Coordinated Denial-of-Service Attacks in IEEE 802.22 Networks

Yi Tan
Department of ECE
Stevens Institute of Technology
Hoboken, NJ
Email: ytan@stevens.edu

Shamik Sengupta
Department of Math. & Comp. Sci.
John Jay College of Criminal Justice
CUNY, New York, NY
Email: ssengupta@jjay.cuny.edu

K.P. Subbalakshmi
Department of ECE
Stevens Institute of Technology
Hoboken, NJ
Email: ksubbala@stevens.edu

***Abstract*— The cognitive radio enabled IEEE 802.22 wireless regional area network (WRAN) is designed to opportunistically utilize the unused or under-utilized TV bands. However, due to the lack of proactive security protocols and proper interaction policies among the secondary networks themselves, the IEEE 802.22 networks are vulnerable to various denial-of-service (DoS) threats. In this paper, we study the impact of coordinated DoS attacks on IEEE 802.22 networks from the malicious nodes' perspective. Assuming that multiple malicious nodes will launch coordinated attacks, we formulate a cooperative game among the malicious nodes. The expression of the net payoff is derived and the optimal decision strategy for the malicious nodes is obtained numerically. Simulation results demonstrate that the coordinated attack approach can enhance as high as 10-15% more net payoff for the malicious nodes than the uncoordinated attack.**

I. Introduction

The conventional fixed spectrum assignment policy has resulted in suboptimal use of spectrum resource leading to over-utilization in some bands and under-utilization in others [1]. This observation has led to the recent spectrum policy reforms by Federal Communication Commission (FCC). This goal, of dynamic spectrum access (DSA), is expected to be achieved via the recently proposed concept of cognitive radios.

The IEEE 802.22 is an emerging standard for cognitive radio-based wireless regional area networks (WRANs). The IEEE 802.22 standard aims at using DSA to allow the geographically unused, licensed TV frequency spectrum to be used by unlicensed users on a non-interfering basis [2]. To protect the primary incumbent services, IEEE 802.22 devices are required to perform periodic spectrum sensing and evacuate promptly upon the return of the licensed users.

Even though the primary user protection mechanisms have been proactively specified, neither the secondary-secondary interaction mechanisms nor the protection of secondary devices/networks have been specifically defined or addressed in IEEE 802.22 standard [3]. Hence, the IEEE 802.22 networks are vulnerable to denial-of-service (DoS) attacks, by which the attacker will prevent the secondary networks from using the spectrum band effectively or at all. Several research works are investigating into the different security aspects in cognitive radio networks [4], [5]. However, most of these works either deal with single malicious node or uncoordinated attacks by multiple malicious nodes or are not specific to IEEE 802.22.

In this paper, we address a key fundamental question: *what if multiple malicious nodes launch DoS attacks in a coordinated manner?* Recently, a hacker brought down the Twitter by using thousands of malware-infected personal computers to launch DoS attacks coordinately, which made millions of Twitter users unable to access the service. In the wireless DSA networks, this kind of threat is even worse as specific security policies have not yet been developed. Thus, understanding this attack model is absolutely critical. In this work, we study the coordinated attack using the concept of cooperative game theory. In our model, the common goal of the malicious nodes is to disrupt the communications of protocol compliant IEEE 802.22 secondary networks. We assume that the malicious nodes are also spectrum agile, but do not have a priori knowledge of the spectrum occupancy at any given time. We model this problem as a cooperative game where the malicious nodes will collaborate to attack as many secondary networks as possible while keeping their costs to a minimum. As a collaborative team, the malicious nodes try to maximize the net payoff rather than their individual payoffs. We derive the theoretical expression of the net payoff as well as the optimal strategy for the malicious nodes. Simulation results demonstrate that the cooperation among malicious nodes can remarkably increase their net payoff compared to the non-cooperative attack. To the best of our knowledge, this work is the first attempt to analyze and understand the coordinated DoS attack in IEEE 802.22 networks.

The rest of this paper is organized as follows. The system model is discussed in Section II. In Section III, we derive the expression of the net payoff and the optimal strategy for malicious nodes. Section IV presents the simulation results and conclusions are drawn in the last Section.

II. System Model

A typical IEEE 802.22 cell is a single-hop, point-to-multipoint wireless network, in which a central Base Station (BS) controls the medium access of a number of associated consumer premise equipments (CPEs). In our model, we consider N available spectrum bands not being used by primary incumbents, and n $(n \leq N)$ such IEEE 802.22 secondary networks. For simplicity, we assume that each secondary network transmits in a spectrum band free of interference of other secondary networks to guarantee high quality-of-service (QoS). This can be achieved via the IEEE 802.22 self-coexistence mechanism as presented in [6]. Thus, n out of N spectrum bands are concurrently used by the secondary networks. We refer to these n spectrum bands as *busy bands* and other $N-n$ spectrum bands as *vacant bands*.

Moreover, let there be m $(m \leq N)$ malicious nodes aiming to attack the secondary networks. They can switch among N bands but do not have a priori knowledge about which bands the secondary networks are using at any given time. We assume that the malicious nodes can use the common control channel (CCC) to coordinate their actions [7].

Before we begin the analysis, we first define the notations that will be used throughout the paper:

- *Net payoff* – The sum of payoffs for all malicious nodes.
- *Individual payoff* – The payoff for one malicious node.
- c – Switching cost: the energy consumed in switching from one spectrum band to another.
- g – Attack gain: the incentive obtained by successfully attacking one secondary network. It is the motivation for the malicious nodes to launch DoS attacks.

A. Cooperative Game Formulation

In the traditional non-cooperative game, all players are assumed selfish and act in a distributed manner, i.e., they make decisions independently to maximize their individual payoffs. The solution to the non-cooperative game is the Nash equilibrium, which is defined as a strategy set such that no player can increase its individual payoff by changing the strategy unilaterally [8].

However, the non-cooperative Nash equilibrium just emphasizes the equilibrium among the independent players rather than their common interests [8]. If all players have the same objective (e.g., in our case, all malicious nodes aim to disrupt the communications of IEEE 802.22 secondary networks), non-cooperative Nash equilibrium might not be the best solution because it does not take into account the cooperation among players. Hence, we study the behaviors of malicious nodes from the cooperative game theoretic point of view and investigate whether the cooperation could improve the benefits for the malicious nodes.

Based on the system model, we consider m malicious nodes as the game players. Rather than being "always greedy and profit seeking", all players are selfless and work as a collaborative team. Each malicious node has two possible choices: staying in the current band (saving switching cost) or switching to other bands (expecting to attack another secondary network). If the malicious nodes successfully attack a secondary network, they will obtain the attack gain, g. On the other hand, every switch will incur a switching cost, c.

The main assumption in a cooperative game is that all players will reach a grand coalition before the game starts and are not allowed to deviate from this coalition. Otherwise, the players will act individually in a non-cooperative way. The challenge in reaching an agreement is to allocate the total utilities to the players fairly and effectively. In our case, we apply Nash Bargaining solution which provides fairness, uniqueness and Pareto-optimization [8]. Due to the homogeneity of all players, the most effective way to divide the utility is equal allocation. Thus, the optimization problem for the cooperative game is to find a mechanism of switching or staying for the malicious nodes such that the net payoff can be maximized.

III. Analysis of Net Payoff and Optimal Strategy

The pure strategies for the malicious nodes, in our case, are to either stay in the current band or to switch to another band. However, if the malicious nodes choose to stay in the same band always, they will miss opportunities to attack other secondary networks. On the other hand, if the strategy is to always switch, this could lead to some unnecessary costs. Therefore, it is necessary for the malicious nodes to adopt a mixed strategy space to find the optimal solution. Assuming all players make their moves simultaneously, we define the mixed-strategy space for the malicious nodes as:

$$S_{\text{mixed}} = \{(\text{Switch prob.} = p), (\text{Stay prob.} = 1-p)\}. \quad (1)$$

That is, the players will switch with probability p and stay with probability $1-p$.

The net payoff for the malicious nodes is equal to the total attack gain, which depends on the number of secondary networks being successfully attacked, minus total switching costs. That in turn depends on how many malicious nodes actually choose to switch.

We consider two cases in this game:

- *Special case*: The game starts with all the malicious nodes coexisting in one busy spectrum band.
- *General case*: The game starts with the malicious nodes scattered over the spectrums bands.

A. Special Case

In order to maximize the net payoff, one malicious node will be selected by the central entity to make sure the secondary network in the current busy band can be successfully attacked, and other $m-1$ can choose to either stay or switch. The malicious nodes staying in this spectrum band will jointly launch DoS attack in this busy band, whereas the malicious nodes that switch will try to attack more secondary networks in other spectrum bands.

As a result, the probability that i out of $m-1$ malicious nodes will switch, $Q(i)$, follows a binomial distribution as:

$$Q(i) = \binom{m-1}{i} p^i (1-p)^{m-1-i}, \ 0 \leq i \leq m-1. \quad (2)$$

Moreover, since the players have no idea about which bands are occupied by the secondary networks, some malicious nodes may switch to vacant bands. Let q be the probability that the malicious node switches to a busy band, which is $q = \frac{n-1}{N-1}$. Hence, the probability that k out of i switching malicious nodes land in the busy bands, $R(k)$, is calculated as:

$$R(k) = \binom{i}{k} q^k (1-q)^{i-k}, \ 0 \leq k \leq i. \quad (3)$$

Note that, among these k malicious nodes who switch to busy bands, some may still land up in the same band. Hence, it is necessary to know the number of busy bands that the malicious nodes have landed in.

Thus, the probability that j out of $n-1$ secondary networks have been successfully attacked by k malicious nodes, $f(j)$, is given by (see details in Appendix-I):

$$f(j) = \frac{\binom{n-1}{j}\binom{k-1}{j-1}}{\binom{k+n-2}{n-2}}. \tag{4}$$

Let j be the random variable representing the number of compromised secondary networks, then, the expected value of j, $E(j)$, is given by:

$$E(j) = \begin{cases} \sum_{j=1}^{k} f(j)\cdot j, & k>0 \\ 0, & k=0 \end{cases} \tag{5}$$

Consolidating Equations (2)–(5), we derive the expected net payoff, $U(p)$, for the malicious nodes as:

$$U(p) = g\left(\sum_{i=0}^{m-1}\sum_{k=0}^{i} Q(i)\cdot R(k)\cdot E(j)+1\right) - c\left(\sum_{i=0}^{m-1} Q(i)\cdot i\right). \tag{6}$$

The first term on the right hand side (RHS) of the equation represents the expected attack gain and the second term represents the expected switching cost for the whole team.

Based on the equal allocation principle, the common goal for the malicious nodes is to maximize the net payoff. Thus, the optimal switching probability p^* is calculated as:

$$p^* = \arg\max_{p\in[0,1]} U(p). \tag{7}$$

B. Generalized Case

In the generalized case, the malicious nodes are randomly scattered over the available spectrum bands. The central entity plays an important role in the decision making process of the players: Every malicious node senses its spectrum band (to see whether it is used by a secondary network or not) and reports back to the central entity before taking actions. The central entity sends the consolidated picture back to the malicious nodes. To maximize the attack gain, the malicious nodes, if they choose to switch, will potentially explore other unknown spectrum bands.

Based on above assumption, the malicious nodes can be divided into two subgroups: those that stand in the vacant bands and those that are in the busy bands. Those in the vacant bands will definitely switch to other spectrum bands because there is no incentive in continuing to stay in a vacant band. On the other hand, those in the busy bands will follow a similar procedure to the special case, i.e., only one malicious node will be selected to stay in each band and others can freely choose to either stay or switch with a certain probability.

Let us suppose that, in a given time slot, the malicious nodes are scattered in L out of N bands, in which h bands are used by h secondary networks. Thus, h malicious nodes will be selected to stay in these busy bands. Let r be the random variable representing the number of malicious nodes landing in vacant bands. Therefore, the malicious node who chooses to switch will try to reach one of the other $N-L$ bands whose status is unknown. Thus, the mixed strategy space in Equation (1) is only applied to $m-h-r$ malicious nodes.

Denoting p_0 as the switching probability for the malicious nodes in the generalized case and using the same logic as in the special case, we have following expressions:

- Since there are h players who definitely stay and r players who definitely switch, we just consider the rest $m-h-r$ players. The probability of i out of $m-h-r$ malicious nodes choosing *Switch*, $Q_0(i)$, is calculated as:

$$Q_0(i) = \binom{m-h-r}{i} p_0^i (1-p_0)^{m-h-r-i}, \quad 0\le i\le m-h-r. \tag{8}$$

- Since switching malicious nodes will explore $N-L$ spectrum bands whose status is unknown, in which $n-h$ bands are used by secondary networks, the probability for them to switch to the busy bands, q_0, is $q_0 = \frac{n-h}{N-L}$. Together with other r switching players, the probability of k out of $i+r$ malicious nodes landing in the busy bands, $R_0(k)$, is calculated as:

$$R_0(k) = \binom{i+r}{k} q_0^k (1-q_0)^{i+r-k}, \ 0\le k\le i+r. \tag{9}$$

- The probability that j out of $n-h$ secondary networks have been successfully attacked is given by

$$f_0(j) = \frac{\binom{n-h}{j}\binom{k-1}{j-1}}{\binom{k+n-h-1}{n-h-1}}. \tag{10}$$

- The expected value for j, $E_0(j)$, is calculated as:

$$E_0(j) = \begin{cases} \sum_{j=1}^{k} f_0(j)\cdot j, & k>0 \\ 0, & k=0 \end{cases} \tag{11}$$

Consolidating Equations (8)–(11), we derive the net payoff for the malicious nodes in the generalized case, $U_0(p)$, as:

$$\begin{aligned} U_0(p) &= g\left(\sum_{i=0}^{m-h-r}\sum_{k=0}^{i+r} Q_0(i)\cdot R_0(k)\cdot E_0(j)+h\right) \\ &\quad - c\left(\sum_{i=0}^{m-h-r} Q_0(i)\cdot i + r\right). \end{aligned} \tag{12}$$

Similarly, the optimal strategy for the malicious nodes in the generalized case is given by:

$$p_0^* = \arg\max_{p_0\in[0,1]} U_0(p) \tag{13}$$

C. Numerical Results

Both Equation (7) and Equation (13) can be solved numerically. We set the parameter values as $g=50$ and $c=20$. For example, with network parameters as: $N=50$, $n=30$ and $m=20$, the numerical results for the special and generalized cases are shown in Fig. 1.

As illustrated in Fig. 1, there exists a maximum net payoff for the malicious nodes in each case, corresponding to a unique optimal strategy, i.e., $p^*=0.6$ and $p_0^*=0.43$ for the special and generalized case respectively.

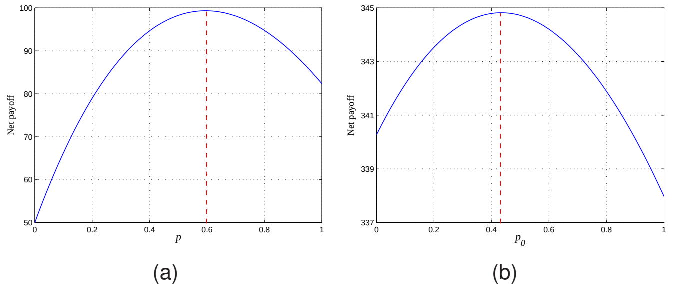

Fig. 1. The net payoff for the malicious nodes with respect to switching probability. (a) special case; (b) generalized case (with temporary state as: $L = 10$, $h = 6$ and $r = 6$).

IV. Simulation Results and Interpretation

In this section, we conduct simulations to evaluate improvement achieved by the cooperation among the malicious nodes. We consider $N = 50$ available spectrum bands and also set $g = 50$ and $c = 20$. The simulation results are averaged over 100,000 Monte Carlo simulations.

A. Simulations for the Special Case

We first conduct the simulation for the special case. Fig. 2 shows the theoretical and simulation results for the optimal switching probability for the malicious nodes, p^*, for $m - 1$ malicious nodes. As evident, the simulation results matches the theoretical results closely. Another observation is that the probability of switching is gradually converging to 1 with the increase in the number of secondary networks, n. This is because, more secondary networks existing around the spectrum bands implies better chance for the malicious nodes to switch to the busy bands. Note that the theoretical results are numerically derived from Equation (7).

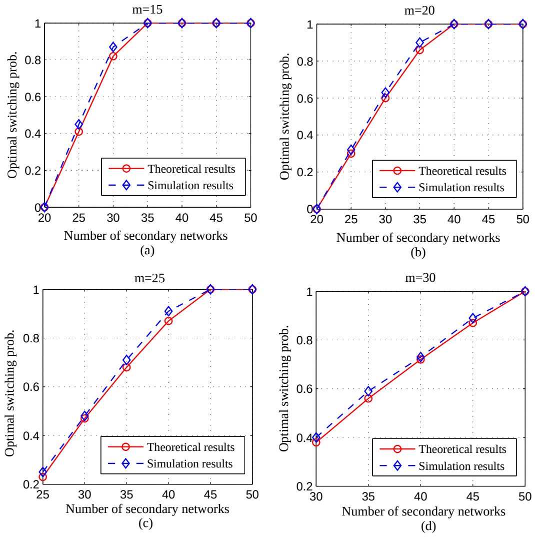

Fig. 2. The optimal probability of switching for the malicious nodes, p^*, for the special case with varying number of malicious nodes, m, and secondary networks, n.

The comparison of the net payoffs between the cooperative game and non-cooperative game is shown in Fig. 3, in which we fix the number of the malicious nodes as $m = 20$, and vary the number of the secondary networks. As illustrated in this figure, the net payoff obtained by coordinated attack achieves approximate $10 - 15\%$ improvement to the non-cooperative attack. Note that the strategy for the non-cooperative game is Nash equilibrium strategy, which, in our case, it is the switching probability for each malicious node (see details in Appendix-II). With the increase in the number of secondary networks, the malicious nodes following the optimal strategies can get greater net payoff as expected.

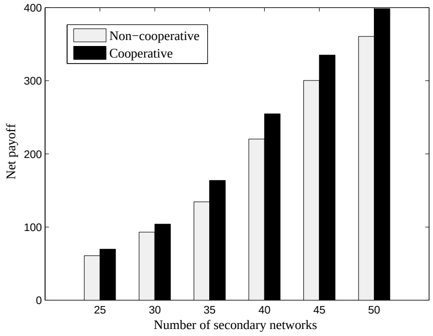

Fig. 3. The comparison of net payoff between the cooperative and non-cooperative game for the special case.

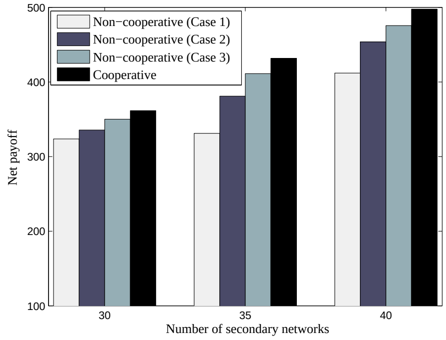

Fig. 4. The comparison of net payoff between the cooperative and non-cooperative game for the generalized case.

B. Simulations for the Generalized Case

In the general case, we consider $m = 20$ malicious nodes with temporary state as: $L = 10$, $h = 6$, $r = 6$. When comparing performances of the cooperative and non-cooperative attacks in the general case, we need to make malicious nodes who have options to stay or switch have the same Nash equilibrium point in the non-cooperative game such that it is calculable. Hence, we consider three particular cases for malicious nodes as follows:

- *Case 1*: 4 out of 6 busy bands have multiple players (each band with 2 players) and the other 2 busy bands have only one player.
- *Case 2*: 2 out of 6 busy bands have multiple players (each band with 5 players) and the other 4 busy bands have only one player.
- *Case 3*: 1 out of 6 busy bands have multiple players (9 players in this band) and the other 5 busy bands have only one player.

In each case mentioned above, the malicious nodes in the busy bands are equivalent and thus have the same Nash equilibrium strategy, which can be calculated following the same logic given in Appendix II.

Fig. 4 shows the simulation results of the comparison of net payoffs between the cooperative and non-cooperative attacks with varying number of secondary networks. Similar to the general case, the cooperative attack in the generalized case also clearly outperforms the non-cooperative attack from the malicious nodes' perspective.

V. Conclusion

In this paper, we investigated the impact of coordinated DoS attacks on IEEE 802.22 networks from the perspective of malicious nodes. Using the concept of cooperative game theory, we modeled the malicious nodes as a collaborative team aiming to maximize their net payoff by disrupting the communications of good secondary networks. We analytically derived the theoretical expression of net payoff and numerically obtained the optimal strategies for the malicious nodes group from two different perspectives. Simulation results demonstrated that by taking the coordinated approach, the malicious nodes can achieve as high as 10-15% more net payoff than that if they do not cooperate.

Acknowledgement

This work is partially supported by NSF Trustworthy Computing with grant number 0917008 and NIJ 2009-92667-NJ-IJ.

Appendix I
Derivation of Probability $f(j)$

$f(j)$ is the probability that j out $n-1$ secondary networks are successfully attacked by k malicious nodes who switch to these $n-1$ busy bands and is given by $f(j) = \frac{X \cdot Y}{Z}$, where

- X: Number of ways in which j out of $n-1$ secondary networks can be selected, which is $\binom{n-1}{j}$.
- Y: Number of ways in which a group of k malicious nodes can bring down exactly j secondary networks. This is equivalent to the number of distinct positive integer-valued vector $(x_1, x_2, \cdots, x_j)$ satisfying $x_1 + x_2 + \cdots + x_j = k$, which is $\binom{k-1}{j-1}$ [9].
- Z: Number of ways in which k malicious nodes can distribute in $n-1$ busy bands. This is equivalent to the number of distinct nonnegative integer-valued vectors $(x_1, x_2, \cdots, x_{n-1})$ satisfying $x_1 + x_2 + \cdots + x_{n-1} = k$, which is $\binom{k+n-2}{n-2}$ [9].

Therefore, $f(j)$ is given by:

$$f(j) = \frac{\binom{n-1}{j}\binom{k-1}{j-1}}{\binom{k+n-2}{n-2}}. \quad (14)$$

Appendix II
The Mixed-strategy Nash Equilibrium of the Non-cooperative Game for the Special Case

In the non-cooperative game, each malicious node is selfish and can choose to switch or stay independently. We assume that if more than one malicious nodes jointly attack the same secondary network in a spectrum band, each of them can get the average attack gain. For example, if 3 malicious nodes land in the same busy band, each can obtain $g/3$ attack gain. Without loss of generality, we consider one typical player, s, and the same reasoning applies to all other players.

(i) Expected payoff for the player s to stay:

Let us denote θ as the switching probability and so the probability that i out of other $m-1$ malicious nodes will also stay, $Q_{\text{stay}}(i)$, is calculated as:

$$Q_{\text{stay}}(i) = \binom{m-1}{i}(1-\theta)^i \theta^{m-1-i}, \ 0 \le i \le m-1. \quad (15)$$

Thus, the expected payoff for player s to stay is given by:

$$E(\text{stay}) = \sum_{i=0}^{m-1} Q_{\text{stay}}(i) \cdot \frac{g}{i+1}. \quad (16)$$

(ii) Expected payoff for the player s to switch:

The probability that i out of other $m-1$ malicious nodes will also switch with player s, Q_{switch}, is calculated as:

$$Q_{\text{switch}}(i) = \binom{m-1}{i}\theta^i (1-\theta)^{m-1-i}, \ 0 \le i \le m-1. \quad (17)$$

Note that the probability for the player s to switch to the busy bands is also $q = \frac{n-1}{N-1}$. Moreover, the probability that exactly j out of i players switch to the same band with player s, $H(j)$, is calculated as:

$$H(j) = \binom{i}{j}\frac{1}{(N-1)^j} \cdot (\frac{N-2}{N-1})^{i-j}. \quad (18)$$

Thus, the expected payoff for player s to switch is given by:

$$E(\text{switch}) = \sum_{i=0}^{m-1}\sum_{j=0}^{i} q \cdot Q_{\text{switch}}(i) \cdot H(j) \cdot \frac{g}{j+1} - c. \quad (19)$$

Consolidating *(i)* and *(ii)*, the mixed-strategy Nash equilibrium for the malicious nodes, θ^*, is obtained by imposing $E(\text{stay}) = E(\text{switch})$, which can be solved numerically.

References

[1] F. C. Commission, "Spectrum policy task force report," *IEEE Transactions on Information Forensics and Security*, pp. 02–155, Nov 2002.

[2] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Communication Magazine*, Jan. 2009.

[3] K. Bian and J.-M. J. Park, "Security vulnerabilities in IEEE 802.22," *WICON '08*, pp. 1–9, 2008.

[4] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and Mitigation," *CrownCom 2008*, pp. 1–8, May 2008.

[5] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[6] S. Sengupta, R. Chandramouli, S. Brahma, and M. Chatterjee, "A game theoretic framework for distributed self-coexistence among IEEE 802.22 networks," *IEEE GLOBECOM*, Dec. 2008.

[7] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006.

[8] R. Myerson, *Game Theory: Analysis of Conflict*. Harvard Univ., 1997.

[9] S. Ross, *A First Course in Probability*. Prentice Hall, 7 edition, 2005.