Worst-Case Sensing Deception in Cognitive Radio Networks

Qihang Peng[†], Pamela C. Cosman[‡], and Laurence B. Milstein[‡]
[†]School of Comm. and Info. Engineering, University of Electronic Science and Technology of China
Chengdu, China 610054, Email: anniepqh@uestc.edu.cn
[‡]Electrical and Computer Engineering Department, University of California, San Diego
San Diego, California 92093-0407, Emails: {pcosman, milstein}@ucsd.edu

***Abstract*—This paper addresses the design of the power-limited intelligent adversary for sensing deception in a cognitive radio network. The average number of successfully spoofed bands by the adversary is analyzed, which can be expressed in terms of the individual spoofing probability on each band. The worst-case sensing deception strategy is obtained by maximizing the average number of successfully spoofed bands, under the adversary's power constraint. Specifically, for a cognitive radio network where energy detection is utilized by secondary users, it is shown that the worst-case deception strategy is equal-power, partial-band spoofing.**

I. Introduction

In order to solve the contradiction between spectrum scarcity and low spectrum utilization, Cognitive Radio (CR) [1], [2], [3], allowing for dynamically accessing unused spectrum bands with only minimal degradation to primary users, is one promising candidate. Spectrum sensing is one of the key technologies in the realization of a CR system, since it enables CR to fill in unused spectrum bands without causing harmful interference to primary users. A spectrum band is unavailable for use by secondary users if it is determined to be busy through sensing; while one judged to be vacant can be used until a primary user appears.

Note that while spectral efficiency can be improved based on this dynamic access paradigm, in comparison to a traditional radio, this sensing-before-accessing scheme makes a CR network more vulnerable to an attack by an intelligent adversary. For a traditional radio, an adversary can interfere with reception by jamming. For a cognitive radio, in addition to jamming, the adversary can interfere with reception, or even prevent transmission, by misleading sensing decisions by emitting signals in the unused bands [4]. The feasibility of launching such a sensing attack is analyzed in [5], and Chen et al. [6] studied mechanisms to combat such attacks.

In this paper, we focus on the problem of sensing deception by an intelligent adversary of the CR system. An intelligent adversary emits spoofing signals in the unused bands, in order to make secondary users, with some probability, think that these bands are being used by primary users and should be avoided. Unused bands taken to be busy by secondary users due to the spoofing signal are termed *successfully spoofed bands*, and the probability of this is the *spoofing probability*. The underlying assumption in this paper is that spoofing a given spectral band can be accomplished more efficiently than can jamming that same spectral band.

The worst-case sensing deception strategy is derived in this paper, whereby the average number of successfully spoofed bands is maximized for an intelligent adversary with a limited power budget. The worst-case sensing deception strategy is derived for a CR network where secondary users utilize energy detection for spectrum sensing. It is shown that the worst-case sensing deception is a partial-band spoofing strategy, with an equal power distribution.

The remainder of this paper is organized as follows. The system model is presented in Section II, and the worst-case sensing deception is derived in Section III. Numerical results are provided in Section IV, and conclusions are presented in Section V.

II. System Model

The spectral range of interest considered in this paper is divided into multiple bands, each with identical bandwidth, as shown in Fig. 1. There are two types of bands: *busy bands* and *allowable bands*. Busy bands are those currently occupied by primary users, while allowable bands are those not currently used by primary users. Ideally, the allowable bands can be accessed by secondary users through spectrum sensing, and hence the spectral efficiency is increased.

The focus of this paper is on the allowable bands. The allowable bands that the adversary chooses to launch signals in are termed *spoofed bands*, while the allowable ones that are not spoofed are called *vacant bands*. It is possible that not every spoofed band of the intelligent adversary will appear to be busy to secondary users. Those bands that appear to be busy are called *successfully spoofed bands*.

Secondary users access vacant bands determined via spectrum sensing. With the presence of thermal noise, an allowable band will be determined to be busy with some non-zero probability. This probability will be further increased by a spoofing signal. If all allowable bands in the spectral range of interest are successfully spoofed, the cognitive radio communication system fails. However, it is not always the optimal strategy for the adversary to spoof all allowable bands, since the intelligent adversary has limited power.

For a spectral range consisting of N allowable bands, the average number of successfully spoofed bands N_J can be

This research was supported by the Office of Naval Research under grant no. N000140810081.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

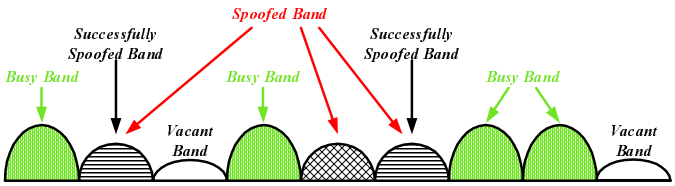

Fig. 1. Spectrum band elaboration

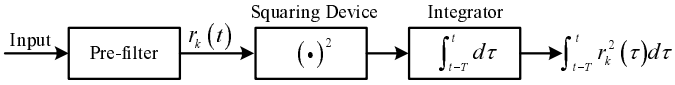

Fig. 2. Radiometer diagram

represented as:

$$N_J = \sum_{k=1}^{N} p_k \tag{1}$$

where p_k is the probability of successfully spoofing (or spoofing probability, for short) in the kth allowable band, and is given in the next section.

Proof: Let X_k $(k = 1, 2, \ldots, N)$ be variables such that $X_k = 1$ means that the kth band is successfully spoofed by the adversary, while $X_k = 0$ indicates that this band is sensed to be vacant by the secondary user. Therefore, the number of successfully spoofed bands is the sum of X_k over all k. The expectation of this sum is the average number of successfully spoofed bands, N_J, and is given by

$$N_J = E[\sum_{k=1}^{N} X_k] = \sum_{k=1}^{N} E[X_k] = \sum_{k=1}^{N} p_k \tag{2}$$

Our goal is to maximize the average number of successfully spoofed bands by an intelligent adversary having a power budget P. That is

$$\begin{aligned} \max \quad & \sum_{k=1}^{N} p_k \\ s.t. \quad & \sum_{k=1}^{N} P_k = P \\ & P_k \geq 0, \quad k = 1, 2, \ldots, N \end{aligned} \tag{3}$$

where P_k is the power the intelligent adversary emits on the kth allowable band.

III. Worst Case Sensing Deception in CR Networks

In order to analyze the worst-case sensing deception, we consider a cognitive radio network where secondary users determine the availability of a spectrum band through the use of a radiometer, as shown in Fig. 2.

The output of the integrator at any time is the energy of the input to the squaring device over a T second interval. The noise pre-filter serves to limit the noise bandwidth to be the same as that of allowable bands.

In the presence of an intelligent adversary, the input $r_k(t)$ to the squaring device of a secondary user's receiver observing the kth allowable band consists of both thermal noise, $n_k(t)$, and the spoofing signal, $j_k(t)$. That is

$$r_k(t) = \alpha j_k(t) + n_k(t) \tag{4}$$

where $j_k(t)$ is assumed to be Gaussian distributed with zero mean, and hence its variance equals the spoofing power emitted on the kth allowable band, i.e. P_k. The path loss factor between the adversary and the secondary user's receiver is denoted as α, which is assumed to be constant across all bands. Thermal noise after the pre-filter is modeled as zero mean additive Gaussian noise $n_k(t)$, i.e., $n_k(t) \sim \boldsymbol{N}(0, \sigma_{n,k}^2)$. The spoofing signal, $j_k(t)$, and the noise, $n_k(t)$ are assumed to be independent of each other.

Using the results from Urkowitz [7], it can be shown that the spoofing probability, p_k, the probability of determining that an allowable band is busy, is given approximately by

$$p_k(P_k) = Q(\frac{K}{2\sqrt{TW}(\alpha^2 P_k + \sigma_{n,k}^2)} - \sqrt{TW}) \tag{5}$$

where TW, as used in [7], refers to the product of the integration time interval and the bandwidth (it is termed time-bandwidth product hereafter), $Q(\cdot)$ is the Gaussian tail function, K is the detection threshold at the secondary user's receiver, and we now express p_k as $p_k(P_k)$ to explicitly denote its dependence on the power. The threshold is used by secondary users for comparison with the radiometer output, to decide whether the band of interest is vacant. If the output is larger than the threshold, the presence of a primary user is assumed; if the output is smaller than the threshold, the absence of a primary user is assumed, thus indicating that this observed band can be accessed by secondary users. The threshold K is usually predetermined by the false alarm probability, p_f, due to thermal noise through the following relation [7],

$$p_f = Q(\frac{K - 2TW\sigma_{n,k}^2}{2\sqrt{TW}\sigma_{n,k}^2}) \tag{6}$$

where it is assumed in (6) that the thermal noise power is identical across all allowable bands, that is, $\sigma_{n,k}^2 = \sigma_n^2$, $k = 1, 2, \ldots, N$. Therefore, from (3), the worst-case sensing deception problem can be formulated as

$$\begin{aligned} \max_{P_k} \quad & \sum_{k=1}^{N} Q(\frac{K}{2\sqrt{TW}(\alpha^2 P_k + \sigma_n^2)} - \sqrt{TW}) \\ s.t. \quad & \sum_{k=1}^{N} P_k - P = 0 \\ & P_k \geq 0, \quad k = 1, 2, \ldots, N \end{aligned} \tag{7}$$

As seen in Eq. (7), our problem is to determine how much power should be allocated to each allowable band in order to maximize the objective function, namely, the average number of successfully spoofed bands, which is a function of spoofing power P_k, thermal noise power σ_n^2, time-bandwidth product TW, and the threshold K. With the presence of spoofing power, the energy in the allowable band is increased, in this way, the probability that an allowable band is determined to be busy is increased. Meanwhile, for the same amount of spoofing power and noise power on the allowable band, it is more likely that this band is determined to be busy when the accumulated energy is compared with a lower threshold. Therefore, for our problem, whereby the intelligent adversary has a limited power budget, the spoofing power it should allocate to each allowable band varies with different values of the threshold.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

Using Lagrange multipliers with inequality constraints [9], [10], a closed-form expression for the worst-case sensing deception strategy for an intelligent adversary with a limited power budget can be obtained [11]. The strategy can be divided into two categories, according to the value of the threshold used by the secondary users.

We define the parameter V as $V \triangleq (TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2$. From [11], when V is smaller than the threshold K, the worst-case sensing deception strategy is to spoof a fraction of the allowable bands, with an identical power allocation. In other words, for a spectral range consisting of N allowable bands, the worst-case deception is to identically distribute spoofing power over N^* allowable bands, where $N^* \leq N$.

When V is greater than or equal to the threshold, all allowable bands should be spoofed, with identical power allocation. That is

$$P_k^* = P/N \qquad k = 1, 2, \ldots, N \tag{8}$$

IV. Results Analysis

We now illustrate this technique with some numerical examples. The optimal number of spoofed bands is illustrated in Fig. 3, where the curves are parameterized by the total spoofer power P. The threshold K corresponds to $p_f = 0.05$, the noise power $\sigma_n^2 = 1$, $\alpha = 1$, and $TW = 100$. It is seen that each curve exhibits a knee, which corresponds to the transition from full-band spoofing to partial-band spoofing. To the left of the knee, the number of spoofed bands equals the number of allowable bands. This is because when the number of allowable bands is small, the adversary has enough power to spoof all of them with high probability of success. To the right of the knee, the number of allowable bands is large, and the adversary can only spoof a fraction of them.

In Fig. 4 and 5, we now assume that the number N of allowable bands is sufficiently large that the optimal number of spoofed bands N^* no longer depends on N, that is, we are operating to the right of the knee in Fig. 3, in the regime of partial-band spoofing. In Fig. 4, the optimal number of spoofed bands N^*, is plotted versus the spoofing-power-to-noise-power ratio $R = P/\sigma_n^2$ for a time-bandwidth product $TW = 100$. Different values of the threshold are used, with each one corresponding to a different false alarm probability. It is seen that N^* increases as R increases, which is reasonable since more spoofing power allows one to spoof more allowable bands. When the thermal noise power and TW are held constant, increasing p_f indicates a decrease in K (as in (6)). This allows a given level of spoofing power to be spread over a larger number of bands.

Consider now Fig. 5, where N^* versus the spoofing-power-to-noise-power ratio R is plotted for a threshold corresponding to $p_f = 0.05$, the thermal noise power $\sigma_n^2 = 1$ and different values of TW. It is seen that for fixed p_f and R, when TW increases, the optimal number of spoofed bands N^* increases. That is, for the same spoofing power, an increase in TW increases the ability to spoof. This is reasonable because, for a fixed spectrum band, an increase in TW means an increase in the integration time interval. A radiometer with a longer integration time has a better ability to determine whether the received power is below or above the threshold.

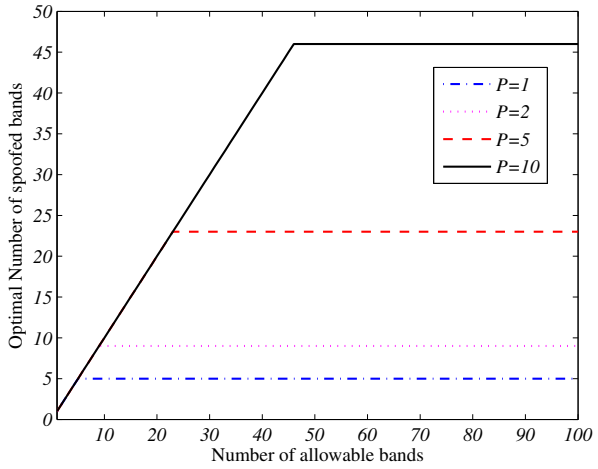

Fig. 3. Optimal number of spoofed bands versus number of allowable bands N with different spoofing powers P ($p_f = 0.05, \sigma_n^2 = 1, TW = 100$)

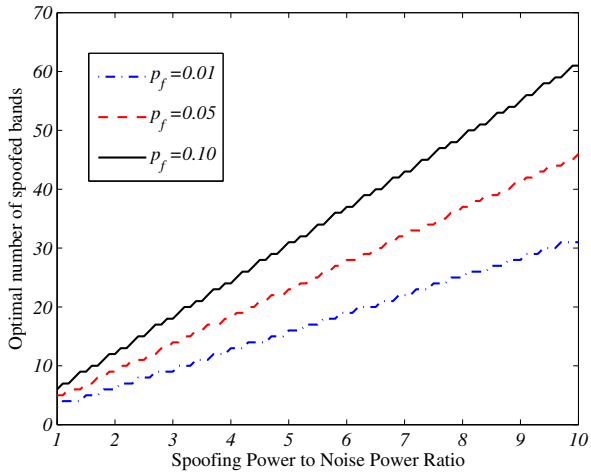

Fig. 4. Optimal number of spoofed bands N^* versus spoofing-power-to-thermal-noise-power ratio with different values of p_f ($TW = 100$)

When V is smaller than the threshold, the average number of successfully spoofed bands versus the number of allowable bands is plotted in Fig. 6. The time-bandwidth product $TW = 100$, the thermal noise power $\sigma_n^2 = 1$, and the threshold K corresponds to $p_f = 0.05$. For a given P, the average number of successfully spoofed bands N_J increases as the number of allowable bands increases. Each curve exhibits a knee. To the left of the knee, the curves increase sharply, because with a small number of allowable bands, the adversary can spoof them all with high probability of success. To the right of the knee, the number of allowable bands is large, so the adversary can only spoof a fraction of them. Therefore, the spoofing probability could be either due to both spoofing and thermal noise power (as in (5)), or only due to thermal noise power, that is, false alarm probability p_f (as in (6)). At this point, when the number of allowable bands increases by ΔN, the average number of successfully spoofed bands increases by $\Delta N \cdot p_f$, resulting in a linear increase, and the slope is equal

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

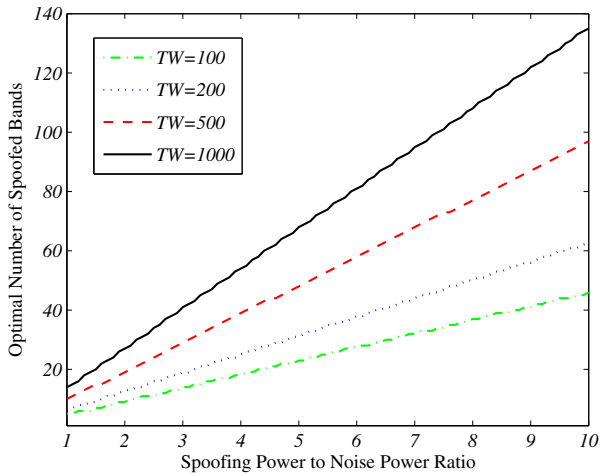

Fig. 5. Optimal number of spoofed bands N^* versus spoofing-power-to-thermal-noise-power ratio with different values of TW ($p_f = 0.05$)

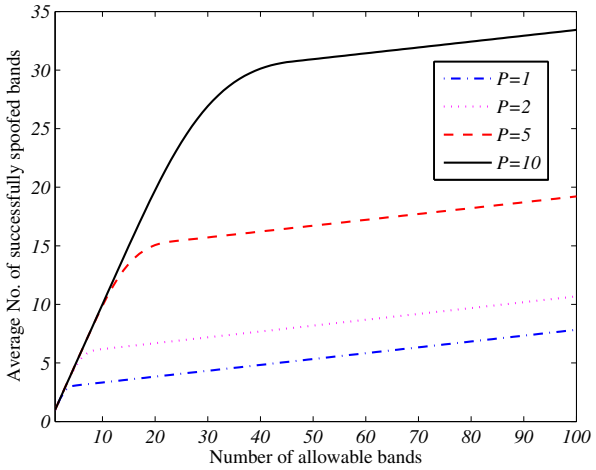

Fig. 6. Average number of successfully spoofed bands N_J versus number of allowable bands N with different spoofing powers P ($p_f = 0.05, \sigma_n^2 = 1, TW = 100$)

to p_f. Comparing different curves in Fig. 6, it is seen that an increase in spoofing power P results in an increase in N_J, which is consistent with the observation made earlier in this section that more spoofing power allows one to spoof more bands.

When V is larger than the threshold, from (8), the worst-case sensing deception strategy is to equally allocate power into all allowable bands, and in this case, the average number of successfully spoofed bands N_J versus the number of allowable bands N is plotted in Fig. 7. The time-bandwidth product $TW = 100$, the thermal noise power $\sigma_n^2 = 1$, and the threshold K corresponds to $p_f = 0.50$. Compared with Fig. 6, the false alarm probability increases from 0.05 to 0.50, leading to a significant decrease in the threshold from above V to below V. When the number of allowable bands N increases, the average number of successfully spoofed bands N_J increases as well, though the increase in N_J becomes smaller as N gets larger. Comparing Fig. 7 with Fig. 6, we see that, for the same spoofing power, the average number of successfully spoofed bands is larger in Fig. 7 than it is in Fig. 6. This shows that a lower threshold increases the probability of successful spoofing for a given level of spoofing power.

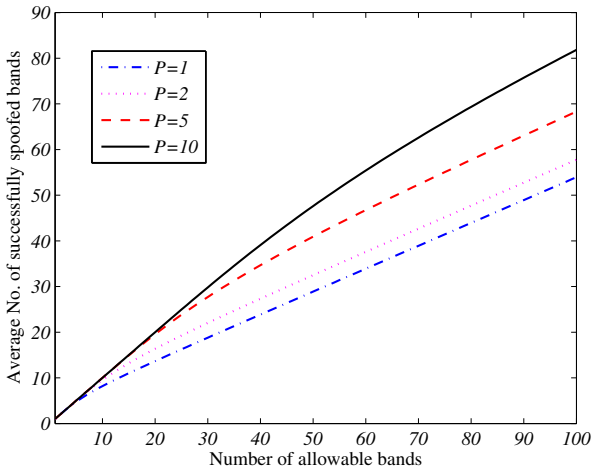

Fig. 7. Average number of successfully spoofed bands N_J versus number of allowable bands N with different spoofing powers P ($p_f = 0.50, \sigma_n^2 = 1, TW = 100$)

V. Conclusions

In this paper, an analysis of worst-case sensing deception in a cognitive radio network is presented, where the average number of allowable bands successfully spoofed by an intelligent adversary is maximized.

In particular, the optimal strategy is derived for a CR network where energy detection is used by secondary users, and is shown to correspond to equal-power, partial-band spoofing. From our analyses, the following observations are made: 1) More spoofing power allows the adversary to spoof more bands; 2) A decrease in the threshold leads to an increase in the probability of successful spoofing; 3) An increase in the time-bandwidth product will increase the spectrum sensing performance of secondary users in a noise-only environment, and it will also boost the probability of successful deception.

References

[1] Federal Communications Commission, "Spectrum Policy Task Force," Rep. ET Docket no. 02-135, Nov. 2002.

[2] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," *Proceedings of the 38th Asilomar Conf. Signals, Systems and Computers*, 2004, vol. 1, pp. 772-776.

[3] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE JSAC*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[4] A. Ghasemi, and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges, and design trade-offs," *IEEE Communications Magzine*, pp. 32-39, Apr. 2008.

[5] S. Anand, Z. Lin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *IEEE 3rd Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008.

[6] R. L. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25-37, Jan. 2008.

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

[8] S. Shellhammer, and G. Chouinard, "IEEE 802.22 Wireless RANs: spectrum sensing requirements summary." [Online]. Available: https://mentor.ieee.org/802.22/file/06/22-06-0089-01-0000-spectrum-sensing-requirements-summary.doc.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[10] S. S. Rao, *Optimization: Theory and Applications*, 2nd edition, John Wiley and Sons, 1983.
[11] Q. H. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," submitted to *IEEE Trans. on Vehicular Technology*.
[12] J. G. Proakis, *Digital Communications*, 4th edition. McGraw-Hill, 2000.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.