Sensing Disruption with Estimation Uncertainty

Qihang Peng[†] [‡], Pamela C. Cosman[‡], and Laurence B. Milstein[‡]
[†] University of Electronic Science and Technology of China, Chengdu 610054, China
[‡] University of California, San Diego, California 92093-0407, USA
Emails: anniepqh@uestc.edu.cn,{pcosman, lmilstein}@ucsd.edu

***Abstract*—In this paper, the sensing disruption for a power limited adversary with estimation uncertainty is formulated and analyzed. The estimation uncertainty of the adversary is modeled in terms of its probability of false alarm in vacant bands and the probability of detection in busy bands. The strategy for the adversary is obtained by maximizing the sum of the conditional probabilities of false detection within the spectral range of interest, conditioned on the adversary's estimated spectrum usage status. The proposed algorithm is shown to be significantly more robust than conventional algorithms. It is shown in simulation results that, as the adversary's power budget increases, the proposed algorithm asymptotically approaches the performance upper bound when the adversary has perfect information on the spectrum usage status.**

I. Introduction

As the demand for wireless spectrum has been growing, the limited wireless spectral resources and its inefficient usage under fixed allocation motivate a new paradigm to maximally exploit spectrum utilization by allowing dynamic spectrum access, where unlicensed users, also called secondary users, could dynamically access those spectral bands not being occupied by primary users. A key to realizing this paradigm is spectrum sensing, since it determines the available bandwidth for secondary users [1]- [3].

Spectrum sensing allows new attacking opportunities for the adversary. In traditional communications jamming, the adversary sends jamming signals toward the receiver to disrupt information transmission by decreasing the signal to interference-plus-noise power ratio. In a spectrum sensing attack, the adversary could send spoofing signals into vacant bands, to make secondary users mistakenly think those bands are occupied by primary users, such that their available bandwidth for access is reduced. An analytical model and the impact of the sensing attack was analyzed in [4] [5]. The optimal sensing attack, also called spoofing, for a power-limited adversary under AWGN was derived in [7] and [8]. This work was extended for different wireless propagation environments including both fast and slow fading in [9] and [10], where it was assumed that the adversary knows perfectly about the spectral usage status.

In this paper, we consider a more practical scenario. The adversary only has an estimate of spectral usage status for each band. Inevitably, the estimation has measurement uncertainties, which alters the attacking strategy and performance. We tackle this problem by relating the estimation uncertainties of the adversary to the probability of false alarm and the probability of detection at the adversary. The spoofing is then proposed, by maximizing the sum of the conditional probability of false detection at the secondary, conditioned on the spectral usage status estimates at the adversary.

The remainder of this paper is organized as follows. In Section II, the system model is presented. Section III details the mathematical formulation and proposes the optimization algorithm. Numerical results along with analyses are described in Section IV. Conclusions and future work are discussed in Section V.

II. System Model

The spectral range of interest consists of N spectral bands with identical width, as illustrated in Fig. 1, with N_P busy bands, i.e., ones occupied by primary users, and N_S vacant bands, i.e., bands that are idle and available for secondary users to access. Therefore, we have $N = N_P + N_S$.

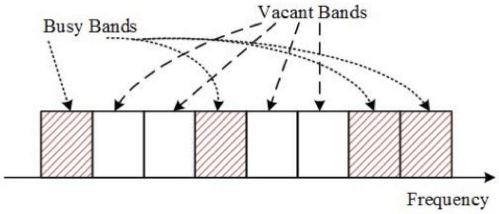

Fig. 1. Spectrum usage status illustration in the frequency domain.

Primary users (PUs) have priority in accessing the spectrum, and their traffic in the time domain is depicted in Fig. 2. Secondary users (SUs) employ a periodic sensing mechanism in the time domain, whereby a sensing interval (denoted as 'S') is followed by a data transmission interval (denoted as 'DT'). An SU carries out spectrum sensing within each sensing interval, to determine the spectrum usage status (busy/vacant) of each band. When an SU finds out there are vacant bands to access, it starts transmission in the following data transmission interval. Therefore, spectrum sensing is critical for the secondary, since it determines the available bandwidth for information transmission.

The adversary aims to degrade the secondary's information in order to decrease the sensed available bandwidth of SUs during the sensing interval, to maximally prevent them from accessing those vacant bands. To achieve this, the adversary

This research was supported by the National Science Foundation of China under Grant No. 61301154, by China Scholarship Council (201506075100), and by the Army Research Office under Grant W911NF-14-1-0340.

978-1-5090-5019-2/17/$31.00 ©2017 IEEE

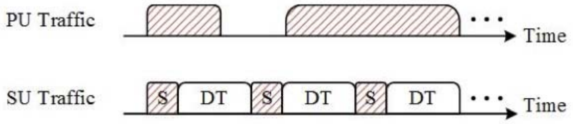

Fig. 2. User traffic models in the time domain.

could emit spoofing signals into those vacant bands, with the aim of making the secondary mistakenly think the vacant bands are occupied by PUs. We consider a scenario where the duration of a typical primary user's message will span multiple sensing/data frames.

The optimal attacking strategy for the adversary during the sensing interval was derived in [7], with the assumption that the adversary has perfect information on which bands are vacant. This corresponds to the performance upper bound from the adversary's perspective, since its attacking power would not be wasted in any busy bands. However, a more practical scenario for the adversary is that the adversary does not have perfect information on the spectral usage status of each band. Instead, it has estimates of which bands are vacant with estimation uncertainties.

A. Estimation Uncertainties at the Adversary

Let $\tilde{D}_{i,A}$ denote the estimated spectrum usage decision of the adversary on the i-th band, where the subscript A indicates the adversary, and $i = 1, 2, \cdots, N$. This decision $\tilde{D}_{i,A}$ equals either 0 or 1, with 0 corresponding to the case that the adversary thinks the i-th band is vacant, and 1 that the i-th band is busy. Accordingly, there are $\tilde{N}_S$ bands sensed to be vacant by the adversary, and $\tilde{N}_P = N - \tilde{N}_S$ bands sensed to be busy by the adversary.

Due to the estimation uncertainties at the adversary, $\tilde{N}_P$ and $\tilde{N}_S$ are random variables. At any particular instant of time, we have $\tilde{N}_P = \tilde{n}_P$ and $\tilde{N}_S = \tilde{n}_S$, where $\tilde{n}_P$ and $\tilde{n}_S$ are integers within the range $[0, N]$. Let $\{\tilde{n}_S\}$ and $\{\tilde{n}_P\}$ denote the set of spectral bands that are sensed by the adversary to be vacant and busy, respectively. For the bands where $i \in \{\tilde{n}_P\}$, $\tilde{D}_{i,A} = 1$, and for $i \in \{\tilde{n}_S\}$, $\tilde{D}_{i,A} = 0$.

When the adversary determines that the i-th band is busy, there is still a nonzero probability that it is actually vacant. This probability, denoted by $\tilde{p}_{0,i}^{(1)}$, is given by

$$\tilde{p}_{0,i}^{(1)} \triangleq p\left(H_{0,i} | \tilde{D}_{i,A} = 1\right) \tag{1}$$

where $H_{0,i}$ represents the event that the i-th band is actually vacant, and $\tilde{p}_{0,i}^{(1)}$ can be further written as

$$\tilde{p}_{0,i}^{(1)} = \frac{\tilde{p}_{f,i} p(H_{0,i})}{\tilde{p}_{f,i} p(H_{0,i}) + \tilde{p}_{d,i} p(H_{1,i})} \tag{2}$$

where $\tilde{p}_{f,i}$ and $\tilde{p}_{d,i}$ are the probability of false alarm and the probability of detection at the adversary in the i-th band, respectively. $H_{1,i}$ is the event that the i-th band is actually busy.

Similarly, when the adversary thinks the i-th band is vacant, i.e., $\tilde{D}_{i,A} = 0$, there is a nonzero probability that it is actually busy. Also, there is a certain probability that the i-th band is actually vacant when the adversary thinks it is vacant. This probability is denoted $\tilde{p}_{0,i}^{(0)}$, given by

$$\tilde{p}_{0,i}^{(0)} \triangleq p(H_{0,i} | \tilde{D}_{i,A} = 0) \tag{3}$$

which can be further written as

$$\tilde{p}_{0,i}^{(0)} = \frac{(1 - \tilde{p}_{f,i}) p(H_{0,i})}{(1 - \tilde{p}_{f,i}) p(H_{0,i}) + (1 - \tilde{p}_{d,i}) p(H_{1,i})} \tag{4}$$

B. Spectrum Sensing at the Secondary

Under $H_{0,i}$ in the i-th band, i.e., the primary signal is absent, no matter whether the sensing decision $\tilde{D}_{i,A}$ at the adversary is equal to 1 or 0, the received signal $r_{i,S}(t)$ at the secondary user can be written in the form:

$$r_{i,S}(t) = n_{i,S}(t) + \sqrt{\beta_{i,J}(t)} j_i(t) \tag{5}$$

where $n_{i,S}(t)$ is the 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 the bands within the spectral range of interest. In (5), $j_i(t)$ is the spoofing signal emitted by the adversary in the i-th band. Its power is denoted as $A_{i,J}$, and it is assumed to be Gaussian distributed with zero mean, and hence its variance equals $A_{i,J}$.

Note that the expression in (5) incorporates cases where the spoofing power by the adversary is either present or absent in the i-th band. When the adversary chooses not to spoof in this band, $A_{i,J}$ is equal to zero; otherwise, $A_{i,J}$ 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 $\tilde{D}_{i,A}$ $(i = 1, 2, \cdots, N)$ are random. Accordingly, the corresponding spoofing power allocations in each band $A_{i,J}$ $(i = 1, 2, \cdots, N)$ are random, due to the random characteristics of the measurements at the adversary. At any particular instant of time, the measurements are obtained by the adversary, and we let $a_{i,J}$ denote the spoofing power $A_{i,J}$ at this time, i.e., $A_{i,J} = a_{i,J}$. Specifically, for the i-th band that is sensed to be busy by the adversary, i.e., $\tilde{D}_{i,A} = 1$, we use the notation $A_{i,J}^{(1)} = a_{i,J}^{(1)}$ to denote the spoofing power the adversary puts in it. Similarly, for the i-th band that $\tilde{D}_{i,A} = 0$, we use the notation $A_{i,J}^{(0)} = a_{i,J}^{(0)}$ to denote the spoofing power the adversary allocates in it.

In the absence of fading, the coefficient $\beta_{i,J}(t) = 1$ in (5). For the secondary utilizing energy detection for sensing, using the results from Urkowitz [6], the probability of false detection in this band can be expressed as Eq. (7) in our previous work [7].

When the spoofing signal $j_i(t)$ experiences fading, the channel coefficient between the adversary and the secondary user $\sqrt{\beta_{i,J}(t)}$ is random, which we assume to be exponentially distributed with mean $\bar{\beta}_{i,J}$. The corresponding probability of false detection in this band can be found in our previous work in [9].

III. Sensing Disruption with Estimation Uncertainty: Formulation and Proposed Algorithm

For the sensing link disruption scenario [7] [9], at the start of the sensing interval, the adversary has the sensing measurements $\tilde{D}_{i,A}$ on the spectral usage status of the i-th band. At the end of the sensing interval, the secondary obtains the decision D_i on the i-th band. Consider the probability that a sensed vacant band by the adversary is actually vacant, but determined to be busy by the secondary. This probability can be mathematically written as

$$\begin{aligned} p(D_i = 1, H_{0,i}|\tilde{D}_{i,A} = 0) = p(H_{0,i}|\tilde{D}_{i,A} = 0) \\ \cdot p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 0) \end{aligned} \tag{6}$$

where $D_i \in \{0, 1\}$ denotes the sensing decision at the secondary on the i-th band.

Over all the $\tilde{N}_S = \tilde{n}_S$ 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 $\tilde{D}_{i,A} = 0$ where $i \in \{\tilde{n}_S\}$, and $\tilde{N}_S = \tilde{n}_S$, is given by

$$N_{J,0}^{\tilde{N}_S=\tilde{n}_S} = \sum_{i=1}^{\tilde{n}_S} p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 0) p(H_{0,i}|\tilde{D}_{i,A} = 0) \tag{7}$$

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

On the other hand, as shown in (1), 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 attacking strategy. Intuitively, whether to spoof in this band for the adversary 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 $\tilde{D}_{i,A} = 1$, 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 $\tilde{D}_{i,A} = 1$ at the adversary, which can be obtained as

$$\begin{aligned} p(D_i = 1, H_{0,i}\big|\tilde{D}_{i,A} = 1) = p(D_i = 1\big|H_{0,i}, \tilde{D}_{i,A} = 1) \\ \cdot p(H_{0,i}|\tilde{D}_{i,A} = 1) \end{aligned} \tag{8}$$

Summing this probability over all the $\tilde{N}_P = \tilde{n}_P$ bands that are sensed to be 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 $\tilde{D}_{i,A} = 1$ where $i \in \{\tilde{n}_P\}$, and $\tilde{N}_P = \tilde{n}_P$, given by

$$N_{J,1}^{\tilde{N}_P=\tilde{n}_P} = \sum_{i=1}^{\tilde{n}_P} p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 1) p(H_{0,i}|\tilde{D}_{i,A} = 1) \tag{9}$$

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

As shown in [7] [9], the average number of successfully spoofed bands can be represented as the sum of the probabilities of false detection over all the actually vacant bands. Therefore, the sensing attack problem for the power-limited adversary with estimation uncertainty can be formulated as maximizing the secondary's sum of the probabilities of false detection when the bands are actually vacant, conditioned on the adversary's sensing estimates $\tilde{D}_{i,A}$ $(i = 1, 2, \cdots, N)$, $\tilde{N}_S = \tilde{n}_S$, with a given power budget A_0, which can be expressed as

$$\begin{aligned} \max \quad & N_{J,0}^{\tilde{N}_S=\tilde{n}_S} + N_{J,1}^{\tilde{N}_P=\tilde{n}_P} \\ s.t. \quad & \sum_{i=1}^{\tilde{n}_S} a_{i,J}^{(0)} + \sum_{i=1}^{\tilde{n}_P} a_{i,J}^{(1)} = A_0 \\ & a_{i,J}^{(0)} \geq 0, \quad i \in \{\tilde{n}_S\} \\ & a_{i,J}^{(1)} \geq 0, \quad i \in \{\tilde{n}_P\} \end{aligned} \tag{10}$$

where $N_{J,0}^{\tilde{N}_S=\tilde{n}_S}$ and $N_{J,1}^{\tilde{N}_P=\tilde{n}_P}$ are given in (7) and (9), respectively.

To obtain the sensing disruption strategy of the adversary, the key task is to relate $N_{J,0}^{\tilde{N}_S=\tilde{n}_S}$ and $N_{J,1}^{\tilde{N}_P=\tilde{n}_P}$ 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. From Section II-B, the received signal model can be written in the same form given in (5), regardless of whether $\tilde{D}_{i,A}$ is equal to 0 or 1. In this way, letting $a_{i,J}^{(0)}$ denote the spoofing power that the adversary intends to put for the bands where $\tilde{D}_{i,A} = 0$, and following the same procedures as that in [6] [7], $p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 0)$ is approximately given by

$$p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 0) \approx Q\Big(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\Big) \tag{11}$$

where TW and K are the integration-time-bandwidth product, and the detection threshold at the secondary user's receiver, respectively.

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

$$p(D_i = 1|H_{0,i}, \tilde{D}_{i,A} = 1) \approx Q\Big(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\Big) \tag{12}$$

And hence, (10) can be further formulated as

$$\begin{aligned} \max \quad & \sum_{i=1}^{\tilde{n}_S} \tilde{p}_{0,i}^{(0)} Q\Big(\frac{K}{2\sqrt{TW}(a_{i,J}^{(0)} + \sigma_n^2)} - \sqrt{TW}\Big) \\ & + \sum_{i=1}^{\tilde{n}_P} \tilde{p}_{0,i}^{(1)} Q\Big(\frac{K}{2\sqrt{TW}(a_{i,J}^{(1)} + \sigma_n^2)} - \sqrt{TW}\Big) \\ s.t. \quad & \sum_{i=1}^{\tilde{n}_S} a_{i,J}^{(0)} + \sum_{i=1}^{\tilde{n}_P} a_{i,J}^{(1)} = A_0 \\ & a_{i,J}^{(0)} \geq 0, \quad i \in \{\tilde{n}_S\} \\ & a_{i,J}^{(1)} \geq 0, \quad i \in \{\tilde{n}_P\} \end{aligned} \tag{13}$$

Because the optimization of (13) is nonlinear and nonconvex, it is difficult to obtain an analytical expression for the global optimal solution. However, note that no matter what the spoofing power allocation strategy is, there would be a portion of the total power budget being assigned to $N_{J,0}^{\tilde{N}_S=\tilde{n}_S}$, and the remaining portion of the total power assigned to $N_{J,1}^{\tilde{N}_P=\tilde{n}_P}$. Utilizing this characteristic of the objective function, we propose a sub-optimal algorithm for the sensing disruption with estimation uncertainty, as given by the following.

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

Step 2: Obtain the sensing disruption strategies for the $\tilde{n}_S$ sensed vacant bands with a power budget of ρA_0, and for the $\tilde{n}_P$ sensed busy bands with a power budget of $(1-\rho)A_0$, according to the attacking strategy derived in [7].

Step 3: Find the maximal value of the objective function by varying the values of ρ from 0 to 1 in discrete steps.

IV. Simulation Results And Analysis

In this section, we analyze the proposed sensing disruption performances under different scenarios through Monte Carlo simulations. In addition, for better illustration of the proposed algorithm, we also include the performances of the following three different algorithms:

1) Perfect Algorithm. In this algorithm, the adversary is assumed to know perfectly the actual spectral usage status. Accordingly, the performance of this algorithm provides an upper bound for the sensing disruption performance of the adversary.
2) Sensed Algorithm. For the sensed algorithm, the adversary only spoofs the bands it has sensed to be vacant.
3) Blind Algorithm. The blind algorithm corresponds to the case that the adversary considers all the spectral bands of interest to be identical, and uses the procedure from [7] to determine the percentage of bands to be spoofed. Note that the above procedure was optimal, 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.

The average number of false detections at the secondary with different values of spoofing power budget is plotted in Fig. 3, where the spoofing power budget is measured in terms of the jamming-power-to-noise-power ratio (JNR) in each band, which we define to be $JNR = A_0/N\sigma_n^2$. In the following numerical results, the total number of spectral bands $N = 6$, and there are $N_S = 4$ actually vacant bands. The threshold utilized by the secondary for determining whether the observed band is vacant is chosen such that, in the absence of spoofing, its probability of false alarm is 0.10. The sensing capability of the adversary is expressed in terms of its probability of false alarm $\tilde{p}_f = 0.10$ and its probability of detection $\tilde{p}_d = 0.90$.

It is shown in Fig. 3 that, for any spoofing power, the average number of false detections for the proposed algorithm is always larger than that of the sensed algorithm, as well as that of the blind algorithm. Also, the average number of false detections of the proposed algorithm asymptotically approaches that of the perfect algorithm.

When JNR is above approximately 0.60, 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 as busy by the adversary due to its estimation uncertainty. 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.

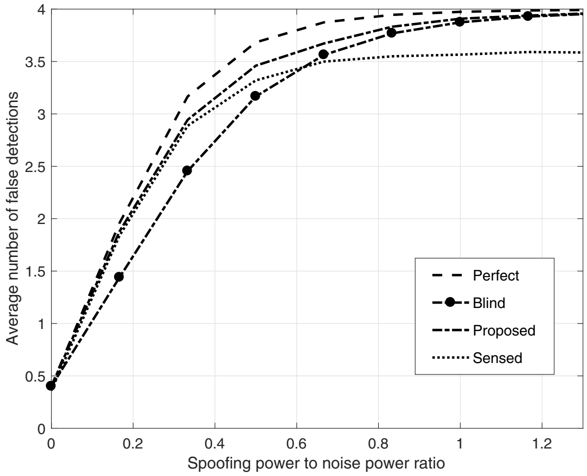

Fig. 3. Average number of false detections versus JNR, where $N = 6$ and $N_S = 4$.

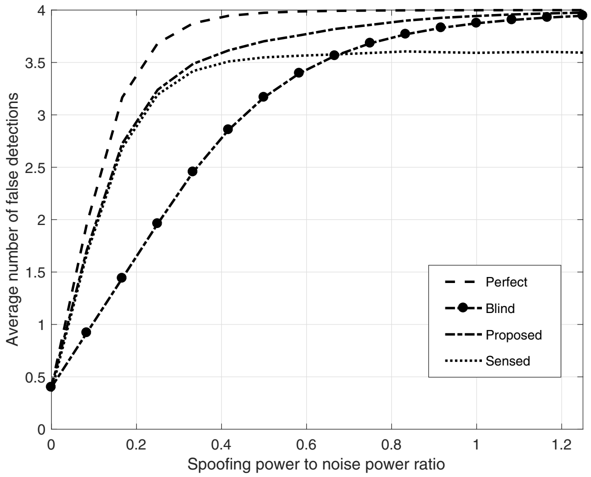

Fig. 4. Average number of false detections versus JNR, where $N = 12$ and $N_S = 4$.

Note that both the proposed algorithm and the blind algorithm 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 as the spoofing power further increases. 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.

Increasing the total number of bands N from 6 to 12, while keeping other parameters unchanged, the average number of false detections at the secondary with various JNR is depicted in Fig. 4. The gap between the average number of false detections of the proposed algorithm and that of the perfect algorithm at the same value of JNR increases when N increases. That is, with the same power budget and the same sensing capability of the adversary, the attacking capability is reduced when the total number of bands N increases. This is reasonable because when N increases, the probability that the adversary makes correct decisions on all the spectral bands' usage status decreases, and hence, the probability that it hits exactly the actually vacant bands is lowered. Accordingly, fewer actually vacant bands are spoofed, resulting in smaller average number of false detections by the secondaries.

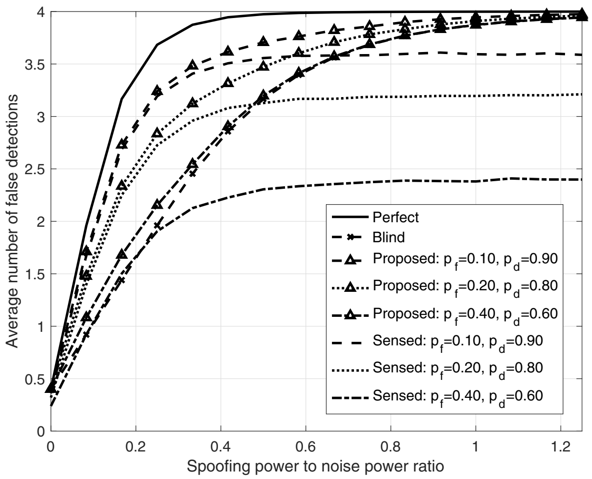

Fig. 5. Average number of false detections versus JNR with different sensing capabilities of the adversary, where $N = 12$ and $N_S = 4$.

The effects of the adversary's different sensing capabilities on the sensing disruption performances are illustrated in Fig. 5, where the total number of bands $N = 12$, and the actually vacant number of bands $N_S = 4$. When the sensing capability of the adversary decreases, e.g., from $p_f = 0.10, p_d = 0.90$ to $p_f = 0.20, p_d = 0.80$, for the same value of the spoofing power, the average number of false detections by the secondaries decreases for both the proposed algorithm and the sensed algorithm. There is more significant performance degradation for the sensed algorithm than for 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 false detections by the secondaries saturates to a much lower level when the adversary uses the sensed algorithm.

V. Conclusions and Future Work

In this paper, we designed and analyzed the sensing disruption for the adversary with estimation error on the spectral usage status of each band. Numerical results show that the proposed strategy outperforms both the sensed algorithm and the blind algorithm. When the power budget of the adversary increases, the performance of the proposed algorithm asymptotically approaches the sensing disruption performance upper bound. When the sensing capabilities of the adversary decrease, the proposed algorithm is significantly more robust than the sensed algorithm.

Future work will extend our model along with corresponding analyses to a more general framework, where the spoofing signals experience fading propagations, including both fast and slow fading scenarios, as well as an in-depth analysis on the sensitivity to the probability of false alarm and the probability of detection at the adversary. Also, the scenario where the secondary users employ cooperative spectrum sensing will be incorporated.

References

[1] Q. Peng, K. Zeng, J. Wang, and S. Li, "A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context," *IEEE PIMRC*, Sep. 2006.

[2] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28-40, Feb. 2008.

[3] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116-130, 2009.

[4] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008.

[5] Z. Jin, S. Anand, and K. Subbalakshmi, "Impact of primary user emulation attacks on dynamic spectrum access networks," *IEEE Trans. Communications*, vol. 60, no. 9, pp. 2635-2643, Sep. 2012.

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

[7] Q. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," *IEEE Trans. on Vehicular Technology*, vol. 59, no. 4, pp. 1801-1810, 2010.

[8] Q. Peng, P. C. Cosman, and L. B. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 903-911, Apr. 2011.

[9] M. Soysa, P. Cosman, and L. Milstein, "Spoofing and jamming optimization over Rayleigh fading channels of a cognitive radio adversary," *IEEE Trans. on Communications*, vol. 62, no. 8, pp. 2681-2695, 2014.

[10] M. Soysa, P. Cosman, and L. Milstein, "Disruptive attacks on video tactical cognitive radio downlinks," *IEEE Trans. on Communications*, vol. 64, no. 4, pp. 1411-1422, 2016.