IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 July 2023, accepted 3 August 2023, date of publication 10 August 2023, date of current version 17 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3304244

RESEARCH ARTICLE

A Different Approach for Sensing Disruption

TURKI Y. ALKHAMEES[1,2], (Student Member, IEEE), AND LAURENCE B. MILSTEIN[1], (Life Fellow, IEEE)

[1]Department of Electrical and Computer Engineering (ECE), University of California at San Diego, La Jolla, CA 92037, USA
[2]Electrical 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 sensing vulnerabilities in cognitive radio networks can significantly degrade performance. Most disruption attacks in the current literature involve spoofing of the free bands used for sensing by making them appear busy. In this study, we proposed a different approach for sensing disruptions. We examined the optimal strategy for an intelligent adversary with a given power to flip busy bands and make them appear free. The mechanism of sensing disruption was established by contaminating the noise power measurements. This is illustrated by a two-step sensing scheme in which energy detection, in conjunction with noise power estimation, is used by secondary users. We show that to flip busy bands, the optimal strategy for sensing link disruptions is equal-power, and partial-band flipping. We demonstrated that the maximum average number of missed detections can be derived under a constraint on power of the adversary. Through analytical and numerical results, we demonstrated the effectiveness of our approach in terms of the impact of disruption attacks on spectrum sensing.

INDEX TERMS Cognitive radio, sensing disruption, intelligent adversary, partial-band jamming, full-band jamming, noise power estimation.

I. INTRODUCTION

As is well known, cognitive radio networks (CRNs) are technologies to address the challenge of efficiently utilizing the spectrum [1]. It allows unlicensed secondary users (SUs) to utilize the spectrum without causing excessive interference to licensed primary users (PUs) [1], [2]. To accomplish this, SUs typically perform Spectrum Sensing (SS), to detect the presence of PUs. Many detection schemes have been studied to sense the band of interest, such as energy detection (ED), matched filter detection and cyclostationary detection [3], [4]. The ED is commonly used because of its simplicity of implementation [1], [3], [4]. However, one of the limitations of the ED is its unknown noise power level [1], [3], [5]. Therefore, the combination of ED and the estimated noise power has been extensively studied [6], [7], [8]. In [6] and [8], noise-only samples were obtained from an outdated (i.e., previous) sensing duration and the noise power was estimated. This is referred to as the estimated noise power (ENP) stage. Reference [8] is for a cooperative spectrum sensing scenario, whereas Reference [6] is for an individual spectrum sensing case. Another way to obtain noise-only samples is through a training phase, as proposed in [7], where the performance achieved is near-optimal. In general, limitations of detection schemes can be exploited by adversaries to disrupt the SS. This underscores the critical importance of developing strategies to effectively examine these malicious activities.

The associate editor coordinating the review of this manuscript and approving it for publication was Ding Xu.

A. BACKGROUND AND RELATED WORKS

The use of SS presents a new opportunity for an adversary to attack CRNs [9], [10], [11]. The types of attacks in sensing disruption can be spectrum sensing data falsification (SSDF) or Primary User Emulation (PUE). First, in SSDF attacks, the adversary acts as the SU, sending a malicious mimic signal to mislead the global decisions. Typically, an adversary conducts SSDF attacks with the objectives of vandalism, exploitation, or both [12]. The objective of vandalism is to increase fake reports about busy bands to the Fusion Center (FC). However, the exploitation objective is to increase false reports regarding the free bands in the FC [9].

The second class is PUE attacks. In this case, the adversary attacks during the SU sensing slot, which is referred to as ''sensing disruption,'' and it is the focus of this study.

In [13], the feasibility of PUE attacks in CR was analyzed, whereas [14] considered the impact of PUE on CRN performance. One example of a PUE attack is spoofing, in which an adversary sends a Gaussian signal to the free bands. The goal is to launch an optimal sensing disruption with a given power, to provide the worst-case performance for SS systems. In [15] an optimal spoofing strategy under additive white Gaussian noise with a power-limited adversary was derived, which was later extended in [16] to different fading channels. The authors of [17] propose a framework for disrupting spectrum sensing by a power-limited adversary that considers uncertainties in the adversary's estimates. The common goal of sensing disruption discussed in [15], [16], and [17] only includes spoofing free bands. Another example of a PUE attack is presented in [18], which is modeled as a zero-sum game between the adversary and the SU, with the assumption that the players know the availability probabilities Nevertheless, detailed information about the countermeasures against SSDF and PUE attacks can be found in [9], [10], and [11].

B. MOTIVATION AND CONTRIBUTION

The primary focus of this paper is to investigate the sensing disruption caused by a power-limited adversary. Power-limited adversaries are relevant to various applications, such as unmanned aircraft, wireless sensor networks, vehicular networks, and Cognitive Internet-of-Things (CIoT). The implications of sensing disruption go beyond academic interests, as they can pose threats and danger to the general public, such as terrorism, vandalism, and other intentional crimes.

Another motivation is to concentrate on an intelligent adversary targeting busy bands and flipping them so that they appear to be free. Despite their significance, these flipping attacks have received limited attention in the existing literature, which primarily focuses on sensing disruptions of free bands to make them seem busy to the SUs (i.e., spoofing attacks). Flipping attacks pose significant harm to CRNs [2] in two ways. These malicious attacks may cause interference between SUs and PUs, contradicting the core principle of CRNs. Additionally, these attacks can result in the incorrect classification of the bands, leading to reduced network performance and potential system failure. To the best of our knowledge, the problem of optimally flipping busy bands with a given total power remains unresolved. In fact, the authors of [10] highlighted the need for further investigation of this type of attack.

The contribution of this paper is summarized below:

- First, we propose a framework that addresses the problem of spectrum sensing vulnerability by contaminating the noise power measurements at the SUs. This contamination reduces the measurement accuracy, resulting in missed detections of busy bands at SUs.
- Next, we employ a two-step sensing model in the presence of an adversary. In this model, we show the analytical probability of missed detections for ED-ENP. The proposed approach models the transmitted signal generated by an adversary as a complex Gaussian random process.
- Finally, we demonstrate that the optimal strategy for an adversary to disrupt spectrum sensing is equal-power allocation, which maximizes the average number of missed detections. This strategy represents the worst-case scenario for the two-step sensing scheme.

C. STRUCTURE

The outline of the paper is as follows: Section II presents the system model and general formulation. The optimal strategy for flipping busy bands is described in Section III. The numerical results are presented in Section IV, and Section V concludes this paper.

II. SYSTEM MODEL AND GENERAL FORMULATION

We examine the impact of an adversary on a CRN where there are at least U SUs that adopt an energy detector in conjunction with the estimated noise power (ED-ENP). Note that the adversary intends to disrupt the sensing slot. We set the spectral range of interest to consist of U bands. The decision to consider the U bands as the same number of SUs aims to achieve a worst-case analysis.

The U bands can be divided into PUs and SUs. Furthermore, SUs have two sets of bands: a set of sensed-free bands (B_{free}) and a set of sensed-busy bands (B_{busy}). It is well known that ED is the simplest detection scheme; however, it is necessary to estimate the noise power level accurately [1], [3], [5], [6]. In [6], a two-step detection scheme was implemented, and the noise power level was estimated. This scheme uses a sophisticated detector to determine whether the PU is present; whenever the PU is not sensed to be present, the scheme estimates the noise power level. However, this approach motivates an intelligent adversary to contaminate (i.e., jam) these noise estimates, potentially disrupting the performance of the CRN.

In Section II-A, we discuss the two-step sensing protocol presented in [6]. The performance of an energy detector with estimated noise power when an adversary is present is evaluated in Section II-B. The assumptions regarding the knowledge available to an intelligent adversary and the framework of the attacks are presented in Section II-C.

A. TWO-STEP SENSING

The two-step sensing procedure is proposed in the IEEE 802.22 [19] and ECMA 392 [20] standards, which use sporadic long sensing periods (SPs) for fine sensing, and more frequent short SPs for fast sensing, as illustrated in Fig.1. A detailed description of the two-step detection scheme is shown in Fig.2, where a high-precision detection algorithm such as a feature detector is employed in the fine-SP mode. If a given band is sensed as being free during the fine-SP mode, the noise power level is estimated. These bands are denoted as B_{ENP}. A simple radiometer was implemented in the fast-SP mode. Therefore, the bands that are sensed as free

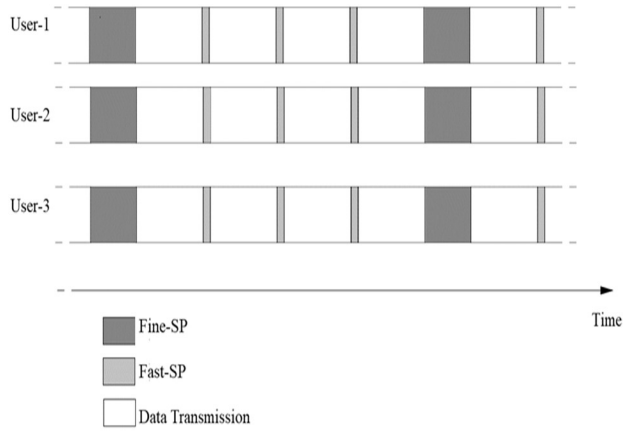

FIGURE 1. The proposed Two step sensing in the IEEE 802.22 scheduling mechanism [19].

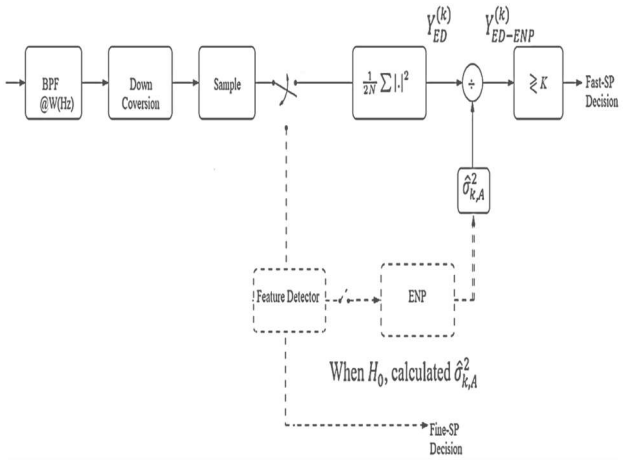

FIGURE 2. Two-step Detection scheme of the k^{th} SU that is proposed in [6].

can be expressed as $B_{free} = B_{ENP} \cup B_{fast}$, where B_{fast} is the set of sensed-free bands in the fast-SP mode.

Based on [19] and [20], the SUs in the network are either in fine-SP mode or fast-SP mode. The rationale behind this was to avoid measurements of overlapping for the SUs. Note that various key parameters of the system, such as sensing schedule and type of sensing, are publicly known [19], [20]. Therefore, an adversary can be aware of this sensing mechanism and use this information to degrade the performance of the CRN.

B. PERFORMANCE OF AN ENERGY DETECTOR WITH ESTIMATED NOISE POWER (ED-ENP)

The detection of a signal in an AWGN channel was investigated in [21]. The energy of the received waveform at the k^{th} band (i.e., the k^{th} SU), $r_k(t)$, was measured over the bandwidth W and approximated as follows:

$$\frac{2}{N_0}\int_0^T [r_k(t)]^2\,dt \approx \frac{1}{\sigma^2_{k,n}}\sum_{i=1}^{N}\left|y_i^{(k)}\right|^2 = Y_{ED}^{(k)}, \qquad (1)$$

where N_0 is the one-sided noise PSD and $\sigma^2_{k,n} = N_0 W$. The summation in (1) from [21] was approximated as a Gaussian statistic; therefore, we have the following detection problem:

$$\begin{aligned} H_0: &\quad y_i^{(k)} = n_i^{(k)} \\ H_1: &\quad y_i^{(k)} = x_i^{(k)} + n_i^{(k)}, \end{aligned} \qquad (2)$$

where $x_i^{(k)}$ is the i-th signal sample, the noise samples $n_i^{(k)} \sim C\mathcal{N}(0, 2\sigma^2_{k,SS})$ are i.i.d., and H_0 and H_1 are the "signal absent" and "signal present" hypotheses, respectively. The ED test statistic, $Y_{ED}^{(k)}$, has either a central chi-square (χ^2) probability density function (PDF) with $2N$ degrees of freedom (DOF) or a noncentral χ^2 PDF with $2N$ DOF [21]. For a given desired probability of a false alarm, denoted as p_{FA}^{DES}, threshold K was set based on the Neyman-Pearson criterion. This is only possible if the noise power is known [1], [3], [4]. If the SU estimates the noise power, the presence of an intelligent adversary can contaminate the estimate. Therefore, the test statistic of ED-ENP for the k^{th} SU can be derived by modifying the result of [6], to include the presence of an intelligent adversary, as shown below:

$$\begin{aligned} Y_{ED-ENP}^{(k)} &= \frac{1}{\hat{\sigma}^2_{k,A}}\left(\frac{1}{2N}\right)\sum_{i=1}^{N}\left|y_i^{(k)}\right|^2 K \\ &= \frac{Y_{ED}^{(k)}}{\hat{\sigma}^2_{k,A}} = \frac{\left(\frac{1}{2N}\right)\sum_{i=1}^{N}\left|y_i^{(k)}\right|^2}{\frac{1}{2M}\sum_{i=1}^{M}\left|n_{-i}^{(k)} + \alpha_k j_{-i}^{(k)}\right|^2} K, \end{aligned} \qquad (3)$$

where $M = WT_{fine}$ is the number of samples in the fine-SP mode, and $N = WT_{fast}$ is the number of samples in the fast-SP mode, T_{fine} is the fine-SP time interval, and T_{fast} is the fast-SP time interval. Also note that the term $\hat{\sigma}^2_{k,A}$ in (3) is a maximum likelihood estimate (MLE) of the noise power. For simplicity, we assume that the samples y_i for $i < 0$, are those in which the SUs estimate the noise power. In this way, y_{-i} is described as an outdated sample, where ideally it contains only the "noisy sample" (i.e., the noise and adversary samples only), and is given by, $n_{-i} + \sqrt{\alpha_k} j_{-i}$, for $i = \{1, .., M\}$. The thermal noise after the bandpass filter is modeled as zero-mean complex additive Gaussian noise at the k^{th} band (i.e., $\sim C\mathcal{N}\left(0, 2\sigma^2_{k,n}\right)$). The adversary and the noise signals are assumed to be independent of each other. In addition, the adversary signal after the bandpass filter is distributed as $\sim C\mathcal{N}\left(0, 2\alpha_k P_{k,A}\right)$, and is transmitted to the k^{th} allowable (i.e., free) band during the fine-SP mode, where α_k is the path loss factor between the intelligent adversary and the k^{th} SU. Also, note that the term $P_{k,A}$ is the power of the adversary signal in the k^{th} band. We assume that the path loss factor, α_k, is constant across all bands (i.e., $\alpha_k = \alpha$) and is assumed to be known to the adversary. This assumption is common in the literature on CRN attacks and examples can be found in [9] and [11]. It can be shown that for a long observation interval, $\hat{\sigma}^2_{k,A} \sim \chi^2$ with $2M$ DOF and a scale parameter equal to $\sigma^2_{k,ENP}$ [22].

One of the popular models used in the literature [1], [3], [6], assumes that the PU signal is a Gaussian signal, with a PDF

of $\sim \mathcal{CN}(0, 2S_k)$, where $2S_k$ is the power of the PU signal on the k^{th} band and the signal-to-noise-ratio (SNR) is denoted by $\gamma_k \triangleq S/\sigma^2_{k,SS}$ of the PU in the k^{th} band.

Because both $\hat{\sigma}^2_{k,A}$ and $Y^{(k)}_{ED}$ have a central chi-square distribution, the ratio of these two distributions in (3), with proper scaling, is a central $\mathcal{F}$-distribution [6], [23], [24]. Therefore, the false alarm probability of ED-ENP, $p^{(k)}_{FA,ED-ENP}$, and the detection probability of ED-ENP, $p^{(k)}_{D,ED-ENP}$, can be expressed as regularized incomplete beta functions as shown below [25]:

$$\begin{aligned} p^{(k)}_{FA,ED-ENP} &= Pr\left\{Y^{(k)}_{ED-ENP} > K|H_0\right\} \\ &= \tilde{B}\left(M, N, \frac{1}{Kw+1}\right), \end{aligned} \tag{4}$$

$$\begin{aligned} p^{(k)}_{D,ED-ENP} &= Pr\left\{Y^{(k)}_{ED-ENP} > K|H_1\right\} \\ &= \tilde{B}\left(M, N, \frac{1}{K\left(\frac{w}{(1+\gamma)}\right)+1}\right), \end{aligned} \tag{5}$$

where $\tilde{B}(u, v, z) = \frac{1}{B(u,v)}\int_0^z x^{u-1}(1-x)^{v-1}\,dx$, $B(u, v)$ is defined as the beta function $B(u, v) = \Gamma(u)\,\Gamma(v)/\Gamma(u+v)$, and $w(N/M)\left(\sigma^2_{k,ENP}/\sigma^2_{k,SS}\right)$. For large N and M, the probabilities $p^{(k)}_{FA,ED-ENP}$ in (4) and $p^{(k)}_{D,ED-ENP}$ in (5) can be expressed using a Gaussian approximation as follows [25]:

$$\begin{aligned} p^{(k)}_{FA,ED-ENP} &\approx Q\left(\frac{K - \frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}\sqrt{\frac{M+N}{MN}}}\right) \\ &= Q\left(\frac{K}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right), \end{aligned} \tag{6}$$

$$\begin{aligned} p^{(k)}_{D,ED-ENP} &\approx Q\left(\frac{K - \frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}(1+\gamma)}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}(1+\gamma)\sqrt{\frac{M+N}{MN}}}\right) \\ &= \mathrm{Q}\left(\frac{K}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}(1+\gamma)\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right). \end{aligned} \tag{7}$$

It is challenging to design a detector if the PU signal has an unknown deterministic waveform. However, the probability of detection can be approximated as in (7) if the PU SNR is in the low-SNR regime (for more details, see [6]). Note that the false alarm probability is similar to that of detecting a Gaussian signal because no PU is present. Therefore, for the remainder of this paper, we consider only the case of a PU signal as a complex Gaussian waveform.

Note that the noise power of the k^{th} SU during the fine-SP mode is equal to $\sigma^2_{k,ENP} = \sigma^2_{k,n}\left(1 + \alpha_k P_{k,A}/\sigma^2_{k,n}\right)$, whereas the noise power during the fast-SP mode is $\sigma^2_{k,SS} = \sigma^2_{k,n}$. If there are no attacks (i.e., $P_{k,A} = 0$), then $\sigma^2_{k,ENP} = \sigma^2_{k,n}$.

However, a perfect estimate of noise power is impossible in two-step sensing (i.e., $\sigma^2_{k,ENP} \neq \sigma^2_{k,n}$) [1], [5], [6]. This implies that there is some residual error when estimating $\hat{\sigma}^2_{k,A}$. In [5], the approach used is a more practical model; that is, the noise process is assumed to be Gaussian, but the variance is off by some factor. As in [5], we can model the same approach for two-step sensing because $Y^{(k)}_{ED-ENP}$ is also approximately a Gaussian random variable, and we can say that the ratio $\sigma^2_{k,SS}/\sigma^2_{k,ENP}$ can be bounded, as $\sigma^2_{k,SS}/\sigma^2_{k,ENP} \in [1/\rho_k, \rho_k]$, for any positive value of ρ_k, where ρ_k is a parameter that quantifies the size of the residual error value of the ratio between $\sigma^2_{k,SS}$ and $\sigma^2_{k,ENP}$. When $\rho_k = 1$, robust detection can be achieved. For $\rho_k \neq 1$, the robustness of detection cannot be achieved at SUs [1], [2], [5], [6] in a low SNR regime. Therefore, a noise uncertainty problem may arise in the detection scheme. Even if the SU observes an infinite number of samples, the robustness of the detection cannot be guaranteed because of a phenomenon known as the SNR wall [5]. The SNR wall is defined as the minimum value of the SNR at which it is impossible to detect values below it, even when the number of observed samples approaches infinity.

For simplicity, we assume that the actual noise variance is identical across all bands, that is $\sigma^2_{k,n} = \sigma^2_n$. Therefore, the residual error is also the same across all the bands, which means $\rho_k = \rho$. In addition, the SNR of the PUs is assumed to be the same across all the bands so that $\gamma_k = \gamma$. All of these assumptions lead to a more tractable solution.

Note that even in the absence of an adversary, there will be missed detections of the busy bands owing to the residual error from estimating the noise power, the probability of which is $\Phi p_{MD} = 1 - \min_{\sigma^2_{k,ss}/\sigma^2_{k,ENP} \in [1/\rho, \rho]} p^{(k)}_{D,ED-ENP} = 1 - Q\left(\frac{K-(1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right) = \left(\frac{K-(1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right)$, where $\Phi(\cdot)$ is the cumulative distribution function of the standard normal distribution. For the remainder of this study, we express $\Phi p_{MD} = \left(\frac{K-(1+\gamma)/\rho}{(1+\gamma)/\rho\sqrt{\frac{M+N}{MN}}}\right)$.

C. FRAMEWORK FOR FLIPPING ATTACKS

We assume that the intelligent adversary knows the receiver structure, type of standard, sensing time, desired probability of false alarm of the SUs, p^{DES}_{FA}, and status of the U bands. Additionally, to ensure the adversary's goal of flipping as many bands as possible, we assume that all the U bands are ENP bands. ENP bands refer to the available free bands during the fine-SP mode. These U bands should be the same in number as the SUs, as seen in [15], [16], and [26]. The adversary cannot precisely estimate/learn all of the aforementioned information that is assumed above. However, it is commonly assumed in the literature [15], [16], [17], [18], [26] that the adversary has full knowledge of at least some information.

Therefore, the results of this study present a worst-case analysis and provide an upper bound for the SS disruption.

Note that the number of missed detections of busy bands is equivalent to the number of flipped bands. This occurs because a missed detection happens when the PU signal is not detected, which can be caused by inaccurate noise power estimation. When the adversary contaminates the estimated noise power, the band is flipped, resulting in it no longer being considered busy by the PU. Our main focus is on determining the average number of missed detections, denoted by B_f.

Lemma 1: Let us now define q_k as the probability of missed detection in the k^{th} band. In addition, let $B = \{1, 2, 3, \ldots, U\}$ be the set of bands available for sensing, and initially assume that all of them are busy when the SUs sense them in fast-SP mode (i.e., $|B_{busy}| = U$). Then, B_f can be expressed as the sum of the individual missed detection probabilities for each band, as shown below in (8):

$$B_f = \sum_{k=1}^{U} q_k \tag{8}$$

Proof: Let $X_k (k = 1, 2, \ldots, U)$ be a binary random variable, such that $X_k = 1$ indicates that the k^{th} band is successfully flipped to be free, and $X_k = 0$ indicates that the attempt to flip the k^{th} band was unsuccessful (i.e., sensed to be busy). Therefore, the expected value of the sum of X_k over all k values was the average number of missed detections.

$$B_f = E\left\{\sum_{k=1}^{U} X_k\right\} = \sum_{k=1}^{U} E\{X_k\} = \sum_{k=1}^{U} q_k \tag{9}$$

■

The objective of the adversary in the flipping attacks with a total power P_A, is to maximize the average number of missed detections of the SUs during the fast-SP mode, subject to the adversary contaminating the ENP bands during the fine-SP mode. Hence, we have the following optimization problem:

$$\max_{p_{k,A} \forall k \in \{1,\ldots U\}} \sum_{k=1}^{U} q_k,$$
$$s.t\ P_{k,A} \geq 0, \forall k \in \{1, ..U\}, \sum_{k=1}^{U} P_{k,A} = P_A. \tag{10}$$

A defense strategy for SUs is to employ a more robust detector in the fine-SP mode. However, implementing this strategy comes at the cost of a longer sensing period, resulting in a reduced throughput.

III. FLIPPING OPTIMIZATION

In this section, we analyze the optimal strategy for sensing link disruption under the assumption that both the number of ENP bands and the number of busy bands equals U, the total number of bands. We then consider a more realistic case, in which the number of ENP bands differs from the number of busy bands.

A. OPTIMAL SENSING DISRUPTION FOR FLIPPING ATTACKS

As discussed earlier, from (7), we can directly determine that the flipping probability is equivalent to q_k, which can be shown to be

$$\begin{aligned} q_k &= 1 - p^{(k)}_{D,ED-ENP} \\ &= \Phi\left(\frac{K - \frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}(1+\gamma)}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}(1+\gamma)\sqrt{\frac{M+N}{MN}}}\right) \\ &= \Phi\left(\frac{K}{\frac{1}{\left(\frac{\alpha P_{k,A}}{\sigma^2_n}+\rho\right)}(1+\gamma)\sqrt{\frac{M+N}{MN}}} - \frac{1}{\sqrt{\frac{M+N}{MN}}}\right). \end{aligned} \tag{11}$$

The spoofing probability p_k, from (6), can be expressed as,

$$p_k = p^{(k)}_{FA,ED-ENP} = Q\left(\frac{K - \frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}}{\frac{\sigma^2_{k,SS}}{\sigma^2_{k,ENP}}\sqrt{\frac{M+N}{MN}}}\right). \tag{12}$$

From (12), the adversary should increase $\sigma^2_{k,SS}$ to spoof free bands. In other words, the adversary should jam during the SP-fast mode, similar to the techniques described in [15], [16], and [17]. It is evident that there exists a trade-off between spoofing and flipping attacks.

By substituting (11) into (10), we formulate the optimal sensing link disruption as follows:

$$\max_{p_{k,A} \forall k \in \{1,\ldots U\}} \sum_{k=1}^{U} \Phi\left(\frac{a}{\frac{1}{(P_{k,A}+\rho)}(1+\gamma)} + b\right),$$
$$s.t \quad P_{k,A} \geq 0, \forall k \in \{1, ..U\}, \sum_{k=1}^{U} P_{k,A} = P_A, \tag{13}$$

where $a \triangleq \frac{K}{\sqrt{\frac{M+N}{MN}}}$, and $b \triangleq \frac{-1}{\sqrt{\frac{M+N}{MN}}}$. The optimization problem in (13) is convex, because the objective and inequality constraints are both convex [27]. Using the Karush–Kuhn–Tucker (KKT) conditions, the optimal power flipping allocation of (12) yields the following solution:

$$P^*_{k,A} = \begin{cases} \frac{P_A}{u}, & k \in \varphi_A \\ 0, & otherwise \end{cases}, \tag{14}$$

where $\varphi_A \triangleq \left\{k | \lambda^*_k = 0, P^*_{k,A} > 0\right\}$ are the flipped bands caused by the adversary's flipping power, and λ^*_k is the Lagrangian multiplier. Note that u is the number of flipped bands (See Appendix A).

The technique described in (14) is known as uniform power allocation and is widely employed, as seen in previous works [14], [15], [16]. However, the key distinction lies in the result of the approach, which involves flipping the busy band, whereas the other techniques spoof the free bands. Additionally, in (14), from the adversary's point of view, equal flipping power allocation is optimal because the adversary is not aware of the system parameter values, in particular, a, b, γ, and ρ for each band.

B. OPTIMAL NUMBER OF FLIPPED BANDS

The optimal number of flips in (14) is unclear. To see this, let the value of the objective function given in (13) for the optimal solution given in (14) as a function of u be as follows:

$$f(u) = (U-u)\,\Phi\left(\frac{a\rho}{(1+\gamma)}+b\right) + u\Phi\left(\frac{a\left(\frac{\alpha P_A}{u\sigma_n^2}+\rho\right)}{(1+\gamma)}+b\right). \tag{15}$$

Then, the terms in (15) can be interpreted as the probability of a missed detection in each band, multiplied by the number of occurrences of each. This probability is enhanced by the inaccuracy of the noise power estimate and/or the presence of an adversary. We now replace u with the real continuous variable x (i.e., $x \in \mathbb{R}^+$). The extreme-value theorem in [28] states if $f(x)$ is continuous on a closed interval $[1, U]$, it must hit its maximum and minimum on that interval. To find the extreme point x^*, we solve $f'(x) = 0$. Thus, the optimal number of flipped bands u^*, is $\lfloor x^* \rfloor$ or $\lceil x^* \rceil$. The derivative of $f(x)$ is given by (16):

$$f'(x) = \Phi\left(\frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)\,x}+\frac{a\rho}{(1+\gamma)}+b\right) - p_{MD} - \frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)\,x\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(\alpha\frac{P_A}{\sigma_n^2}\right)}{(1+\gamma)x}+\frac{a\rho}{(1+\gamma)}+b\right)^2}. \tag{16}$$

Note that setting $f'(x) = 0$, results in a nonlinear equation, which means that the expression x^* cannot be derived directly. However, the result in Appendix B shows that $f'(x) > 0, for\ 0 \le x < \infty$ (i.e., $f(x)$ continuously increases as x increases for $x > 0$). In other words, when the number of flipped bands increases, the average number of missed detections also increases. Note that, while the adversary attacks the ENP bands during the fine-SP mode, the consequence of flipping busy bands is observed during the fast-SP mode. Previously, it was assumed that ENP and busy bands were the same as the total number of bands. Because this will not always be the case, we now evaluate the case in which $|B_{ENP}|$ and $|B_{busy}|$ are different. As a result, x^* is upper bounded by $|B_{ENP}|$ or $|B_{busy}|$, depending on which of them is smaller. This can be expressed as follows:

-When $|B_{ENP}| \ge |B_{busy}|$, then x^* is upper bounded by $|B_{busy}|$, because it is impossible to flip more than number of busy bands, regardless of how many bands the adversary attacks. If P_A is sufficiently large to contaminate all ENP bands (i.e., $P^*_{k,A} \le P_A/|B_{busy}|$), the optimal strategy is full-band flipping. That is, the flipping power is identically distributed and can be expressed as:

$$f(x^*)\big|_{x^*=|B_{busy}|} = |B_{busy}|\,\Phi\left(\frac{a\left(\frac{\alpha P_A}{|B_{busy}|}+\rho\right)}{1+\gamma}+b\right). \tag{17}$$

However, if the number of busy bands increase, the result is flipping a portion of the busy bands (i.e., partial-band flipping). This case can be mathematically expressed as follows:

$$f(x^*)\big|_{x^*<|B_{busy}|} = x^*\Phi\left(\frac{a\left(\frac{\alpha P_A}{\sigma_n^2 x^*}+\rho\right)}{1+\gamma}+b\right) + \left(|B_{busy}|-x^*\right)p_{MD}. \tag{18}$$

-When $|B_{ENP}| < |B_{busy}|$, the adversary's goal is to flip all busy bands, but this cannot be done because the adversary cannot contaminate more than the ENP bands. Thus, x^* cannot be greater than $|B_{ENP}|$, which shows that the attack strategy is partial-band flipping. From Appendix B, $f(x)$ continuously increases as x increases for $x \ge 0$; thus, the maximum of $f(x)$ is achieved when $x^* = |B_{ENP}|$, as shown below:

$$f(x) = |B_{ENP}|\,\Phi\left(\frac{a\left(\frac{\alpha P_A}{\sigma_n^2|B_{ENP}|}+\rho\right)}{(1+\gamma)}+b\right) + \left(|B_{busy}|-|B_{ENP}|\right)p_{MD}. \tag{19}$$

Based on the analysis provided, we can conclude that it is impossible for SUs to be flipped more than the number of busy bands, whereas the adversary cannot contaminate more than the number of ENP bands. Therefore, the maximum average number of missed detections B_f, is given by

$$B_f = u^*\Phi\left(\frac{a\left(\frac{(\alpha P_A/\sigma_n^2)}{u^*}+\rho\right)}{(1+\gamma)}+b\right) + \left(|B_{busy}|-u^*\right)p_{MD}. \tag{20}$$

Overall, the ratio $\frac{(\alpha P_A/\sigma_n^2)}{u^*}$ in (20) plays an important role in the optimal strategy for sensing link disruption. Furthermore, with sufficiently large adversary power, full-band flipping is optimal, as long as $|B_{ENP}| \ge |B_{busy}|$. Otherwise, the partial-band flipping is optimal.

C. AVERAGE NUMBER OF MISSED DETECTIONS DUE TO THE PRESENCE OF THE ADVERSARY

In the absence of an adversary (i.e., $u^* = 0$), the average number of missed detections in (20), caused by the residual error from estimating the noise power, is equals to $|B_{busy}|\,p_{MD}$. To demonstrate the effect of flipping attacks dominated by the adversary, we define the average number of missed detections primarily because of the presence of the adversary as

$$\Delta B_f = B_f - |B_{busy}|\,p_{MD}. \tag{21}$$

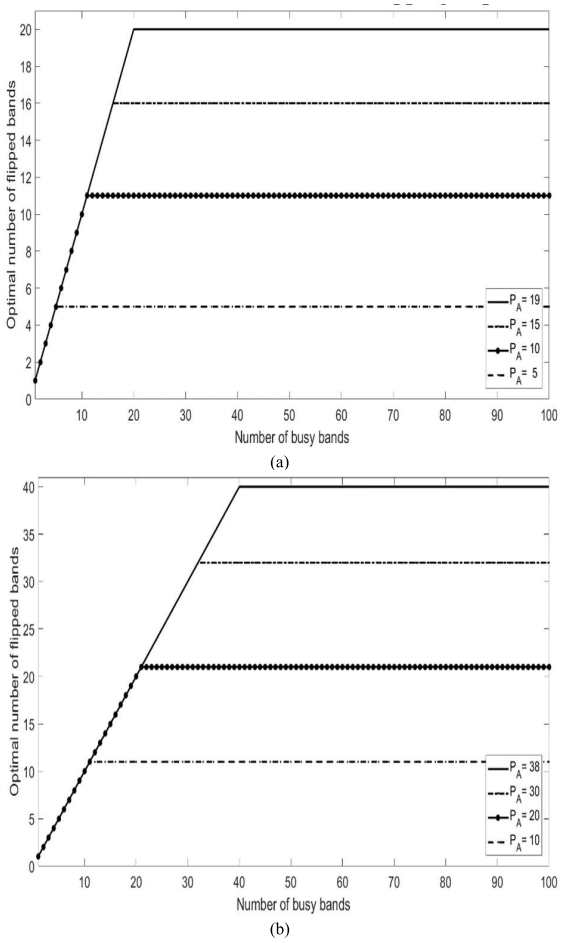

FIGURE 3. Optimal number of flipped bands u^* versus the number of busy bands $|B_{busy}|$: $|B_{ENP}| = 20$. (b) $|B_{ENP}| = 40$.

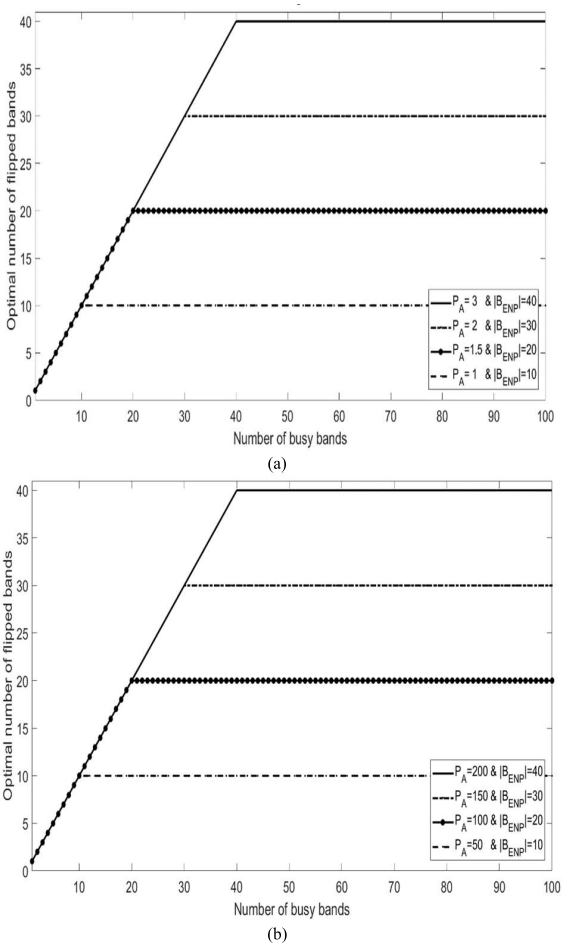

FIGURE 4. Optimal number of flipped bands u^* versus the number of busy bands $|B_{busy}|$: (a) $\gamma = -3dB$. (b) $\gamma = 3dB$.

When we substitute B_f in (20) into (21), we have

$$\Delta B_f = u^* \left(\Phi \left(\frac{a\left(\frac{P_A}{u^*} + \rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha\,(1+\gamma)} + b \right) - p_{MD} \right). \quad (22)$$

Here, in the case of partial-band flipping, ΔB_f is proportional to the adversary power, P_A, and can be expressed as:

$$\Delta B_f = \frac{aP_A}{(1+\gamma)\,\sigma_n^2/\alpha\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^*+\rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)}+b\right)^2}. \quad (23)$$

To illustrate the intuition behind (23), consider (16) and define $c^* = P_A/x^*$. This allows us to express the derivative of the function $f'(x^*)$ as:

$$f'\left(x^*\right) = \Phi\left(\frac{a\left(c^* + \frac{\rho\sigma_n^2}{\alpha}\right)}{\frac{\sigma_n^2}{\alpha(1+\gamma)}} + b \right) - p_{MD} - \frac{ac^*}{(1+\gamma)\,\sigma_n^2/\alpha\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^*+\rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2}. \quad (24)$$

If at $f'(x^*) = 0$, then (24) can be simplified as:

$$\Phi\left(\frac{a\left(c^* + \rho\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha\,(1+\gamma)} + b \right) - p_{MD} = \frac{(ac^*)\, e^{-\frac{1}{2}\left(\frac{a\left(c^*+\frac{\rho\sigma_n^2}{\alpha}\right)}{\frac{(1+\gamma)\sigma_n^2}{\alpha}}+b\right)^2}}{\frac{(1+\gamma)\sigma_n^2}{\alpha}\sqrt{2\pi}}. \quad (25)$$

In (25), when $N, M, \gamma, \rho, \alpha, \sigma_n^2$, and p_{FA}^{DES} are fixed, then c^* is determined. Moreover, the optimal flipping power required for each of the flipping bands mentioned in the previous section is equivalent to c^*. Recall that $\lfloor x^* \rfloor$ or $\lceil x^* \rceil$ is equal to u^*, a positive finite number that can be expressed as, $u^* = P_A/c^*$. Finally, substituting (25) into (22), we obtain:

$$\Delta B_f = P_A/c^* \left(\frac{ac^*}{(1+\gamma)\,\sigma_n^2/\alpha\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^*+\rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2} \right) = \frac{aP_A}{(1+\gamma)\,\sigma_n^2/\alpha\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(c^*+\rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2}. \quad (26)$$

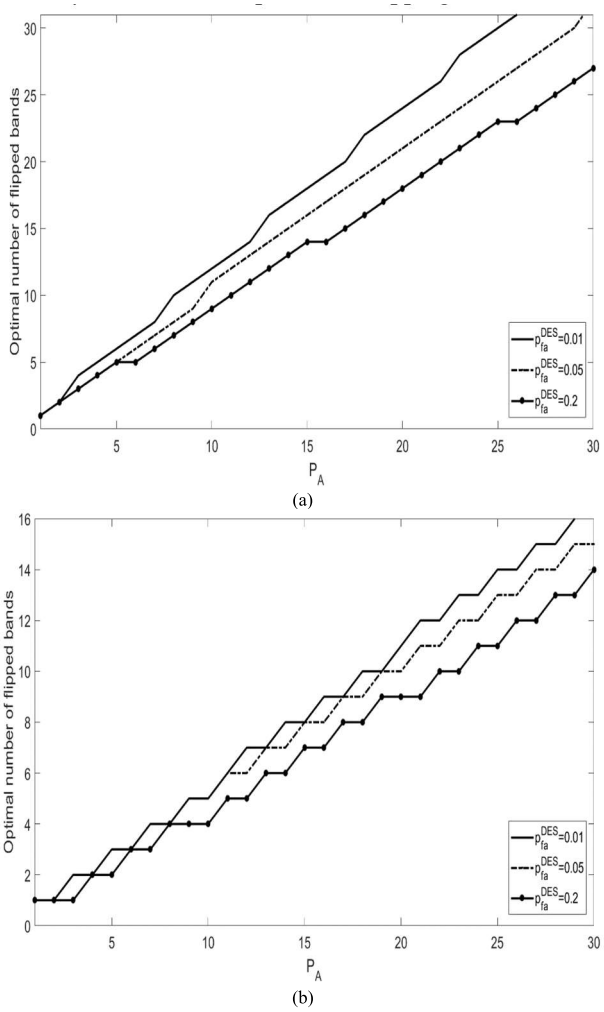

FIGURE 5. Optimal number of flipped bands u^* versus P_A: (a) $\gamma = 0dB$. (b) $\gamma = 3dB$.

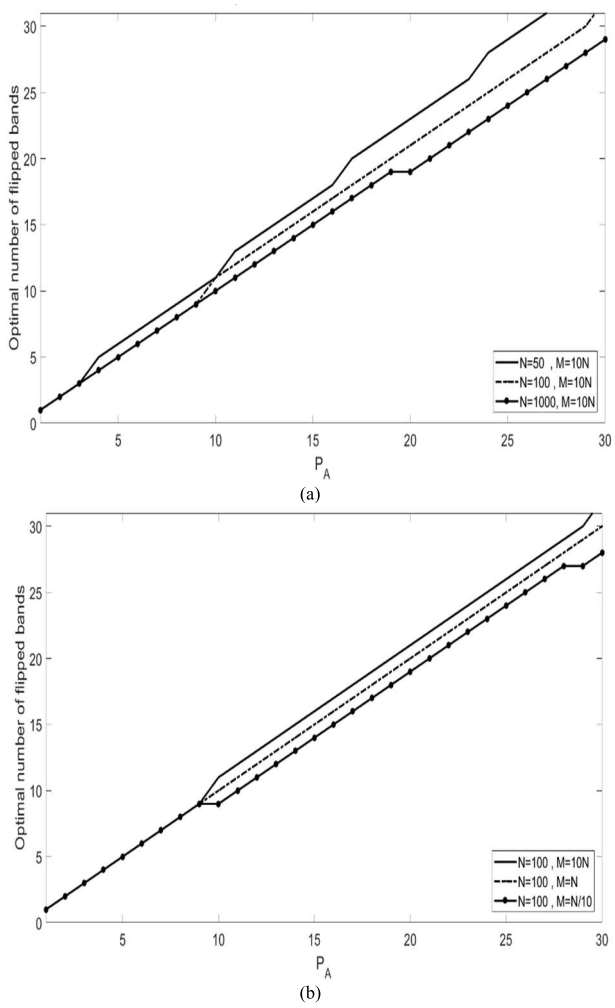

FIGURE 6. Optimal number of flipped bands u^* versus P_A for different values of: (a) N. (b) M.

In conclusion, for the case $|B_{ENP}| > |B_{busy}|$, the adversary will not utilize more power than c^* in each ENP band. If the adversary has excess power, it would look for more ENP bands to contaminate until all the ENP bands are contaminated. In the other case, when $|B_{ENP}| < |B_{busy}|$, according to the discussion in Section III-B, the optimal number of flipped bands cannot be greater than $|B_{ENP}|$. Even when the adversary increases the flipping power, there are no additional contaminated ENP bands.

IV. NUMERICAL RESULT

In this section, the optimal sensing disruption technique is demonstrated through numerical simulations. The adversary performs equal power flipping across the ENP bands because there is no knowledge of the system parameters such as N, M, γ, p_{FA}^{DES}, and ρ. We employed equal power flipping with varying system parameter values to evaluate flipping optimization. Without loss of generality, we assume that $\sigma_n^2 = 1$ and $\alpha = 1$. Finally, it is desirable to compare flipping attacks with existing sensing disruptions. However, the unconventional nature of flipping attacks makes it difficult to formulate a single metric that simultaneously incorporates both spoofing and flipping.

A. OPTIMAL NUMBER OF FLIPPED BANDS

We demonstrate how the optimal number of flipped bands, u^*, varies with $|B_{busy}|$ for different values of $|B_{ENP}|$, γ, and P_A. Fig.3 shows u^* versus $|B_{busy}|$, where the curves are parameterized by P_A for various ENP bands. The remaining system parameters are set as follows: $p_{FA}^{DES} = 0.05$, $\rho = 1$, $N = 100$ and $M = 10N$. In Fig.3, each curve exhibits a knee, that shows a shift from full-band flipping to partial-band flipping. The region to the left of the knee indicates that u^* equals the number of busy bands. As discussed in Section III, if the number of ENP bands is greater than the number of busy bands, and the adversary has sufficient power to contaminate the ENP measurements of the available SUs, the optimal strategy is to flip all busy bands. To the right of the knee, we have $|B_{busy}| > |B_{ENP}|$; thus, u^* is upper bounded by $|B_{ENP}|$, and even if the flipping power increases,

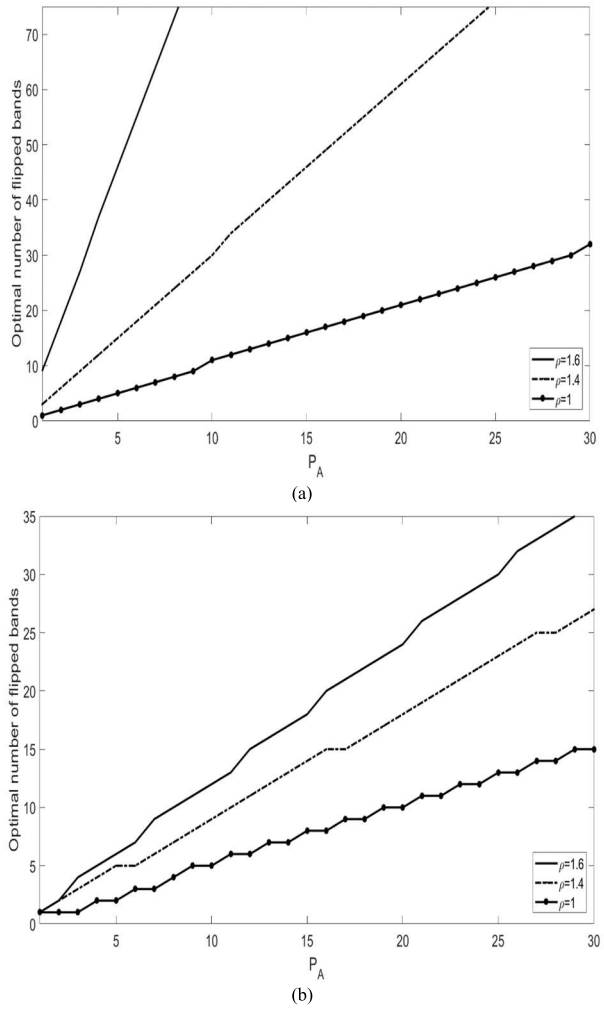

FIGURE 7. Optimal number of flipped bands u^* versus P_A: (a) $\gamma = 0dB$. (b) $\gamma = 3dB$.

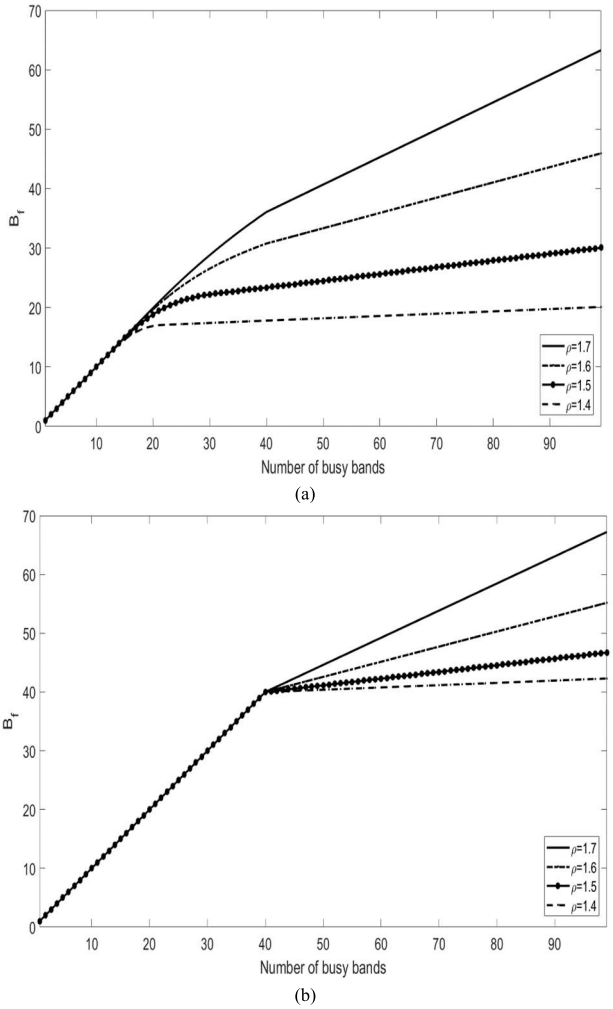

FIGURE 8. Average number of missed detection, B_f, versus $|B_{busy}|$: (a) P_A= 10. (b) P_A= 38.

the adversary cannot contaminate more than the number of ENP bands. Thus, the optimal flipping strategy is partial-band flipping. In the second case, the partial-band flipping region occurs when $|B_{ENP}| > |B_{busy}|$, but P_A is not sufficiently large to contaminate all available ENP bands. Thus, the optimal flipping strategy is to flip a fraction of busy bands. With the same setup as in Fig.3, Fig.4 shows that γ of the PUs' signals plays an important role in degrading u^*, regardless of the number of bands that the adversary attacks. Comparing Fig. 4(b) with Fig. 4(a) for the same values of u^*, and $|B_{ENP}|$, we see that Fig. 4(a) utilizes a smaller value of P_A than Fig. 4(b) to flip the same number of busy bands. This is because γ in Fig. 4(a) was lower than that in Fig. 4(b). Finally, each curve exhibits a knee, which is determined by $|B_{ENP}|$ and $|B_{busy}|$.

B. THE EFFECT OF SYSTEM PARMETERS

In Fig.5, Fig.6, and Fig.7, we operate in the region to the right of the knee of Fig.3, which means that the optimal strategy for the adversary is partial-band flipping. In particular, we operate in the region where $|B_{ENP}| > |B_{busy}|$. In these figures, u^* is plotted versus P_A, with different system parameter setup values. From Appendix B, it is clear that u^* increases as P_A increases, up to the point where all ENP bands are contaminated. In Fig.5, we set $N = 100$; $M = 10N$ and $\rho = 1$, and plot u^* for different values of γ, as well as different values of the desired probability of false alarm p_{FA}^{DES}.

Note that each value of p_{FA}^{DES} corresponds to a different threshold value. Fig.5 (a) shows that when $\gamma = 0dB$, u^* increases as P_A increases. This is reasonable, because increasing the flipping power implies attacking more ENP bands. As a result of γ increasing, u^* significantly decreases, as shown in Fig.5 (b).

In both Fig.5 (a) and Fig.5 (b), if p_{FA}^{DES} decreases, then the adversary can utilize less power for flipping over the same $|B_{ENP}|$, resulting in flipping more of the busy bands. The reason is that the threshold, K, increases, so that it is harder to detect the busy bands.

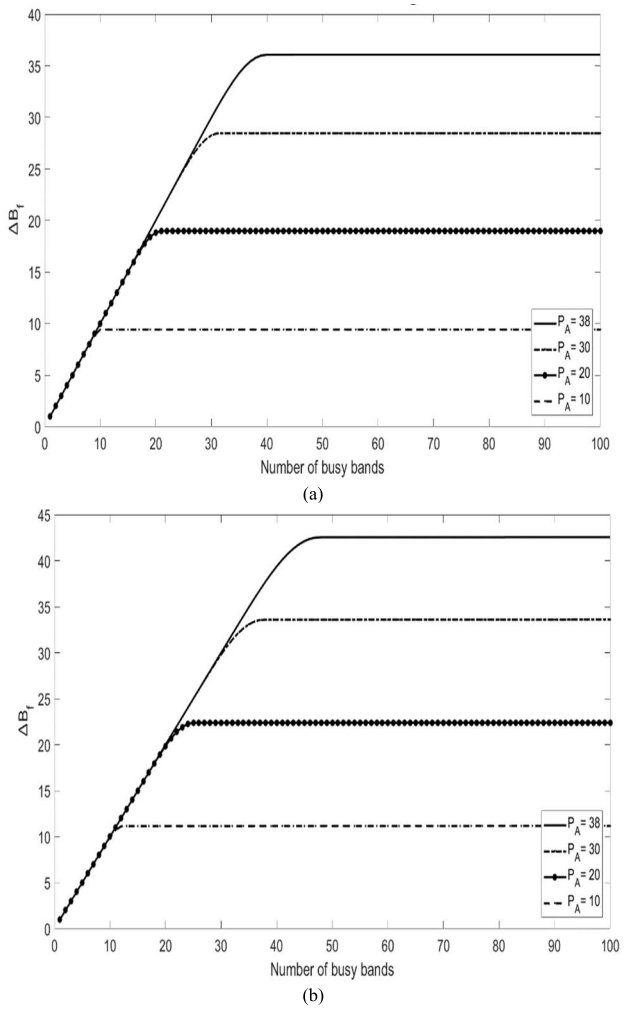

FIGURE 9. Average number of missed detection, ΔB_f, versus $|B_{busy}|$: (a) $p_{FA}^{DES} = 0.05$. (b) $p_{FA}^{DES} = 0.005$.

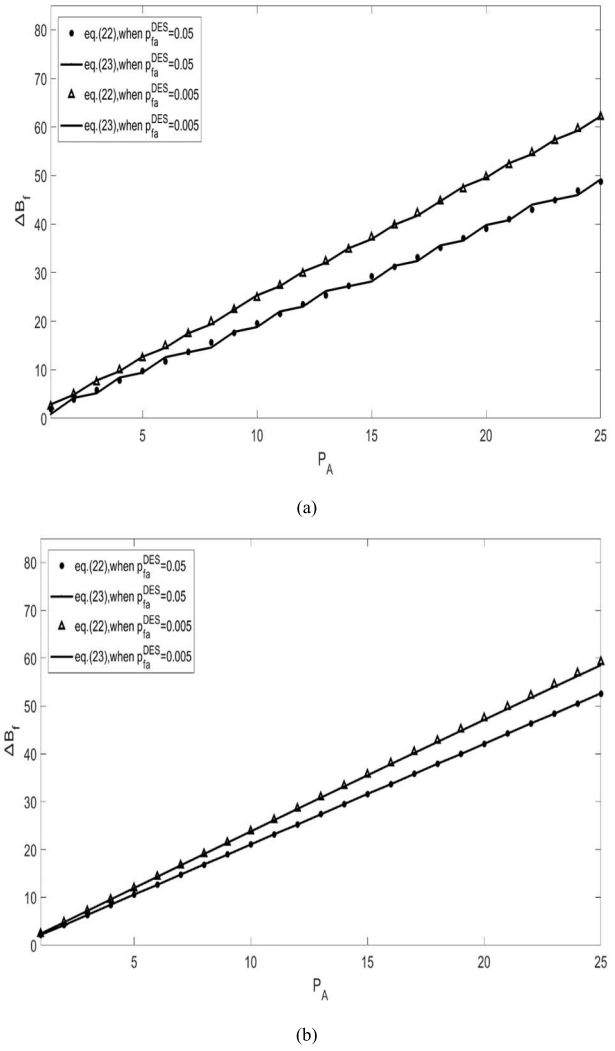

FIGURE 10. Average number of missed detection, ΔB_f, versus $|B_{busy}|$: (a) $\gamma = -3dB$ and $\rho = 1$ (b) $\gamma = 0dB$ and $\rho = 1.6$.

As shown in Figs.6(a) and 6(b), we plot u^* for different values of N and M, but we set $p_{FA}^{DES} = 0.05$, $\gamma = 0dB$, and $\rho = 1$. The results show that u^* increased as N decreased, as seen in Fig.6 (a). This is because the more samples the SUs observe during fast-SP, the more correct the decisions the SU makes regarding the busy bands. In contrast, Fig.6 (b) shows that as M increases, u^* also increased. This is because an increase in M implies that the SUs estimate the contaminated noise power more effectively.

In Figs.7 (a) and 7 (b), u^* is plotted for different values of γ and ρ, with the other parameters set as follows: $p_{FA}^{DES} = 0.05$, $N = 100$ and $M = 10N$. Clearly, u^* increases when ρ increases because robust detection can no longer be guaranteed at the SUs, as shown in both Fig.7 (a) and Fig.7 (b). However, if γ increases, as shown in Fig.7 (b), u^* decreases compared to Fig.7 (a) because the SNR of the PU increases; thus, the SUs can better detect the busy bands.

In conclusion, the optimal number of flipped bands is affected by p_{FA}^{DES}, N, M, γ, and ρ. This implies that the optimal flipping power allocation is also affected by these parameters, because $P_{k,A}^* = P_A/u^*$.

C. AVERAGE NUMBER OF MISSED DETECTION

Fig.8 shows the plots of B_f versus $|B_{busy}|$, where the curves are parameterized by ρ. In Fig.8 (a) $P_A = 10$, and in Fig.8 (b) $P_A = 38$. The other parameters were set to $N = 100$, $M = 10N$, $p_{FA}^{DES} = 0.05$ and $\gamma = 0$ dB. The interpretation of each knee in the curves in Fig.8 is that full-band flipping becomes partial-band flipping, for the same reasons as those in Fig.3. As shown in Fig.8, when the slope of the curve is 45^o, we are in the full-band flipping region (i.e., $u^* = |B_{busy}|$). In this region, the missed detections of the busy bands are owing to both the presence of the adversary and $\rho \neq 1$, as shown in (20). When the slope of B_f is determined only by p_{MD}, the slope only increases linearly with ρ. It should be noted that Fig.8 (b) has a larger full-band region than Fig.8 (a). This is because the adversary increases P_A to contaminate all the available ENP bands.

D. AVERAGE NUMBER OF MISSED DETECTION DUE TO THE PRESENCE OF THE ADVERSARY

In Fig.9, ΔB_f is plotted for the case of $|B_{ENP}| \geq |B_{busy}|$.

The remaining parameters were set as $N = 100$, $M = 10N$, $\gamma = 0\,dB$ and $\rho = 1$. The interpretation of each knee in the curves in Fig.9 is equivalent to that in Fig.3. The difference between Fig.8 and Fig.9 is in the value of ρ, which shows that in the partial-band region, ΔB_f in Fig.9 becomes constant when $|B_{busy}|$ increases, compared with B_f in Fig.8. Note that an increase in P_A, leads to an increase in ΔB_f, as discussed in Section III-C. A comparison between Fig.9(b) and Fig.9(a) shows that increasing p_{FA}^{DES} results in a decrease in K. For the same flipped power, ΔB_f is more significant in Fig.9 (b) than in Fig.9 (a). This provides an advantage to the adversary in spreading less flipping power over ENP bands.

In Fig.10, ΔB_f is plotted against P_A, with $N = 100$, $M = 10N$, and various values of p_{FA}^{DES}, γ and ρ. Additionally, we operated in the partial-band region, particularly when $|B_{ENP}| \geq |B_{busy}|$. Fig.10 shows that ΔB_f linearly increases when the P_A increases. In addition, we can see that ΔB_f of (23) is consistent with (22), for both Figs.10 (a) and 10 (b).

V. CONCLUSION AND FUTURE WORK

In this paper, we analyzed the optimal sensing link disruption of a CRN subject to a constraint on power of the adversary. We formulated the optimal sensing link disruption by maximizing the average number of missed detections. In particular, for a CRN in which the ED-ENP is used by the SUs, the optimal strategy corresponds to equal-power partial-band flipping. Our analysis leads us to conclude that increasing the flipping power allows the adversary to flip more bands, up to the point where all the ENP bands are contaminated. Additionally, we observed that an increase in the threshold, parameter ρ, or the number of samples during fine-SP (i.e., M) increases the chance of successful flipping attacks, while a decrease in the number of samples during fast-SP (i.e., N) also increases flipping attacks. Furthermore, for the given system parameters (ρ, N, M, and p_{FA}^{DES}), ΔB_f is proportional to the flipping power.

Future work will involve extending the problem to CRNs with randomly distributed locations of SUs and PUs, with an adversary that is probabilistically aware of these locations. In addition, future work will involve examining the performances of various fading channels.

APPENDIX A

Let $\vec{P}_A\left[P_{1,A}, \ldots, P_{U,A}\right]$ (i.e., the power in each of the U bands), and define the objective function to be, $f_a\left(\vec{P}_A\right) \triangleq \sum_{k=1}^{U} \Phi\left(\frac{a\left(f_k\left(\vec{P}_A\right)+\rho\sigma_n^2/\alpha\right)}{(1+\gamma)\sigma_n^2/\alpha} + b\right)$, where $f_k\left(\vec{P}_A\right) \triangleq P_{k,A}$. Finally, also let the constraint to be, $h\left(\vec{P}_A\right) \triangleq \sum_{k=1}^{U} f_k\left(\vec{P}_A\right) - P_A$. Then, we can rewrite (13) as,

$$\begin{aligned} \min_{P_{1,A},\ldots,P_{U,A}} \; & -f_a\left(\vec{P}_A\right) \\ s.t \; & -f_k\left(\vec{P}_A\right) \leq 0, \forall k \in \{1, \ldots, U\}, \\ & h\left(\vec{P}_A\right) = 0. \end{aligned} \tag{A-1}$$

The Lagrangian associated with (V)-1), is given by

$$L\left(\vec{P}_A, \vec{\lambda}, v\right) = f_a\left(\vec{P}_A\right) - \sum_{k=1}^{U} \lambda_k f_k\left(\vec{P}_A\right) + v h\left(\vec{P}_A\right), \tag{A-2}$$

where $\vec{\lambda} = \left[\lambda_1 \lambda_2 \ldots \lambda_U\right] \in \mathbb{R}^U$ and $v \in \mathbb{R}$ are the Lagrangian multipliers. Suppose $\vec{P}_A^*$, $\vec{\lambda}^*$ and v^* are optimal sets of points. The necessary KKT conditions are as follows [27]:

$$\sum_{k=1}^{U} f_k\left(\vec{P}_A^*\right) - P_A = 0, \text{ and } \vec{P}_A^* \succcurlyeq 0, \tag{A-3}$$

$$\lambda_k^* \geq 0, \; \forall k \in \{1, \ldots, U\}, \tag{A-4}$$

$$\lambda_k^* P_{k,A}^* = 0, \forall k \in \{1, \ldots, U\}, \tag{A-5}$$

$$\frac{-a}{\sqrt{2\pi}\sigma_n^2/\alpha\,(1+\gamma)} e^{-\frac{1}{2}\left(\frac{\left(P_{k,A}^*+\rho\sigma_n^2/\alpha\right)a}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2} - \lambda_k^* + v^* = 0, \quad \forall k \in \{1, \ldots, U\}. \tag{A-6}$$

By satisfying the complementary slackness condition (V)-5), for some value of k, we observe that $P_{k,A}^* > 0$ and $\lambda_k^* = 0$, and from (V)-6), we have

$$v^* = \frac{-ae^{-\frac{1}{2}\left(\frac{\left(P_{k,A}^*+\rho\sigma_n^2/\alpha\right)a}{(1+\gamma)\sigma_n^2/\alpha}+b\right)^2}}{\sqrt{2\pi}\sigma_n^2/\alpha\,(1+\gamma)}. \tag{A-7}$$

Let the set φ_A be defined as $\varphi_A = \left\{k | \lambda_k^* = 0, P_{k,A}^* > 0\right\}$, and let the cardinality of φ_A be $u (0 < u \leq U)$. From (V)-7), we can see that v^* is the same for each $k \in \varphi_A$; thus, $P_{k,A}^*$ needs to be uniformly distributed over all flipping bands, that is, $P_{k,A}^* = P_A/u$.

In the other case, $P_{k,A}^* = 0$, and $\lambda_k^* > 0$. For those values of k in this case, from (V)-6), we can see that λ_k^* is independent of k. Let the set $\varphi_\lambda \triangleq \left\{k | \lambda_k^* > 0, P_{k,A}^* = 0\right\}$. By definition, the cardinality of φ_λ is $U - u$. This means that λ_k^* is the same $\forall k \in \varphi_\lambda$. Clearly, in (V)-1), the objective function is strictly convex because the Hessian matrix is positive definite. Therefore, KKT conditions are both necessary and sufficient [27]. In conclusion, $P_{k,A}^*$ is equal to either $P_{k,A}^* = P_A/u$, for $k \in \varphi_A$, or $P_{k,A}^* = 0$, for $k \in \varphi_\lambda$.

APPENDIX B

From (16), it is difficult to obtain the solution of $f'(x^*) = 0$, because it is a nonlinear expression. Consequently, we evaluated $f'(x)$ on its boundary. Since

$x \in (0, \infty)$, then,

$$f'(x)\,|_{x=0} = \Phi(\infty) - p_{MD} - \lim_{x\to 0^+} \frac{aP_A}{(1+\gamma)\,x\sigma_n^2/\alpha\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(P_A+x\rho\sigma_n^2/\alpha\right)}{(1+\gamma)x\sigma_n^2/\alpha}+b\right)^2}. \tag{B-1}$$

We define $\varepsilon \triangleq \frac{aP_A}{(1+\gamma)\sigma_n^2/\alpha}$, and let $\eta(x) = \frac{\varepsilon}{x\sqrt{2\pi}}$, $\theta(x) = e^{\frac{1}{2}\left(\frac{\varepsilon}{x}+\frac{a\rho}{(1+\gamma)}+b\right)^2}$. Then $\lim_{x\to 0^+} \frac{\eta(x)}{\theta(x)} = \frac{\infty}{\infty}$, and thus, we can apply L'Hospital's rule:

$$\lim_{x\to 0^+} \frac{\eta'(x)}{\theta'(x)} = \lim_{x\to 0^+} \frac{\frac{1}{\sqrt{2\pi}}}{e^{\frac{1}{2}\left(\frac{\varepsilon}{x}+\frac{a\rho}{(1+\gamma)}+b\right)^2}\left(\frac{\varepsilon}{x}+\frac{a\rho}{(1+\gamma)}+b\right)} = \frac{\frac{1}{\sqrt{2\pi}}}{\infty} = 0. \tag{B-2}$$

Substituting (V)-2) into (V)-1), we have

$$f'(x)\,|_{x=0} = 1 - \Phi\left(\frac{a}{\frac{1}{\rho}(1+\gamma)}+b\right) = Q\left(\frac{a}{\frac{1}{\rho}(1+\gamma)}+b\right). \tag{B-3}$$

$\because$ $Q(\cdot)$ is a monotonically decreasing function, thus $Q\left(\frac{a}{\frac{1}{\rho}(1+\gamma)}+b\right) > 0$. Additionally,

$$\lim_{x\to\infty} f'(x) = \Phi\left(\frac{a\rho}{1+\gamma}+b\right) - \Phi\left(\frac{a}{\frac{1}{\rho}(1+\gamma)}+b\right) = 0. \tag{B-4}$$

Therefore, from (V)-3) and (V)-4), $f'(x)$ has a positive value at $x = 0$, and approaches 0 as x approaches infinity. To examine $f'(x)$, as x increases throughout the range of $(0, \infty)$, we need to derive $f''(x)$. The second derivative is given by:

$$f''(x) = \frac{\partial}{\partial x}\left(\left(\Phi\frac{aP_A}{\sigma_n^2/\alpha\,(1+\gamma)\,x}+\frac{a\rho}{(1+\gamma)}+b\right) - p_{MD} - \frac{aP_A\left(\alpha/\sigma_n^2\right)}{(1+\gamma)\,x\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{aP_A}{\sigma_n^2/\alpha(1+\gamma)x}+\frac{a\rho}{(1+\gamma)}+b\right)^2}\right). \tag{B-5}$$

Let $y(x) \triangleq \Phi\left(\frac{aP_A}{\sigma_n^2/\alpha(1+\gamma)x}+\frac{a\rho}{(1+\gamma)}+b\right) - p_{MD}$, and $q(x) - \frac{aP_A\left(\alpha/\sigma_n^2\right)}{(1+\gamma)x\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(P_A+\rho x\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)x}+b\right)^2}$. Then, we can express (V)-5) as

$$f''(x) = \frac{\partial}{\partial x}(y(x)+q(x)) = y'(x)+q'(x) \tag{B-6}$$

The last term in (16) represents the derivative of $y(x)$, which is, $y'(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{a\left(P_A+\rho x\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)x}+b\right)^2}\left(\frac{aP_A\left(\alpha/\sigma_n^2\right)}{(1+\gamma)x^2}\right)$, and therefore $q(x) = xy'(x)$. The derivative of $q(x)$ can be shown to be, $q'(x) = y'(x) + xy''(x)$. Therefore, after some algebraic manipulation, $f''(x)$ is given by,

$$f''(x) = -\frac{(aP_A)^2\left(aP_A+\left(\frac{a\rho\sigma_n^2}{\alpha}+\frac{b(1+\gamma)\sigma_n^2}{\alpha}\right)x\right)}{\sqrt{2\pi}\left(\frac{\sigma_n^2}{\alpha}\right)^3(1+\gamma)^3x^4} \times e^{-\frac{1}{2}\left(\frac{a\left(P_A+\frac{\rho x\sigma_n^2}{\alpha}\right)}{\frac{\sigma_n^2}{\alpha(1+\gamma)x}}+b\right)^2} \tag{B-7}$$

From (V)-7), $f''(x)$ is dependent upon a linear function, that is, $f_0(x)\,aP_A + \left(a\rho\sigma_n^2/\alpha + b\,(1+\gamma)\,\sigma_n^2/\alpha\right)x$, since $\gamma > 0$, $\alpha > 0$, $\sigma_n^2 > 0$, $b > 0$, $a > 0$, $P_A > 0$, $\rho > 0$, and $e^{-\frac{1}{2}\left(\frac{a\left(P_A+\rho x\sigma_n^2/\alpha\right)}{\sigma_n^2/\alpha(1+\gamma)x}+b\right)^2} > 0$, then $f_0(x)$ is a first-order polynomial function; thus, the slope of $f_0(x)$ is $\left(\rho\sigma_n^2/\alpha + b\,(1+\gamma)\,\sigma_n^2/\alpha\right) > 0$, and $f_0(x)\,|_{x=0} = aP_A > 0$. It is then straightforward to say that $f'(x) > 0$, for any $x \geq 0$. From the analysis above, we can conclude that $f(x)$ continuously increases as x increases for $x \geq 0$.

ACKNOWLEDGMENT

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

REFERENCES

[1] S. Atapattu, C. Tellambura, and H. Jiang, *Energy Detection for Spectrum Sensing in Cognitive Radio*, New York, NY, USA: Springer-Verlag, 2014.
[2] S. K. Sharma, T. E. Bogale, S. Chatzinotas, B. Ottersten, L. B. Le, and X. Wang, "Cognitive radio techniques under practical imperfections: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1858–1884, 4th Quart., 2015, doi: 10.1109/COMST.2015.2452414.
[3] Y. Zeng, Y.-C. Liang, A. T. Hoang, and R. Zhang, "A review on spectrum sensing for cognitive radio: Challenges and solutions," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, Dec. 2010, Art. no. 381465.
[4] R. Umar, A. U. H. Sheikh, and M. Deriche, "Unveiling the hidden assumptions of energy detector based spectrum sensing for cognitive radios," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 713–728, 2nd Quart., 2014, doi: 10.1109/SURV.2013.081313.00054.
[5] R. Tandra, "Fundamental limits on detection in low SNR," M.S. thesis, Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, 2005.
[6] A. Mariani, A. Giorgetti, and M. Chiani, "Effects of noise power estimation on energy detection for cognitive radio applications," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3410–3420, Dec. 2011, doi: 10.1109/TCOMM.2011.102011.100708.
[7] Y. Ma, S. Dehnie, and V. D. Chakravarthy, "On the near-optimality of training-based GLRT spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4894–4906, Sep. 2015, doi: 10.1109/TWC.2015.2429136.
[8] V. Rakovic, D. Denkovski, V. Atanasovski, P. Mähönen, and L. Gavrilovska, "Capacity-aware cooperative spectrum sensing based on noise power estimation," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2428–2441, Jul. 2015, doi: 10.1109/TCOMM.2015.2433297.

[9] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015, doi: 10.1109/COMST.2015.2422735.

[10] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013, doi: 10.1109/SURV.2011.122211.00162.

[11] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015, doi: 10.1109/COMST.2014.2380998.

[12] G. Ding, J. Wang, Q. Wu, L. Zhang, Y. Zou, Y.-D. Yao, and Y. Chen, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014, doi: 10.1109/TCOMM.2014.2346775.

[13] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectr. Access Netw.*, Chicago, IL, USA, Oct. 2008, pp. 1–6, doi: 10.1109/DYSPAN.2008.16.

[14] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Impact of primary user emulation attacks on dynamic spectrum access networks," *IEEE Trans. Commun.*, vol. 60, no. 9, pp. 2635–2643, Sep. 2012, doi: 10.1109/TCOMM.2012.071812.100729.

[15] Q. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1801–1810, May 2010, doi: 10.1109/TVT.2010.2043966.

[16] M. Soysa, P. C. Cosman, and L. B. Milstein, "Optimized spoofing and jamming a cognitive radio," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 2681–2695, Aug. 2014, doi: 10.1109/TCOMM.2014.2331964.

[17] Q. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption: A generalized framework for a power-limited adversary," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1341–1355, Feb. 2019, doi: 10.1109/TCOMM.2018.2874888.

[18] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems—Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011, doi: 10.1109/TWC.2010.112310.100630.

[19] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios," *J. Commun.*, vol. 1, no. 1, pp. 38–47, Apr. 2006.

[20] Ecma International Standard. (Dec. 2012). *Ecma 392: MAC and PHY for Operation in TV White Spaces*. [Online]. Available: http://www.ecma-international.org/publications/standards/Ecma-392.htm

[21] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[22] S. M. Kay, *Fundamentals of Statistical Processing: Estimation Theory*, vol. 1. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[23] D. A. Shnidman, "Radar detection probabilities and their calculation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 3, pp. 928–950, Jul. 1995, doi: 10.1109/7.395246.

[24] J. J. Lehtomaki, M. Juntti, and H. Saarnisaari, "CFAR strategies for channelized radiometer," *IEEE Signal Process. Lett.*, vol. 12, no. 1, pp. 13–16, Jan. 2005, doi: 10.1109/LSP.2004.839701.

[25] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (National Bureau of Standards Applied Mathematics Series), vol. 55. Washington, DC, USA: U.S. Government Printing Office, 1964.

[26] M. Soysa, P. C. Cosman, and L. B. Milstein, "Disruptive attacks on video tactical cognitive radio downlinks," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1411–1422, Apr. 2016, doi: 10.1109/TCOMM.2016.2535257.

[27] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[28] H. Hancock, *Theory of Maxima and Minima*. New York, NY, USA: Dover, 1960.

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 network (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, 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. 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 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. He 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 the Former Chair of the IEEE Fellows Selection Committee. He was the Vice-President of Technical Affairs of the IEEE Communications Society, in 1990 and 1991. 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.