Tradeoff between Spoofing and Jamming a Cognitive Radio

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, Emails: {pcosman, milstein}@ucsd.edu

Abstract*—Recent studies show that spectrum sensing in cognitive radio exposes vulnerabilities to adversaries. An intelligent adversary can launch sensing disruption in the sensing duration, by putting spoofing signals in allowable bands to prevent secondary users from accessing. In the meantime, the adversary can also attack secondary users by traditional jamming, once they access the spectral bands and start transmission. Both attacks can significantly degrade the performance of a cognitive radio system. In this paper, we address the design of an energy constrained intelligent adversary. More specifically, a global optimization problem is formulated, to optimally distribute its energy between spoofing and jamming, so that the average sum throughput of the secondary users is minimized. To simplify the computation complexities, we divide our optimization into a 2-step problem: first optimally spoof and then optimally jam. Numerical results show that, to induce the worst effect on the average sum throughput of the secondary users, there is a tradeoff between spoofing and jamming: 1) when spoofing and jamming capabilities are comparable, the optimal attack is a combination of partial-band spoofing and partial-band jamming; 2) when spoofing is more effective, a spoofing only strategy is required; 3) when jamming capability dominates, a jamming only attack should be adopted.

***Index Terms*—Cognitive Radio, spoofing, jamming, optimization, tradeoff.**

I. Introduction

COGNITIVE Radio (CR) [1] has been widely studied as one promising solution to the contradiction between spectrum shortage and low spectral utilization. A CR network allows for dynamic access of unused bands with minimal interference to primary users, thus spectral efficiency is increased.

However, the sensing-before-accessing paradigm of CR exposes vulnerabilities [2], [3] to a rival entity of secondary users, namely, an adversary. In sensing durations, secondary users identify spectral vacancies through spectrum sensing, whereby an intelligent adversary can launch sensing disruption so that available bandwidth for a secondary user can be significantly degraded [4], [5]. On the other hand, when a communication link is established for a secondary user, it can be interfered with transmission by an intelligent adversary through traditional jamming [6], and hence effective transfer of information is denied.

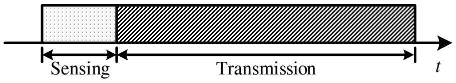

Fig. 1. Frame structure for cognitive radio with periodic spectrum sensing

Both attacks (spoofing and jamming) serve for the degradation of secondary users' performances in CR. Ideally, if the intelligent adversary has enough energy, it can first spoof in the sensing duration, to maximally reduce available bandwidth for the secondary user; and then jam in the transmission slot, to maximally degrade the secondary's transfer of information in the bands the secondary accesses. However, the adversary usually has limited energy budget. Here comes a problem: how to choose between spoofing and jamming for the intelligent adversary?

In this paper, an intelligent adversary is designed, by minimizing throughput of the secondary user, through optimal energy distribution between spoofing and jamming. A joint spoofing and jamming optimization problem is mathematically formulated. In order to reduce the complexity of computation, we transform this global optimization into a 2-step scheme: first optimally spoof in sensing duration, and then optimally jam in the transmission slot. Numerical results indicate that there is a tradeoff between spoofing and jamming: for the intelligent adversary, a portion of the energy should be allocated in spoofing, and the remaining should be distributed in jamming.

The remainder of this paper is organized as follows: Section II outlines the system model. Section III formulates a global optimization of joint spoofing and jamming, and describes the 2-step optimization technique. Section IV demonstrates the numerical results, and Section V presents our conclusions.

II. System Model

The cognitive radio system considered in this paper employs periodic spectrum sensing. The frame structure [7] in time-domain of this CR network consists of one sensing slot and one data transmission slot, as illustrated in Fig. 1.

In the sensing slot, the secondary identifies spectral vacancies through sensing, so as to access those vacant bands and then start transmission in the data transmission slot. Let T_0 be the duration of the sensing slot, and T_1 the duration

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

of the transmission slot. The ratio of transmission-to-sensing duration, α, is defined as $\alpha \triangleq T_1/T_0$.

For an intelligent adversary, it can spoof in the sensing duration [4], and then jam in the data transmission slot [6]. Spectral bands not currently used by primary users are termed *allowable bands*. Those allowable bands in which the adversary chooses to emit spoofing signals are termed *spoofed bands*. The allowable bands that are not spoofed are called *vacant bands*. In the transmission duration, the bands that the adversary puts jamming signals in are called *jammed bands*. Assuming we have, at the start of the sensing slot, N allowable bands.

A. Spoofing in the Sensing Slot

In spectrum sensing, the probability that a vacant band is sensed to be busy by a secondary user is nonzero, due to thermal noise. This probability, termed false detection probability [5], will be further increased by spoofing. This, in turn, increases the average number of false detections, N_J, which is the sum of false detection probability of each allowable band, thereby reducing the average number of available bands (i.e., $N - N_J$) for a secondary user.

For a secondary using energy detection for sensing, the false detection probability in the kth allowable band, p_k, can be expressed as a function of spoofing power in that band, and is given by [4], [5] and [8]

$$p_k(P_{D,k}) = Q\left(\frac{a}{P_{D,k} + \sigma_n^2} + b\right) \tag{1}$$

where σ_n^2 is the thermal noise power, and $P_{D,k}$ is the spoofing power in the kth band. Parameters a and b are given by $a = K/2\sqrt{T_0 W}$, and $b = -\sqrt{T_0 W}$, where K is the threshold used by the secondary for sensing, W is the bandwidth of one allowable band, and $T_0 W$ corresponds to the integration-time-bandwidth product at the energy detection receiver.

B. Jamming in the Data Transmission Slot

After spectrum sensing, some allowable bands are falsely determined to be busy, while the others are identified as vacant. The throughput of the secondary in the kth band, Γ_k, is given by [9]

$$\Gamma_k = (1 - PER_k(\gamma))(z log_2 M) \tag{2}$$

where z is the total number of modulated symbols in one packet, $log_2 M$ is the number of bits in one symbol, and $PER_k(\gamma)$ is the packet error rate of the kth allowable band, given by

$$PER_k(\gamma) = 1 - (1 - SER_k(\gamma))^z \tag{3}$$

where $SER_k(\gamma)$ is the conditional symbol error probability of the kth allowable band, conditioned on the channel state. For QPSK modulation, it is expressed as

$$SER_k(\gamma) = 2Q\left(\sqrt{2\gamma}\right)\left[1 - \frac{1}{2}Q\left(\sqrt{2\gamma}\right)\right] \tag{4}$$

where $\gamma = E_b/N_0$.

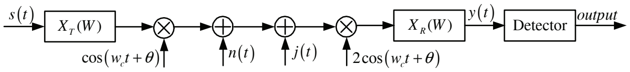

Fig. 2. System model for secondary users in the presence of noise jamming

The throughput defined in (2) can be degraded by jamming of the intelligent adversary. A Gaussian noise jammer is considered in this paper, and is assumed to be independent of the background additive Gaussian noise. The spectrum of the jamming signal is rectangular (with bandwidth, W_0) in each jammed band. The block diagram of the system model for a secondary user in the presence of jamming signal is presented in Fig. 2. $X_T(W)$ is the frequency response of the root raised cosine filter, which serves to limit the bandwidth of the secondary user's signal without causing ISI. $X_R(W)$ at the receiver corresponds to the matching filter of $X_T(W)$, and $X_T(W) \cdot X_R(W) = X(W)$, where $X(W)$ is the frequency response of the raised cosine filter given by [Eq. 9.2-26,10]. Therefore, the conditional symbol error probability in the presence of noise jamming is given by

$$SER_k = 2Q\left(\sqrt{\frac{E_b}{N_0/2 + J_{0,k}}}\right)\left[1 - \frac{1}{2}Q\left(\sqrt{\frac{E_b}{N_0/2 + J_{0,k}}}\right)\right] \tag{5}$$

where $J_{0,k}$ is the jamming power spectral density in the kth allowable band.

III. Joint Spoofing and Jamming a Cognitive Radio

As elaborated in Section II, both spoofing and jamming contribute, in different manners, to the degradation of the throughput of a secondary user. As a practical matter, the adversary has a limited energy budget. To induce the worst effect on a secondary user, joint spoofing and jamming by an intelligent adversary is needed.

Let i $(0 \le i \le N)$ denote the number of bands sensed to be vacant by the secondary user, and N_r denote the number of bands required by the secondary users. We assume that N_r is a random variable with a Poisson distribution. At any instant of time, $N_r = n$ $(n \ge 1)$. The probability of this event is given by

$$p(N_r = n) = \frac{e^{-\lambda}\lambda^n}{n!} \tag{6}$$

where λ is a positive real number, equal to the expected number of bands required by the cognitive radio system. The number of bands used by secondary users, N_S, is jointly determined by i and $N_r = n$. That is,

$$N_S = \begin{cases} i & i \le n \\ n & i > n \cdot \end{cases} \tag{7}$$

The conditional average sum throughput of the secondary user, $\Gamma_{N_r=n}^{sum}$, conditioned on N_r, is then given by

$$\Gamma_{N_r=n}^{sum} = \sum_{i=1}^{n} p_{N,i}\left(\sum_{k=1}^{i}\Gamma_k\right) + \sum_{i=n+1}^{N} p_{N,i}\left(\sum_{k=1}^{n}\Gamma_k\right) \tag{8}$$

where $p_{N,i}$ is the probability that i out of N allowable bands are sensed to be vacant by the secondary, and is expressed as

$$\begin{aligned} p_{N,1} &= (1-p_1)\prod_{k\neq 1} p_k + \cdots + (1-p_N)\prod_{k\neq N} p_k && (9)\\ p_{N,2} &= (1-p_1)(1-p_2)\prod_{k\neq 1,2} p_k + \cdots + (1-p_1)\cdot \\ & \quad (1-p_N)\prod_{k\neq 1,N} p_k + (1-p_2)(1-p_3)\cdot && (10)\\ & \quad \prod_{k\neq 2,3} p_k + \cdots + (1-p_2)(1-p_N)\prod_{k\neq 2,N} p_k \\ & \quad \vdots \\ & \quad +(1-p_{N-1})(1-p_N)\prod_{k\neq N-1,N} p_k && (11)\\ p_{N,N} &= \prod_{k=1}^{N}(1-p_k) && (12) \end{aligned}$$

where p_k is the false detection probability defined in (1). The throughput in the kth band, Γ_k, is expressed in (2).

The average sum throughput, Γ^{sum}, is then given by

$$\Gamma^{sum} = \sum_{n=1}^{+\infty} \Gamma^{sum}_{N_r=n} p(N_r = n)\cdot \qquad (13)$$

From Eqs. (7) and (8), we can see that, when $n \geq N$, the conditional average sum throughout, $\Gamma^{sum}_{N_r=n} = \Gamma^{sum}_{N_r=N}$. Therefore, (13) can be written as

$$\begin{aligned} \Gamma^{sum} &= \sum_{n=1}^{N-1} \Gamma^{sum}_{N_r=n} p(N_r = n) \\ &+ \Gamma^{sum}_{N_r=N}\left[1 - \sum_{n=0}^{N-1} p(N_r = n)\right] \qquad (14) \end{aligned}$$

The expression for the average sum throughput, Γ^{sum}, (as in (14)), reflects two functions of the intelligent adversary: one is in $p_{N,i}$, which serves to reduce the secondary user's bandwidth by spoofing in the sensing slot, and the other one is in Γ_k, which serves to degrade the transmission of the secondary by jamming in the data transmission slot, in the bands that are accessed by the secondary user after sensing. Therefore, the joint spoofing and jamming for an intelligent adversary with energy constraint, is given by

$$\begin{aligned} min \quad & \Gamma^{sum} \\ s.t. \quad & T_0 \sum_{k=1}^{N} P_{D,k} + \alpha T_0 \sum_{k=1}^{N} P_{J,k} = E \end{aligned} \qquad (15)$$

where P is the maximum instant power constraint on the adversary, and E is the total energy budget.

The expression for the average sum throughput in (15) is very complicated, which involves two main functions of the intelligent adversary: 1) spoofing, as reflected in $p_{N,i}$; 2) jamming, as indicated in Γ_k. In order to simplify this optimization, we can think in the following way. Assume that a portion, ρ $(0 \leq \rho \leq 1)$ of the adversary's energy is allocated for spoofing, and the remaining portion, $1-\rho$, is distributed for jamming. In the spoofing, an optimal noise spoofing strategy is used; In the jamming, an optimal noise jamming is adopted. The optimal attack by the intelligent adversary is then obtained by minimizing the average sum throughput, Γ^{sum}, over all possible values of ρ.

A. *Optimal Spoofing*

As shown in [4] and [5] that the optimal noise spoofing is an equal-power, partial-band strategy. That is, to spread spoofing power equally into N^* (the optimal number of spoofed bands) out of N allowable bands, where $0 \leq N^* \leq N$. Let ϕ^* denote the set of spoofed bands, and ϕ be the set of vacant bands. Therefore, for the kth band, the false detection probability, i.e., the probability that the secondary will avoid this band, is given by

$$\begin{cases} p_k = Q(\dfrac{a}{P_D + \sigma_n^2} + b) & k \in \phi^* \\ p_k = Q(\dfrac{a}{\sigma_n^2} + b) & k \in \phi \end{cases} \qquad (16)$$

where P_D is the spoofing power allocated in each spoofed band, and is identical across all spoofed bands.

B. *Optimal Partial-Band Noise Jamming*

A partial-band noise jamming is utilized by the adversary in the transmission slot, where it spreads power over a fraction of the total bands the secondary is occupying. At the instant of time, there are N_S bands used by the secondary. The adversary puts its remaining energy into N_{Jam} bands, where $1 \leq N_{Jam} \leq N_S$. The optimal number of jammed bands, N^*_{Jam} $(1 \leq N^*_{Jam} \leq N_S)$, is chosen such that the average sum throughput during this transmission phase is minimized, with respect to the given energy for jamming.

IV. Tradeoff between Spoofing and Jamming a Cognitive Radio

In this section, numerical results are provided for a cognitive radio network where the transmission-to-sensing duration ratio, α, is set to be 10 [7], the integration-time-bandwidth product $T_0W_0 = 100$, the threshold used by the secondary users corresponds to a false alarm probability $p_f = 10^{-2}$, and $z = 255$ [9]. The thermal noise power (in watts) in one allowable band at the energy detection receiver, σ_n^2, is taken to be unity, and E_b/N_0 for a secondary user is $8.79dB$, which corresponds to a symbol error rate of 10^{-4}. We define J/S to be the jamming-to-signal power ratio, where J is the jamming power when all the adversary's energy is put into jamming, i.e., $J = E/\alpha T_0$, and S is the signal power of a secondary user.

In Fig. 3, the average sum throughput, Γ^{sum}, versus the percentage of energy for spoofing is plotted, for the case when there are 100 allowable bands, and only a small fraction of them are required by the cognitive radio system, e.g., $\lambda = 1$. It is seen that the minimum of Γ^{sum} is obtained when no energy is allocated for spoofing. That is, all the energy should be allocated to jamming, in order to maximally degrade the secondaries' average sum throughput.

We now increase the average number of bands required by secondary users, λ, from 1 to 10, and keep the other parameters

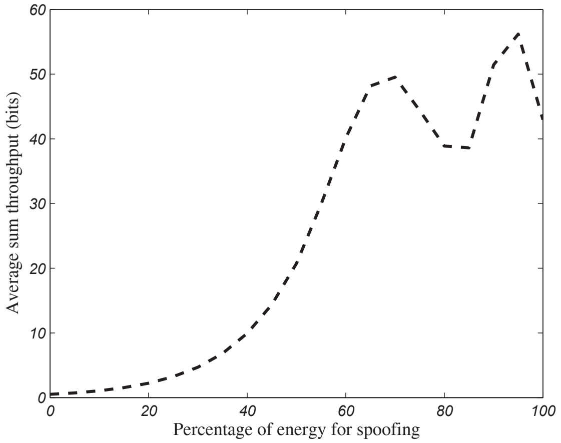

Fig. 3. Average sum throughput versus percentage of energy for spoofing (The total number of allowable bands $N = 100$, $\lambda = 1$, $E_b/N_0 = 8.79dB$, and $J/S = 0dB$)

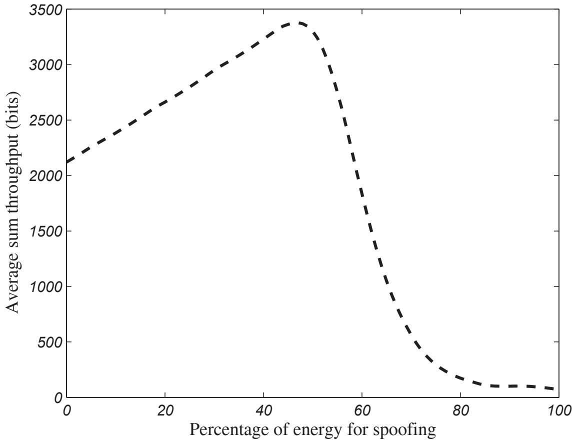

Fig. 4. Average sum throughput versus percentage of energy for spoofing (The total number of allowable bands $N = 100$, $\lambda = 10$, $E_b/N_0 = 8.79dB$, and $J/S = 0dB$)

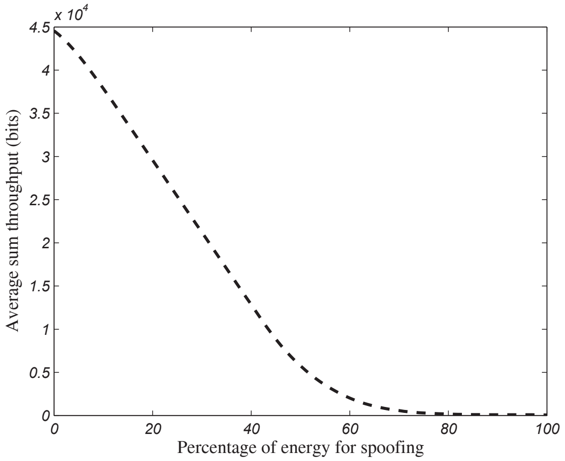

Fig. 5. Average sum throughput versus percentage of energy for spoofing (The total number of allowable bands $N = 100$, $\lambda = 100$, $E_b/N_0 = 8.79dB$, and $J/S = 0dB$)

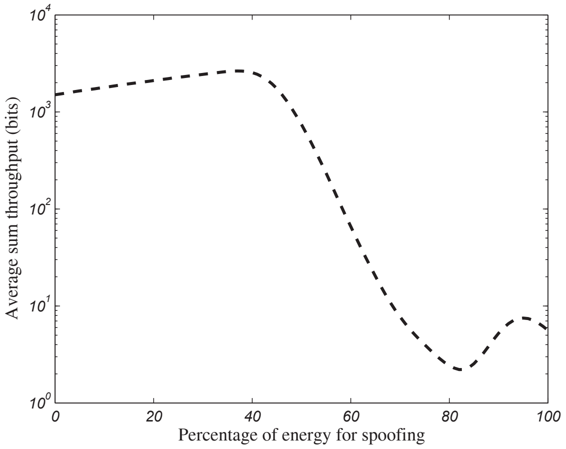

Fig. 6. Average sum throughput versus percentage of energy for spoofing (The total number of allowable bands $N = 100$, $\lambda = 10$, $E_b/N_0 = 8.79dB$, and $J/S = 1dB$)

unchanged, as in Fig. 3. The average sum throughput versus the percentage of energy for spoofing is plotted in Fig. 4. It is seen that the minimum of Γ^{sum} is achieved when all the energy is allocated to spoofing. This is further illustrated in Fig. 5, where $\lambda = 100$, i.e., all the allowable bands are required by secondaries, and other parameters stay unchanged. It is seen that the average sum throughput monotonically decreases as the percentage of energy for spoofing increases. The minimum of Γ^{sum} occurs when all the energy is allocated for spoofing.

Consider now Fig. 6, where Γ^{sum} versus the percentage of energy for spoofing is plotted for a jamming-to-signal power ratio $J/S = 1dB$ and $\lambda = 10$. It is seen that the minimum of the average sum throughput, Γ^{sum}, is achieved when roughly 80 percent of the energy is allocated for spoofing. That is, the remaining 20 percent of energy should be allocated for jamming. In this case, to induce the worst effect on the cognitive radio system, a combination of partial-band spoofing and partial-band jamming is needed.

In Fig. 7, the average sum throughput versus the percentage of energy for spoofing is plotted for the case where $\lambda = 100$, and $J/S = 10dB$. With fixed value of αT_0, the increase in J/S means an increase in the energy budget of the intelligent adversary. It is seen that the minimum of Γ^{sum} is obtained when all the energy is put into spoofing.

V. Conclusion

A global optimization combing both spoofing and jamming for an intelligent adversary is formulated, by minimizing the average sum throughput of the secondary user. To simplify this optimization, a two-step algorithm is proposed: first optimally spoof and then optimally jam. Numerical results show that, to induce the worst effect on the secondary user, there is a tradeoff between spoofing and jamming: 1) when spoofing and jamming capabilities are comparable, the optimal attack is a combination of partial-band spoofing and partial-band jamming; 2) when spoofing capability is more effective, a spoofing only strategy is required; 3) when jamming capability dominates, a jamming only attack should be adopted.

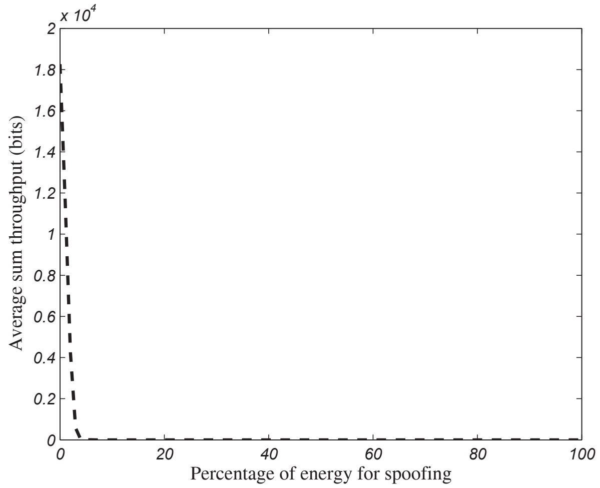

Fig. 7. Average sum throughput versus percentage of energy for spoofing (The total number of allowable bands $N = 100$, $\lambda = 100$, $E_b/N_0 = 8.79dB$, and $J/S = 10dB$)

References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE Journal of Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] T. X. Brown, and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," *IEEE International Conf. on Cognitive Radio Oriented Wireless Networks and Communications*, Aug. 2007, pp. 456-464.

[3] 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.

[4] Q. H. Peng, P. C. Cosman, and L. B. Milstein, "Worst-case sensing deception for cognitive radio networks," *IEEE Globecom 2009*, accepted.

[5] Q. H. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," submitted to *IEEE Transactions on Vehicular Technology*, 2009.

[6] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, Vol. 1, Computer Science Press, 1985.

[7] Y. C. Liang, Y. H. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

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

[9] S. S. Tan, M. Rim, P. C. Cosman, and L. B. Milstein, "Adaptive Modulation for OFDM-based Multiple Description Progressive Image Transmission," *IEEE Globecom*, 2008.

[10] J. Proakis, *Digital Communications*, 4th edition, Cambridge University Press, 2006.