Title

Optimal Sensing Disruption: A Generalized Framework for a Power-Limited Adversary

Permalink

https://escholarship.org/uc/item/81s7r2mj

Journal

IEEE Transactions on Communications, 67(2)

ISSN

0090-6778

Authors

Peng, Qihang
Cosman, Pamela C
Milstein, Laurence B

Publication Date

2019-02-01

DOI

10.1109/tcomm.2018.2874888

Peer reviewed

Optimal Sensing Disruption: A Generalized Framework for a Power-Limited Adversary

Qihang Peng, *Member, IEEE*, Pamela C. Cosman, *Fellow, IEEE*, and Laurence B. Milstein, *Fellow, IEEE*

***Abstract*— A generalized framework of spectrum sensing disruption for a power-limited adversary is proposed in this paper. In the literature, a conventional sensing attack typically assumes that the adversary has perfect knowledge of the spectral usage status. The framework in this paper considers a more general case where there are uncertainties in the estimates at the adversary. These uncertainties are modeled utilizing the probability of detection and the probability of false alarm. Then, the sum of the conditional probabilities of false detection at the secondary within the spectral range of interest, conditioned on the adversary's estimated spectrum usage status, is maximized. It is shown that the optimal sensing attack, given perfect estimation is a special case of the proposed framework. When the adversary has perfect spectrum usage information, this framework reduces to a previously demonstrated optimal sensing disruption. When the adversary has imperfect information on the spectral status, the proposed framework is significantly more robust than conventional sensing attacks. Further, when the adversary's power budget increases, it asymptotically approaches the sensing disruption performance upper bound.**

***Index Terms*— Spectrum sensing, cognitive radio, intelligent adversary, estimation uncertainty.**

I. Introduction

COGNITIVE radio (CR) can help the problem arising from inefficient usage of limited electromagnetic spectrum under fixed allocation [1], [2]. In CR networks, secondary users (SUs) are allowed to opportunistically access those spectral bands not being used by primary users (PUs), under the constraint that interference to PUs is below some threshold.

Spectrum sensing [3]–[6] is an essential component in realizing dynamic spectrum access for CR [7]. It enables SUs to be aware of the electromagnetic surroundings by identifying whether PUs are present within the spectral range of interest. However, spectrum sensing introduces new opportunities for an adversary [8]–[10]. Spectrum sensing attacks [9], [11], [12] can be categorized as sensing link disruption, also termed spoofing, and sensing cooperation disruption, also called a spectrum sensing data falsification (SSDF) attack. In spoofing, the adversary sends electromagnetic signals into vacant bands, to make the secondary mistakenly believe that these bands are used by PUs. Sensing cooperation disruption targets the cooperation process of cooperative spectrum sensing, where the CR network collects measurements from individual SUs and the adversary pretends to be an SU sending out falsified measurements so as to mislead the CR network in the final sensing decision. The focus of this paper is on sensing link disruption, since it applies to both local sensing and cooperative sensing.

A. Related Work

Numerous research papers considered sensing-link disruption in spectrum sensing [13]–[20]. By assuming that PU location is known, a countermeasure to a sensing-link attack is proposed, based on localization information from received signal strength measurements in [14]. Jin *et al.* [15] presented the detection of a sensing attack using Fenton's approximation and Wald's sequential probability ratio test (WSPRT), and extended this work in [16], where a Neyman-Pearson composite hypothesis test and a Wald's sequential probability ratio test are analyzed. Secure spectrum sensing based on cryptographic techniques were proposed in [17] and [18], where a public-key cryptography mechanism is used between primary and secondary users. In [19] and [20], learning techniques were applied to mitigate the destructive effects of a sensing attack. The above research mainly focuses on proposing various approaches against sensing-link attacks. However, to better combat this attack, an in-depth analysis and optimal design on the attack itself is necessary.

Spoofing feasibility was analyzed in [21], and its impact on CR network performance was investigated in [22]. How to optimally launch a sensing link disruption with a given power budget is important, since it provides a worst-case performance analysis for spectrum sensing mechanisms in the presence of a sensing-link attack. Optimal spoofing for an adversary with a limited power budget under additive white Gaussian noise (AWGN) was derived and analyzed in [11], [23], and [24]. This work was extended for fading propagation environments in [25] and [26]. However, it was assumed that the adversary knows spectral usage status perfectly. In [27], the adversary is assumed to conduct the attack in a blind way such that it does not know the true status of primary signals. However, the adversary could obtain the spectral usage status

Manuscript received April 10, 2018; revised August 20, 2018; accepted September 30, 2018. Date of publication October 9, 2018; date of current version February 14, 2019. This research was supported by the National Science Foundation of China under Grant No. 61301154, by the China Scholarship Council (201506075100), and by Office of Naval Research under Grant No. N00014-17-S-B00. The associate editor coordinating the review of this paper and approving it for publication was K. Tourki. *(Corresponding author: Qihang Peng.)*

Q. Peng is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: anniepqh@uestc.edu.cn).

P. C. Cosman and L. B. Milstein are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093 USA (e-mail: pcosman@ucsd.edu; lmilstein@ucsd.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2018.2874888

based on its own measurements. Haghighat and Sadough [28] and Saber and Sadough [29] propose a smart radio-aware adversary that performs its own spectrum sensing, and it consumes resources in a way that causes more destruction than current attackers. However, it lacks an in-depth analysis of the optimal attacking strategy.

B. Motivation and Contributions

In this paper, we investigate an intelligent adversary which has the ability to estimate the usage status within the spectral range of interest. A general scenario is considered where there could be estimation uncertainties on the spectral usage status at the adversary. That is, there is a non-zero probability at the adversary that a band is estimated to be busy but is actually vacant. Similarly, a band could be estimated to be vacant but actually be busy. We derived the optimal spoofing strategy with the assumption that the estimation at the adversary is perfect in [11], where it was shown that the optimal spoofing is equal-power, partial-band spoofing. To the best of our knowledge, the problem of how to optimally spoof with a given power budget given realistic estimation uncertainties remains unresolved.

We tackle this problem in this paper by introducing the conditional probability that a band is actually vacant, given the sensed result on that band at the adversary. The sum of the conditional probabilities of false detection at the secondary, conditioned on the spectral usage status estimates at the adversary, is then derived and maximized. Numerical results show that the proposed spoofing outperforms conventional sensing disruption strategies, and asymptotically approaches the performance upper bound when there is no sensing estimation uncertainty at the adversary.

The contributions of this paper are as follows:

- We propose a generalized framework for sensing disruption by a power-limited adversary, which provides an intelligent transition for the adversary to launch different sensing disruptions. It is shown that the optimal sensing disruption strategy, given perfect estimation, is a special case of our proposed framework.
- We show that by applying the proposed framework, the sensing-attack performance of the adversary outperforms conventional algorithms, and asymptotically approaches the ideal sensing disruption performance when the adversary has perfect information.
- We provide an optimal disruption strategy for a sensing-link attack by optimally allocating an adversarial power budget across subcarriers in the sense of causing maximally destructive effects to the target CR network. Meanwhile, it provides a worst-case performance analysis for secure spectrum sensing in the presence of sensing link disruption.

This power-limited adversary framework has a variety of applications, including military and border patrol scenarios (unmanned aircraft, wireless sensor networks, vehicular networks, etc.) as well as Cognitive Internet-of-Things (CIoT) scenarios. Many CIoT applications, which are seen as good fits for spectrum sensing and dynamic spectrum access, such as healthcare, environmental monitoring, smart grids, intelligent traffic systems, and in-home systems, are not usually considered as adversarial scenarios. However, there are adversarial situations which can arise in all these applications, including terrorism, vandalism, and various financially motivated crimes (home burglary, waste dumping, avoiding speeding tickets, etc.) where sensor overrides or attacks could be deployed.

The rest of this paper is organized as follows. The system model and the generalized framework are presented in Section II. In Section III, a sub-optimal solution is given, and relationships of existing sensing disruption strategies with our proposed framework are analyzed. Performance analysis is described in Section IV and numerical results are presented in Section V. Finally, conclusions and future work are discussed in Section VI.

Regarding notation: random processes are written as functions of time, e.g., $w_i(t)$, random variables are denoted by uppercase bold letters, e.g., $\boldsymbol{N}_P$, and values that the random variables equal are represented by lowercase letters, e.g., n_P. Variables or parameters associated with the adversary are denoted either with a tilde ($\sim$) above the symbol or with a subscript or superscript A, and the notation $\rightarrow$ above a symbol denotes a vector.

II. System Model and Generalized Framework for Sensing Disruption

The spectral range of interest consists of N bands, where some are busy bands occupied by PUs and the rest are vacant bands, not accessed by PUs and available for SUs. The transmissions of PUs are random, so the number of busy bands, $\boldsymbol{N}_P$, and the number of vacant bands, $\boldsymbol{N}_S$, are random, and at any particular instant of time, $\boldsymbol{N}_P = n_P$ and $\boldsymbol{N}_S = n_S$. An SU carries out spectrum sensing within each periodic sensing interval, to determine the spectrum usage status (busy/vacant) of each band. The sensing decision at the SU on the ith band is denoted $\boldsymbol{D}_i$ where $i = 1, 2, \cdots, N$, which equals 1 or 0, indicating the observed band is busy or vacant, respectively. Each sensing interval is followed by a data transmission interval.

The adversary, who is a rival entity of the secondary, makes decisions on the spectral usage status at the start of the sensing interval. During the SU sensing interval, it sends spoofing signals into vacant bands, in order to mislead SU sensing decisions.

With the assumption that the spectral usage information at the adversary is perfect, optimal spoofing under AWGN was shown to be an equal-power, partial-band strategy in [11]. This corresponds to the ideal performance upper bound of adversary spoofing, since its attacking power would not be wasted in any busy bands. However, for a more realistic case, the estimates of which bands are vacant have uncertainties which can result in error decisions on the spectral usage status.

A. Estimation Uncertainties at the Adversary

Let $\boldsymbol{D}_{i,A}$ denote the spectrum usage decision of the adversary on the i-th band, where $i = 1, 2, \cdots, N$ and the subscript A indicates the adversary. $\boldsymbol{D}_{i,A}$ equals 0 or 1, with 0 indicating that the adversary thinks the i-th band is vacant, and 1 indicating that the i-th band is busy. Consequently, within the N spectral bands, there are $\tilde{\boldsymbol{N}}_S$ bands sensed to be vacant by the adversary, and $\tilde{\boldsymbol{N}}_P = N - \tilde{\boldsymbol{N}}_S$ bands sensed to be busy by the adversary. Both $\tilde{\boldsymbol{N}}_S$ and $\tilde{\boldsymbol{N}}_P$ are random variables arising from the estimation uncertainties of $\boldsymbol{D}_{i,A}$. At any particular time, $\tilde{\boldsymbol{N}}_S = \tilde{n}_S$ and $\tilde{\boldsymbol{N}}_P = \tilde{n}_P$, where $\tilde{n}_S$ and $\tilde{n}_P$ are integers within the range $[0, N]$ and $\tilde{n}_P = N - \tilde{n}_S$. Let $\{\tilde{n}_S\}$ and $\{\tilde{n}_P\}$ denote the sets of spectral bands that are sensed by the adversary to be vacant and busy, respectively. For the bands where $i \in \{\tilde{n}_P\}$, $\boldsymbol{D}_{i,A} = 1$, and for $i \in \{\tilde{n}_S\}$, $\boldsymbol{D}_{i,A} = 0$. When the adversary determines that the i-th band is busy, i.e., $\boldsymbol{D}_{i,A} = 1$, the probability that it is actually vacant, denoted by $\tilde{p}_{0,i}^{(1)}$, is given by

$$\begin{aligned}\tilde{p}_{0,i}^{(1)} &\triangleq p\left(H_{0,i}|\boldsymbol{D}_{i,A}=1\right)\\ &= \frac{p(H_{0,i})p_{f,i}^{A}}{p(H_{0,i})p_{f,i}^{A} + p(H_{1,i})p_{d,i}^{A}},\end{aligned} \tag{1}$$

where $H_{0,i}$ represents the event that the i-th band is actually vacant, and $H_{1,i}$ denotes the event that the i-th band is actually busy. Similarly, the probability that the i-th band is actually vacant when the adversary thinks it is vacant, denoted $\tilde{p}_{0,i}^{(0)}$, is

$$\begin{aligned}\tilde{p}_{0,i}^{(0)} &\triangleq p(H_{0,i}|\boldsymbol{D}_{i,A}=0)\\ &= \frac{p(H_{0,i})(1-p_{f,i}^{A})}{p(H_{0,i})(1-p_{f,i}^{A}) + p(H_{1,i})(1-p_{d,i}^{A})}.\end{aligned} \tag{2}$$

Note that when there is no estimation uncertainty at the adversary, $\tilde{p}_{0,i}^{(1)}$ in (1) equals 0 and $\tilde{p}_{0,i}^{(0)}$ in (2) equals 1. Otherwise, both of them fall in the range $(0, 1)$.

B. Motivation for the Proposed Framework

The generalized spoofing framework, incorporating the adversary's estimation uncertainty, originates from maximizing the conditional average number of false detections by the SUs over the actually vacant bands, as described below.

Let $\boldsymbol{D}_i$ $\left(i = 1, 2, \cdots, N\right)$ be variables such that $\boldsymbol{D}_i = 1$ means that the i-th band is determined to be busy by the secondary, while $\boldsymbol{D}_i = 0$ indicates that this band is sensed to be vacant by the secondary. Therefore, the number of bands sensed to be busy by the secondary is the sum of $\boldsymbol{D}_i$ over all i. The expectation of this sum is the average number of bands sensed to be busy by the secondary, N_1, and is given by

$$\begin{aligned}N_1 &= E\Big(\sum\nolimits_{i=1}^{N} \boldsymbol{D}_i\Big)\\ &= \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\Big) + \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{1,i}\Big),\end{aligned} \tag{3}$$

where $H_{0,i}$ and $H_{1,i}$ denote the events that the i-th band is actually vacant and that the i-th band is actually busy, respectively. The two parts composing N_1 in (3), denoted $N_{1,0}$ and $N_{1,1}$, are given by

$$\begin{aligned}N_{1,0} &= \sum\nolimits_{i=1}^{N} p(\boldsymbol{D}_i = 1, H_{0,i})\\ N_{1,1} &= \sum\nolimits_{i=1}^{N} p(\boldsymbol{D}_i = 1, H_{1,i}).\end{aligned} \tag{4}$$

For the i-th band, the probability that it is actually busy is denoted $p\big(H_{1,i}\big)$, and the probability that it is actually vacant is denoted $p\big(H_{0,i}\big)$. There are a total of 2^N different spectrum usage combinations of these N bands. Let $\vec{H}_m = \big(H_{1,m},\ H_{2,m},\ ,\cdots, H_{N,m}\big)$ denote the m-th $(m = 1, 2, \cdots, 2^N)$ spectrum usage status of the total of N bands, where the ith element in the vector $H_{i,m} = 0$ means that the i-th band is vacant, and $H_{i,m} = 1$ indicates that the i-th band is busy $(i = 1, 2, \cdots, N)$. For a given value of m, $\vec{H}_m = \big(H_{1,m},\ H_{2,m},\ ,\cdots, H_{N,m}\big)$ is determined. Specifically, if $H_{i,m} = 0$, then $p\big(H_{1,i}|H_{i,m} = 0\big) = 0$ and $p\big(H_{0,i}|H_{i,m} = 0\big) = 1$. If $H_{i,m} = 1$, then $p\big(H_{1,i}|H_{i,m} = 1\big) = 1$ and $p\big(H_{0,i}|H_{i,m} = 1\big) = 0$.

The probability of this spectrum usage status of the N bands is denoted $p\Big(\vec{H}_m\Big)$, and we have

$$\sum\nolimits_{m=1}^{2^N} p\Big(\vec{H}_m\Big) = 1. \tag{5}$$

In this way, we have

$$\sum_{m=1}^{2^N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\big|\vec{H}_m\Big) p\Big(\vec{H}_m\Big) = p\Big(\boldsymbol{D}_i = 1, H_{0,i}\Big) \tag{6}$$

and

$$\sum_{m=1}^{2^N} p\Big(\boldsymbol{D}_i = 1, H_{1,i}\big|\vec{H}_m\Big) p\Big(\vec{H}_m\Big) = p\Big(\boldsymbol{D}_i = 1, H_{1,i}\Big). \tag{7}$$

Substituting (6) and (7) into (3),

$$\begin{aligned}N_1 = \sum_{m=1}^{2^N} \Bigg\{ &\sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\big|\vec{H}_m\Big) p\Big(\vec{H}_m\Big)\\ &+ \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{1,i}\big|\vec{H}_m\Big) p\Big(\vec{H}_m\Big)\Bigg\}.\end{aligned} \tag{8}$$

The summation $\sum\limits_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\big|\vec{H}_m\Big) p\Big(\vec{H}_m\Big)$ in (8) sums for i from 1 to N, and for each i, the value of $p\Big(\vec{H}_m\Big)$ stays constant. So we can take $p\Big(\vec{H}_m\Big)$ out of the summation, and (8) can be written as

$$\begin{aligned}N_1 = \sum_{m=1}^{2^N} \Bigg\{ &p\Big(\vec{H}_m\Big) \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\Big|\vec{H}_m\Big)\\ &+ p\Big(\vec{H}_m\Big) \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{1,i}\Big|\vec{H}_m\Big)\Bigg\}.\end{aligned} \tag{9}$$

Let

$$\begin{aligned}N_{1,m}^{(0)} &= \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{0,i}\Big|\vec{H}_m\Big)\\ N_{1,m}^{(1)} &= \sum_{i=1}^{N} p\Big(\boldsymbol{D}_i = 1, H_{1,i}\Big|\vec{H}_m\Big).\end{aligned} \tag{10}$$

Substituting (10) into (8),

$$N_1 = \sum_{m=1}^{2^N} \Bigg\{ N_{1,m}^{(0)} p\Big(\vec{H}_m\Big) + N_{1,m}^{(1)} p\Big(\vec{H}_m\Big)\Bigg\}. \tag{11}$$

We next analyze the physical interpretations for $N_{1,m}^{(0)}$ and $N_{1,m}^{(1)}$. At any particular instant of time, there is a particular spectrum usage status. Without loss of generality, we use the notation $\vec{H}_m$ to denote this status, whereby there are $N_{S,m}$ actually vacant bands, and $N_{P,m}$ actually busy bands. That is, $\sum_{i=1}^{N} H_{i,m} = N_{P,m}$ and $N_{S,m} = N - N_{P,m}$. In this way, $N_{1,m}^{(0)}$ from (10) can be further written as

$$\begin{aligned} N_{1,m}^{(0)} &= \sum_{i=1}^{N} p\left(\boldsymbol{D}_i = 1, H_{0,i} \middle| \vec{H}_m\right) \\ &= \sum\nolimits_{i\in\left\{N_{S,m}\right\}} \frac{p\left(\boldsymbol{D}_i = 1, H_{0,i}, \vec{H}_m\right)}{p\left(\vec{H}_m\right)} \\ &\quad + \sum\nolimits_{i\in\left\{N_{P,m}\right\}} \frac{p\left(\boldsymbol{D}_i = 1, H_{0,i}, \vec{H}_m\right)}{p\left(\vec{H}_m\right)}, \end{aligned} \tag{12}$$

where $\left\{N_{S,m}\right\}$ and $\left\{N_{P,m}\right\}$ denote the sets of spectral bands which are actually vacant and actually busy, respectively. For the spectral bands which are actually vacant, i.e., $i \in \left\{N_{S,m}\right\}$, $p\left(H_{0,i}\middle|\vec{H}_m\right) = 1$, and for the bands that are actually busy, i.e., $i \in \left\{N_{P,m}\right\}$, $p\left(H_{0,i}\middle|\vec{H}_m\right) = 0$. Then (12) can be further written as

$$N_{1,m}^{(0)} = \sum\nolimits_{i=1}^{N_{S,m}} p\left(\boldsymbol{D}_i = 1\middle|H_{0,i}, \vec{H}_m\right), \tag{13}$$

which is the average number of false detections within the actually vacant bands for the m-th spectral usage status of the N bands $\vec{H}_m$, where $m = 1, 2, \cdots, 2^N$. Similarly, $N_{1,m}^{(1)}$ in (10) can be written as

$$\begin{aligned} &N_{1,m}^{(1)} \\ &= \sum_{i\in\left\{N_{S,m}\right\}} \frac{p\left(\boldsymbol{D}_i = 1\middle|H_{1,i}, \vec{H}_m\right)p\left(H_{1,i}\middle|\vec{H}_m\right)p\left(\vec{H}_m\right)}{p\left(\vec{H}_m\right)} \\ &\quad + \sum_{i\in\left\{N_{P,m}\right\}} \frac{p\left(\boldsymbol{D}_i=1\middle|H_{1,i}, \vec{H}_m\right)p\left(H_{1,i}\middle|\vec{H}_m\right)p\left(\left\{H_i\right\}_m\right)}{p\left(\vec{H}_m\right)} \\ &= \sum\nolimits_{i=1}^{N_{P,m}} p\left(\boldsymbol{D}_i = 1\middle|H_{1,i}, \vec{H}_m\right), \end{aligned} \tag{14}$$

where for $i \in \left\{N_{S,m}\right\}$: $p\left(H_{1,i}\middle|\vec{H}_m\right) = 0$, and for $i \in \left\{N_{P,m}\right\}$: $p\left(H_{1,i}\middle|\vec{H}_m\right) = 1$. This shows that $N_{1,m}^{(1)}$ is the average number of bands sensed busy by the secondary within those actually busy bands, i.e., $i \in \left\{N_{P,m}\right\}$, given that at this instant of time, the actual spectrum usage status is $\vec{H}_m$. And thus, we have

- N_1 is the average number of bands sensed to be busy by the secondary, averaged over all possible spectral usage status combinations, within which
  - $N_{1,m}^{(0)}$ is the average number of bands sensed busy by the secondary among the actually vacant bands, for a given spectral usage status $\vec{H}_m$, and
  - $N_{1,m}^{(1)}$ is the average number of bands sensed busy by the secondary among the actually busy bands, for a given spectral usage status $\vec{H}_m$.
- N_1 is the sum of $N_{1,m}^{(0)}$ and $N_{1,m}^{(1)}$ averaged over all the spectral usage status, given by

$$N_1 = \sum_{m=1}^{2^N} \left\{ \left(N_{1,m}^{(0)} + N_{1,m}^{(1)}\right) p\left(\vec{H}_m\right) \right\}. \tag{15}$$

- Maximizing $N_{1,m}^{(0)} = \sum_{i=1}^{N} p\left(H_{0,i}\right) p(\boldsymbol{D}_i = 1\middle|H_{0,i})$ is the goal of our proposed algorithm.

C. Generalized Framework for Sensing Disruption

Motivated by the derivations in Section II-B, we propose a generalized framework for sensing disruption. In the framework, estimation uncertainties at the adversary are incorporated. In this section, the formulation of the proposed framework is described.

Consider the probability that a band is vacant, but has been sensed to be busy by a SU, conditioned on the event that the adversary sensed the band to be vacant. This probability can be written as

$$\begin{aligned} &p(\boldsymbol{D}_i = 1, H_{0,i}|\boldsymbol{D}_{i,A} = 0) \\ &\quad = p(H_{0,i}|\boldsymbol{D}_{i,A} = 0)p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0), \end{aligned} \tag{16}$$

Over all the $\tilde{\boldsymbol{N}}_S = \tilde{n}_S$ bands that are sensed to be vacant by the adversary, the sum of the conditional probabilities of false detection at the secondary while the spectral bands are actually vacant, conditioned on $\boldsymbol{D}_{i,A} = 0$ where $i \in \{\tilde{n}_S\}$, and $\tilde{\boldsymbol{N}}_S = \tilde{n}_S$, is given by

$$\begin{aligned} M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} &= \sum_{i=1}^{\tilde{n}_S} p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0) \\ &\qquad\qquad \cdot p(H_{0,i}|\boldsymbol{D}_{i,A} = 0), \end{aligned} \tag{17}$$

where the subscript "0" of $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ indicates the condition that $\boldsymbol{D}_{i,A} = 0$. The superscript $\tilde{\boldsymbol{N}}_S = \tilde{n}_S$ corresponds to the condition that the number of bands $\tilde{\boldsymbol{N}}_S$ that are sensed vacant by the adversary at some particular instant of time is equal to $\tilde{n}_S$.

On the other hand, when the adversary believes the i-th band is busy, it might be actually vacant, and the adversary does not want to miss out on the attacking opportunity if the band is actually vacant. So we create a more general formulation for the adversary to incorporate this band into the optimal attacking strategy. Intuitively, whether to spoof in this band is related to the probability of this band being actually vacant. In this way, the probability of a successful sensing attack, given that the sensed decision at the adversary $\boldsymbol{D}_{i,A} = 1$, can be formulated as the conditional probability that this band is determined to be busy by the secondary when it is actually vacant, conditioned on $\boldsymbol{D}_{i,A} = 1$ at the adversary, which can be expressed as

$$\begin{aligned} &p(\boldsymbol{D}_i = 1, H_{0,i}\middle|\boldsymbol{D}_{i,A} = 1) \\ &\quad = p(\boldsymbol{D}_i = 1\middle|H_{0,i}, \boldsymbol{D}_{i,A} = 1)p(H_{0,i}|\boldsymbol{D}_{i,A} = 1). \end{aligned} \tag{18}$$

Summing this probability over all the $\tilde{\boldsymbol{N}}_P = \tilde{n}_P$ bands that are sensed busy by the adversary, we obtain the sum of the probabilities of false detection at the secondary when these bands are actually vacant, conditioned on $\boldsymbol{D}_{i,A} = 1$, where $i \in \{\tilde{n}_P\}$, and $\tilde{\boldsymbol{N}}_P = \tilde{n}_P$. This is by

$$M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} = \sum_{i=1}^{\tilde{n}_P} p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1) \cdot p(H_{0,i}|\boldsymbol{D}_{i,A} = 1), \quad (19)$$

where the subscript "1" of $M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ indicates the condition that $\boldsymbol{D}_{i,A} = 1$. The superscript $\tilde{\boldsymbol{N}}_P = \tilde{n}_P$ corresponds to the condition that the number of bands $\tilde{\boldsymbol{N}}_P$ that are sensed vacant by the adversary at some particular instant of time is equal to $\tilde{n}_P$.

Spoofing for a power-limited adversary with estimation uncertainty can be formulated as maximizing the secondary's sum of probabilities of false detection when the bands are actually vacant, conditioned on the adversary's sensing estimates $\boldsymbol{D}_{i,A}$ $(i = 1, 2, \cdots, N)$, $\tilde{\boldsymbol{N}}_S = \tilde{n}_S$, with a given power budget A_0, which can be expressed as

$$\begin{aligned} \max \ & \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0) \\ & + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1) \\ \textit{s.t.} \ & \sum_{i=1}^{\tilde{n}_S} a_{i,J}^{(0)} + \sum_{i=1}^{\tilde{n}_P} a_{i,J}^{(1)} \leq A_0 \\ & a_{i,J}^{(0)} \geq 0, \quad i \in \{\tilde{n}_S\} \text{ and } a_{i,J}^{(1)} \geq 0, \ i \in \{\tilde{n}_P\}, \end{aligned} \quad (20)$$

where $a_{i,J}^{(0)}$ denotes the spoofing power the adversary allocates in the i-th band for $i \in \{\tilde{n}_S\}$, and $a_{i,J}^{(1)}$ represents the spoofing power the adversary distributes in the i-th band for $i \in \{\tilde{n}_P\}$.

III. Problem Formulation and Proposed Sub-Optimal Solution

To obtain the optimal spoofing strategy of the adversary, the key task is to relate $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ and $M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ to the adversary's attacking parameters, i.e., spoofing power in each band and sensing capabilities including the probability of false alarm and the probability of detection.

A. Spectrum Sensing at the Secondary

Under $H_{0,i}$ in the i-th band, i.e., the primary signal is absent, the received signal at the SU is

$$r_{i,S}(t) = w_{i,S}(t) + hj_i(t), \quad (21)$$

where $w_{i,S}(t)$ is additive Gaussian noise in the i-th band with zero mean and variance σ_n^2. It is assumed that the thermal noise is identical across all bands. The spoofing signal emitted by the adversary in the i-th band is $j_i(t)$, which is assumed to be Gaussian distributed with zero mean, and hence its variance equals the spoofing power the adversary puts in this band. The path loss factor between the adversary and the SU in the i-th band is denoted h, assumed constant across all bands.

The expression in (21) incorporates cases where the spoofing power of the adversary is either present or absent in the i-th band. When the adversary chooses not to spoof in this band, $\boldsymbol{A}_{i,J}$ is equal to zero; otherwise, $\boldsymbol{A}_{i,J}$ is a positive value and not larger than the adversary's spoofing power budget A_0.

Further, the decisions at the adversary on the spectrum usage status $\boldsymbol{D}_{i,A}$ $(i = 1, 2, \cdots, N)$ are random. Accordingly, the corresponding spoofing power allocations in each band $\boldsymbol{A}_{i,J}$ $(i = 1, 2, \cdots, N)$ are random, due to the random characteristics of the measurements. At any particular instant of time, measurements are obtained by the adversary, and we let $a_{i,J}$ denote the spoofing power $\boldsymbol{A}_{i,J}$ at this time, i.e., $\boldsymbol{A}_{i,J} = a_{i,J}$. Specifically, for the i-th band that is sensed to be busy by the adversary, i.e., $\boldsymbol{D}_{i,A} = 1$, we use the notation $\boldsymbol{A}_{i,J}^{(1)} = a_{i,J}^{(1)}$ to denote the spoofing power the adversary puts in it. Similarly, for the i-th band when $\boldsymbol{D}_{i,A} = 0$, $\boldsymbol{A}_{i,J}^{(0)} = a_{i,J}^{(0)}$ denotes the spoofing power the adversary allocates to it.

B. Problem Formulation

From Section III-A, the received signal model can be written in the same form given in (21), regardless of whether $\boldsymbol{D}_{i,A}$ is equal to 0 or 1. Letting $a_{i,J}^{(0)}$ denote the spoofing power that the adversary intends to allocate to the bands where $\boldsymbol{D}_{i,A} = 0$, and following the same procedures as in [11] and [32], we obtain

$$p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0) \approx Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\right), \quad (22)$$

where $Q(\cdot)$ is the Gaussian tail function, TW is the integration-time-bandwidth product, and K is the detection threshold at the SU's receiver.

Similarly, let $a_{i,J}^{(1)}$ denote the spoofing power that the adversary intends to allocate to the bands where $\boldsymbol{D}_{i,A} = 1$, so that $p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1)$ is approximately given by

$$p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1) \approx Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\right). \quad (23)$$

And hence, (20) can be further formulated as

$$\begin{aligned} \max \ & \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\right) \\ & + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\right) \\ \textit{s.t.} \ & \sum_{i=1}^{\tilde{n}_S} a_{i,J}^{(0)} + \sum_{i=1}^{\tilde{n}_P} a_{i,J}^{(1)} \leq A_0 \\ & a_{i,J}^{(0)} \geq 0, i \in \{\tilde{n}_S\} \text{ and } a_{i,J}^{(1)} \geq 0, i \in \{\tilde{n}_P\}. \end{aligned} \quad (24)$$

C. Proposed Sub-Optimal Solution

This optimization is nonlinear and nonconvex. However, $\tilde{p}_{0,i}^{(0)}$ is identical for all $i \in \{\tilde{n}_S\}$, and $\tilde{p}_{0,i}^{(1)}$ is identical for all $i \in \{\tilde{n}_P\}$, where we assume that the probability of false alarm $p_{f,i}^A$ and the probability of detection $p_{d,i}^A$ at the adversary are identical across the bands. We also assume that the a priori probabilities of $H_{0,i}$ and $H_{1,i}$ are independent of i. In this way, if we only focus on maximizing either $M_{J,0}^{\tilde{N}_S=\tilde{n}_S}$ or $M_{J,1}^{\tilde{N}_P=\tilde{n}_P}$, then the optimal spoofing power allocation can be directly obtained by using the algorithm derived in [11]. For brevity, we call this algorithm *perfect spoofing*, where the adversary is assumed to have perfect knowledge of the spectral usage status. Specifically, let $V = \left(TW + \sqrt{(TW)^2 + 8TW}\right)\sigma_n^2$. When $V \geq K$, the perfect spoofing strategy corresponds to equal-power, full-band spoofing. When $V < K$, the perfect spoofing strategy is equal-power, partial-band spoofing. The optimal number of spoofed bands equals either $\lceil x^* \rceil$ or $\lfloor x^* \rfloor$, where $\lceil\cdot\rceil$ and $\lfloor\cdot\rfloor$ represent ceiling and floor operations respectively, and x^* satisfies

$$\frac{bx^* A_0}{\sqrt{2\pi}(A_0 + x^*\sigma_n^2)^2} \exp\left(-\left(\frac{bx^*}{A_0 + x^*\sigma_n^2} + d\right)^2 / 2\right) + Q\left(\frac{bx^*}{A_0 + x^*\sigma_n^2} + d\right) = p_f, \quad (25)$$

where $b = K/2\sqrt{TW}$, $d = -\sqrt{TW}$, and p_f represents the probability of false alarm at the secondary in the absence of spoofing.

However, our objective is to maximize $M_{J,0}^{\tilde{N}_S=\tilde{n}_S} + M_{J,1}^{\tilde{N}_P=\tilde{n}_P}$, which is nonlinear and nonconvex. Considering that the values of $\tilde{p}_{0,i}^{(0)}$ and $\tilde{p}_{0,i}^{(1)}$ are typically not equal, the equal-power, partial-band strategy would no longer be the optimal solution for the problem in this paper. On the other hand, no matter what the optimal spoofing power allocation strategy is, there would be a portion of the total power budget assigned to the $\tilde{n}_S$ spectral bands, with the rest assigned to the $\tilde{n}_P$ bands. Using this characteristic of the objective function, we propose a sub-optimal algorithm for spoofing with estimation uncertainty:

Step 1: Assign a specific portion ρ $(0 \leqslant \rho \leqslant 1)$ of the power budget A_0 to $M_{J,0}^{\tilde{N}_S=\tilde{n}_S}$, and consequently, the remaining power $(1-\rho)A_0$ is allocated to $M_{J,1}^{\tilde{N}_P=\tilde{n}_P}$.

Step 2: With a power budget ρA_0 for the $\tilde{n}_S$ sensed vacant bands, obtain the spoofing strategy via the perfect spoofing algorithm. Similarly, with a power budget $(1-\rho)A_0$ for the $\tilde{n}_P$ sensed busy bands, calculate the spoofing via the perfect spoofing algorithm.

Step 3: Maximize the objective function by varying ρ from 0 to 1 in discrete steps.

D. Intelligent Transition for Different Scenarios

In this section, we will show that the proposed framework provides an intelligent transition for the adversary to spoof under different scenarios.

1) When the Adversary Has Perfect Information: When the adversary has perfect knowledge of which bands are vacant and which bands are busy, $p_{d,i}^A = 1$ and $p_{f,i}^A = 0$. Then we have

$$\tilde{p}_{0,i}^{(1)} = 0 \quad \text{and} \quad \tilde{p}_{0,i}^{(0)} = 1. \quad (26)$$

In this case, the sensed vacant bands by the adversary are the actually vacant bands. That is, $\tilde{n}_S = n_S$. Substituting (26) into (20), the formulation of the proposed spoofing reduces to

$$\begin{aligned} \max \ & \sum_{i=1}^{n_S} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\right) \\ \textit{s.t.} \ & \sum_{i=1}^{n_S} a_{i,J}^{(0)} \leq A_0 \\ & a_{i,J}^{(0)} \geq 0, \quad i \in \{n_S\}, \end{aligned} \quad (27)$$

where $\{n_S\}$ denotes the set of actually vacant bands. Note that (27) is identical with the formulation for the optimal sensing disruption in [11]. In other words, optimal spoofing when the adversary has perfect spectral information is a special case of the proposed framework.

2) When the Spectrum Is Fully Loaded: When the spectrum is fully loaded, $p(H_{0,i}) = 0$ and $p(H_{1,i}) = 1$, and we have

$$\tilde{p}_{0,i}^{(1)} = 0 \quad \text{and} \quad \tilde{p}_{0,i}^{(0)} = 0. \quad (28)$$

Then the objective in (20) becomes

$$\sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\right) + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\right) = 0. \quad (29)$$

That is, no matter what spoofing power the adversary puts in each band, the objective is always constant and equal to 0. In this case, the best option for the adversary is not to spoof. This is reasonable, because when the spectrum is fully loaded, there is no vacant band for the secondary to access.

3) When the Spectrum Is Totally Vacant: When the spectrum is totally vacant, $p(H_{0,i}) = 1$ and $p(H_{1,i}) = 0$. Then we have $\tilde{p}_{0,i}^{(1)} = \frac{p_{f,i}^A}{p_{f,i}^A} = 1$ and $\tilde{p}_{0,i}^{(0)} = \frac{1 - p_{f,i}^A}{1 - p_{f,i}^A} = 1$. The objective in (20) becomes

$$\begin{aligned} & \sum\nolimits_{i=1}^{\tilde{n}_S} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\right) \\ & \quad + \sum\nolimits_{i=1}^{\tilde{n}_P} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\right) \\ & \quad = \sum\nolimits_{i=1}^{N} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J} + \sigma_n^2)} - \sqrt{TW}\right), \end{aligned} \quad (30)$$

where $a_{i,J} = a_{i,J}^{(0)}$ for $i \in \{\tilde{n}_S\}$ and $a_{i,J} = a_{i,J}^{(1)}$ for $i \in \{\tilde{n}_P\}$. We can see from (30) that when all the spectral bands are actually vacant, the proposed algorithm for the adversary is to treat all the spectral bands identically, no matter whether the sensed decision at the adversary is 0 or 1.

We can see that the proposed framework provides an intelligent transition for the adversary to spoof under different scenarios.

IV. Performance Analysis

We use the performance criterion “conditional average number of SU false detections N_J, conditioned on the number of actually vacant bands $\boldsymbol{N}_S = n_S$,” to evaluate the performance. We use the expression “conditional average number of SU false detections N_J” for brevity hereafter. N_J corresponds to the conditional average number of actually vacant bands that are falsely determined to be busy by the secondary, conditioned on the spectrum occupancy status at this particular instant of time. It is given by

$$N_J = \sum_{i \in \{n_S\}} p(\boldsymbol{D}_i = 1 | H_{0,i}), \tag{31}$$

where $\boldsymbol{N}_S = n_S$ is the number of actually vacant spectral bands at this instant of time, and $\{n_S\}$ denotes the set of spectral bands which are actually vacant.

At a particular instant of time, we use $\tilde{\mathbf{D}}^{(t)}$ to denote the measurement set at the adversary, that is $\tilde{\mathbf{D}}^{(t)} = (\tilde{D}^{(t)}_{1,A} = \delta_1, \tilde{D}^{(t)}_{2,A} = \delta_2, \cdots, \tilde{D}^{(t)}_{N,A} = \delta_N)$, where $\delta_i \in \{0, 1\}$ and $i = 1, 2, ..., N$. The superscript t denotes each different measurement set at the adversary. Since there are N spectral bands, there are 2^N different possible measurement sets $\tilde{\mathbf{D}}^{(t)}$ on the spectral usage status. Accordingly, $t = 1, 2, \cdots, 2^N$.

Based on a given measurement set $\tilde{\mathbf{D}}^{(t=t_0)}$, the adversary carries out the proposed optimization given in (10), and obtains the spoofing power allocation $\mathbf{A}^{(t=t_0)}_J = (A^{(t=t_0)}_{1,J} = a_{1,J}, \cdots, \boldsymbol{A}^{(t=t_0)}_{i,J} = a_{i,J}, ..., A^{(t=t_0)}_{N,J} = a_{N,J})$. For brevity, we use $\boldsymbol{A}^{(t=t_0)}_{i,J} = a_{i,J}$ to denote the spoofing power in the i-th spectral band corresponding to the $t = t_0$ measurement set at the adversary $\tilde{\mathbf{D}}^{(t=t_0)}$, where $i = 1, 2, \cdots, N$.

The conditional average number of false detections at the secondary over the actually vacant bands, conditioned on the number of actually vacant bands $\boldsymbol{N}_S$, the particular measurement set $\tilde{\mathbf{D}}^{(t=t_0)}$ and corresponding spoofing power $\mathbf{A}^{(t=t_0)}_J$ by the adversary, can be calculated as

$$N_J^{\tilde{\mathbf{D}}^{(t=t_0)}, \mathbf{A}_J^{(t=t_0)}} = \sum_{i \in \{n_S\}} p(\boldsymbol{D}_i = 1 | H_{0,i}, \tilde{\mathbf{D}}^{(t=t_0)}, \mathbf{A}_J^{(t=t_0)}). \tag{32}$$

Due to estimation uncertainties, there are a total of 2^N different measurement sets by the adversary. Accordingly, there are 2^N spoofing power allocations. When the adversary’s measurement set $\tilde{\mathbf{D}}^{(t=t_0)}$ is determined, the corresponding spoofing power allocation $\mathbf{A}^{(t=t_0)}_J$ is determined, through solving the optimization in (20). In this way, $\mathbf{A}^{(t=t_0)}_J$ can be taken as a function of $\tilde{\mathbf{D}}^{(t=t_0)}$, i.e., $\mathbf{A}^{(t=t_0)}_J = f(\tilde{\mathbf{D}}^{(t=t_0)})$. Then we have $p(\mathbf{A}^{(t=t_0)}_J | \tilde{\mathbf{D}}^{(t=t_0)}) = 1$.

The conditional average number of false detections at the secondary, averaged over all possible measurements and corresponding spoofing power allocations at the adversary, is given by

$$N_J = \sum_{t_0=1}^{2^N} \sum_{\{\mathbf{A}_J^{(t=t_0)}\}} N_J^{\tilde{\mathbf{D}}^{(t=t_0)}, \mathbf{A}_J^{(t=t_0)}} \times p(\tilde{\mathbf{D}}^{(t=t_0)}) p(\mathbf{A}_J^{(t=t_0)} | \tilde{\mathbf{D}}^{(t=t_0)}), \tag{33}$$

where $p(\tilde{\mathbf{D}}^{(t=t_0)})$ is the probability that the adversary’s measurement set is $\tilde{\mathbf{D}}^{(t=t_0)}$. For example, for the case where there are i actually vacant bands sensed to be busy by the adversary, and there are j actually busy bands sensed to be vacant by the adversary, this probability can be calculated by

$$\binom{n_S}{i} \left(1 - p_f^A\right)^{(n_S - i)} \left(p_f^A\right)^i \cdot \binom{N - n_S}{j} \left(1 - p_d^A\right)^j \left(p_d^A\right)^{N - n_S - j}, \tag{34}$$

where n_S is the number of actually vacant bands at this time, and p_f^A and p_d^A denote the probability of false alarm and the probability of detection at the adversary.

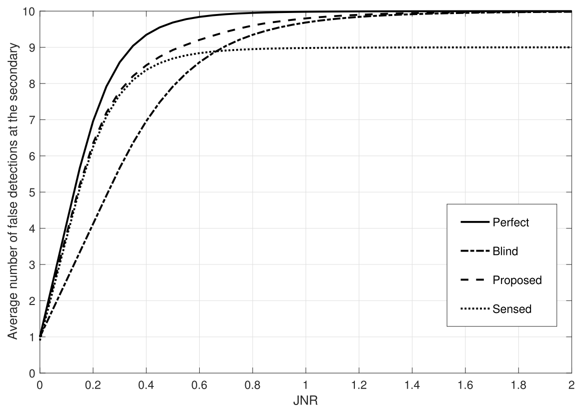

Fig. 1. Average number of false detections versus JNR, where $N = 20$ and $\boldsymbol{N}_S = 10$.

V. Numerical Results

Based on the calculations for N_J from (31) to (33), we generate numerical results for performance analysis of the proposed algorithm, as well as comparisons with these three conventional algorithms:

1) Perfect Algorithm: the adversary is assumed to know perfectly the actual spectral usage status. This algorithm provides an upper bound for the sensing disruption performance of the adversary.
2) Sensed Algorithm: The adversary only spoofs the bands it has sensed to be vacant.
3) Blind Algorithm: The adversary considers all the spectral bands to be vacant, and uses the procedure from [11] to determine the percentage of bands to be spoofed. Note that the above procedure was optimal in [11], because the adversary knows with certainty which bands were vacant. However, in this baseline algorithm, the adversary has no knowledge as to which bands are vacant.

A. Performance Comparisons

The average number of SU false detections with different values of spoofing power budget is plotted in Fig.1, where the spoofing power budget is measured in terms of the jamming to noise ratio $JNR = A_0/N\sigma_n^2$ in each band. The total number of spectral bands $N = 20$, and there are $\boldsymbol{N}_S = 10$ actually vacant bands. The SU threshold for determining whether the

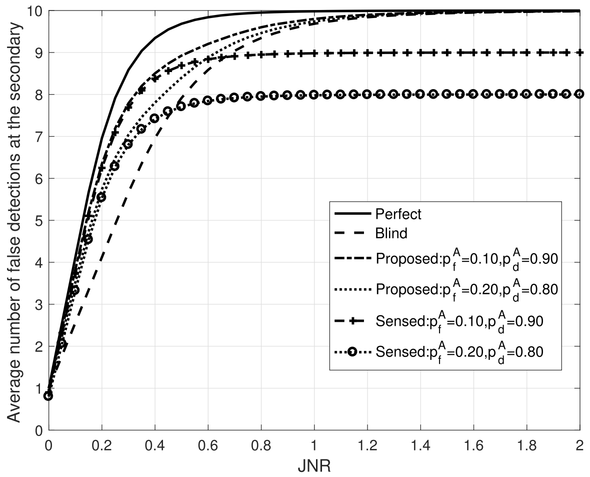

Fig. 2. Average number of false detections versus JNR, where $N = 20$ and $\boldsymbol{N}_S = 10$.

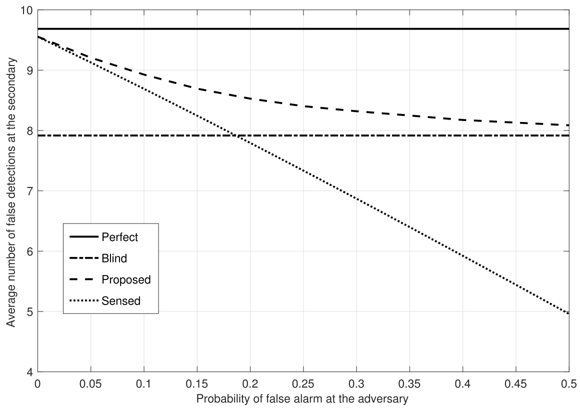

Fig. 3. Average number of SU false detections vs. probability of false alarm at the adversary, where $N = 20$, $\boldsymbol{N}_S = 10$, and $JNR = 0.50$.

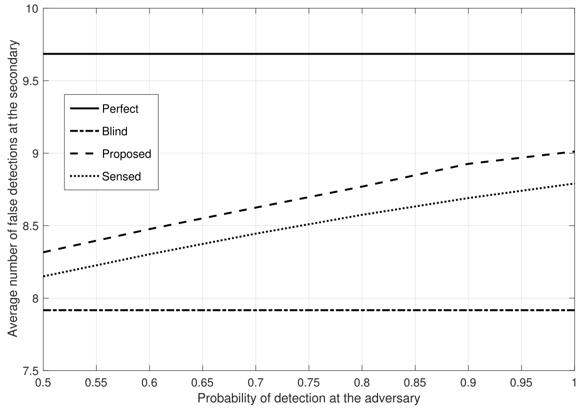

Fig. 4. Average number of SU false detections vs. probability of detection at the adversary, where $N = 20$, $\boldsymbol{N}_S = 10$, and $JNR = 0.50$.

observed band is vacant is chosen such that, in the absence of spoofing, its probability of false alarm is 0.10. For the adversary, $p_f^A = 0.10$ and $p_d^A = 0.90$.

In Fig.1, for any spoofing power, the average number of false detections for the proposed algorithm is always larger than those of the sensed and blind algorithms, and asymptotically approaches that of the perfect algorithm. When JNR is above approximately 0.70, the blind algorithm outperforms the sensed algorithm. This is because the sensed algorithm only attacks the sensed vacant spectral bands, but some of the actually vacant bands are misidentified. When the spoofing power is not large, it is better for the adversary to attack only the sensed vacant bands rather than spreading its power over all the spectral bands. However, when the spoofing power is large enough, it should spread its power across all the spectral bands to affect the ones misidentified as busy, since the spoofing power allocated in each band is still large enough to make the sensing attack successful.

Both the proposed and blind algorithms asymptotically approach the performance upper bound as the spoofing power increases. In contrast, the average number of false detections of the sensed algorithm first increases as the spoofing power increases, but beyond a certain point, it saturates to a constant. This is because neither the proposed algorithm nor the blind algorithm limits its attack within the sensed vacant bands, while the sensed algorithm only disrupts the sensed vacant ones. As a result, there would be a certain number of actually vacant bands not being spoofed.

The effects of the adversary's different sensing capabilities are illustrated in Fig.2. When the sensing capability of the adversary decreases, e.g., from $p_f^A = 0.10, p_d^A = 0.90$ to $p_f^A = 0.20, p_d^A = 0.80$, for the same value of the spoofing power, the average number of SU false detections decreases for both the proposed and sensed algorithms because there is a lower probability of hitting the actually vacant bands by the adversary. That is, the sensed algorithm is less effective than our proposed algorithm. Also, note that, under different sensing capabilities, the proposed algorithm asymptotically approaches the performance upper bound as the spoofing power increases, while the average number of SU false detections saturates to a much lower level for the sensed algorithm.

B. Attacking Performance With Varying Probabilities of False Alarm and Detection

The average number of SU false detections versus p_f^A is plotted in Fig.3, where $p_d^A = 0.90$. As p_f^A increases, the average number of SU false detections for both the proposed and sensed algorithms decreases, while the average number of false detections for the perfect and blind algorithms stays constant. This is because neither the perfect nor the blind algorithm relies on the adversary's usage measurements. On the other hand, when p_f^A increases, more actually vacant bands are mistakenly determined to be busy by the adversary, leading to a lower chance for the adversary to hit the actually vacant bands. As a result, the average number of false detections for either the proposed or the sensed algorithm decreases. However, the average number of SU false detections is always larger for the proposed algorithm than for the sensed algorithm and the gap increases with p_f^A.

In Fig.4, we observe how the average number of false detections varies with p_d^A, when $p_f^A = 0.10$. When p_d^A increases, the average number of SU false detections for both the proposed and sensed algorithms increases because

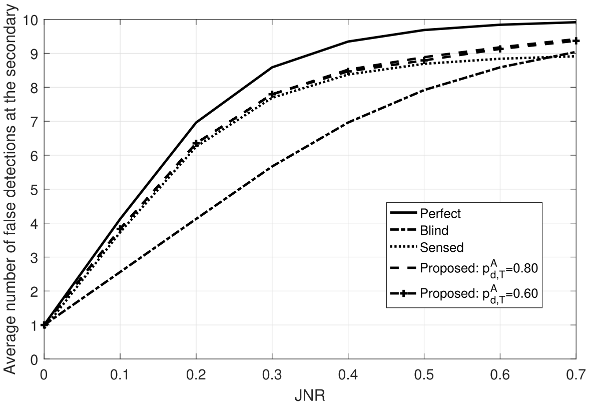

Fig. 5. Average number of false detections at the secondary versus JNR, where $N = 20$, $\boldsymbol{N}_S = 10$, $p_f^A = 0.10$, and $p_d^A = 0.90$.

the chance that the adversary spoofs actually vacant bands increases. The proposed algorithm always outperforms the sensed algorithm.

C. Sensitivity Analysis

In this section, we analyze how the performance varies for the proposed algorithm when the actual probability of detection at the adversary is p_d^A, and the adversary thinks its probability of detection is $p_{d,T}^A$.

In Fig.5, the average number of false detections at the secondary is plotted. Here, $p_f^A = 0.10$. We consider the cases when the adversary thinks its probability of detection is 0.60 or 0.80, while its actual probability of detection is 0.90. The average number of SU false detections of the proposed algorithm is higher than that of the sensed and blind algorithms. There is no significant performance degradation for these cases because, as shown in Appendix A, $\tilde{p}_{0,i}^{(0)} \geq \tilde{p}_{0,i}^{(1)}$. That is, the weight of the optimization for the sensed vacant bands is always larger than the weight for the sensed busy bands. Accordingly, the adversary favors the sensed vacant bands. Furthermore, when the spoofing power is small enough (small enough will be defined in Appendix B), then the adversary only spoofs the sensed vacant bands. On the other hand, when the spoofing power is large enough, then the adversary should allocate a certain portion ρ of its power budget to the sensed vacant bands, and the remaining portion $1 - \rho$ of the spoofing power budget to the sensed busy bands. We will show in Appendix C that the adversary favors the sensed vacant bands, that is, the parameter ρ is approximately no smaller than the ratio $\dfrac{\tilde{n}_S}{\tilde{n}_S + \tilde{n}_P}$.

VI. Conclusions and Future Work

This paper presented a generalized framework for a power limited adversary. It can be applied for either the case where the adversary has perfect knowledge of the spectral usage status or the scenario where the adversary's estimates of spectral usage have uncertainties. The framework utilizes the conditional probability that, given the adversary's sensing results, the spectral band of interest is actually vacant. The sensing disruption strategy obtained under this framework maximizes the sum of conditional probabilities of false detection at the secondary, conditioned on the spectral usage status estimates at the adversary, with the constraint that the adversary has a limited power budget. Results show that, by utilizing the proposed sensing disruption, the adversary can achieve better performance than conventional algorithms. Our future work will extend this formulation to both the sensing and the data transmission durations of a cognitive radio network, and investigate optimal spoofing given cooperative spectrum sensing.

Appendix A
Proof of the Relation Between $\tilde{p}_{0,i}^{(0)}$ and $\tilde{p}_{0,i}^{(1)}$

Lemma 1: Given that

$$\begin{aligned}\tilde{p}_{0,i}^{(0)} &= p(H_{0,i}|\boldsymbol{D}_{i,A} = 0)\\ &= \frac{p(H_{0,i})(1 - p_{f,i}^A)}{p(H_{0,i})(1 - p_{f,i}^A) + p(H_{1,i})(1 - p_{d,i}^A)} \qquad \text{(A-1)}\\ \tilde{p}_{0,i}^{(1)} &= p(H_{0,i}|\boldsymbol{D}_{i,A} = 1)\\ &= \frac{p(H_{0,i})p_{f,i}^A}{p(H_{0,i})p_{f,i}^A + p(H_{1,i})p_{d,i}^A} \qquad \text{(A-2)}\end{aligned}$$

the following relationship holds:

$$\tilde{p}_{0,i}^{(0)} \geq \tilde{p}_{0,i}^{(1)}. \qquad \text{(A-3)}$$

Specifically,

$$\begin{cases} 0 < p(H_{0,i}) < 1: & \tilde{p}_{0,i}^{(0)} > \tilde{p}_{0,i}^{(1)} \\ p(H_{1,i}) = 0 \text{ or } p(H_{1,i}) = 1: & \tilde{p}_{0,i}^{(0)} = \tilde{p}_{0,i}^{(1)}, \end{cases} \qquad \text{(A-4)}$$

where $p_{d,i}^A$ and $p_{f,i}^A > 0$ denote the probability of detection at the adversary and the probability of false alarm at the adversary, respectively, and we have $p_{d,i}^A > p_{f,i}^A$.

Proof:

Case 1: When $0 < p(H_{1,i}) < 1$.

Multiplying $p(H_{1,i})$ on both sides of the inequality $p_{d,i}^A > p_{f,i}^A$, and subtracting $p(H_{1,i})p_{d,i}^A p_{f,i}^A$ on both sides and regrouping terms, we have

$$p(H_{1,i})p_{d,i}^A(1 - p_{f,i}^A) > p(H_{1,i})p_{f,i}^A(1 - p_{d,i}^A). \qquad \text{(A-5)}$$

Adding $p(H_{0,i})p_{f,i}^A(1 - p_{f,i}^A)$ on both sides of (A-5), we have

$$\begin{aligned}&\big(1 - p_{f,i}^A(p(H_{1,i})p_{d,i}^A + p(H_{0,i})p_{f,i}^A\big)\\ &\quad > p_{f,i}^A\big(p(H_{1,i})(1 - p_{d,i}^A) + p(H_{0,i})(1 - p_{f,i}^A)\big). \qquad \text{(A-6)}\end{aligned}$$

Since $0 < p(H_{0,i}) < 1$, $0 < p(H_{1,i}) < 1$, we have $p(H_{1,i})p_{d,i}^A + p(H_{0,i})p_{f,i}^A > 0$ and $p(H_{1,i})(1 - p_{d,i}^A) + p(H_{0,i})(1 - p_{f,i}^A) > 0$. Then (A-6) can be written as

$$\begin{aligned}&\frac{p(H_{0,i})(1 - p_{f,i}^A)}{p(H_{1,i})(1 - p_{d,i}^A) + p(H_{0,i})(1 - p_{f,i}^A)}\\ &\qquad > \frac{p(H_{0,i})p_{f,i}^A}{p(H_{1,i})p_{d,i}^A + p(H_{0,i})p_{f,i}^A}. \qquad \text{(A-7)}\end{aligned}$$

Substituting (A-2) and (A-2), we obtain

$$\tilde{p}_{0,i}^{(0)} > \tilde{p}_{0,i}^{(1)}. \qquad \text{(A-8)}$$

Case 2: When $p(H_{1,i}) = 0$.

When $p(H_{1,i}) = 0$, we have $p(H_{0,i}) = 1$. Substituting the equalities into (A-2) and (A-2),

$$\tilde{p}_{0,i}^{(0)} = \frac{p(H_{0,i})(1-p_{f,i}^{A})}{p(H_{0,i})(1-p_{f,i}^{A})+p(H_{1,i})(1-p_{d,i}^{A})} = \frac{p(H_{0,i})(1-p_{f,i}^{A})}{p(H_{0,i})(1-p_{f,i}^{A})} = 1 \tag{A-9}$$

and

$$\tilde{p}_{0,i}^{(1)} = \frac{p(H_{0,i})p_{f,i}^{A}}{p(H_{0,i})p_{f,i}^{A}} = 1. \tag{A-10}$$

Comparing (A-9) and (A-10), we have

$$\tilde{p}_{0,i}^{(0)} = \tilde{p}_{0,i}^{(1)}. \tag{A-11}$$

Case 3: When $p(H_{1,i}) = 1$.

When $p(H_{1,i}) = 1$, we have $p(H_{0,i}) = 0$. Substituting the equalities into (A-2) and (A-2),

$$\tilde{p}_{0,i}^{(0)} = \frac{p(H_{0,i})(1-p_{f,i}^{A})}{p(H_{0,i})(1-p_{f,i}^{A})+p(H_{1,i})(1-p_{d,i}^{A})} = 0 \tag{A-12}$$

and

$$\tilde{p}_{0,i}^{(1)} = \frac{p(H_{0,i})p_{f,i}^{A}}{p(H_{0,i})p_{f,i}^{A}+p(H_{1,i})p_{d,i}^{A}} = 0. \tag{A-13}$$

Comparing (A-12) and (A-13), we have

$$\tilde{p}_{0,i}^{(0)} = \tilde{p}_{0,i}^{(1)}. \tag{A-14}$$

■

Appendix B
Proof of Lemma 2

Lemma 2: For a particular instant of time, there are $\tilde{n}_S$ bands sensed to be vacant and $\tilde{n}_P$ bands sensed to be busy by the adversary. When the adversary's spoofing power budget A_0 is small enough that $A_0 \leq c^* \cdot min(\tilde{n}_S, \tilde{n}_P)$, where c^* satisfies the following equation

$$Q\Big(\frac{K}{2\sqrt{TW}\big(c^*+\sigma_n^2\big)} - \sqrt{TW}\Big) - \frac{c^* K}{2\sqrt{2\pi TW}\Big(c^*+\sigma_n^2\Big)^2} \cdot \exp\left(-\frac{1}{2}\left(\frac{K}{2\sqrt{TW}\big(c^*+\sigma_n^2\big)} - \sqrt{TW}\right)^2\right) = p_f, \tag{B-1}$$

the optimal spoofing strategy for the adversary is to spoof only the sensed vacant bands.

Proof: Recall that the spoofing strategy for the adversary is to maximize $N_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}+N_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$. When the primary signal is absent, the received signal $r_{i,S}(t)$ at the SU can be written as,

$$r_{i,S}(t) = w_{i,S}(t) + hj_i(t), \tag{B-2}$$

where h is set to unity.

Letting $a_{i,J}^{(0)}$ denote the spoofing power that the adversary intends to allocate to the bands where $\boldsymbol{D}_{i,A} = 0$, and following the same procedures as in [32], $p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0)$ is approximately given by

$$p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 0) \approx Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)}+\sigma_n^2)} - \sqrt{TW}\right), \tag{B-3}$$

where TW is the integration-time-bandwidth product, and K is the detection threshold at the SU's receiver.

Similarly, let $a_{i,J}^{(1)}$ denote the spoofing power that the adversary intends to put for the bands where $\boldsymbol{D}_{i,A} = 1$, so that $p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1)$ is approximately given by

$$p(\boldsymbol{D}_i = 1|H_{0,i}, \boldsymbol{D}_{i,A} = 1) \approx Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)}+\sigma_n^2)} - \sqrt{TW}\right). \tag{B-4}$$

Therefore, the objective of the optimization $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} + M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ can be expressed as

$$\begin{aligned} M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} + M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} &= \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} p(\boldsymbol{D}_i = 1|\boldsymbol{D}_{i,A} = 0) \\ &\quad + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} p(\boldsymbol{D}_i = 1|\boldsymbol{D}_{i,A} = 1) \\ &\approx \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)}+\sigma_n^2)} - \sqrt{TW}\right) \\ &\quad + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)}+\sigma_n^2)} - \sqrt{TW}\right). \end{aligned} \tag{B-5}$$

To solve the optimization problem, we proposed a sub-optimal algorithm in Section III, where ρA_0 $(0 \leqslant \rho \leqslant 1)$ spoofing power is allocated to $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$, which is

$$M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} = \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)}+\sigma_n^2)} - \sqrt{TW}\right), \tag{B-6}$$

and $(1-\rho)A_0$ spoofing power $(0 \leqslant \rho \leqslant 1)$ is allocated to $M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$, which is

$$N_{J,0}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} = \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)}+\sigma_n^2)} - \sqrt{TW}\right). \tag{B-7}$$

Recall in Section III-C that, to obtain the sub-optimal solution for the proposed algorithm as well as a theoretical analysis of the proposed algorithm, we assume $p_{f,i}^{A}$ is identical across the bands. Similarly, we assume that $p_{d,i}^{A}$ is identical across these bands. We also assume that the a priori probabilities of $H_{0,i}$ and $H_{1,i}$ are independent of i. In this case, for the sensed vacant bands by the adversary where $\boldsymbol{D}_{i,A} = 0$, the probability that this band is actually vacant, $\tilde{p}_{0,i}^{(0)} = p\big(H_{0,i}\big|\boldsymbol{D}_{i,A}=0\big)$, is identical, since

$$\tilde{p}_{0,i}^{(0)} = \frac{(1-p_{f,i}^{A})p(H_{0,i})}{(1-p_{f,i}^{A})p(H_{0,i}) + (1-p_{d,i}^{A})p(H_{1,i})}. \quad \text{(B-8)}$$

Similarly, for the sensed busy bands by the adversary where $\boldsymbol{D}_{i,A}=1$, the probability that this band is actually vacant, $\tilde{p}_{0,i}^{(1)} = p\big(H_{0,i}\big|\boldsymbol{D}_{i,A}=1\big)$, is identical, since

$$\tilde{p}_{0,i}^{(1)} = \frac{p_{f,i}^{A}p(H_{0,i})}{p_{f,i}^{A}p(H_{0,i}) + p_{d,i}^{A}p(H_{1,i})}. \quad \text{(B-9)}$$

In this case, $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ in (B-6) can be further written as

$$M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} = \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(0)} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)}+\sigma_n^2)} - \sqrt{TW}\right), \quad \text{(B-10)}$$

where the total spoofing power budget for these $\tilde{n}_S$ bands is ρA_0. It can be seen from (B-10) that maximizing $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ with spoofing power budget ρA_0 is equivalent to

$$\begin{aligned} \max \quad & \sum_{i=1}^{\tilde{n}_S} Q\left(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)}+\sigma_n^2)} - \sqrt{TW}\right) \\ s.t. \quad & \sum_{i=1}^{\tilde{n}_S} a_{i,J}^{(0)} = \rho A_0 \\ & a_{i,J}^{(0)} \geqslant 0, \quad i=1,\cdots,\tilde{n}_S. \end{aligned} \quad \text{(B-11)}$$

It was shown in [11] that the optimal strategy for the adversary under the scenario in (B-11) is equal-power, partial-band spoofing. Further, in the case considered for Lemma 2, the spoofing power budget A_0 is not large enough to spoof all the $\tilde{n}_S$ sensed vacant bands and the $\tilde{n}_P$ sensed busy bands simultaneously. That is, for this scenario, the optimal number n_0^* of bands that the adversary should spoof with the power budget ρA_0 within the $\tilde{n}_S$ bands is smaller than $\tilde{n}_S$, i.e., $n_0^* < \tilde{n}_S$. When $\rho = 0$, i.e., no spoofing power is allocated for sensed vacant bands (this is not a sensible strategy but is included here for mathematical completeness), then in this case $n_0^* = 0$; when $0 < \rho \le 1$, $\rho A_0 > 0$ spoofing power is allocated to the sensed vacant bands, then in this case $n_0^* > 0$. The resulting $N_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ can be expressed as follows:

- When $\rho = 0$,

$$\begin{aligned} M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} &= \tilde{p}_{0,i}^{(0)}\left\{\sum_{i=1}^{\tilde{n}_S} Q\left(\frac{K}{2\sqrt{TW}\sigma_n^2} - \sqrt{TW}\right)\right\} \\ &= \tilde{p}_{0,i}^{(0)} \tilde{n}_S p_f, \end{aligned} \quad \text{(B-12)}$$

  where p_f is the probability of false alarm at the SU. Here we assume the noise power is identical over all bands, and hence the false alarm probabilities in different bands at the secondary, when the spoofing signal is absent, are identical and denoted as p_f.

- When $0 < \rho \le 1$,

$$\begin{aligned} & M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} \\ &= \tilde{p}_{0,i}^{(0)}\left\{\sum_{i=1}^{n_0^*} Q\left(\frac{K}{2\sqrt{TW}\left(\frac{\rho A_0}{n_0^*}+\sigma_n^2\right)} - \sqrt{TW}\right)\right. \\ &\qquad \left. + \sum\nolimits_{i=n_0^*+1}^{\tilde{n}_S} Q\left(\frac{K}{2\sqrt{TW}\sigma_n^2} - \sqrt{TW}\right)\right\} \\ &= \tilde{p}_{0,i}^{(0)}\left\{n_0^* Q\left(\frac{K}{2\sqrt{TW}\left(\frac{\rho A_0}{n_0^*}+\sigma_n^2\right)} - \sqrt{TW}\right)\right. \\ &\qquad \left. + \left(\tilde{n}_S - n_0^*\right)p_f\right\}. \end{aligned} \quad \text{(B-13)}$$

Note that n_0^* corresponds to the optimal number of spoofed bands that maximizes $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ in (B-11) with spoofing power budget ρA_0. We derive the optimal value of ρ making use of the optimality of n_0^*. We (1) *first analyze* what equality relationship n_0^* should satisfy to make it the optimal number of spoofed bands within the $\tilde{n}_S$ sensed vacant bands by the adversary, and (2) *then substitute* this relationship into (B-11) to obtain the optimal value of ρ, i.e., the optimal portion of the spoofing power that the adversary should allocate to the sensed vacant bands. Since $n_0^* > 0$ is the optimal number that maximizes $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ in (B-11), we use a continuous variable x $\big(0 < x < \tilde{n}_S\big)$ for exploring the exact value of $n_0^* > 0$. Let

$$g(x) = xQ\left(\frac{K}{2\sqrt{TW}\left(\frac{\rho A_0}{x}+\sigma_n^2\right)} - \sqrt{TW}\right) + \left(\tilde{n}_S - x\right)p_f, \quad \text{(B-14)}$$

where $x^* \approx n_0^*$ is the value of x that maximizes $g(x)$. That is, $n_0^* \approx x^* = \arg\max\limits_{x} g(x)$.

Let $b = K/2\sqrt{TW}$, $d = -\sqrt{TW}$, and $P_J = \rho A_0$. Then $g(x)$ in (B-14) can be further written as

$$g(x) = xQ\left(\frac{b}{P_J/x+\sigma_n^2} + d\right) + \left(\tilde{n}_S - x\right)p_f. \quad \text{(B-15)}$$

The first derivative of $g(x)$ with respect to x is

$$\begin{aligned} & \frac{dg(x)}{dx} \\ &= Q\left(\frac{b}{P_J/x+\sigma_n^2} + d\right) - p_f \\ &\quad - \frac{P_J b x}{\sqrt{2\pi}\left(P_J + x\sigma_n^2\right)^2} \exp\left(-\frac{1}{2}\left(\frac{b}{P_J/x+\sigma_n^2} + d\right)^2\right). \end{aligned} \quad \text{(B-16)}$$

Since the extreme point x^* satisfies the relation that $\frac{dg(x)}{dx}\Big|_{x=x^*}=0$, from (B-16), we have

$$Q\left(\frac{b}{P_J/x^*+\sigma_n^2}+d\right)-p_f = \frac{P_J/x^*\cdot b}{\sqrt{2\pi}\left(P_J/x^*+\sigma_n^2\right)^2}\exp\left(-\frac{1}{2}\left(\frac{b}{P_J/x^*+\sigma_n^2}+d\right)^2\right). \tag{B-17}$$

It can be seen from (B-17) that P_J and x^* always appear together in the form of $\frac{P_J}{x^*}$. As P_J is the spoofing power budget and x^* represents the optimal number of spoofed bands, we define

$$c^* = \frac{P_J}{x^*}, \tag{B-18}$$

where x^* can be interpreted as the optimal spoofing power within each spoofed band. Substituting (B-18) into (B-17),

$$Q\left(\frac{b}{c^*+\sigma_n^2}+d\right)-p_f = \frac{c^*b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2}\cdot\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right), \tag{B-19}$$

or equivalently,

$$Q\left(\frac{b}{c^*+\sigma_n^2}+d\right)-p_f - \frac{c^*b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2}\cdot\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right)=0. \tag{B-20}$$

It can be seen from (B-20) that the value of c^* is determined by the sensing parameters b, d, σ_n^2, and p_f, and can be obtained by solving the nonlinear equation (B-20). In other words, as long as the sensing parameters b, d, σ_n^2, and p_f are determined, then c^* is determined. That is, $c^*=f(b,d,\sigma_n^2,p_f)$, where the function $f(\cdot)$ can be determined through (B-20). Following the same derivations in [11], we can show that Eq. (B-20) has one and only one solution for $c^*>0$. Substituting (B-18) and (B-19) into (B-15) yields

$$g(x^*) = \frac{P_J b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2}\cdot\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right)+\tilde{n}_S p_f. \tag{B-21}$$

Since $P_J=\rho A_0$,

$$g(x^*) = \rho A_0\frac{b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2}\cdot\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right)+\tilde{n}_S p_f. \tag{B-22}$$

Considering that $n_0^*\approx x^*=\arg\max_x g(x)$, $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ in (B-13) is approximately given by

$$\begin{aligned} M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} &\approx \tilde{p}_{0,i}^{(0)}g(x^*) \\ &= \tilde{p}_{0,i}^{(0)}\rho A_0\frac{b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2} \\ &\quad\cdot\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right)+\tilde{p}_{0,i}^{(0)}\tilde{n}_S p_f. \end{aligned} \tag{B-23}$$

Let

$$\triangle = \frac{b}{\sqrt{2\pi}\left(c^*+\sigma_n^2\right)^2}\exp\left(-\frac{1}{2}\left(\frac{b}{c^*+\sigma_n^2}+d\right)^2\right). \tag{B-24}$$

Because c^* is determined by the sensing parameters of the system, $\triangle$ can be considered constant, as long as these sensing parameters are fixed. Substituting (B-24) into (B-23),

$$M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} \approx \tilde{p}_{0,i}^{(0)}\rho A_0\triangle+\tilde{p}_{0,i}^{(0)}\tilde{n}_S p_f. \tag{B-25}$$

Combining (B-12) and (B-25), we can obtain the expression for $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}$ when $0\leqslant\rho\leqslant 1$ as

$$M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} \approx \tilde{p}_{0,i}^{(0)}\rho A_0\triangle+\tilde{p}_{0,i}^{(0)}\tilde{n}_S p_f, \quad 0\leqslant\rho\leqslant 1. \tag{B-26}$$

Following the same procedures from (B-12) to (B-25), $M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ in (B-7) is given by

$$M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} \approx \tilde{p}_{0,i}^{(1)}(1-\rho)A_0\triangle+\tilde{p}_{0,i}^{(1)}\tilde{n}_S p_f, \quad 0\leqslant\rho\leqslant 1. \tag{B-27}$$

Therefore, the objective of the optimization $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}+M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ in (B-5) can be expressed as

$$\begin{aligned} M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}+M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} &\approx \tilde{p}_{0,i}^{(0)}\rho A_0\triangle+\tilde{p}_{0,i}^{(0)}\tilde{n}_S p_f \\ &\quad+\tilde{p}_{0,i}^{(1)}(1-\rho)A_0\triangle+\tilde{p}_{0,i}^{(1)}\tilde{n}_S p_f \\ &= \rho A_0\triangle\left(\tilde{p}_{0,i}^{(0)}-\tilde{p}_{0,i}^{(1)}\right)+\tilde{p}_{0,i}^{(0)}\tilde{n}_S p_f \\ &\quad+\tilde{p}_{0,i}^{(1)}\tilde{n}_S p_f+\tilde{p}_{0,i}^{(1)}A_0\triangle. \end{aligned} \tag{B-28}$$

Discussion: Appendix A proved that $\tilde{p}_{0,i}^{(0)}-\tilde{p}_{0,i}^{(1)}>0$, based on the fact that the probability of detection at the adversary is always larger than its probability of false alarm. Accordingly, when $0<p(H_{1,i})<1$, the coefficient of ρ is positive, i.e., $A_0\triangle\left(\tilde{p}_{0,i}^{(0)}-\tilde{p}_{0,i}^{(1)}\right)>0$. This leads to the case that $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}+M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ monotonically increases as ρ increases. The maximal value of the objective $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S}+M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ is reached when $\rho=1$. That is, in this case, the optimal strategy is to spoof only the sensed vacant bands.

APPENDIX C
PROOF OF LEMMA 3

Lemma 3: When the spoofing power budget at the adversary is large enough to spoof all the spectral bands of interest, that is, the adversary allocates a certain portion ρ of its spoofing power budget to the sensed vacant bands, and the remaining portion $1-\rho$ to the sensed busy bands, the optimal value of ρ satisfies $\rho \geq \dfrac{\tilde{n}_S}{\tilde{n}_p + \tilde{n}_S}$.

Proof: When all the spectral bands of interest are spoofed, the objective of the optimization $M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} + M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$ can be expressed as

$$\begin{aligned} & M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} + M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P} \\ &\quad = \tilde{p}_{0,i}^{(0)} \tilde{n}_S Q\left(\frac{b}{\rho A_0/\tilde{n}_S + \sigma_n^2} + d \right) \\ &\quad\quad + \tilde{p}_{0,i}^{(1)} \tilde{n}_P Q\left(\frac{b}{(1-\rho)A_0/\tilde{n}_P + \sigma_n^2} + d \right), \end{aligned} \tag{C-1}$$

where $b = K/2\sqrt{TW}$, and $d = -\sqrt{TW}$. Let $F(\rho) = M_{J,0}^{\tilde{\boldsymbol{N}}_S=\tilde{n}_S} + M_{J,1}^{\tilde{\boldsymbol{N}}_P=\tilde{n}_P}$. Then we have

$$\begin{aligned} F(\rho) &= \tilde{p}_{0,i}^{(0)} \tilde{n}_S Q\left(\frac{b}{\rho A_0/\tilde{n}_S + \sigma_n^2} + d \right) \\ &\quad + \tilde{p}_{0,i}^{(1)} \tilde{n}_P Q\left(\frac{b}{(1-\rho)A_0/\tilde{n}_P + \sigma_n^2} + d \right). \end{aligned} \tag{C-2}$$

Let

$$g_1(\rho) = \frac{b}{\rho A_0/\tilde{n}_S + \sigma_n^2} + d = b\left(\frac{A_0}{\tilde{n}_S}\rho + \sigma_n^2 \right)^{-1} + d, \tag{C-3}$$

$$\begin{aligned} g_2(\rho) &= \frac{b}{\dfrac{(1-\rho)A_0}{\tilde{n}_P} + \sigma_n^2} + d \\ &= b\left(\frac{A_0}{\tilde{n}_P} + \sigma_n^2 - \frac{A_0}{\tilde{n}_P}\rho \right)^{-1} + d \\ &= b\Big(d_P + \sigma_n^2 - d_p\rho \Big)^{-1} + d, \end{aligned} \tag{C-4}$$

where $d_S = A_0/\tilde{n}_S$, and $d_P = A_0/\tilde{n}_P$. Substituting (C-3) and (C-4) into (C-2),

$$F(\rho) = \tilde{p}_{0,i}^{(0)} \tilde{n}_S Q\Big(g_1(\rho) \Big) + \tilde{p}_{0,i}^{(1)} \tilde{n}_P Q\Big(g_2(\rho) \Big). \tag{C-5}$$

We need to find out what value of ρ leads to the maximal point of $F(\rho)$. The first derivative of $F(\rho)$ with respect to ρ is

$$\begin{aligned} & \frac{dF(\rho)}{d\rho} \\ &\quad = \tilde{p}_{0,i}^{(0)} \tilde{n}_S \Big[-\frac{1}{\sqrt{2\pi}} \exp\Big(-\frac{1}{2} g_1^2(\rho) \Big) \Big] \frac{dg_1(\rho)}{d\rho} \\ &\quad\quad + \tilde{p}_{0,i}^{(1)} \tilde{n}_P \Big[-\frac{1}{\sqrt{2\pi}} \exp\Big(-\frac{1}{2} g_2^2(\rho) \Big) \Big] \frac{dg_2(\rho)}{d\rho}, \end{aligned} \tag{C-6}$$

where

$$\frac{dg_1(\rho)}{d\rho} = -\frac{b d_S}{\Big(d_S\rho + \sigma_n^2 \Big)^2}, \tag{C-7}$$

$$\frac{dg_2(\rho)}{d\rho} = \frac{b d_P}{\Big(d_P + \sigma_n^2 - d_P\rho \Big)^2}. \tag{C-8}$$

Substituting (C-7) and (C-8) into (C-6) yields,

$$\begin{aligned} \frac{dF(\rho)}{d\rho} &= \frac{\tilde{p}_{0,i}^{(0)} \tilde{n}_S b d_S}{\sqrt{2\pi}\Big(d_S\rho + \sigma_n^2 \Big)^2} \exp\Big(-\frac{1}{2} g_1^2(\rho) \Big) \\ &\quad - \frac{\tilde{p}_{0,i}^{(1)} \tilde{n}_P b d_P}{\sqrt{2\pi}\Big(d_S + \sigma_n^2 - d_P\rho \Big)^2} \exp\Big(-\frac{1}{2} g_2^2(\rho) \Big). \end{aligned} \tag{C-9}$$

Considering that $d_S = \dfrac{A_0}{\tilde{n}_S}$, and $d_P = \dfrac{A_0}{\tilde{n}_P}$, (C-9) can be further written as

$$\begin{aligned} \frac{dF(\rho)}{d\rho} &= \frac{\tilde{p}_{0,i}^{(0)} b A_0}{\sqrt{2\pi}\Big(d_S\rho + \sigma_n^2 \Big)^2} \exp\Big(-\frac{1}{2} g_1^2(\rho) \Big) \\ &\quad - \frac{\tilde{p}_{0,i}^{(1)} b A_0}{\sqrt{2\pi}\Big(d_S + \sigma_n^2 - d_P\rho \Big)^2} \exp\Big(-\frac{1}{2} g_2^2(\rho) \Big). \end{aligned} \tag{C-10}$$

The optimal value of ρ, denoted ρ^*, is such that $\left.\dfrac{dF(\rho)}{d\rho}\right|_{\rho=\rho^*} = 0$. That is,

$$\begin{aligned} & \frac{\tilde{p}_{0,i}^{(0)} b A_0}{\sqrt{2\pi}\Big(d_S\rho^* + \sigma_n^2 \Big)^2} \exp\Big(-\frac{1}{2} g_1^2(\rho^*) \Big) \\ &\quad - \frac{\tilde{p}_{0,i}^{(1)} b A_0}{\sqrt{2\pi}\Big(d_S + \sigma_n^2 - d_P\rho^* \Big)^2} \exp\Big(-\frac{1}{2} g_2^2(\rho^*) \Big) = 0. \end{aligned} \tag{C-11}$$

When the spoofing power is very large, $g_1(\rho^*) \approx d$ and $g_2(\rho^*) \approx d$, and we have

$$\exp\Big(-\frac{1}{2} g_1^2(\rho^*) \Big) \approx \exp\Big(-\frac{1}{2} g_2^2(\rho^*) \Big). \tag{C-12}$$

Substituting (C-12) into (C-11) yields,

$$\begin{aligned} & \frac{\tilde{p}_{0,i}^{(0)} b A_0}{\sqrt{2\pi}\Big(d_S\rho^* + \sigma_n^2 \Big)^2} \\ &\quad \approx \frac{\tilde{p}_{0,i}^{(1)} b A_0}{\sqrt{2\pi}\Big(d_P + \sigma_n^2 - d_P\rho^* \Big)^2} \Rightarrow \sqrt{\tilde{p}_{0,i}^{(1)}}\big(d_S\rho^* + \sigma_n^2 \big) \\ &\quad \approx \sqrt{\tilde{p}_{0,i}^{(0)}}(d_P + \sigma_n^2 - d_P\rho^*). \end{aligned} \tag{C-13}$$

Solving (C-13), we have

$$\rho^* \approx \frac{\sqrt{\tilde{p}_{0,i}^{(0)}} d_P + \sqrt{\tilde{p}_{0,i}^{(0)}} \sigma_n^2 - \sqrt{\tilde{p}_{0,i}^{(1)}} \sigma_n^2}{\sqrt{\tilde{p}_{0,i}^{(1)}} d_S + \sqrt{\tilde{p}_{0,i}^{(0)}} d_P}. \tag{C-14}$$

Since $d_S = A_0/\tilde{n}_S$, and $d_P = A_0/\tilde{n}_P$,

$$\rho^* \approx \frac{\sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P}} + \sqrt{\tilde{p}_{0,i}^{(0)}\sigma_n^2} - \sqrt{\tilde{p}_{0,i}^{(1)}\sigma_n^2}}{\sqrt{\tilde{p}_{0,i}^{(1)}\dfrac{A_0}{\tilde{n}_S}} + \sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P}}}$$

$$= \frac{\sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P\sigma_n^2}} + \sqrt{\tilde{p}_{0,i}^{(0)}} - \sqrt{\tilde{p}_{0,i}^{(1)}}}{\sqrt{\tilde{p}_{0,i}^{(1)}\dfrac{A_0}{\tilde{n}_S\sigma_n^2}} + \sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P\sigma_n^2}}}. \tag{C-15}$$

Note that $\tilde{p}_{0,i}^{(0)} \geq \tilde{p}_{0,i}^{(1)}$, so that

$$\rho^* \geq \frac{\sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P\sigma_n^2}}}{\sqrt{\tilde{p}_{0,i}^{(1)}\dfrac{A_0}{\tilde{n}_S\sigma_n^2}} + \sqrt{\tilde{p}_{0,i}^{(0)}\dfrac{A_0}{\tilde{n}_P\sigma_n^2}}}$$

$$= \frac{\sqrt{\tilde{p}_{0,i}^{(0)}}\tilde{n}_S}{\sqrt{\tilde{p}_{0,i}^{(1)}}\tilde{n}_P + \sqrt{\tilde{p}_{0,i}^{(0)}}\tilde{n}_S}$$

$$\geq \frac{\sqrt{\tilde{p}_{0,i}^{(0)}}\tilde{n}_S}{\sqrt{\tilde{p}_{0,i}^{(0)}}\tilde{n}_P + \sqrt{\tilde{p}_{0,i}^{(0)}}\tilde{n}_S}$$

$$= \frac{\tilde{n}_S}{\tilde{n}_P + \tilde{n}_S}. \tag{C-16}$$

That is

$$\rho^* \geq \frac{\tilde{n}_S}{\tilde{n}_P + \tilde{n}_S}. \tag{C-17}$$

■

References

[1] J. Mitola and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 28–40, Feb. 2008.

[4] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

[5] 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, p. 381465, Dec. 2010, doi: 10.1155/2010/381465

[6] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[7] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Conf. Rec. 38th Asilomar Conf. Signals, Syst. Comput.*, vol. 1, Nov. 2004, pp. 772–776.

[8] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerailities and protection countermeasures: A multi-dimensional analysis and assessment," in *Proc. 2nd Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, Aug. 2007, pp. 456–464.

[9] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

[10] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1876–1884.

[11] 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.

[12] J. Wang, I.-R. Chen, J. J. P. Tsai, and D.-C. Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," *Comput. Commun.*, vol. 116, pp. 90–100, Jan. 2018.

[13] 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.

[14] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[15] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE ICC*, Jun. 2009, pp. 1–5.

[16] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, Apr. 2009.

[17] K. M. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Proc. IEEE ICASSP*, May 2013, pp. 2935–2939.

[18] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 772–781, May 2014.

[19] S. A. Selvi and M. Sundararajan, "SVM based two level authentication for primary user emulation attack detection," *Indian J. Sci. Technol.*, vol. 9, no. 29, Aug. 2016.

[20] Y. Li and Q. Peng, "Achieving secure spectrum sensing in presence of malicious attacks utilizing unsupervised machine learning," in *Proc. IEEE MILCOM*, Nov. 2016, pp. 174–179.

[21] 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.

[22] 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.

[23] Q. Peng, P. C. Cosman, and L. B. Milstein, "Worst-case sensing deception in cognitive radio networks," in *Proc. IEEE Globecom*, Honolulu, HI, USA, Dec. 2009, pp. 1–5.

[24] Q. Peng, P. C. Cosman, and L. B. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 903–911, Apr. 2011.

[25] 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.

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

[27] N. Nguyen-Thanh, P. Ciblat, A. T. Pham, and V.-T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4981–4993, Sep. 2015.

[28] M. Haghighat and S. M. S. Sadough, "Smart primary user emulation in cognitive radio networks: Defence strategies against radio-aware attacks and robust spectrum sensing," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 9, pp. 1154–1164, 2015, doi: 10.1002/ett.2848.2014.

[29] M. J. Saber and S. M. S. Sadough, "Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, p. e2885, 2017, doi: 10.1002/ett.2885.2017.

[30] Q. Dong, Y. Chen, X. Li, and K. Zeng. (Apr. 2018). "An adaptive primary user emulation attack detection mechanism for cognitive radio networks." [Online]. Available: https://arxiv.org/abs/1804.09266

[31] D.-T. Ta, N. Nguyen-Thanh, P. Maillé, and V.-T. Nguyen, "Strategic surveillance against primary user emulation attacks in cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 3, pp. 582–596, Sep. 2018.

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

Qihang Peng received the B.S., M.S., and Ph.D. degrees from the School of Information and Communication Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2004, 2007, and 2011, respectively. She was a Visiting Scholar with the Department of Electronic and Computer Engineering, University of California at San Diego, La Jolla, CA, USA. She is currently an Associate Professor of UESTC. Her research interests include spectrum sensing, wireless communication systems, and machine learning in cognitive radio.

Pamela C. Cosman (S'88–M'93–SM'00–F'08) received the B.S. degree (Hons.) in electrical engineering from the California Institute of Technology in 1987, and the Ph.D. degree in electrical engineering from Stanford University in 1993. Following an NSF Post-Doctoral Fellowship at Stanford and at the University of Minnesota (1993–1995), she joined the Faculty of the Department of Electrical and Computer Engineering, University of California at San Diego, San Diego, where she is currently a Professor.

Her research interests are in the areas of image and video compression and processing, and wireless communications. She has written over 250 technical papers in these fields, and one children's book, *The Secret Code Menace*, that introduces error correction coding through a fictional story. His awards include the ECE Departmental Graduate Teaching Award, the Career Award from the National Science Foundation, the GLOBECOM 2008 Best Paper Award, HISB 2012 Best Poster Award, the 2016 UC San Diego Affirmative Action and Diversity Award, and the 2017 Athena Pinnacle Award (Individual in Education). Her administrative positions include serving as the Director of the Center for Wireless Communications (2006–2008), the ECE Department Vice Chair (2011–2014), and the Associate Dean for Students (2013–2016).

Dr. Cosman is a member of Tau Beta Pi and Sigma Xi. She has been a member of the Technical Program Committee or the Organizing Committee for numerous conferences, including most recently serving as a Technical Program Co-Chair of ICME 2018. She was an Associate Editor of the IEEE COMMUNICATIONS LETTERS (1998–2001), and an Associate Editor of the IEEE SIGNAL PROCESSING LETTERS (2001–2005). She was the Editor-in-Chief (2006–2009) and a Senior Editor (2003-2005 and 2010–2013) of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

Laurence B. Milstein (S'66–M'68–SM'77–F'85) received the B.E.E. degree 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, in 1966 and 1968, respectively. From 1968 to 1974, he was with the Space and Communications Group of 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. Since 1976, he has been with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, where he is currently the Ericsson Professor of wireless communications and a former Department Chairman, involved 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.

Dr. Milstein has been a member of the board of governors of both 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, an Academic Senate 1999 UCSD Distinguished Teaching Award, an 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, and the CTTC Achievement Award in 2012. In 2015, he received the UCSD Chancellor's Associates Award for Excellence in Graduate Teaching. He was a Former Chair of the IEEE Fellows Selection Committee. He was an Associate Editor for Communication Theory for the IEEE TRANSACTIONS ON COMMUNICATIONS, an Associate Editor for Book Reviews for the IEEE TRANSACTIONS ON INFORMATION THEORY, an Associate Technical Editor for the *IEEE Communications Magazine*, and the Editor-in-Chief of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He was the Vice President for Technical Affairs of the IEEE Communications Society in 1990 and 1991.