligned}$$

where (a) is obtained using $z \rightarrow g^{-1}$. $\square$

IV. SIR 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 mentioned, this involves exploiting random fluctuations in the interference 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 [37] 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 our metric for measuring the physical layer security our setup can achieve.

Partial-NOMA is susceptible to eavesdropping for two main reasons: 1) the overlap α of the resource-block shared by the two UEs, 2) the use of FSIC which at times requires UE₁ to decode the message of UE₂. While in theory a malicious UE₂ could attempt to decode the message of UE₁ as well, in this work we focus on the security of the message of UE₂. Thus in the context of our work, we are concerned about the security of the message intended for UE₂, i.e., UE₂ is the legitimate receiver and UE₁ is the eavesdropper. We study the following two scenarios:

- UE₁ is malicious and prioritizes decoding the message of UE₂.
- UE₁ is innocent and its main goal is not eavesdropping. It therefore only decodes the message of UE₂ when it is required for decoding its own message.

To be explicit, in our setup, we define secrecy as the event that UE₂ is able to decode its own message and that UE₁ is unable to decode the message of UE₂.

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 [15, Lemma 1], [20] as

$$\mathcal{L}_{I_i^\phi|R_i,\rho}(s) \approx \exp\left(\frac{-2\pi\lambda s}{(\eta-2)(\rho-R_i)^{\eta-2}} {}_2F_1\left(1, 1-\delta; 2-\delta; \frac{-s}{\rho-R_i^\eta}\right)\right) \frac{1}{1+s\rho^{-\eta}} \quad (26)$$

$$\stackrel{\eta=4}{=} e^{-\pi\lambda\sqrt{s}\tan^{-1}\left(\frac{\sqrt{s}}{(\rho-R_i)^2}\right)} \frac{1}{1+s\rho^{-4}}. \quad (27)$$

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

1) *Malicious UE₁*: In the case of a malicious UE₁, secure communication is achieved when UE₂ is in coverage (i.e., the event C_2 occurs) and UE₁ is in one of the following situations:

- UE₁ can only decode its own message while treating the message of UE₂ as noise and also cannot extract the message of UE₂.
- UE₁ is unable to decode its own message and also cannot extract the message of UE₂.

Note that as UE₁ is malicious, we consider the possibility of UE₁ decoding UE₂'s message even if it cannot decode its own message after removing the message of UE₂. Based on these, we can write the secrecy probability of a malicious UE₁ as

$$\mathbb{P}_{\text{sec}} = \mathbb{P}\left(C_2 \cap \left(\left(\widetilde{\text{SIR}}_1^1 > \theta_1 \cap \text{SIR}_2^1 < \theta_2\right) \cup \left(\mathbb{1}_{\bar{M}_1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\phi \bar{M}_1\right) \cap \text{SIR}_2^1 < \theta_2\right)\right)\right). \quad (28)$$

Theorem 1: The secrecy probability when UE_1 is a malicious eavesdropper is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_{\rho} \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\circ|R_2,\rho} \left(\frac{\hat{P}_2 \bar{M}_2}{R_2^{-\eta}} \right) \right] \left(\mathbb{E}_{R_1|\rho} \left[\mathbb{1}_{\tilde{P}_1 > 0} \mathbb{1}_{\frac{\theta_2}{\tilde{P}_2^1} > M_0} \left(\mathcal{L}_{I_1^\circ|R_1,\rho} \left(\frac{\hat{P}_1 M_0}{R_1^{-\eta}} \right) - \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\frac{\hat{P}_1 R_1^\eta \theta_2}{\tilde{P}_2^1} \right) \right) \right] \right. \right. \\ \left. \left. + \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \mathbb{1}_{\tilde{P}_2^1 > 0} \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\hat{P}_1 R_1^\eta \min \left(\bar{M}_1, \frac{\theta_2}{\tilde{P}_2^1} \right) \right) - \mathbb{1}_{\tilde{P}_2^1 \leq 0} \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\hat{P}_1 R_1^\eta \bar{M}_1 \right) \right) \right] \right) \right], \quad (29)$$

where $\mathcal{L}_{I_i^\circ|R_i,\rho}(s)$ for $i \in \{1, 2\}$ is given in (26).

Proof: Based on (28), we can rewrite the secrecy probability as

$$\mathbb{P}_{\text{sec}} = \underbrace{\mathbb{P} \left(C_2 \cap \left(\widetilde{\text{SIR}}_1^1 > \theta_1 \cap \text{SIR}_2^1 < \theta_2 \right) \right)}_{A_{\text{mal}}} + \underbrace{\mathbb{P} \left(C_2 \cap \left(\mathbb{1}_{\bar{M}_1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\circ \bar{M}_1 \right) \cap \text{SIR}_2^1 < \theta_2 \right) \right)}_{B_{\text{mal}}}.$$

Here

$$\begin{aligned} A_{\text{mal}} &= \mathbb{P} \left(h_2 > R_2^\eta \tilde{I}_2^\circ \bar{M}_2 \cap \mathbb{1}_{\tilde{P}_1 > 0} \left(h_1 > R_1^\eta \tilde{I}_1^\circ M_0 \right) \cap \mathbb{1}_{\frac{\theta_2}{\tilde{P}_2^1} > M_0} \left(h_1 \leq R_1^\eta \tilde{I}_1^\circ \frac{\theta_1}{\tilde{P}_2^1} \right) \right) \\ &\stackrel{(a)}{=} \mathbb{E} \left[\exp \left(-R_2^\eta \tilde{I}_2^\circ \bar{M}_2 \right) \mathbb{1}_{\tilde{P}_1 > 0} \mathbb{1}_{\frac{\theta_2}{\tilde{P}_2^1} > M_0} \left(\exp \left(-R_1^\eta \tilde{I}_1^\circ M_0 \right) - \exp \left(-R_1^\eta \tilde{I}_1^\circ \frac{\theta_2}{\tilde{P}_2^1} \right) \right) \right] \\ &\stackrel{(b)}{=} \mathbb{E}_{\rho} \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\circ|R_2,\rho} \left(\frac{\hat{P}_2 \bar{M}_2}{R_2^{-\eta}} \right) \right] \mathbb{1}_{\tilde{P}_1 > 0} \mathbb{1}_{\frac{\theta_2}{\tilde{P}_2^1} > M_0} \mathbb{E}_{R_1|\rho} \left[\mathcal{L}_{I_1^\circ|R_1,\rho} \left(\frac{\hat{P}_1 M_0}{R_1^{-\eta}} \right) - \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\frac{\hat{P}_1 \theta_2}{R_1^{-\eta} \tilde{P}_2^1} \right) \right] \right], \end{aligned}$$

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

$$\begin{aligned} B_{\text{mal}} &= \mathbb{P} \left(h_2 > R_2^\eta \tilde{I}_2^\circ \bar{M}_2 \cap \mathbb{1}_{\bar{M}_1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\circ \bar{M}_1 \right) \cap \left(\mathbb{1}_{\tilde{P}_2^1 \leq 0} \cup \mathbb{1}_{\tilde{P}_2^1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\circ \frac{\theta_2}{\tilde{P}_2^1} \right) \right) \right) \\ &= \mathbb{P} \left(h_2 > \tilde{I}_2^\circ \frac{\bar{M}_2}{R_2^{-\eta}} \cap \left(\mathbb{1}_{\bar{M}_1 > 0} \left(\mathbb{1}_{\tilde{P}_2^1 \leq 0} \left(h_1 < \tilde{I}_1^\circ \frac{\bar{M}_1}{R_1^{-\eta}} \right) \cup \mathbb{1}_{\tilde{P}_2^1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\circ \min \left(\bar{M}_1, \frac{\theta_2}{\tilde{P}_2^1} \right) \right) \right) \right) \right) \\ &= \mathbb{E}_{\rho} \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\circ|R_2,\rho} \left(\hat{P}_2 R_2^\eta \bar{M}_2 \right) \right] \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \mathbb{E}_{R_1|\rho} \left[\mathbb{1}_{\tilde{P}_2^1 \leq 0} \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\hat{P}_1 R_1^\eta \bar{M}_1 \right) + \right. \right. \right. \\ &\quad \left. \left. \mathbb{1}_{\tilde{P}_2^1 > 0} \mathcal{L}_{I_1^\circ|R_1,\rho} \left(\hat{P}_1 R_1^\eta \min \left(\bar{M}_1, \frac{\theta_2}{\tilde{P}_2^1} \right) \right) \right] \right) \right]. \end{aligned}$$

□

2) *Innocent UE_1 :* In the case of a rather innocent UE_1 , 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) UE₁ can decode both messages and it can also decode its own message while treating the message of UE₂ as noise. However, the latter is chosen as it is easier for UE₁.
- iii) UE₁ is unable to decode its own message, i.e., it is in outage.

Based on these, we can write the secrecy probability of an innocent UE₁ as

$$\mathbb{P}_{\text{sec}} = \mathbb{P} \left(C_2 \cap \left(\left(\widetilde{\text{SIR}}_1^1 > \theta_1 \cap \left(\text{SIR}_2^1 < \theta_2 \cup \text{SIR}_1^1 < \theta_1 \right) \right) \cup \left(\widetilde{\text{SIR}}_1^1 > \theta_1 \cap \left(\mathbb{1}_{M_0 < M_1} \left(\text{SIR}_2^1 > \theta_2 \cap \text{SIR}_1^1 > \theta_1 \right) \right) \cup \left(\mathbb{1}_{\bar{M}_1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\phi \bar{M}_1 \right) \right) \right) \right). \quad (30)$$

Theorem 2: The secrecy probability when UE₁ is an innocent eavesdropper is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(\hat{P}_2 \frac{\bar{M}_2}{R_2^{-\eta}} \right) \right] \left(\mathbb{E}_{R_1|\rho} \left[\left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 \leq 0 \cup \hat{P}_1 \leq 0} + \mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \mathbb{1}_{M_0 < M_1} \right) \times \right. \right. \right. \\ \left. \left. \left. \mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta M_0 \right) + \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta \bar{M}_1 \right) \right) \right] \right) \right], \quad (31)$$

where $\mathcal{L}_{I_i^\phi|R_i,\rho}(s)$ for $i \in \{1, 2\}$ is given in (26).

Proof: Based on (30), we can rewrite the secrecy probability as

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

Along the lines of the proof of Theorem 1

$$A_{\text{inn}} = \mathbb{P} \left(h_2 > R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \cap \left(\left(\mathbb{1}_{\hat{P}_1 > 0} \left(h_1 > R_1^\eta \tilde{I}_1^\phi M_0 \right) \cap \left(\mathbb{1}_{\hat{P}_2^1 \leq 0 \cup P_1 \leq 0} \cup \mathbb{1}_{\hat{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \left(h_1 < R_1^\eta \tilde{I}_1^\phi M_1 \right) \right) \right) \right. \right. \\ \left. \left. \cup \left(\mathbb{1}_{\hat{P}_1 > 0} \left(h_1 > R_1^\eta \tilde{I}_1^\phi M_0 \right) \cap \left(\mathbb{1}_{\hat{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 M_1 \right) \right) \right) \right) \right) \\ = \mathbb{P} \left(h_2 > \tilde{I}_2^\phi \frac{\bar{M}_2}{R_2^{-\eta}} \cap \left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 \leq 0 \cup P_1 \leq 0} \left(h_1 > \tilde{I}_1^\phi \frac{M_0}{R_1^{-\eta}} \right) \cup \left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \mathbb{1}_{M_0 < M_1} \times \right. \right. \right. \\ \left. \left. \left(R_1^\eta \tilde{I}_1^\phi M_0 < h_1 < R_1^\eta \tilde{I}_1^\phi M_1 \right) \cup \left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{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) \right) \right) \\ = \mathbb{E} \left[\exp \left(-R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \right) \left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 \leq 0 \cup P_1 \leq 0} \exp \left(-R_1^\eta \tilde{I}_1^\phi M_0 \right) + \right. \right. \\ \left. \left. \mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \mathbb{1}_{M_0 < M_1} \left(\exp \left(-R_1^\eta \tilde{I}_1^\phi M_0 \right) - \exp \left(-R_1^\eta \tilde{I}_1^\phi M_1 \right) + \exp \left(-R_1^\eta \tilde{I}_1^\phi M_1 \right) \right) \right) \right] \\ = \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(\hat{P}_2 \frac{\bar{M}_2}{R_2^{-\eta}} \right) \right] \mathbb{E}_{R_1|\rho} \left[\left(\mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 \leq 0 \cup P_1 \leq 0} + \mathbb{1}_{\hat{P}_1 > 0} \mathbb{1}_{\hat{P}_2^1 > 0} \mathbb{1}_{P_1 > 0} \mathbb{1}_{M_0 < M_1} \right) \mathcal{L}_{I_1^\phi|R_1,\rho} \left(\frac{\hat{P}_1 M_0}{R_1^{-\eta}} \right) \right] \right]$$

and

$$\begin{aligned} B_{\text{inn}} &= \mathbb{E} \left[\exp \left(-R_2^\eta \tilde{I}_2^\phi \bar{M}_2 \right) \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \exp \left(-R_1^\eta \tilde{I}_1^\phi \bar{M}_1 \right) \right) \right] \\ &= \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(\hat{P}_2 R_2^\eta \bar{M}_2 \right) \right] \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \mathbb{E}_{R_1|\rho} \left[\mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta \bar{M}_1 \right) \right] \right) \right]. \end{aligned}$$

□

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. We thus study the following two cases for both the innocent and malicious UE₁:

- (I) When SIC is used by UE₁ instead of FSIC, i.e., UE₁ always decodes and removes the message of UE₂ 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 3: The secrecy probability of a malicious UE₁ in (I) is

$$\begin{aligned} \mathbb{P}_{\text{sec}} &= \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(\hat{P}_2 R_2^\eta \bar{M}_2 \right) \right] \mathbb{1}_{M_1 > 0} \times \right. \\ &\quad \left. \mathbb{E}_{R_1|\rho} \left[1 - \mathbb{1}_{\hat{P}_2 > 0} \mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta \min \left(M_1, \frac{\theta_2}{\hat{P}_2} \right) \right) - \mathbb{1}_{\hat{P}_2 \leq 0} \mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta M_1 \right) \right] \right]. \end{aligned} \quad (32)$$

Proof: With SIC the terms in (29) from A_{mal} become 0. Additionally, as SIC does not allow UE₁ to decode its own message while treating the message of UE₂ as noise, $\bar{M}_1 = M_1$. □

Corollary 4: The secrecy probability of an innocent UE₁ in (I) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(\hat{P}_2 R_2^\eta \bar{M}_2 \right) \right] \mathbb{1}_{M_1 > 0} \left(1 - \mathbb{E}_{R_1|\rho} \left[\mathcal{L}_{I_1^\phi|R_1,\rho} \left(\hat{P}_1 R_1^\eta M_1 \right) \right] \right) \right]. \quad (33)$$

Proof: Following the proof of Coroll. 3, the terms in (31) from A_{inn} become 0 and $\bar{M}_1 = M_1$. □

Corollary 5: The secrecy probability of a malicious UE₁ in (II) is

$$\begin{aligned} \mathbb{P}_{\text{sec}} &= \mathbb{E}_\rho \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^\phi|R_2,\rho} \left(R_2^\eta \bar{M}_2 \right) \right] \mathbb{1}_{\bar{M}_1 > 0} \times \right. \\ &\quad \left. \mathbb{E}_{R_1|\rho} \left[1 - \mathbb{1}_{\hat{P}_2 > 0} \mathcal{L}_{I_1^\phi|R_1,\rho} \left(R_1^\eta \min \left(\bar{M}_1, \frac{\theta_2}{\hat{P}_2} \right) \right) - \mathbb{1}_{\hat{P}_2 \leq 0} \mathcal{L}_{I_1^\phi|R_1,\rho} \left(R_1^\eta \bar{M}_1 \right) \right] \right] \Big|_{\mathcal{I}(\alpha,\beta)=1}. \end{aligned} \quad (34)$$

Proof: As $\mathcal{I}(\alpha, \beta) = 1$, the high interference results in the terms in (29) from A_{mal} to become 0. Additionally, note that $\hat{P}_i|_{\mathcal{I}(\alpha,\beta)=1} = P_i + (1 - P_i) = 1$. □

Corollary 6: The secrecy probability of an innocent UE₁ in (II) is

$$\mathbb{P}_{\text{sec}} = \mathbb{E}_{\rho} \left[\mathbb{E}_{R_2|\rho} \left[\mathcal{L}_{I_2^e|R_2,\rho} (R_2^{\eta} \bar{M}_2) \right] \mathbb{1}_{\bar{M}_1 > 0} \left(1 - \mathbb{E}_{R_1|\rho} \left[\mathcal{L}_{I_1^e|R_1,\rho} (R_1^{\eta} \bar{M}_1) \right] \right) \right] \Bigg|_{\mathcal{I}(\alpha,\beta)=1}. \quad (35)$$

Proof: Following the proof of Coroll. 5, the terms in (31) from A_{inn} become 0 and $\hat{P}_i|_{\mathcal{I}(\alpha,\beta)=1} = 1$. $\square$

In Section V-B, we also compare the secrecy probability achievable with traditional NOMA (i.e., $\alpha = 1$) for the both the case of innocent and malicious UE₁ to highlight the benefit that adapting partial-NOMA (i.e., $\alpha \leq 1$) can have on physical layer security.

V. RESULTS

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 resource allocation is used in some of the figures while the other figures use the optimum resource allocation associated with a problem that aims to maximize cell sum throughput while constrained to a threshold minimum throughput (TMT) according to [20, Algorithm 1]. Note that solving such a problem results in resource allocation such that the minimum required resources are spent on UE₂ to attain throughput equal to the TMT and the remaining resources are given to UE₁ to maximize its throughput with. In Section V-A, the exact moments of the meta distribution are used unless specified otherwise.

A. Meta Distribution of Partial-NOMA

Fig. 1 is a plot of the meta distribution for $\alpha = 0.3$ using fixed resource allocation. The figure validates the analysis in Section III as the simulation results are a tight match. The figure also shows the impact of increasing P_1 on the meta distribution. In particular, when $P_1 = 0.1$, 81.8% of UE₁ and 79.1% of UE₂ achieve a coverage probability of at least 0.8. Increasing P_1 to $1/3$ improves the percentage to 93% for UE₁ and degrades it to 78.2% for UE₂. As anticipated, increasing P_1 (decreasing P_2) increases the percentage of UE₁ and decreases the percentage of UE₂ that can achieve a certain coverage probability. We observe that the impact on UE₁ is higher than that on UE₂ in this scenario. This can be attributed to the fact that the transmission rate for UE₂ is lower in this scenario. Additionally, UE₁ generally has to make more of an effort in decoding its message as it has to decode a message with lower power and at times has to decode two messages, thus the impact of changing P_1 is more drastic for UE₁.

Fig. 1: Meta distribution vs. μ with $\alpha = 0.3$, $\beta = (1 - \alpha)/2$, $\theta_1 = 1$ dB and $\theta_2 = 0.5$ dB. Markers show Monte Carlo simulations.

Fig. 2: Meta distribution vs. μ with $P_1 = 1/3$, $\theta_1 = 1$ dB and $\theta_2 = 0.5$ dB. Solid lines represent $\beta = 0$ and dotted lines represent $\beta = (1 - \alpha)/2$.

Fig. 2 is a plot of the meta distribution for $\alpha = 0.3$ and $\alpha = 0.7$ using $\beta = 0$ and $\beta = (1 - \alpha)/2$. We observe that the meta distribution for $\alpha = 0.3$ is in general superior to $\alpha = 0.7$. This stems from the superiority of an overlap of 0.3 to 0.7 as the users can take better advantage of receive filtering suppressing interference and FSIC. For $\alpha = 0.3$ and $\beta = 0$ ($\beta = (1 - \alpha)/2$), 91.9% (93%) of UE₁ and 77.7% (78.2%) of UE₂ can achieve a coverage probability of at least 0.8. On the other hand, for $\alpha = 0.7$ and $\beta = 0$ ($\beta = (1 - \alpha)/2$), 65.3% (69.4%) of UE₁ and 59.6% (58.2%) of UE₂ can achieve a coverage probability of at least 0.8. Note that for $\alpha = 0.3$ ($\alpha = 0.7$), $\mathcal{I}(\alpha, \beta)$ decreases (increases) from $\beta = 0$ to $(1 - \alpha)/2$ [20, Fig. 2(b)]. It is thus interesting to note that while increasing β from 0 to $(1 - \alpha)/2$ increases the performance of both UEs for $\alpha = 0.3$, in the case of $\alpha = 0.7$ the performance of UE₁ improves while the performance of UE₂ deteriorates. The improvement in performance of the UEs with $\alpha = 0.3$ can be attributed to the reduction in $\mathcal{I}(\alpha, \beta)$ reducing interference. For the case of $\alpha = 0.7$, the performance deterioration of UE₂ can be attributed to the increase in $\mathcal{I}(\alpha, \beta)$. The improvement in performance of UE₁, on the other hand, comes from a switch in decoding from treating the message of UE₂ as noise to UE₁ decoding and removing the message of UE₂ before decoding its own message. This switch in decoding is also why we see the largest impact of increasing β on UE₁ with $\alpha = 0.7$.

Fig. 3 is a plot of the meta distribution for different α values using fixed resource allocation. We observe that the meta distribution of the UEs is not plotted for $\alpha = 0.6$. This is because for $\alpha = 0.6$, the choice of resource allocation used results in guaranteed outage. We observe that

Fig. 3: Meta distribution vs. μ with $P_1 = 1/3$, $\theta_1 = 1$ dB, $\theta_2 = 0.5$ dB and $\beta = (1 - \alpha)/2$. Black (red) lines represent UE₁ (UE₂).

Fig. 4: Meta distribution vs. μ using optimum RA for each α with TMT=0.25. Solid (dashed) lines represent UE₁ (UE₂).

Fig. 5: SCP and variance of the meta distribution vs. θ (identical transmission rates for both UEs) with $\alpha = 0.3$, $P_1 = 1/3$ and $\beta = (1 - \alpha)/2$. Black (red) lines represent UE₁ (UE₂).

in general, when resource allocation is fixed, increasing α deteriorates the performance of UE₂ as the percentage of UE₂ that can achieve atleast a certain coverage probability μ decreases. We also observe that the amount of deterioration increases at first (from $\alpha = 0$ to 0.8) and then decreases (from $\alpha = 0.8$ to 1). The deterioration of UE₂'s performance with α can be attributed to the increasing interference associated with increasing $\mathcal{I}(\alpha, \beta)$. The trend in amount of deterioration corresponds to the rate at which $\mathcal{I}(\alpha, \beta)$ grows with α . The performance of UE₁, on the other hand, deteriorates as α increases from 0 to 0.5 and then improves from $\alpha = 0.5$ to $\alpha = 1$. Note that $\alpha = 0.6$ occurs just in between the switch from performance deteriorating with α to improving with α . The performance trend of UE₁ is more complex as at lower α values the message of UE₂ is treated as noise; increasing α thus increases $\mathcal{I}(\alpha, \beta)$ and therefore the interference encountered from the message of UE₂. At $\alpha = 0.6$, $\mathcal{I}(\alpha, \beta)$ is too high for the message of UE₂ to be treated as noise but too low to decode the message of UE₂ before decoding the message of UE₁; thus outage is experienced. After $\alpha = 0.6$ the message of UE₂ is decoded by UE₁ before decoding its own message; increasing α and therefore $\mathcal{I}(\alpha, \beta)$ in this case increases the power of the message of UE₂ making it easier to decode and improving the performance of UE₁.

Fig. 4 is a plot of the meta distribution for different α values using the optimum resource allocation associated with a TMT value of 0.25. Unlike Fig. 3, the resource allocation here is not the same for all α values. This is also why unlike Fig. 3, $\alpha = 0.6$ is not in outage. The performance of UE₂ first decreases from $\alpha = 0$ to 0.1 and then increases from $\alpha = 0.1$ to 0.5. The initial decrease in performance is attributed to $\mathcal{I}(\alpha, \beta)$ increasing from 0. The performance

increase after this is associated with the fact that increasing α increases the bandwidth of UE₂, resulting in the requirement of a lower θ_2 to achieve a TMT of 0.25. From $\alpha = 0.5$ to 0.9 we observe a decrease in performance; this is due to the dominance of the growing impact of $\mathcal{I}(\alpha, \beta)$ increasing interference. From $\alpha = 0.9$ to 1 there is a slight improvement in performance of UE₂; although $\mathcal{I}(\alpha, \beta) = 1$ (the maximum), the small improvement comes from the bigger gain in bandwidth which decreases the θ_2 required thereby improving performance.

While the goal of UE₂ is to use the minimum resources to achieve TMT, the goal of UE₁ is to achieve the largest possible throughput. The performance in terms of the meta distribution for UE₁ in Fig. 4 initially increases from $\alpha = 0$ to 0.3, as the increasing bandwidth reduces the θ_1 required to achieve maximum throughput, resulting in an improvement of performance in terms of the meta distribution. An abrupt decrease is seen in the performance of UE₁ from $\alpha = 0.3$ to 0.4, this corresponds to a switch in decoding so that at $\alpha = 0.4$, UE₁ decodes the message of UE₂ before decoding its own message. As $\mathcal{I}(\alpha, \beta)$ is still not very high, P_2 increases a lot to decode the message of UE₂; this in turn leaves behind less P_1 for the message of UE₁, thereby deteriorating the performance of UE₁. An increase in performance is seen from $\alpha = 0.4$ to 0.5. This coincides with the increase in P_1 as less P_2 is required by UE₁ to decode the message of UE₂ as $\mathcal{I}(\alpha, \beta)$ grows. The performance again decreases from $\alpha = 0.5$ to 0.6; this is because θ_1 increases. Note that while performance here decreases in terms of the percentage of UE₁ that can achieve at least a certain minimum coverage μ , θ_1 increases because a larger throughput can be supported because of the increasing bandwidth. The performance in general increases from 0.6 to 1 with minor fluctuations as the increasing bandwidth for both UEs allows more power to be left for UE₁, resulting in improved performance.

Fig. 5 assumes identical transmission rates for both UEs, thus we use θ to represent both θ_1 and θ_2 . The figure plots the SCP and variance of the meta distribution vs. θ for both UEs using both the exact moments of the meta distribution as well as the approximate moments. We observe that for both UEs, at lower values of θ the approximate moments underestimate the SCP while at higher θ they overestimate the SCP. The fact that at some values the approximate moments underestimate the exact and overestimate at others comes from the opposing nature of approximations A1 and A2 and the impact they have. It should be noted that overall in terms of SCP, the approximate is close to the exact. We observe that the approximate moments always seem to overestimate the variance of the meta distribution. The difference between the exact and approximate variance grows with θ and then drops when θ is too high and all the UEs are

Fig. 6: SCP, throughput and variance of the meta distribution vs. α with $P_1 = 1/3$, $\beta = (1 - \alpha)/2$, $\theta_1 = 1$ dB and $\theta_2 = 0.5$ dB.

in outage. This increase in difference with θ can be attributed to the fact that when θ is low more UEs can guarantee similar performance thus the variance is lower, and the error in the approximate variance grows with θ .

Fig. 6 is a plot of the SCP, throughput and variance of the meta distribution for each UE vs. α using fixed resource allocation. Like in Fig. 3, we observe that at $\alpha = 0.6$ the UEs are in outage. This occurs because of the switch in decoding where UE₁ treats the message of UE₂ as noise at low α but decodes and removes it at high α . Because of the fixed resource allocation in Fig. 6, $\alpha = 0.6$ is unable to use either technique and is thus in outage. Other than the abrupt fall due to outage at $\alpha = 0.6$, UE₂'s SCP slowly decreases with α because of the increasing $\mathcal{I}(\alpha, \beta)$ and therefore interference. The SCP for UE₁, on the other hand, decreases as α increases until $\alpha = 0.6$ because of the increasing interference but grows after this as increasing α makes decoding the message of UE₂ easier for UE₁, improving its SCP. The throughput of UE₂ increases with α (excluding $\alpha = 0.6$) as the increasing bandwidth plays a stronger role on throughput than the decreasing coverage. The throughput of UE₁ also generally increases with α . The only exception to this, other than the discrepancy at $\alpha = 0.6$, is the decrease in throughput from $\alpha = 0.4$ to 0.5 , where the impact on throughput of reduced outage is greater than the impact of increased bandwidth. Excluding the outage at $\alpha = 0.6$, the variance of UE₂ increases with α while the variance of UE₁ first increases and then decreases with α . In Fig. 6b, we observe that using the approximate moments we get a very close match to the exact SCP.

The variance of the meta distribution obtained using the approximate moments is less tight but follows the same trends as the exact moments, overestimating them for all α .

Fig. 7: SCP, throughput and variance of the meta distribution vs. θ_1 using optimum P_1 , θ_2 and β associated with TMT=0.05 for each α value. Black (red) lines represent UE₁ (UE₂)

Fig 7 is a plot of the SCP and variance of the meta distribution vs. θ_1 . Fig. 7a is for $\alpha = 0.2$ and Fig. 7b is for $\alpha = 0.4$. The optimum P_1 , θ_2 and β are used in each so that UE₂ attains a TMT of 0.05 and with the optimum θ_1 the cell sum throughput can be maximized. While the variance of UE₂ is fixed for both α values because of the resources associated with it being fixed, the variance of UE₁ increases and then decreases. We observe that the maximum variance does not correspond with the optimum θ_1 which maximizes the throughput of UE₁ for either α value. We also observe that while in Fig. 7a, the SCP of UE₁ decreases continuously with θ , this is not the case in Fig. 7b, where from $\theta_1 = 8$ dB to 16 dB, the SCP is constant. The variance of UE₁ in Fig. 7b for $\alpha = 0.4$ is also constant in this range of θ_1 unlike its $\alpha = 0.2$ counterpart. This happens because for $\alpha = 0.4$ at $\theta_1 = 8$ dB, the decoding technique switches from UE₁ treating the message of UE₂ as noise to UE₁ decoding and removing UE₂'s message before decoding its own. As $P_1 (= 1 - P_2)$ and θ_2 are fixed, it appears that until $\theta = 16$ dB, the resources are more than sufficient for UE₁ such that increasing θ_1 does not reduce SCP. Note that $\alpha = 0.2$ does not have a switch in decoding technique as the lower value of α makes it difficult for UE₁ to decode the message of UE₂ and thus UE₁ always treats the message of UE₂ as noise.

Fig. 8 is a plot of the SCP, throughput and variance of the meta distribution using the optimum resource allocation for each value of α associated with a TMT constraint of 0.25. We observe

Fig. 8: SCP, throughput and variance of the meta distribution vs. α . The optimum resource allocation associated with TMT=0.25 for each α value is used. Black (red) lines represent UE₁ (UE₂).

Fig. 9: Secrecy probability vs. α with $P_1 = 1/3$ and $\beta = (1 - \alpha)/2$. Black (red) lines represent the case of an innocent (malicious) UE₁. Markers represent Monte Carlo simulations.

that the SCP of UE₂ increases with α and then decreases. The SCP for UE₁ decreases a little and then increases again with α , remaining roughly similar for most α values. Since the resource allocation is for a TMT constrained problem, UE₂ attains throughput equal to the TMT for all α values. UE₁, on the other, hand attempts to maximize its throughput. While the variation in throughput of UE₁ is not significant for different α values, the maximum is attained around $\alpha = 0.1$ after which the throughput decreases a little and then increases again with α . The variance of UE₂ decreases and then increases with α . The variance of UE₁, on the other hand, does not fluctuate too much with α . In general, UE₁ sees little variation in terms of both SCP and variance of the meta distribution than UE₂; this is due to UE₂ attempting to attain throughput equal to TMT so that maximum resources can be left for UE₁.

B. Physical Layer Security in Partial-NOMA

Fig. 9 is a plot of the secrecy probability vs. α for the case of an innocent and a malicious UE₁ using different values of θ_1 and θ_2 . The figure validates our analysis in Section IV as the simulations are a tight match. For both the case of the innocent and the malicious UE₁, the secrecy probability is high at low α . This happens due to the 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 both cases. The drop in secrecy probability occurs at lower α for the malicious UE₁ than its innocent counterpart, highlighting the increased susceptibility to eavesdropping in the case of a

malicious UE_1 . Additionally, at higher α , the secrecy probability in the case of the malicious UE_1 is lower. As the secrecy probability of the innocent and malicious UE_1 is identical and large at low α , it should be highlighted that partial-NOMA using low α can be used to reduce security threats from a malicious eavesdropper to the levels of an innocent eavesdropper; this is in contrast to what can be done in the case of traditional NOMA ($\alpha = 1$).

In Fig. 9 we also observe that decreasing θ_2 increases secrecy probability for the innocent UE_1 case as it becomes easier for UE_2 to decode its message. The secrecy for the malicious UE_1 case also increases at low α due to this. At higher α , however, the secrecy probability decreases as it also becomes easier for the malicious UE_1 to decode UE_2 's message. Decreasing θ_1 decreases the secrecy probability for the innocent UE_1 case at high α as decoding becomes easier for UE_1 and in the process it decodes UE_2 's message, decreasing secrecy.

Fig. 10: Secrecy probability vs. α with $P_1 = 1/3$, $\theta_1 = 0$ dB, $\theta_2 = -3$ dB and $\beta = (1 - \alpha)/2$.

Fig. 11: Secrecy probability vs. α using optimum RA associated with each α value for TMT=0.25

Fig. 10 is a plot of the secrecy probability vs. α using fixed resource allocation. The black curves represent the setup that employs both receive filtering and FSIC (i.e., the partial-NOMA decoding approach). For this approach and (I), the secrecy probability of the innocent and malicious UE_1 at low α is identical, while at high α the malicious UE_1 has lower secrecy probability. For (II) and NOMA, the malicious UE_1 always has lower secrecy probability than the innocent UE_1 . At low α , we observe a drastic difference between the secrecy probabilities for a partial-NOMA setup that employs receive filtering and FSIC compared to the setups in (I) and (II) that do not employ both of these, highlighting the importance of each on the physical layer security in a network. While the performance of (II) is unaffected by α since $\mathcal{I}(\alpha, \beta)$ is set to 1 and fixed resource allocation is used, we observe that (I) has a local maxima at $\alpha = 0.5$.

This occurs because at $\alpha < 0.5$, the low $\mathcal{I}(\alpha, \beta)$ results in a negative $\tilde{P}_2^1$ (i.e., $M_1 = 0$) and thus transmission does not occur in (I); we therefore have zero secrecy in this range for both the case of the malicious and the innocent UE_1 . When $\alpha \geq 0.5$, $M_1 > 0$ and we have positive secrecy probability. As α increases, the malicious UE_1 's secrecy probability decreases because decoding the message of UE_2 becomes easier for UE_1 with increasing $\mathcal{I}(\alpha, \beta)$. Additionally, the increasing $\mathcal{I}(\alpha, \beta)$ also increases interference for UE_2 making it harder for UE_2 to decode its own message. In the case of the innocent UE_1 , although the increasing $\mathcal{I}(\alpha, \beta)$ makes decoding harder for UE_2 , the impact of the increasing $\mathcal{I}(\alpha, \beta)$ increasing intercell interference and making it harder for UE_1 to decode the message of UE_2 is stronger. This results in a slow increase in the secrecy probability in the innocent UE_1 case as α increases from 0.5. Note that after $\alpha = 0.5$ ($\alpha = 0.6$) the malicious (innocent) UE_1 's secrecy probability in (I) coincides with its counterpart that uses both FSIC and receive filtering. This occurs due to the switch in decoding with FSIC at high α which obligates UE_1 to decode and remove the message of UE_2 , like in the case of (I). We also observe that the secrecy probability of partial-NOMA at lower α significantly outperforms that of NOMA for both the case of the malicious and innocent UE_1 , highlighting the significance of a partial overlap.

Fig. 11 is a plot of the secrecy probabilities vs. α using the optimum resource allocation associated with each α for a TMT of 0.25. Partial-NOMA outperforms traditional NOMA (i.e., $\alpha = 1$) in terms of secrecy probability for all α values in case of both the innocent and malicious UE_1 . For each scenario the secrecy probability for the malicious UE_1 case never exceeds the innocent UE_1 case. Similar to Fig. 10, the black and the blue curves for both the cases of innocent and malicious UE_1 coincide at higher α values as in this regime UE_1 employing FSIC also always decodes and removes the message of UE_2 , as in the case of SIC, i.e., (I). Before this range of α , the secrecy probability using (I) is zero for both the case of the innocent and malicious UE_1 as $\tilde{P}_2^1 < 0$, i.e., $M_1 = 0$, and thus transmission does not occur. In the case of (II) where there is no receive filtering, i.e., $\mathcal{I}(\alpha, \beta) = 1$, at low α the bottleneck is UE_2 decoding its own message due to the high interference it encounters from UE_1 's message. This results in outage for UE_2 until $\alpha = 0.3$ and therefore the secrecy probability is zero. 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 , 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 as decoding the message of UE_2 is easy for the malicious UE_1 even when it cannot decode its own message.

VI. CONCLUSION

In the first part of this paper, the meta distribution of a partial-NOMA network is studied to obtain fine-grained information on the network performance. Integral expressions are obtained for the moments of the meta distribution. We are able to reduce the integrals for the first two moments; these are the two moments required for approximating the meta distribution using the beta distribution via moment matching. By proposing the use of two approximations, accurate approximate moments of the meta distribution are derived that further simplify the integral calculation. The impact of different parameters on the percentile performance of each UE in a partial-NOMA network with different overlap values is shown. The second part of this paper focused on physical layer security achievable in a partial-NOMA network. As UE_2 is susceptible to eavesdropping because of the nature of FSIC, we defined the event of secure communication or secrecy as UE_2 being able to decode its message while UE_1 is unable to decode UE_2 's message. Two scenarios were studied: 1) where a malicious UE_1 prioritizes decoding UE_2 's message, 2) where an innocent UE_1 only decodes UE_2 's message when it is required for decoding its own message. Our results show that as anticipated, at high α secrecy in the case of the innocent UE_1 is higher than that of the malicious UE_1 ; at lower α , however, the secrecy probability is equal. Additionally, we find that for both the innocent and malicious UE_1 , secrecy at lower α values is significantly higher than at higher α values including $\alpha = 1$ (i.e., traditional NOMA) highlighting the superiority of a smaller overlap to a full overlap in NOMA. These results shed light on the fact that partial-NOMA with low α can not only be used to achieve higher secrecy but also be used to offer physical layer security to the network from a malicious eavesdropper. We also study the secrecy achieved when traditional SIC is used instead of FSIC and when there is no receive filtering. A significant deterioration in secrecy is observed in both scenarios particularly at lower α . This highlights the importance of receive filtering and FSIC, not just for coverage, but also for secure communication.

REFERENCES

- [1] A. Sasi, A. Al-Dweik, and A. Shami, "Direct data detection of OFDM signals over wireless channels," *IEEE Trans. Vehicular Tech.*, vol. 69, no. 11, pp. 12432–12448, 2020.

- [2] T. Assaf, A. Al-Dweik, M. Moursi, H. Zeineldin, and M. Al-Jarrah, "Exact bit error-rate analysis of two-user NOMA using QAM with arbitrary modulation orders," *IEEE Comm. Lett.*, vol. 24, no. 12, pp. 2705–2709, 2020.
- [3] T. Assaf, A. Al-Dweik, M. S. E. Moursi, H. Zeineldin, and M. Al-Jarrah, "NOMA receiver design for delay-sensitive systems," *IEEE Systems Journal*, pp. 1–12, 2020.
- [4] Y. Liu, Z. Qin, M. ElKashlan, Y. Gao, and A. Nallanathan, "Non-orthogonal multiple access in massive MIMO aided heterogeneous networks," in *Proc. of IEEE Global Communications Conf. (GLOBECOM16)*, Dec. 2016.
- [5] J. Choi, "Power allocation for max-sum rate and max-min rate proportional fairness in NOMA," *IEEE Comm. Letters*, vol. 20, no. 10, pp. 2055–2058, Oct. 2016.
- [6] Y. Liu, Z. Ding, M. ElKashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Select. Areas Commun.*, vol. 34, no. 4, pp. 938–953, Apr. 2016.
- [7] H. Tabassum, E. Hossain, and M. J. Hossain, "Modeling and analysis of uplink non-orthogonal multiple access (NOMA) in large-scale cellular networks using poisson cluster processes," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3555–3570, Aug. 2017.
- [8] K. S. Ali, H. ElSawy, A. Chaaban, M. Haenggi, and M. Alouini, "Analyzing non-orthogonal multiple access (NOMA) in downlink Poisson cellular networks," in *Proc. of IEEE Int. Conf. on Communications (ICC18)*, May 2018, pp. 1–6.
- [9] 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.
- [10] Y. Liu, Z. Ding, M. ElKashlan, and J. Yuan, "Nonorthogonal multiple access in large-scale underlay cognitive radio networks," *IEEE Trans. Vehicular Tech.*, vol. 65, no. 12, pp. 10 152–10 157, Dec. 2016.
- [11] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Comm. Letters*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.
- [12] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Proc. Letters*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.
- [13] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Proc. Letters*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.
- [14] J. Zhu, J. Wang, Y. Huang, S. He, X. You, and L. Yang, "On optimal power allocation for downlink non-orthogonal multiple access systems," *IEEE J. Selec. Areas Commun.*, vol. 35, no. 12, pp. 2744–2757, Dec. 2017.
- [15] 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.
- [16] Z. Zhang, H. Sun, R. Q. Hu, and Y. Qian, "Stochastic geometry based performance study on 5G non-orthogonal multiple access scheme," in *Proc. of IEEE Global Communications Conf. (GLOBECOM16)*, Dec. 2016, pp. 1–6.
- [17] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. of IEEE 77th Vehicular Technology Conf. (VTC13)*, Jun. 2013, pp. 1–5.
- [18] C. L. Wang, J. Y. Chen, and Y. J. Chen, "Power allocation for a downlink non-orthogonal multiple access system," *IEEE Wireless Comm. Letters*, vol. 5, no. 5, pp. 532–535, Oct. 2016.
- [19] Z. Zhang, H. Sun, and R. Q. Hu, "Downlink and uplink non-orthogonal multiple access in a dense wireless network," *IEEE J. Selec. Areas Commun.*, vol. 35, no. 12, pp. 2771–2784, Dec. 2017.
- [20] 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, 2020.
- [21] B. Blaszczyszyn, M. Haenggi, P. Keeler, and S. Mukherjee, *Stochastic Geometry Analysis of Cellular Networks*. Cambridge University Press, 2018.

- [22] 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.
- [23] 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.
- [24] 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>
- [25] 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.
- [26] M. Salehi, H. Tabassum, and E. Hossain, "Accuracy of distance-based ranking of users in the analysis of noma systems," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5069–5083, Jul. 2019.
- [27] M. Haenggi, "The meta distribution of the SIR in Poisson bipolar and cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2577–2589, Apr. 2016.
- [28] M. Salehi, H. Tabassum, and E. Hossain, "Meta distribution of the SIR in large-scale uplink and downlink NOMA networks," *ArXiv e-prints*, Apr. 2018.
- [29] P. D. Mankar and H. S. Dhillon, "Meta distribution for downlink noma in cellular networks with 3gpp-inspired user ranking," in *2019 IEEE Global Communications Conf. (GLOBECOM)*, 2019, pp. 1–6.
- [30] 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, April 2011.
- [31] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third 2014.
- [32] 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.
- [33] 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.
- [34] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "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.
- [35] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. ElKashlan, "Physical layer security for 5g non-orthogonal multiple access in large-scale networks," in *2016 IEEE Int. Conf. on Communications (ICC)*, 2016, pp. 1–6.
- [36] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *2018 IEEE Global Communications Conf. (GLOBECOM)*, 2018, pp. 1–6.
- [37] 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, 2017.
- [38] A. AlAmmouri, H. ElSawy, O. Amin, and M. Alouini, "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.
- [39] 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.
- [40] H. A. David, *Order statistics*. NJ: John Wiley, 1970.
- [41] R. K. Ganti and M. Haenggi, "Asymptotics and approximation of the SIR distribution in general cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2130–2143, Mar. 2016.