

RESEARCH ARTICLE

Impact of Sharing Disruption in MC CR-NOMA

TURKI Y. ALKHAMEES^{1,2}, (Student Member, IEEE),
AND LAURENCE B. MILSTEIN¹, (Life Fellow, IEEE)

¹Department of Electrical and Computer Engineering (ECE), University of California at San Diego, La Jolla, CA 92037, USA

²Electrical Engineering Department, Imam Mohammad Ibn Saud Islamic University, Riyadh 11564, Saudi Arabia

Corresponding author: Turki Y. Alkhamees (tykhamees@imamu.edu.sa)

This work was supported in part by the Office of Naval Research under Grant N00014-21-1-2470.

ABSTRACT Spectrum sharing disruption in cognitive radio networks (CRNs) can significantly degrade network performance. Most sharing disruption attacks in the literature focus on orthogonal multiple access (OMA) or higher layers, such as medium access control (MAC). However, this paper focuses on multi-carrier cognitive radio non-orthogonal multiple access (MC CR-NOMA). The sharing disruption mechanism is established by jamming the channel estimation phase. This is shown to cause a denial-of-service (DoS) for secondary users. We derive the optimal power allocation to disrupt spectrum sharing for a number of secondary users. This is demonstrated by deriving the maximum average number of DoS bands under a constraint on power of the adversary. Furthermore, a comparison between optimal power allocation and uniform power allocation is provided. Both the analytical and numerical results of the optimal sharing disruption are presented. Overall, this study highlights the vulnerabilities in spectrum sharing for MC CR-NOMA and presents a new type of attack.

INDEX TERMS Spectrum sharing, cognitive radio-non-orthogonal multiple access (CR-NOMA), intelligent adversary, pilot jamming attack (PJA), denial-of-service attacks.


I. INTRODUCTION

Cognitive-radio-non-orthogonal multiple access (CR-NOMA) is the integration of cognitive radio (CR) with non-orthogonal multiple access (NOMA) [1], [2], [3]. CR aims to use the spectrum efficiently [4], whereas NOMA multiplexes users to increase capacity [1], [2]. In this integration, licensed primary users (PUs) share their resources (e.g., frequency bands or time slots [1]) with unlicensed secondary users (SUs) using the NOMA principle, as described in [1], [2], and [3]. The power allocation scheme of CR-NOMA is constructed to ensure the quality-of-service (QoS) of PUs. Thus, the co-existence of these two technologies can impact spectrum efficiency, support massive connectivity, and guarantee fairness between users [3], [4], [5].

A. BACKGROUND AND MOTIVATION

Some research results, for example, [6] and [7], treat NOMA as a special case of the CR underlay mode. The literature on CR-NOMA can be divided into two categories: The first

category applies the NOMA technique to users of a secondary network (SN), where the SN is allowed to operate under any of the CR paradigms (e.g., interweave, underlay, or overlay), see [3], [4], and [5] for more insight. The second category considers a network in which a combination of PUs and SUs is performed under the NOMA principle. This indicates that the power allocated to PUs and SUs is fulfilled to protect the QoS of the PUs, which is the focus of this study. Ding et al. [6] investigated the impact of user pairing using a CR-NOMA setup. The authors considered NOMA as a special case of a CR system and called it a CR-inspired NOMA. Reference [7] extended this result by applying CR-NOMA to a multiple-input multiple-output (MIMO) scenario. In [8], power allocation strategies for multi-carrier (MC) NOMA were explored under different performance criteria. All these studies [6], [7], [8] assumed perfect channel state information (CSI). For several reasons, acquiring accurate CSI is often unrealistic. Reference [9] quantified the outage performance of a downlink NOMA system with an imperfect CSI. The results of [9] show that degradation in the channel estimate is a key factor in the outage performance of an NOMA system. Moreover, the authors of [5] emphasized that resource

The associate editor coordinating the review of this manuscript and approving it for publication was Hayder Al-Hraishawi .

allocation in CR-NOMA with imperfect CSI is an open issue. Motivated by the above discussion, if there exists an adversary whose goal is to degrade the performance of CR-NOMA, then the question to be imposed is “How can the adversary best take advantage of this?”

Before answering the proposed question, note that the vulnerability of CSI has been pointed out in many papers [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20]. In addition, [10], [11], [12] discussed many scenarios of attack by adversaries. One such attack occurs when an adversary sends a replica pilot signal of a legitimate user to mislead the base station (BS) or access point (AP). This type of attack is called a pilot contamination attack (PCA), and has two different goals. One is to contaminate the channel estimation phase to increase eavesdropping performance, as in [13] and [14], and the other is to impersonate (i.e., spoof) legitimate users (e.g., [15], [16]). The pilot contamination problem in a physical-layer security setup was first introduced by Zhou et al. [13]. In the downlink transmission phase of a multiple-input single-output (MISO) system, the attacker’s goal is to improve eavesdropping performance. Another study on the performance of a massive MIMO system from the adversary’s perspective was presented in [14]. In [14], it is assumed that there is only a single cell, where the attacker’s goal is to minimize the sum rate of downlink transmissions under both non-secrecy and secrecy performance. Another example is called a pilot jamming attack (PJA), the goal of which is to degrade the overall performance (e.g., bit error rate or signal-to-noise ratio (SNR)). In this example, the adversary sends a jamming signal during the channel estimation phase. Clancy et al. [17] pointed out that jamming channel measurements appear to be an efficient type of attack. Inspired by [17], the impact of PJA was studied in [18] and extended to MIMO scenarios such as [12]. In [19] and [20], the authors studied jamming of the pilot and data transmission phases in MIMO and massive MIMO systems, respectively. In fact, the difference between PJA and PCA is based on the objectives of the adversary. This depends on the model of a particular system (e.g., physical-layer security) being implemented as well as the metric of the system’s performance (e.g., downlink secrecy rate). The common focus of the pilot attacks discussed in [13], [14], [15], [16], [18], [19], and [20] is limited to orthogonal multiple access (OMA) systems. This motivated us to investigate pilot attacks within the context of NOMA systems.

To address the question proposed above, an adversary can exploit pilot attacks to disrupt the CR-NOMA system. The main objective of an adversary in a CR-NOMA system is to cause a denial-of-service (DoS) to the SU. To accomplish this, the adversary needs to implement a PJA rather than a PCA. It is important to note that the adversary’s goal is not to intercept users’ messages or impersonate SUs, as the system lacks a secrecy protocol. Therefore, in this study, PJA in a CR-NOMA system was emphasized.

Another motivation to discuss is that most of the current research on NOMA systems focuses on the mechanisms of

possible attacks and the proposed countermeasure schemes, without examining the optimal attack strategies. For example, in [10] and [21], the authors pointed out the possibility of spoofing attacks if there is a large disruption to the PCA in different scenarios. Another example is [22], where the authors proposed a power allocation and beamforming technique to improve the physical layer security of CR-NOMA networks. However, the countermeasures are beyond the scope of this study, and for more details about jamming attacks and their countermeasures, surveys such as [10], [11], [12], and [23] provide further information.

The primary focus of this study is to design an intelligent adversary attack that causes DoS to multiple SUs. These are types of DoS attacks, because the intelligent adversary desires to shut down the SUs from utilizing the bands. DoS attacks destroy the main purposes of MC CR-NOMA, including spectrum efficiency and massive connectivity [2], [4]. To the best of our knowledge, the number of SUs that an adversary can cause a DoS with a given total power in an MC CR-NOMA remains unsolved.

The power-limited adversary framework in a CR-NOMA system is relevant to many military and traffic patrol applications, and it boils down to unmanned aircrafts, wireless sensor networks, and vehicular networks. Additionally, Cognitive Internet-of-Things (CIoT) applications include environmental monitoring, smart grids, e-healthcare, and smart transportation. Most examples were vulnerable to adversarial scenarios. Consequently, threats and dangers to the public can arise, including terrorism, vandalism, and other motivated crimes.

B. CONTRIBUTION

The contribution of this paper can be summarized in three points:

- First, we propose a framework for sharing disruption by a power-limited intelligent adversary, in which the adversary jams the uplink pilot transmissions in an MC system. Consequently, several SUs suffer from the denial of entering the spectrum in an MC CR-NOMA downlink transmission.
- Next, we derive an analytical closed-form expression for DoS probability, assuming that the adversary experiences flat Rayleigh fading, and that the transmitted signal is a complex Gaussian random process. The analytical results were compared with those of the Monte Carlo simulations.
- Finally, we provide a disruption strategy for spectrum sharing by optimally allocating an adversarial power budget across multiple bands with the goal of causing maximally destructive effects on the MC CR-NOMA system. Furthermore, we demonstrated that this approach results in a worst-case performance analysis of sharing disruptions. In addition, we present a comparison between the uniform power allocation and optimal power allocation at the adversary.

TABLE 1. Summary of pilot attacks.

Ref.	Scenario	Metric	Type
[13]	MISO with single eavesdropper	Maximize the SNR of the eavesdropper	PCA and OMA
[14]	Massive MIMO with single eavesdropper	Minimize the achievable downlink sum-rate	PCA and OMA
[15]	MISO with multiple eavesdroppers	Maximize the SNR of the eavesdroppers.	PCA and OMA
[16]	Massive MIMO with multiple eavesdroppers	minimize the achievable downlink sum-rate	PCA and OMA
[18]	SISO with single jammer	minimize the bit error rate	PJA and OMA
[19]	MIMO with single jammer	minimize the ergodic capacity	PJA and OMA
[20]	Massive MIMO with single jammer	minimize the spectral efficiency	PJA and OMA

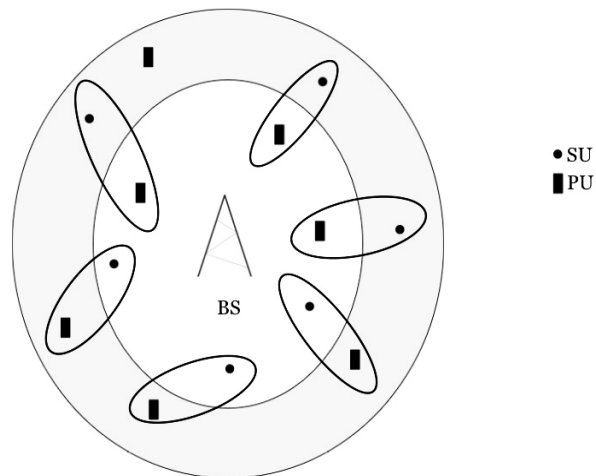


FIGURE 1. An illustration of MC CR-NOMA.

BS needs to divide power allocation into two goals. The first is the PU’s reliable reception, and the second is the opportunistic transmission to the SU’s [5]. Consequently, the key advantage of CR-NOMA is its ability to achieve a balance between throughput and fairness [3].

To perform CR-NOMA, the BS transmits a superimposed signal to both the SU and PU in the k^{th} cluster (i.e., band), as follows [1], [4]:

$$x_k(n) = \sqrt{P_{k,T}} (a_{k,p}s_{k,p}(n) + a_{k,s}s_{k,s}(n)). \quad (1)$$

where $s_{k,p}(n)$ and $s_{k,s}(n)$ denote the transmitted data signal from the BS to the PU and the SU in the k^{th} band, respectively. In addition, the total transmitted power is denoted by $P_{k,T}$ in the k^{th} band. The terms $a_{k,p}^2$ and $a_{k,s}^2$ correspond to the power allocation coefficients of PU and SU, respectively, with a constraint of $a_{k,p}^2 + a_{k,s}^2 = 1$. For each cluster k , $\forall k = \{1, \dots, U\}$, and user i , $\forall i \in \{p, s\}$, that is, the PU or SU, respectively, the channel from the BS to the user is represented as $\underline{g}_{k,i} = \sqrt{\beta_{k,i}}\underline{h}_{k,i}$, where $\underline{h}_{k,i} \sim \mathcal{CN}(0, 1)$, and $\beta_{k,i}$ denotes the large-scale fading expressed as $\beta_{k,i} = d_{k,i}^{-\alpha}$, where $d_{k,i}$ is the distance between the BS and user i in cluster k . Parameter α represents the path loss exponent.

MC CR-NOMA [8] aims to allocate power among users (i.e., PU and SU) within each band. This power allocation relies on the availability of users’ CSI at the BS. In other words, the BS needs to estimate the CSIs from all clusters and separate the pilot signals of each user in each cluster, whether it is a PU or SU. To guarantee that the BS gives higher priority to the PUs, as in [7] and [22], PUs in the cell must transmit a designated pilot signal to the BS. If we assume that the CSI of the i^{th} user in the k^{th} cluster is estimated at the BS, similar to [22], then from the orthogonality principle, the minimum mean square error (MMSE) estimate [24], denoted as, $\hat{h}_{k,i}$, which has a distribution of, $\mathcal{CN}(0, 1 - \sigma_{i,k}^2)$, where $\sigma_{i,k}^2 =$

C. STRUCTURE

The outline of the paper is as follows. Section II presents the preliminaries and general formulation. The downlink outage performance is described in Section III. The numerical results are presented in Section IV, and Section V concludes this paper.

II. PRELIMINARIES AND GENERAL FORMULATION

In this section, we discuss the communication model framework. Subsequently, we present the assumptions regarding the knowledge available to an adversary, followed by an overview of the attack mechanism. Finally, we addressed the problem formulation related to DoS attacks.

A. COMMUNICATION MODEL

Consider a downlink MC CR-NOMA system with U clusters. In each of the U clusters, the PU and SU are grouped together to serve the same frequency band (or subcarrier), following the NOMA principle [1], [3], and different groups are allocated to different frequency bands, as shown in Fig.1. We also assume that the system employs time-domain duplexing (TDD).

Spectrum sharing in MC CR-NOMA is obtained by constraining the power allocated to the SU on each band (cluster) to satisfy the QoS of the PU [1], [6]. This means that the

$\sigma_{wBS}^2/(\beta_{k,i} + \sigma_{wBS}^2)$. The term σ_{wBS}^2 is due to the thermal noise at the BS, which is distributed as $\sim \mathcal{CN}(0, \sigma_{wBS}^2)$.

The intended received signal for users in the k^{th} band was shown in [9] with an imperfect channel estimate. Considering that NOMA is a special case of CR systems, as mentioned in [6], and assuming that channel reciprocity holds, similar to [7] and [22], the intended received signals for the PU and SU can be expressed as follows:

$$y_{k,p}(n) = g_{k,p}x_k(n) + w_{k,p}(n) = (\hat{h}_{k,p} + \varepsilon_{k,p}) \sqrt{\beta_{k,p}P_{k,T}}(a_{k,p}s_{k,p}(n) + a_{k,s}s_{k,s}(n)) + w_{k,p}(n), \quad (2)$$

$$y_{k,s}(n) = g_{k,s}x_k(n) + w_{k,s}(n) = (\hat{h}_{k,s} + \varepsilon_{k,s}) \sqrt{\beta_{k,s}P_{k,T}}(a_{k,p}s_{k,p}(n) + a_{k,s}s_{k,s}(n)) + w_{k,s}(n), \quad (3)$$

where $w_i(n)$ is the received background noise sample at either the PU or SU, and each one is a zero-mean complex Gaussian with variance $\sigma_{w_{k,i}}^2$, for $i \in \{p, s\}$.

B. ATTACK MODEL

In MC CR-NOMA, constructing PJAs for multiple clusters (i.e., users) appears to be a more practical and simple form of attack than PCAs. This is because a single adversary cannot eavesdrop on multiple legitimate user messages simultaneously. Moreover, there is always a possibility that an adversary cannot exactly know the pilot signal (sequence) of a legitimate user. Therefore, the adversary transmits a jamming signal during the channel estimation phase at the BS.

In this study, we assume that the adversary knows the total number of bands U , and the targeted signal-to-interference-plus-noise ratio (SINR) of the users. We further assume that the adversary is synchronized with the user signal during the channel estimation, which is a common assumption in pilot attacks [12], [13], [14], [15], [16], [17], [18], [19], [20]. In addition, we assume that the adversary has full knowledge of the distances between the BS and users in accordance with pilot attacks, as in [12], [13], [15], [16], [18], [19], and [20]. In practice, an adversary does not know the aforementioned information. However, it is widespread in the electronic warfare literature (see [10], [11], [12], [23]), assuming that the adversary has full knowledge of at least some information, and this allows the adversary to inflict worst-case performance. Therefore, this study emphasizes worst-case analysis, which is an upper bound for spectrum sharing disruption. Note that the worst-case analysis is from the perspective of legitimate users (i.e., SUs), whereas it is considered optimal jamming on the part of the adversary. Note that the worst-case analysis is from the perspective of legitimate users (i.e., SUs), whereas it is considered optimal jamming on the part of the adversary.

The authors of [9] indicated that the parameter $\sigma_{p,k}^2$, defined in the previous subsection, indicates the quality of channel estimation. Based on this, the adversary’s goal of

degrading the quality of the channel estimate implies that the adversary needs to increase $\sigma_{p,k}^2$. The channel estimate of the k^{th} PU is a modified result from the previous subsection that includes the adversary, as shown below:

$$\underline{h}_{k,p} = \underbrace{\hat{h}_{k,p}}_{\text{estimated channel coefficient}} + \underbrace{\varepsilon_{k,p} + g_{k,A}z_{k,A}}_{\text{effective noise}}, \quad (4)$$

where the channel coefficient from adversary-to-BS is assumed to have a Rayleigh distribution. This means that $g_{k,A} = \sqrt{\beta_{k,A}}h_{k,A}$, where $h_{k,A} \sim \mathcal{CN}(0, 1)$, and $\beta_{k,A} = d_{k,A}^{-\alpha}$. Finally, $d_{k,A}$ denotes the distance between the BS and the adversary. Note that $\varepsilon_{k,p}$ is still the error term, which is modeled as a complex Gaussian random variable distributed as in [9].

From [25], for a given Gaussian channel and Gaussian target signal, the worst-case jamming scenario occurs when a Gaussian signal is transmitted. To accomplish this, the adversary must transmit a complex Gaussian signal on the k^{th} band distributed as $z_{k,A} \sim \mathcal{CN}(0, P_{k,A})$, where $P_{k,A}$ is the adversary power in the k^{th} band. The adversary signal is assumed to be independent of both $\varepsilon_{k,p}$ and $\underline{h}_{k,p}$. It is also assumed that the adversary signal is independent of $h_{k,A}$. Conditioned on $\underline{h}_{k,A}$, we apply the linear MMSE principle [24]. Then, the variance is obtained by modifying the variance from the previous subsection to include the adversary and is given by

$$\begin{aligned} \text{var}(\hat{h}_{k,p}) &= \text{var}(\underline{h}_{k,p}) - \text{var}\left(\varepsilon_{k,p} + \sqrt{\frac{\beta_{k,A}}{\beta_{k,p}}}h_{k,A}z_{k,A}\right) \\ &= 1 - \frac{\sigma_{p,k}^2 \left(\sigma_{wBS}^2 + \beta_{k,A} |\underline{h}_{k,A}|^2 P_{k,A}\right)}{\beta_{k,p} + \left(\sigma_{wBS}^2 + \beta_{k,A} |\underline{h}_{k,A}|^2 P_{k,A}\right)}. \end{aligned} \quad (5)$$

C. PROBLEM FORMULATION

In the context of CR-NOMA, launching DoS attacks on SUs within each band involves PUs exclusively utilizing those bands. To achieve this, the adversary aims to trick the BS to allocate a substantial portion of the transmitted power in the k^{th} cluster (i.e., band) solely for the PU’s (i.e., $a_{k,s}^2 = 0$). This can be illustrated by the worst-case outage performance of SU. Consider the single-carrier CR-NOMA case as an example, which can be obtained from [6] as follows:

$$\begin{aligned} \mathbb{P}_{out,SU}^{(k)} &= \Pr\left\{\left(a_{k,s}^2 = 0\right) \cup \left(\gamma_{k,s} < \theta_{k,SU}, a_{k,s}^2 \neq 0\right)\right\} \\ &= \Pr\left\{a_{k,s}^2 = 0\right\} + \Pr\left\{\gamma_{k,s} < \theta_{k,SU}, a_{k,s}^2 \neq 0\right\}, \end{aligned} \quad (6)$$

where $\gamma_{k,s}$ is the instantaneous SINR of SU in the k^{th} band. In (6), $\theta_{k,SU}$ is the SU’s targeted SINR in the k^{th} band. An outage event at the SU was defined as the union of two events. These events can be described using the following

two scenarios: In the first scenario sufficient QoS is not guaranteed to the PU, which results in the SU not being able to serve. The second scenario arises when $\underline{\gamma}_{k,s}$ falls below $\theta_{k,SU}$, provided that the SU has been served and the QoS requirements for the PU are fulfilled. Clearly, in (6), $\Pr \left\{ a_{k,s}^2 = 0 \right\}$ can be expressed as a DoS probability of the SU in the k^{th} band, because it is the event where the PU is unable to share the spectrum with the SU, and these bands are called DoS bands. We are interested in the average number of DoS bands, denoted by B_A .

Note that a DoS event exists when the SU is both a cell-edge user and a cell-center user. This is because the PU must always be served with a higher priority than the SU. Thus, the PU outage performance was evaluated as a worst-case scenario, which was modeled in [7] and [22]. This assumption also leads to the SU having a similar outage expression for the cell-edge SU and the cell-center SU, as illustrated in [22].

For simplicity, the targeted SINR of the PUs is assumed to be the same across all bands, such that $\theta_{k,PU} = \theta_{PU}$. Therefore, the targeted SINR of the SUs is also the same across all bands, which means $\theta_{k,SU} = \theta_{SU}$.

Let us now define $\mathbb{P}_{DoS}^{(k)}$ as the probability of a DoS in the k^{th} band: Additionally, let $B = \{1, 2, 3, \dots, U\}$ be the set of bands available to be shared between users, and assume that all users' CSI is known and noisy at the BS. Then, B_A can be expressed as the sum of the individual DoS probabilities in each band, as shown in (7).

$$B_A = \sum_{k=1}^U \mathbb{P}_{DoS}^{(k)} \quad (7)$$

In the next step, we need to formulate an optimal sharing disruption over U bands. The objective of an adversary with total power P_A is to maximize the average number of DoS bands of (7). Hence, we have the following optimization problem:

$$\begin{aligned} & \max_{P_{1,A}, \dots, P_{U,A}} \sum_{k=1}^U \mathbb{P}_{DoS}^{(k)}, \\ & \text{s.t } P_{k,A} \geq 0 \text{ for } k = 1, \dots, U, \sum_{k=1}^U P_{k,A} = P_A. \end{aligned} \quad (8)$$

III. OUTAGE PERFORMANCE OF DOWNLINK TRANSMISSION

In this section, we analyze the performance of the downlink transmission. First, we present the probability of a DoS at an SU when an adversary is present. Subsequently, we formulate the result of the DoS probability into an optimization problem. We then suggest two power allocation techniques for the adversary to implement.

A. PERFORMANCE WHEN AN ADVERSARY IS PRESENT

If the adversary jams the PU channel estimation at the BS, as in (5), the intended received signal at the PU can be derived by modifying the result of (2) to include the presence of an

adversary, as shown below:

$$\begin{aligned} y_{k,p}(n) &= g_{k,pA} x_k(n) + w_{k,p}(n) \\ &= \left(\hat{h}_{k,p} + \varepsilon_{k,p} + \sqrt{\beta_{k,A}/\beta_{k,p}} \hat{h}_{k,A} z_{k,A} \right) \\ &\quad \times \sqrt{\beta_{k,p} P_{k,T}} \left(a_{k,p} s_{k,p}(n) + a_{k,s} s_{k,s}(n) \right) \\ &\quad + w_{k,p}(n). \end{aligned} \quad (9)$$

To satisfy the QoS requirements for the PU, the BS first needs to allocate power to the PU [1], [6]. This means that the BS needs to adjust the choices of the power allocation coefficients such that the QoS of the PU is satisfied. From (9), the SINR of the PU in the k^{th} can be expressed as follows:

$$\underline{\gamma}_{k,p} = \frac{\beta_{k,p} a_{k,p}^2 \left| \hat{h}_{k,p} \right|^2}{\beta_{k,p} \left(a_{k,s}^2 \left| \hat{h}_{k,p} \right|^2 + \sigma_{p,k}^2 \right) + \rho_k} \quad (10)$$

where $\rho_k = \sigma_{w_{k,p}}^2 / P_{k,T}$. Note that, in (10), the numerator is the desired signal of the PU in the k^{th} band. The denominator represents the intra-cluster interference, imperfection of the channel estimation including the adversary, and received noise sample at the PU. Note that inter-cluster interference is beyond the scope of this study. However, the rejection techniques for inter-cluster interference are suggested as in [22] or [26], and for more details see [1], [2], and [3].

In line with references [6], [22], and [25], when the QoS requirements for PUs are not fulfilled, a significant portion of the transmitted power is allocated to the PU. More specifically, the PU outage event is defined as a failure to meet the QoS requirements, represented by $\underline{\gamma}_{k,p} < \theta_{PU}$. Then, by substituting (10) with the PU outage event, we obtain

$$\frac{\beta_{k,p} a_{k,p}^2 \left| \hat{h}_{k,p} \right|^2}{\beta_{k,p} \left(a_{k,s}^2 \left| \hat{h}_{k,p} \right|^2 + \sigma_{p,k}^2 \right) + \rho_k} < \theta_{PU}. \quad (11)$$

If we now substitute $a_{k,p}^2 = 1 - a_{k,s}^2$, then with some algebraic manipulation, we have

$$\frac{\left| \hat{h}_{k,p} \right|^2 - \theta_{PU} \left[\sigma_{p,k}^2 + \rho_k / \beta_{k,p} \right]}{\left| \hat{h}_{k,p} \right|^2 (1 + \theta_{PU})} > a_{k,s}^2. \quad (12)$$

Hence, (12) implies that the maximal transmit power that can be allocated to the SU in the k^{th} band is given by

$$a_{k,s}^2 = \max \left\{ 0, \frac{\left| \hat{h}_{k,p} \right|^2 - \theta_{PU} \left[\sigma_{p,k}^2 + \frac{\rho_k}{\beta_{k,p}} \right]}{\left| \hat{h}_{k,p} \right|^2 (1 + \theta_{PU})} \right\}. \quad (13)$$

Note that $a_{k,s}^2$ is a function of the channel coefficient of the k^{th} PU. This indicates that the power allocated to the SU was constrained to satisfy the QoS requirements of the PU. From (13), we can conclude that a DoS to the SU in the k^{th} band (i.e., $a_{k,s}^2 = 0$) can occur when $\left| \hat{h}_{k,p} \right|^2 <$

$\theta_{PU} [\sigma_{p,k}^2 + \rho_k/\beta_{k,p}]$. This means that the BS have to allocate all of its available power to the PU to satisfy the QoS. To study the outage performance at the SU, in particular, the probability of DoS at the SU in the k^{th} band, conditioned upon $|h_{k,A}|^2$, is defined as

$$\begin{aligned} P_{DoS}^{(k)} &= Pr \{a_{k,s}^2 = 0\} \\ &= Pr \left\{ |\hat{h}_{k,p}|^2 < \theta_{PU} \left[\sigma_{p,k}^2 + \frac{\rho_k}{\beta_{k,p}} \right] \right\} \\ &= 1 - e^{-\left(\frac{\theta_{PU} [\sigma_{p,k}^2 + \frac{\rho_k}{\beta_{k,p}}]}{(1-\sigma_{p,k}^2)} \right)}, \end{aligned} \quad (14)$$

because $\hat{h}_{k,p}$ follows a complex Gaussian distribution. Thus, in (14), $|\hat{h}_{k,p}|^2$ follows an exponential distribution with parameters $(1 - \sigma_{p,k}^2)$. Let $\eta_k \sigma_{p,k}^2 + \rho_k/\beta_{k,p}$, $Y_k |h_{k,A}|^2$, and $\bar{P}_k \triangleq \mathbb{E}_{Y_k} \{P_{DoS}^{(k)}\}$. Then, averaging (15) over Y_k , is the total probability of DoS at SU and is given by

$$\begin{aligned} \bar{P}_k &= \int_0^\infty Pr \{Y_k < \eta_k \theta_{PU} | Y_k = z_k\} f_{Y_k}(z_k) dz_k \\ &= 1 - \frac{\beta_{k,p}^2}{\theta_{PU} P_{k,A} \beta_{k,A} [\beta_{k,p} + \rho_k] + \beta_{k,p}^2} e^{-\left(\frac{\theta_{PU} A_2}{\beta_{k,p}^2} \right)}, \end{aligned} \quad (15)$$

where $A_2 = \beta_{k,p} \rho_k + \sigma_{wBS}^2 (\beta_{k,p} + \rho_k)$. For the derivations of \bar{P}_k see Appendix A.

As a sanity check, if the estimation is error-free, then $\sigma_{p,k}^2 = 0$. Thus, (15) is equivalent to the result in [6]. In addition, consider the case where only the adversary is absent. Then, the DoS probability of the k^{th} band can be expressed as

$$\mathbb{P}_{DoS}^{(k)}(0) = 1 - e^{-\left(\frac{\theta_{PU} A_2}{\beta_{k,p}^2} \right)}. \quad (16)$$

Substituting (16) into (4), the optimal spectrum sharing disruption can be formulated as

$$\begin{aligned} \max_{P_{1,A}, \dots, P_{U,A}} \sum_{k=1}^U \left(1 - \frac{1}{P_{k,A} \beta_{k,A} a_k + 1} e^{-(a_k \sigma_{wBS}^2 + b_k)} \right), \\ \text{s.t } P_{k,A} \geq 0, \text{ for } k = 1, \dots, U, \sum_{k=1}^U P_{k,A} = P_A \end{aligned} \quad (17)$$

where $a_k \theta_{PU} [\beta_{k,p} + \rho_k] / \beta_{k,p}^2$ and $b_k \theta_{PU} \rho_k / \beta_{k,p}$.

B. OPTIMAL POWER ALLOCATION

Note that (17) is a convex optimization problem because the objective, inequality constraint, and equality constraint are convex. By applying the KKT conditions [27], the optimal

power allocated to k^{th} band can be expressed as

$$P_{k,A}^* = \begin{cases} \mu_k, & \mathbb{P}_{DoS}^{(k)}(0) < 1 - \frac{v^*}{a_k \beta_{k,A}} \\ 0, & \mathbb{P}_{DoS}^{(k)}(0) \geq 1 - \frac{v^*}{a_k \beta_{k,A}}, \end{cases} \quad (18)$$

where,

$$\mu_k = \sqrt{\frac{1 - \mathbb{P}_{DoS}^{(k)}(0)}{a_k \beta_{k,A} v^*}} - \frac{1}{a_k \beta_{k,A}}, \quad (19)$$

and v^* satisfies the constraint $\sum_{k=1}^U P_{k,A}^* = P_A$, which is an increasing function of $1/\sqrt{v^*}$ (see Appendix B). This function can be computed using the bisection method. When the optimal strategy of spectrum sharing disruption is implemented, the adversary efficiently allocates jamming power in each band. This implies that the adversary approaches at full-band jamming strategy.

C. EQUAL-POWER ALLOCATION

A more realistic case is when the adversary has no prior knowledge of terms $\beta_{k,A}$, a_k , b_k or σ_{wBS}^2 . In this case, the optimal $P_{k,A}$ that maximizes (17) is the equal-power strategy. Similar to Appendix B, fulfilling the complementary slackness condition yields only two cases. In these cases, all terms (i.e., $\beta_{k,A}$, a_k , b_k and σ_{wBS}^2) are assumed to be the same in each band for some k , where $k \in \{1, 2, \dots, U\}$, and for the rest of the bands, $P_{k,A} = 0$. Therefore, the optimal spectrum sharing disruption power allocation is as follows:

$$P_{k,A}^* = \begin{cases} \frac{P_A}{u}, & k \in \varphi_A \\ 0, & \text{otherwise,} \end{cases} \quad (20)$$

where $\varphi_A \triangleq \{k | P_{k,A}^* > 0\}$ is expressed as a set of DoS bands caused by the adversary. By definition, the cardinality of φ_A is u ($0 < u \leq U$), representing the number of DoS bands. In this case, the adversary's goal is to increase the DoS to as many bands as possible. Because there are U available bands, the optimal number of DoS bands, u^* , is upper bounded by U . Hence, the optimal strategy is to jam all available bands, U , which implies that

$$P_{k,A}^* = \frac{P_A}{U}, \quad k = 1, \dots, U. \quad (21)$$

Full-band jamming was optimal (i.e., $u^* = U$) when the adversary has a sufficiently large P_A . Otherwise, the partial-band jamming was optimal.

IV. NUMERICAL RESULT

In this section, the optimal sharing disruption technique is illustrated using numerical simulations. For simplicity, in these simulations, we assume that the BS transmits fixed power in each cluster (i.e., $P_{k,T} = P_T/U$). In addition, we assume that the noise variance of all PUs is the same as the noise variance at the BS, that is $\sigma_{w1,p}^2 = \sigma_{w2,p}^2 = \dots = \sigma_{wu,p}^2 = \dots = \sigma_{wU,p}^2 = \sigma_{wBS}^2 = N_0$. Small-scale fading

is assumed to be Rayleigh fading for both the PUs and the adversary. Finally, it is desirable to compare CR-NOMA pilot attacks with the existing OMA pilot attacks. However, the unconventional nature of CR-NOMA pilot attacks makes it difficult to formulate a meaningful metric for direct comparisons.

A. DoS PROBABILITY

The parameters used in the simulations were set as follows: $N_0 = -64$ dBm, $P_{k,T} = 30$ dBm, $d_{k,A} = 1/2$ km, and $\alpha = 2$. Monte Carlo simulation results were averaged over 10^6 independent trials. Figs.2 and 3 plot $\mathbb{P}_{DoS}^{(k)}$ versus $P_{k,A}$, where the curves are parameterized for various values of θ_{PU} and $d_{k,p}$, respectively. Both Figs.2 and 3 show that $\mathbb{P}_{DoS}^{(k)}$ increases when $P_{k,A}$ increases up to the point where the k^{th} band approaches full-band jamming (i.e., a full-band DoS attack). Furthermore, the numerical results obtained from (15) were matched with those of the Monte Carlo simulations. In addition, Fig.2 illustrates the impact of θ_{PU} on DoS probability in a single-carrier CR-NOMA. As shown in Fig.2, when θ_{PU} increased, the DoS probability also increased. This is because the targeted data rate of the PU increases, in which case, the bandwidth to be shared with the SU decreases. This means that the adversary needs to utilize less power to launch a full-band DoS when the targeted data rate of the PU increases. Fig.3 shows the effect of PU distance on $\mathbb{P}_{DoS}^{(k)}$ in CR-NOMA. The results show that $\mathbb{P}_{DoS}^{(k)}$ also shifts to a full-band DoS faster as well. This was because the free-space loss factor increased. Therefore, the adversary needs to use less power than when the PU distance is relatively shorter. We conclude that each curve undergoes a shifting transition to a full-band DoS, and the shift is determined by θ_{PU} , $d_{k,p}$, and other parameters, as described in the next section.

B. AVERAGE NUMBER OF DoS BANDS

We illustrate the impact of system parameters on the average number of DoS bands. Fig.4 shows plots of B_A versus the available total number of bands, where the curves are parameterized by P_A for different values of $d_{k,A}$. The other parameters were set as follows: $N_0 = -64$ dBm, $P_{k,T} = 30$ dBm, $\theta_{PU} = 1$, and $\alpha = 2$. The PUs are distributed over a circular ring, where the distance vector is denoted by $\mathbf{d}_p = [d_{1,p}, d_{2,p}, \dots, d_{U,p}]$, $d_{k,p} \in [0, 1]$ km. The curves in Fig.4 show the transition from full-band to partial-band jamming. The reason for full-band jamming is that the adversary has a sufficiently large P_A to launch a PJA on all the available bands. In this case, each curve B_A is equal to the available number of bands (i.e., the slope is 45°) because of the presence of both the adversary and system parameters. The second case is the partial-band jamming region because the adversary's total power is not large enough to cause a DoS attack on all available SUs. Because of the insufficient power of the adversary, the slope decreases, as shown in Fig.4. In this case, the value of the slope was determined solely by the system parameters. Therefore, the result shows that adversary

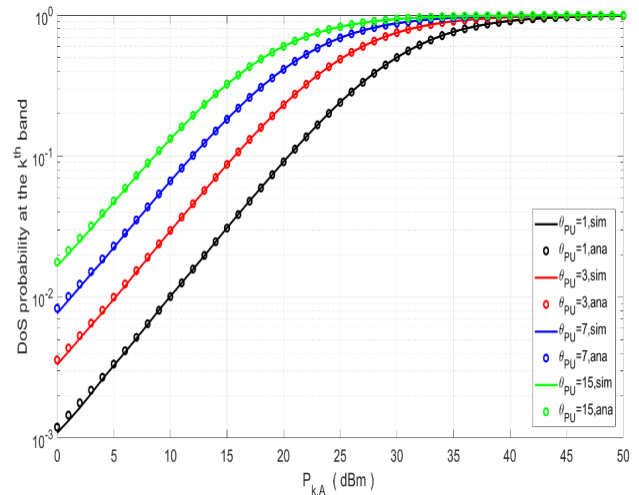


FIGURE 2. DoS probability at the k^{th} band $\mathbb{P}_{DoS}^{(k)}$ versus the adversary power in the k^{th} band $P_{k,A}$ (dBm).

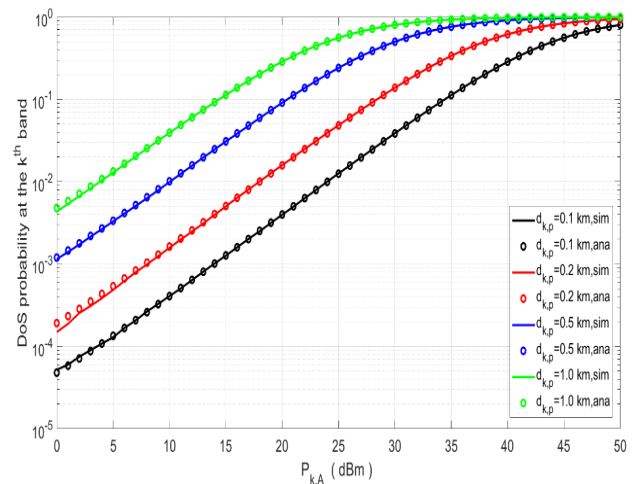


FIGURE 3. DoS probability at the k^{th} band $\mathbb{P}_{DoS}^{(k)}$ versus the adversary power in the k^{th} band $P_{k,A}$ (dBm).

is jammed a fraction of the available bands. An increase in P_A , leads to an increase in B_A , as shown in Figs.4 (a) and 4 (b). This is expected because, as shown in Figs.2 and 3, when the adversary's power in the k^{th} band increases, the probability of DoS also increases. Comparing Fig.4 (b) with Fig.4 (a), we see that when $d_{k,A}$ increases for the same value of P_A , Fig.4 (a) outperforms Fig.4 (b) in terms of B_A . This is because the adversary in Fig.4 (a) is closer to the BS during the PJA than in Fig.4 (b).

In Figs.5 and 6, B_A is plotted versus P_A , for various values of $P_{k,T}$ and N_0 , respectively, and the remaining parameters are the same as in Fig.4. The only difference was that $U = 100$, where previously, we set $U = 1$, because we considered a single-carrier CR-NOMA. As expected, Figs.5 and 6 show that B_A increases when P_A increases. Note that in both Figs.5 and 6, B_A is almost constant in the low P_A region. From

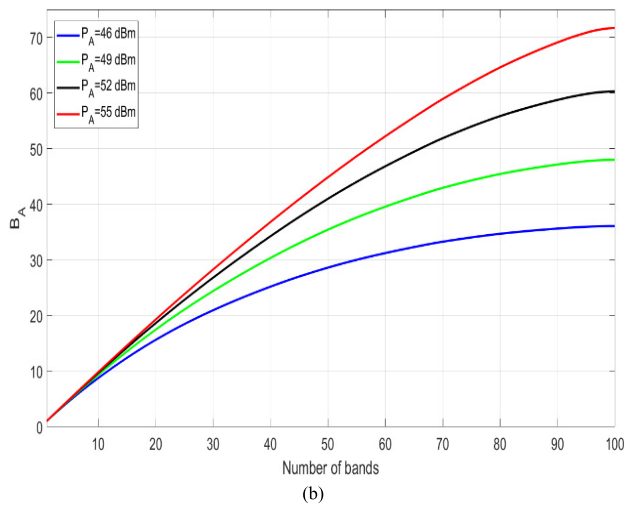
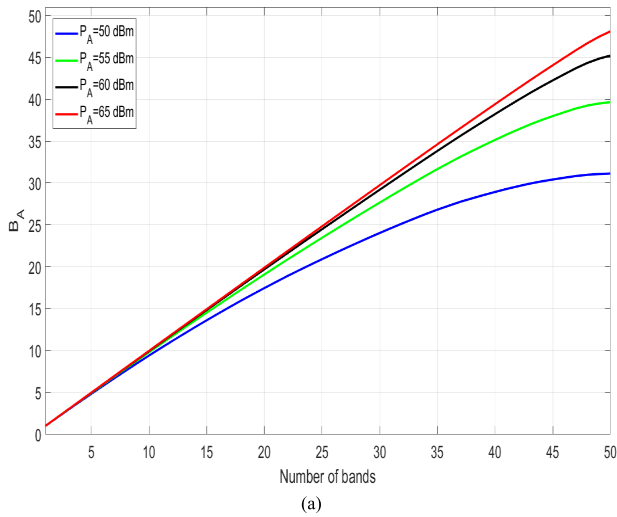


FIGURE 4. Average number of DoS bands B_A versus the number of bands: (a) $d_{k,A} = 1/2$ km (b) $d_{k,A} = 1$ km.

Figs.2 and 3, we know that the adversary needs the power to be around $P_A = 30$ dBm for an adversary to cause a DoS attack. However, for an MC CR-NOMA system, the adversary would need to use even higher power levels to achieve a successful DoS attack. Furthermore, the use of equal-power is not the best strategy for an adversary with a low power budget. As shown in Fig.5, $P_{k,T}$ decreases and B_A starts at a higher value, and as a result, B_A continues to shift faster to full-band jamming than the other curves. However, for the high P_A regime, the difference between the values of $P_{k,T}$ indicates that the value of B_A is unnoticeable. This is because the adversary has a very high total power to disrupt spectrum sharing. In contrast, in Fig.6, when N_0 increases, B_A starts at a higher value. In addition, B_A shifted faster toward full-band jamming. The observations in Fig.5 are the same as those in Fig.6, and the reasons for these observations in Fig.6 are the same as those in Fig.5. In conclusion, $P_{k,A}^*$ is affected by θ_{PU} , $d_{k,A}$, $d_{k,p}$, $P_{k,T}$ and N_0 .

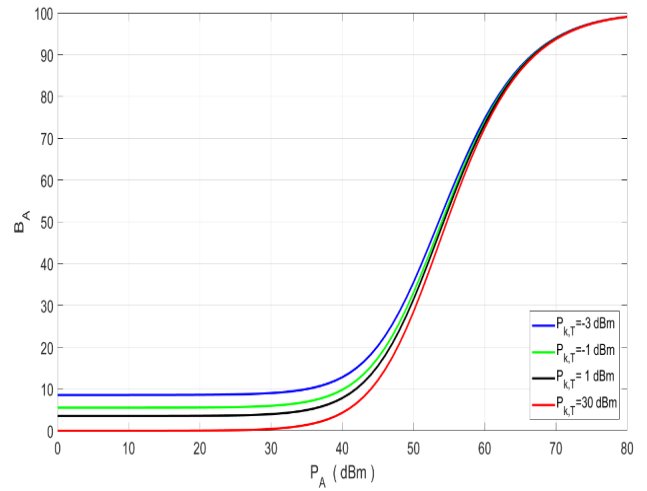


FIGURE 5. Average number of DoS bands B_A versus P_A for different values of $P_{k,T}$ (dBm).

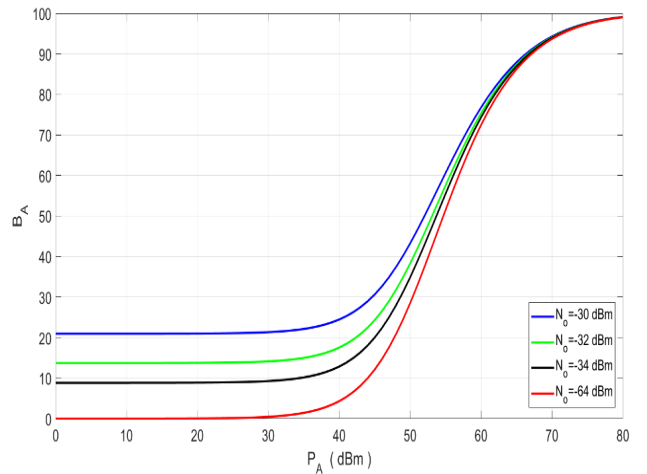


FIGURE 6. Average number of DoS bands B_A versus P_A for different values of N_0 (dBm).

C. EQUAL-POWER VS OPTIMAL POWER ALLOCATION

The effect of the power allocation algorithm on the average number of DoS bands is shown in Fig.7. In particular, an adversary employs two strategies: optimal and equal - power allocation. In Fig.7, the parameters follow the same setup as that shown in Fig.4.

In the low P_A region, there is a slight difference between the two strategies. This is because to conduct a full-band DoS attack for a single band, the adversary needs to have approximately 5dB power, as shown in Figs.2 and 3. If there are U bands, the adversary may not have sufficient power to disturb all U bands in either strategy. As P_A increases, the difference between the two strategies becomes noticeable. Specifically, the terms $P_{k,T}$, $\sigma_{wk,p}^2$ and $\theta_{k,PU}$ do not vary in each band. However, the increase between the two strategies is around at most 3 DoS bands for the same P_A . This is because the optimal allocated power in each band is based on

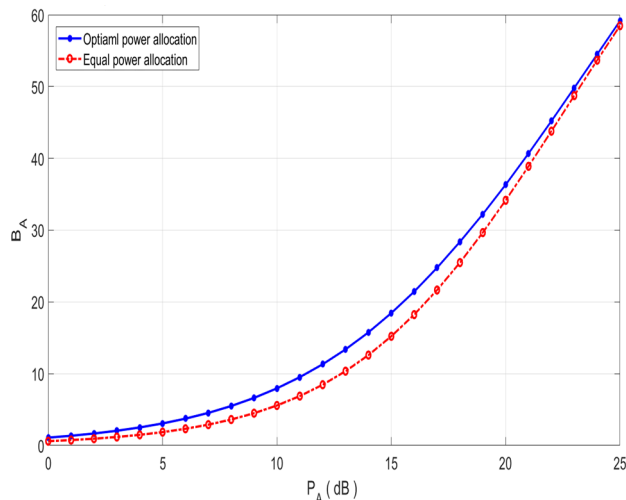


FIGURE 7. Average number of DoS bands B_A versus P_A (dB).

the values of $\beta_{k,A}$, a_k , b_k and σ_{wBS}^2 as expressed by (20). This implies that effective DoS attacks can be conducted when an adversary is aware of the environment. As P_A is further increased, both strategies shift from partial-band jamming to full-band jamming; hence, the curves match each other at a sufficiently high P_A . This illustrates that the adversary should increase the power budget, rather than attempt to learn the values of $\beta_{k,A}$, a_k , b_k and σ_{wBS}^2 . However, if the adversary increases the power, it is very likely that the BS will be able to detect these attacks.

V. CONCLUSION AND FUTURE WORK

In this study, we analyzed the optimal sharing link disruption of MC CR-NOMA under a constraint on the adversary’s power. The formulation of optimal sensing link disruption was achieved by maximizing the average number of DoS bands. In particular, for MC CR-NOMA, where the adversary launches pilot jamming attacks, the optimal strategy is derived and compared with equal-power allocations. We conclude key points from our analysis that 1) increasing the adversary’s power enables the adversary to cause a full-band DoS attack. 2) An increase in the targeted SINR, distance of PUs, or N_o , increase the chances of successful DoS attacks. 3) A decrease in the distance of the adversary or the transmitted power also increases the chance of a successful full DoS attack. 4) For the given system parameters ($d_{k,p}$, $d_{k,A}$, N_o , P_T , and θ_{PU}), B_A is proportional to the total adversary power and the optimal power strategy outperforms the equal-power strategy.

Future work will involve extending the problem of sharing disruption in CR-NOMA where the SUs and PUs locations are distributed randomly, and the adversary is aware of users’ locations probabilistically. Furthermore, we aim to explore various detection schemes and mitigation techniques to effectively counter these types of attacks.

APPENDIX A. AVERAGE PROBABILITY OF DoS

In this appendix, we evaluated the average probability of the DoS at the SU. From (14), we obtain

$$\begin{aligned} \bar{P}_k &= \mathbb{E}_{Y_k} \left\{ \mathbb{P}_{\text{Dos}}^{(k)} \right\} \\ &= \int_0^\infty \Pr \left\{ \underline{Y}_k < \theta_{PU} \eta_k \mid \underline{Y}_k = z_k \right\} f_{Y_k}(z_k) dz_k \\ &= \int_0^\infty \Pr \left\{ \underline{Y} < \frac{\theta_{PU} \eta_k}{1 - \sigma_{p,k}^2} \mid \underline{Y}_k = z_k \right\} f_{Y_k}(z_k) dz_k, \end{aligned} \tag{A.1}$$

where $\underline{Y} \sim \text{Exp}(1)$, as $|\hat{h}_{k,p}|^2 \sim \text{Exp}\left(\frac{1}{1 - \sigma_{p,k}^2}\right)$. From (6) if we substitute $\sigma_{p,k}^2 = \frac{(\sigma_{wBS}^2 + P_{k,A} \beta_{k,A} z_k)}{\beta_{k,p} + (\sigma_{wBS}^2 + P_{k,A} \beta_{k,A} z_k)}$, then the term $\frac{\eta_k}{(1 - \sigma_{p,k}^2)}$ can be simplified as follows:

$$\frac{\overbrace{z_k (P_{k,A} \rho_k + P_{k,A} \beta_{k,p})}^{A_1} + \overbrace{\beta_{k,p} \rho_k + \sigma_{wBS}^2 (\beta_{k,p} + \rho_k)}^{A_2}}{\beta_{k,p}^2}. \tag{A.2}$$

Now substitute (A.2) into (A.1), we have,

$$\begin{aligned} \bar{P}_k &= \int_0^\infty \Pr \left\{ \underline{Y} < \frac{\theta_{PU}}{\beta_{k,p}^2} [z_k A_1 + A_2] \mid \underline{Y}_k = z_k \right\} f_{Y_k}(z_k) dz_k \\ &= \int_0^\infty \left[1 - e^{-\left(\frac{\theta_{PU}}{\beta_{k,p}^2} [A_2 + z_k A_1]\right)} \right] \frac{1}{\beta_{k,A}} e^{-\frac{z_k}{\beta_{k,A}}} dz_k \\ &= 1 - \frac{e^{-\left(\frac{\theta_{PU}}{\beta_{k,p}^2} A_2\right)}}{\beta_{k,A}} \int_0^\infty e^{-z_k \left(\frac{\theta_{PU} A_1}{\beta_{k,p}^2} + \frac{1}{\beta_{k,A}}\right)} dz_k \\ &= 1 - \frac{\beta_{k,p}^2}{\theta_{PU} P_{k,A} \beta_{k,A} [\beta_{k,p} + \rho_k] + \beta_{k,p}^2} e^{-\left(\frac{\theta_{PU} A_2}{\beta_{k,p}^2}\right)}. \end{aligned} \tag{A.3}$$

APPENDIX B. SPECTRUM SHARING DISRUPTION OPTIMIZATION

Let $\vec{P}_A \triangleq [P_{1,A}, \dots, P_{U,A}]$ (i.e., the power in each of the U bands), and define the objective function to be, $f_0(\vec{P}_A) \sum_{k=1}^U \frac{q_k}{(a_k \beta_{k,A} f_k(\vec{P}_A) + 1)} - 1$, where $f_k(\vec{P}_A) = P_{k,A}$. Finally, let the constraint to be, $h(\vec{P}_A) \sum_{k=1}^U f_k(\vec{P}_A) - P_A$. Then,

$$P_{k,A}^* = \begin{cases} \frac{e^{-\frac{1}{2}(\sigma_w^2 \beta_{k,A} a_k + b_k)}}{\sqrt{a_k \beta_{k,A} v^*}} - \frac{1}{a_k \beta_{k,A}}, & \text{if } \frac{v^*}{a_k \beta_{k,A}} < e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)} \\ 0, & \text{if } \frac{v^*}{a_k \beta_{k,A}} \geq e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)} \end{cases} \quad (\text{B.9})$$

we can rewrite the optimization problem of (17) as,

$$\begin{aligned} \min_{P_{1,A}, \dots, P_{U,A}} & f_0(\vec{P}_A), \\ \text{s.t.} & -f_k(\vec{P}_A) \leq 0, \quad \forall k \in \{1, \dots, U\}, \\ & h(\vec{P}_A) = \sum_{k=1}^U P_{k,A} - P_A = 0. \end{aligned} \quad (\text{B.1})$$

The Lagrangian associated with (B.1) is given by

$$L(\vec{P}_A, \vec{\lambda}, v) = f_0(\vec{P}_A) - \sum_{k=1}^U \lambda_k f_k(\vec{P}_A) + v h(\vec{P}_A), \quad (\text{B.2})$$

where $\vec{\lambda} = [\lambda_1 \lambda_2 \dots \lambda_U] \in R^U$ and $v \in R$ are Lagrangian multipliers. Let \vec{P}_A^* , $\vec{\lambda}^*$ and v^* be the optimal sets of points. The KKT conditions are as follows [27].

$$\vec{P}_A^* \succcurlyeq 0 \text{ and } \sum_{k=1}^U P_{k,A}^* = P_A, \quad (\text{B.3})$$

$$\lambda_k^* \geq 0, \quad \forall k \in \{1, \dots, U\}, \quad (\text{B.4})$$

$$\lambda_k^* P_{k,A}^* = 0, \quad \forall k \in \{1, \dots, U\}, \quad (\text{B.5})$$

$$\frac{-a_k \beta_{k,A} a_k q_k}{(a_k \beta_{k,A} P_{k,A}^* + 1)^2} - \lambda_k^* + v^* = 0, \quad \forall k \in \{1, \dots, U\}. \quad (\text{B.6})$$

From (B.6), we see that if $v^* - \frac{(a_k \beta_{k,A}) e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)}}{(a_k \beta_{k,A} P_{k,A}^* + 1)^2}$, then $\lambda_k^* = 0$. Thus, relations (B.4) and (B.5) are as follows:

$$v^* \geq \frac{a_k \beta_{k,A} e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)}}{(a_k \beta_{k,A} P_{k,A}^* + 1)^2}, \quad (\text{B.7})$$

$$\left(v^* - \frac{a_k \beta_{k,A} e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)}}{(a_k \beta_{k,A} P_{k,A}^* + 1)^2} \right) P_{k,A}^* = 0, \quad (\text{B.8})$$

where $k \in \{1, \dots, U\}$. For some values of k , from (B.7), we can state that $P_{k,A}^*$ has a positive root if and only if $v^* < a_k \beta_{k,A} e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)}$. This implies that when $v^* \geq a_k \beta_{k,A} e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)}$, then $P_{k,A}^* = 0$. Combining these arguments, we need to fulfill the complementary slackness condition of (B.8). Hence, we have (B.9), as shown at the top of the page.

The term v^* is determined from (B.3), and is given by

$$\sum_{k=1}^U \max \left(0, \left(\frac{e^{-\frac{1}{2}(\sigma_w^2 \beta_{k,A} a_k + b_k)}}{\sqrt{a_k \beta_{k,A} v^*}} - \frac{1}{a_k \beta_{k,A}} \right) \right) = P_A. \quad (\text{B.10})$$

From (16), we can say that $e^{-(\sigma_w^2 \beta_{k,A} a_k + b_k)} = 1 - P_{DoS}^{(k)}(0)$, from which we can rewrite (B.10) as follows:

$$P_{k,A}^* = \begin{cases} \sqrt{\frac{1 - P_{DoS}^{(k)}(0)}{a_k \beta_{k,A} v^*}} - \frac{1}{a_k \beta_{k,A}}, & P_{DoS}^{(k)}(0) < 1 - \frac{v^*}{a_k \beta_{k,A}} \\ 0, & P_{DoS}^{(k)}(0) \geq 1 - \frac{v^*}{a_k \beta_{k,A}} \end{cases} \quad (\text{B.11})$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments, which helped to improve the manuscript. Turki Alkhamees would like to thank Imam Mohammad Ibn Saud Islamic University for their support during his doctoral study.

REFERENCES

- [1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017, doi: 10.1109/JSAC.2017.2725519.
- [2] Y. Liu, Z. Qin, M. El-kashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017, doi: 10.1109/JPROC.2017.2768666.
- [3] M. Vaezi, G. A. A. Baduge, Y. Liu, A. Arafa, F. Fang, and Z. Ding, "Interplay between NOMA and other emerging technologies: A survey," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 900–919, Dec. 2019, doi: 10.1109/TCCN.2019.2933835.
- [4] L. Lv, J. Chen, Q. Ni, Z. Ding, and H. Jiang, "Cognitive non-orthogonal multiple access with cooperative relaying: A new wireless frontier for 5G spectrum sharing," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 188–195, Apr. 2018, doi: 10.1109/MCOM.2018.1700687.
- [5] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 100–108, Apr. 2018, doi: 10.1109/MWC.2018.1700113.
- [6] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G downlink multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016, doi: 10.1109/TVT.2015.2480766.
- [7] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4438–4454, Jun. 2016, doi: 10.1109/TWC.2016.2542066.
- [8] 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. Sel. Areas Commun.*, vol. 35, no. 12, pp. 2744–2757, Dec. 2017, doi: 10.1109/JSAC.2017.2725618.

- [9] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 654–667, Feb. 2016, doi: [10.1109/TCOMM.2015.2511078](https://doi.org/10.1109/TCOMM.2015.2511078).
- [10] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019, doi: [10.1109/JIOT.2019.2927379](https://doi.org/10.1109/JIOT.2019.2927379).
- [11] C. Shahrar, M. L. Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart., 2015, doi: [10.1109/COMST.2014.2349883](https://doi.org/10.1109/COMST.2014.2349883).
- [12] R. Miller and W. Trappe, "On the vulnerabilities of CSI in MIMO wireless communication systems," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1386–1398, Aug. 2012, doi: [10.1109/TMC.2011.156](https://doi.org/10.1109/TMC.2011.156).
- [13] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012, doi: [10.1109/TWC.2012.020712.111298](https://doi.org/10.1109/TWC.2012.020712.111298).
- [14] B. Akgun, M. Krunz, and O. Ozan Koyluoglu, "Vulnerabilities of massive MIMO systems to pilot contamination attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1251–1263, May 2019, doi: [10.1109/TIFS.2018.2876750](https://doi.org/10.1109/TIFS.2018.2876750).
- [15] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018, doi: [10.1109/TWC.2018.2859949](https://doi.org/10.1109/TWC.2018.2859949).
- [16] H.-M. Wang and S.-D. Wang, "Cooperative pilot spoofing in MU-MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1956–1960, Nov. 2020, doi: [10.1109/LWC.2020.3009370](https://doi.org/10.1109/LWC.2020.3009370).
- [17] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. 3rd Int. Conf. Cognit. Radio Oriented Wireless Netw. Commun. (CrownCom)*, Singapore, May 2008, pp. 1–8, doi: [10.1109/CROWNCOM.2008.4562534](https://doi.org/10.1109/CROWNCOM.2008.4562534).
- [18] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5, doi: [10.1109/ICC.2011.5962467](https://doi.org/10.1109/ICC.2011.5962467).
- [19] X. Zhou, D. Niyato, and A. Hjørungnes, "Optimizing training-based transmission against smart jamming," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 2644–2655, Jul. 2011, doi: [10.1109/TVT.2011.2151890](https://doi.org/10.1109/TVT.2011.2151890).
- [20] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 20–23, Feb. 2016, doi: [10.1109/LWC.2015.2487960](https://doi.org/10.1109/LWC.2015.2487960).
- [21] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1363–1378, 2020, doi: [10.1109/TIFS.2019.2939742](https://doi.org/10.1109/TIFS.2019.2939742).
- [22] N. Nandan, S. Majhi, and H.-C. Wu, "Beamforming and power optimization for physical layer security of MIMO-NOMA based CRN over imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5990–6001, Jun. 2021, doi: [10.1109/TVT.2021.3079136](https://doi.org/10.1109/TVT.2021.3079136).
- [23] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022, doi: [10.1109/COMST.2022.3159185](https://doi.org/10.1109/COMST.2022.3159185).
- [24] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
- [25] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001, doi: [10.1109/18.959289](https://doi.org/10.1109/18.959289).
- [26] Z. Ding, F. Adachi, and H. V. Poor, "The application of MIMO to non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 537–552, Jan. 2016, doi: [10.1109/TWC.2015.2475746](https://doi.org/10.1109/TWC.2015.2475746).
- [27] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



TURKI Y. ALKHAMEES (Student Member, IEEE) received the B.S. degree in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2014, and the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 2018. He is currently pursuing the Ph.D. degree in electrical engineering with the University of California at San Diego. His research interests include wireless communications under hostile jamming attacks, cognitive radio networks (CRN), non-orthogonal multiple access (NOMA), and radio resource management.



LAURENCE B. MILSTEIN (Life Fellow, IEEE) received the B.E.E. degree in electrical engineering from The City College of New York, New York City, NY, USA, in 1964, and the M.S. and Ph.D. degrees in electrical engineering from the Polytechnic Institute of Brooklyn, Brooklyn, NY, USA, in 1966 and 1968, respectively. From 1968 to 1974, he was with the Space and Communications Group, Hughes Aircraft Company, and from 1974 to 1976, he was a member of the Department of Electrical and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, USA. Since 1976, he has been with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA, USA, where he is currently a Distinguished Professor, the Holder of the Ericsson Chair of Wireless Communications Access Techniques, and a former Department Chairperson, working in the area of digital communication theory with a special emphasis on spread-spectrum communication systems. He has also been a consultant to both government and industry in the areas of radar and communications.

He has been a member of the Board of Governors of the IEEE Communications Society and the IEEE Information Theory Society and was the Vice-President of Technical Affairs of the IEEE Communications Society, in 1990 and 1991. He was the former Chair of the IEEE Fellows Selection Committee and was a recipient of the 1998 Military Communications Conference Long Term Technical Achievement Award, the Academic Senate 1999 UCSD Distinguished Teaching Award, the IEEE Third Millennium Medal, in 2000, the 2000 IEEE Communications Society Armstrong Technical Achievement Award, and various prize paper awards. He was also a recipient of the IEEE Communications Theory Technical Committee (CTTC) Service Award, in 2009, the CTTC Achievement Award, in 2012, and the 2015 UCSD Chancellor's Associates Award for Excellence in Graduate Teaching. He was an Associate Editor of *Communication Theory* for IEEE TRANSACTIONS ON COMMUNICATIONS, an Associate Editor of *Book Reviews* for IEEE TRANSACTIONS ON INFORMATION THEORY, an Associate Technical Editor of *IEEE Communications Magazine*, and the Editor-in-Chief of IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

• • •