Analysis of Coordinated Denial-of-Service Attacks in IEEE 802.22 Networks

Yi Tan, Shamik Sengupta, *Member, IEEE* and K.P. Subbalakshmi, *Senior Member, IEEE*

***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 open paradigm of cognitive radio networks and lack of proactive security protocols, the IEEE 802.22 networks are vulnerable to various denial-of-service (DoS) threats. In this paper, we study the coordinated DoS attacks on IEEE 802.22 networks from the malicious users' perspective. We formulate this problem from both a one-stage and a multi-stage scenario. In the one-stage scenario, we formulate a cooperative game among the malicious nodes and derive the optimal decision strategy for the them. In the multi-stage case, we propose a discrete-time Markov chain model for the dynamic behavior of both malicious nodes and the 802.22 secondary networks. Simulation and numerical results demonstrate that in the one-stage case, the coordinated attack achieves 10-15% improvement compared to the non-cooperative attack from the perspective of malicious nodes, and, in the multi-stage case, there exists an optimal number of malicious nodes participating in the attack for the steady system to maximize the net payoff.**

***Index Terms*— IEEE 802.22 network, Cognitive Radio, Coordinated Denial-of-service attacks, Cooperative game, Discrete-time Markov chain.**

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 [2]–[4]. This observation has led to the recent spectrum policy reforms by the U.S. Federal Communication Commission (FCC). This goal, of dynamic spectrum access (DSA), is expected to be achieved via the recently proposed concept of the cognitive radio (CR) [5], [6].

The IEEE 802.22 is an emerging standard for CR-based wireless regional area networks (WRANs). The IEEE 802.22 standard aims at using DSA to allow the unused, licensed TV frequency spectrum to be used by unlicensed users on a non-interfering basis [7]. To protect the primary incumbent services, IEEE 802.22 devices (e.g., base station and consumer premise equipment) are required to perform periodic spectrum sensing and evacuate promptly upon the return of the licensed users [8].

Manuscript received December 1, 2009; revised May 23, 2010; accepted August 13, 2010. A preliminary version of portion of this material has been presented in [1]. This work was supported in part by NSF 0916180, NIJ 2009-92667-NJ-IJ and PSC-CUNY AWARD 60079-40 41.

Yi Tan and K.P. Subbalakshmi are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030 (email: {ytan, ksubbala}@stevens.edu).

Shamik Sengupta is with the Department of Mathematics and Computer Science, John Jay College of Criminal Justice, City University of New York, New York, NY 10019 (email: ssengupta@jjay.cuny.edu).

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 [9]. 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 CR networks [10], [11]. 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 work, 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 website by using thousands of malware-infected personal computers to launch DoS attacks coordinately, which made millions of Twitter users unable to access the service [12]. In wireless DSA networks, this kind of threat is even worse since specific security policies have not yet been developed. Thus, understanding this attack model is absolutely critical.

In this paper, 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. Contrary to the independent attack model, the malicious nodes in the coordinated attack try to maximize utilities as a group rather than their individual benefits. We assume that the malicious nodes are also spectrum agile, but do not have a prior knowledge of the spectrum occupancy at any given time. We investigate the problem from two perspectives: one-stage and multi-stage scenario. In the one-stage scenario, we formulate 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 intend to maximize the net payoff rather than their individual payoffs. We derive the theoretical expression for the net payoff and numerically obtain the optimal strategy (switching probability) for the malicious nodes.

We then look into the multi-stage case and incorporate the behaviors of 802.22 secondary networks. A discrete-time Markov chain is proposed to model the change of states in one typical spectrum band. We theoretically prove that as the system reaches steady state, the net payoff of malicious nodes team is independent of their switching probability but related to the number of malicious nodes participating in the attack. Simulation results corroborate the theoretical analysis and demonstrate that the cooperation among malicious nodes

can remarkably increase the net payoff of the malicious nodes compared to the non-cooperative attack manner. In addition, the numerical results indicate that when the system reaches steady state, there exists an optimal number of attacking malicious nodes to maximize the net payoff.

The main contributions of this paper are as follows:

- Formulation of the coordinated DoS attack in IEEE 802.22 networks as a cooperative game among multiple malicious nodes.
- Derivations of the net payoff and optimal strategy for malicious nodes in the one-stage case.
- A new discrete-time Markov model for the multi-stage case and investigation of the optimal number of malicious nodes participating in the coordinated attack.

The rest of this paper is organized as follows. In Section II, we discuss the body of work that relates with this paper. The system model is discussed in Section III. In Section IV, we formulate a cooperative game among the malicious nodes. In Section V, we analytically derive the expression of the net payoff and solve the optimal strategy for the malicious nodes via the numerical analysis. The discrete-time Markov chain is proposed for the multi-stage scenario in Section VI. Section VII presents the simulation and numerical results and the conclusions are drawn in last section.

II. Related Work

While other aspects of CR networks have received significant attention over the past decade, research in the area of DSA network security is still in its nascence.

The security vulnerabilities in IEEE 802.22 networks were discussed in [9], where the security sub-layer in IEEE 802.22 was discussed in brief and a description of the effects of various DoS attacks on the performance of 802.22 networks were discussed. Clancy *et al.* described a new class of attacks in CR networks [10], by which the secondary users can be trained to respond inappropriately for several stimuli. They give some specific examples of these attacks and discussed some potential mitigation approaches. More general discussions about the security issues in CR networks are given in [13]–[15]. Most of the above works are review articles rather than the thorough and comprehensive analysis for those security issues.

Recently, serval research groups have investigated specific DoS attacks in CR Networks. Chen *et al.* [16] described the Byzantine failure problem in the context of data fusion in the cooperative spectrum sensing. In this Byzantine attack, a malicious node intentionally sends falsified local spectrum sensing reports to the data collector in an attempt to cause the data collector to make incorrect spectrum sensing decisions. A novel reputation based mechanism called Weighted Probability Ratio Test was proposed to improve the robustness of data fusion against attacks. Another popular attack drawing much attection is primary user emulation (PUE) attack, which was originally introduced by Chen *et al.* [17]. In the PUE attack, one or multiple attacking nodes transmit in forbidden time slots and effectively emulate the primary user to make the protocol compliant secondary users erroneously conclude that the primary user is present and evacuate that spectrum band. In order to thwart this attack, a localization based defense method was developed in [11], in which a non-interactive localization scheme is employed to detect and pinpoint the PUE attack. However, these localization mechanisms require a dedicated sensor network which may not be available in practical distributed DSA networks. Jin *et al.* [18], [19] proposed a hypothesis based approach to mitigate PUE attacks using an analytical model for the received power at the secondary users without assuming any prior knowledge about the position of either the malicious or the secondary users. The first analytical model for the received power was proposed in [20].

Radio Jamming is another common and disruptive DoS attack in wireless networks. In [21], Sampath *et al.* showed that jamming attackers can utilize CRs' fast channel switching capability to amplify their jamming impact across multiple channels using a single radio. Later, a security-enhanced virtual channel rendezvous algorithm was proposed in [22] to improve the robustness of a DSA network against smart jamming attacks. Ma *et al.* discussed the jamming and anti-jamming procedures in multichannel CR systems [23]. As discussed in these works, the most effective way for the secondary transmitters to prevent the jamming attack is to avoid the jamming signal through frequency hopping.

In spite of all the above-mentioned work, there is still no framework that studies the coordination from the perspective of malicious nodes. In this paper, we propose a coordinated attack framework based on the cooperative game theory. To the best of our knowledge, this work is the first attempt to analyze and understand coordinated DoS attack in IEEE 802.22 networks.

III. System Model

A. IEEE 802.22 WRAN

IEEE 802.22 WRAN standard specifies the PHY/MAC/air_interface for the unlicensed devices in a CR network operating in the TV Broadcast bands. 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).

The IEEE 802.22 standard supports cognitive capabilities for the reliable protection of incumbent services. The spectrum sensing is performed by both the BS and CPEs in the scheduled quiet periods. The CPEs must report the spectrum sensing results to the BS and the final decision on whether a given band is available for use or not is then made by the BS. In order to satisfy the quality-of-service (QoS) requirement for every cell, IEEE 802.22 prescribes two types of inter-BS dynamic spectrum sharing mechanisms: non-exclusive and exclusive spectrum sharing. In the non-exclusive spectrum sharing, multiple 802.22 networks can transmit in the same band with appropriate transmission power control settings. On the other hand, in the case of exclusive spectrum sharing, one 802.22 network will exclusively occupy the selected band via On-Demand Spectrum Contention protocol [24].

B. Attack Model

We consider N available spectrum bands, i.e., bands not used by primary incumbents, and n $(n < N)$ IEEE 802.22 secondary networks, each of which consists of one BS and multiple CPEs. We assume exclusive spectrum sharing in our model, i.e., each 802.22 secondary network can use the spectrum band only if it is free interference of other secondary networks. This can be achieved via the 802.22 self-coexistence mechanism as presented in [25]. Thus, n out of N spectrum bands are concurrently used by the 802.22 secondary networks. We refer to these n spectrum bands as *busy bands* and other $N - n$ spectrum bands as *vacant bands*.

Let there be m $(m \leq n)$ malicious nodes aiming to attack the secondary networks by launching DoS attacks. They can switch among N bands but do not have prior knowledge about which bands the secondary networks are using at any given time. We assume that there exists a malicious central entity which collects and distributes the information regarding the secondary networks' occupancy of spectrum bands that the malicious nodes have already reached. Note that the malicious central entity will not specifically assign each individual malicious node with distinct spectrum band because too many actions will cause a lot of delay and additional overhead. To eliminate such overhead, we assume a minimum shadow coordination procedure in this work.

We now define the notations that will be used throughout the paper:

- *Net payoff* – The sum of total payoffs for all malicious nodes.
- *Individual payoff* – The payoff for a single malicious node.
- c – Switching cost: the cost incurred by the malicious nodes while switching from one spectrum band to another, e.g., the energy consumed in switching.
- g – Attack gain: the incentive obtained by the malicious nodes while successfully attacking a IEEE 802.22 secondary network.

The constraints of relationship between g and c are as follows:

- $g > c$: This constraint guarantees that malicious nodes have incentives to launch attacks. If not held, the malicious nodes will keep silent because the benefit of a successful attack cannot compensate the cost incurred by one switch.
- g should *not* be much greater than c: This constraint makes the malicious nodes consider the tradeoff between switching and staying. If not held, the malicious nodes will keep switching because even one successful attack still outweighs the cost incurred by many switches.
- c should *not* be very close to g: This constraint guarantees that the malicious nodes have enough incentive to switch to another spectrum band. If not held, the malicious nodes will always choose to stay in order to avoid high switching costs if the number of busy bands is small.

IV. DoS Attacks as a Cooperative Game

In this section, we formulate the DoS attack in IEEE 802.22 networks as a one-stage cooperative game among the malicious nodes, in which the malicious nodes will make a one-shot move cooperatively to maximize their benefits. Later, we will study the multi-stage case of the system model.

A. Cooperative Game Formulation

In the 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 its strategy unilaterally [26].

However, the non-cooperative Nash equilibrium just deals with the equilibrium among the independent players rather than their common interests [26]. 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 be a sub-optimal solution because it does not take into account the cooperation among players. Thus, we propose a coordinated attack approach where all players are selfless and work as a collaborative team rather than being "always individually greedy and profit seeking" in the non-cooperative attack, and study the behavior of malicious nodes from the cooperative game theoretic perspective.

Based on the system model, we consider m malicious nodes as the game players. We define two possible choices for the malicious nodes: staying in the current spectrum band (saving switching cost) or switching to other spectrum bands (expecting to attack another secondary network). If the malicious nodes successfully disrupt the communication of a secondary network, they will obtain the attack gain, g. On the other hand, every switch will incur a switching cost, c.

B. Nash Bargaining Solution

The main assumption in a cooperative game is that all players would reach a grand coalition before the game is played and players are not allowed to deviate from this coalition. Otherwise, the players will act individually in a non-cooperative way. The challenge to reach an agreement is to allocate the total utilities to the players fairly and effectively. Among different cooperative game solutions, Nash Bargaining Solution (NBS) provides fairness, uniqueness and Pareto-optimality [26]. The following theorem, originally proposed by Nash [27], shows how to derive the unique NBS [26].

Theorem: In a K-player cooperative game, let $\mathbb{U}$ be the set of all feasible payoff allocations and $\mathbb{R} = (r_1, r_2, \cdots r_i, \cdots)$ be the vector of achievable payoffs that the players can get without cooperation (disagreement payoff), the unique NBS u^* is calculate as:

$$< u^* >= \arg\max_{u \in \mathbb{U}} \prod_{i=1}^{K} (u_i - r_i). \tag{1}$$

The NBS is also the point where "*egalitarian*" and "*utilitarian*" solutions of the bargaining problem coincide [26]. Due to the homogeneity of the malicious nodes, the disagreement payoff for every player would be identical, i.e., $r_1 = r_2 =$

$\cdots = r_K$. Hence, according to the geometric inequality, the NBS based on Eqn (1) is to maximize u_i^* and make $u_i^* = u_j^*$ for all $i, j \in [1, K]$. Therefore, maximizing u_i^* subject to the equal allocation is equivalent to maximizing the total utility that the players can get. Thus, the optimization problem for our cooperative game is to find a mechanism of switching or staying for the malicious nodes such that the net payoff can be maximized.

V. Analysis of Net Payoff and Optimal Strategy for One-stage Case

In our model, the pure strategies for malicious nodes are to either stay in the current band or to switch to another band. However, if all 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. Hence, following a pure strategy is sub-optimal. 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:

$$S_{\text{mixed}} = \{(\text{Switch prob.} = p), (\text{Stay prob.} = 1 - p)\}. \quad (2)$$

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. In the one-stage game, we assume that once the malicious nodes land in the busy bands, they can successfully disrupt the communications of secondary networks in there. Later, we will relax this assumption and analyze different specific attacks in the multi-stage case.

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 the special case, all malicious nodes are in the same busy band. In order to maximize the net payoff, one malicious node will be selected 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 node that stays in this spectrum band will be a part of the attacking group, i.e., launching attacks joining with other staying malicious nodes, whereas the malicious node that switches 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:

$$Q(i) = \binom{m-1}{i} p^i (1-p)^{m-1-i}, \ 0 \le i \le m-1. \quad (3)$$

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 given by:

$$q = \frac{n-1}{N-1}. \quad (4)$$

Hence, the probability that k out of i switching malicious nodes will land in the busy bands, $R(k)$, is calculated as:

$$R(k) = \binom{i}{k} q^k (1-q)^{i-k}, \ 0 \le k \le i. \quad (5)$$

Among these k malicious nodes who switch to busy bands, some may still land up in the same band. However, based on our game formulation, the total attack gain only depends on how many secondary networks have been successfully attacked. Hence, it is necessary to know the number of *distinct* busy bands that the malicious nodes have actually landed in.

The probability that k malicious nodes land in j busy bands (i.e., 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):

$$f(j) = \frac{\binom{n-1}{j}\binom{k-1}{j-1}}{\binom{k+n-2}{n-2}}. \quad (6)$$

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

$$E(j) = \begin{cases} \sum_{j=1}^{k} f(j) \cdot j, & k > 0 \\ 0, & k = 0 \end{cases} \quad (7)$$

Consolidating Eqns (3)–(7), we derive the expected net payoff, $U(p)$, for the malicious nodes as:

$$U(p) = g\left(\sum_{i=0}^{m-1}\sum_{k=0}^{i} Q(i) \cdot R(k) \cdot E(j) + 1\right) - c\left(\sum_{i=0}^{m-1} Q(i) \cdot i\right). \quad (8)$$

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:

$$p^* = \arg\max_{p \in [0,1]} U(p). \quad (9)$$

B. General Case

In the general case, the malicious nodes are randomly scattered over the available spectrum bands. Every malicious node observes its current spectrum band (to see whether it is used by a secondary network or not) and sends a beacon to the malicious central entity before taking actions. The malicious central entity will distribute the consolidated picture about the secondary networks' occupancy of these spectrum bands back to the malicious nodes. For sake of simplicity, we ignore the delay and overhead due to this coordination procedure in our analysis because sending a beacon and multicasting an

identical information will be quick and cost-efficient. Thus, in order to maximize the attack gain, the malicious nodes, if they choose to switch, will potentially explore other unknown spectrum bands.

Based on the above assumption, the malicious nodes can be divided into two subgroups: those that fall in the vacant bands and those that are in the busy bands. Those in the vacant bands would have no incentive to continue to stay there because this just amounts to them wasting time waiting idly. Thus, they will definitely switch to other spectrum bands to search for another attacking opportunity. On the other hand, those in the busy bands will follow the similar procedure to the special case, i.e., only one malicious node will be selected to stay in the current band and others choose to either stay or switch with a 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 nodes who choose to switch will try to reach one of the other $N-L$ bands whose status is unknown. Thus, the mixed strategy space in Eqn (2) is only applied to $m-h-r$ malicious nodes.

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

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

$$Q_0(i) = \binom{m-h-r}{i} p_0^i (1-p_0)^{m-h-r-i}, \quad 0 \le i \le m-h-r. \tag{10}$$

- Since the switching malicious nodes will explore the $N-L$ spectrum bands whose status is unknown, in which $n-h$ bands are being used by secondary networks, the probability for them to switch to the busy bands, q_0, is given by:

$$q_0 = \frac{n-h}{N-L}. \tag{11}$$

  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:

$$R_0(k) = \binom{i+r}{k} q_0^k (1-q_0)^{i+r-k}, \ 0 \le k \le i+r. \tag{12}$$

- The probability that j out of $n-h$ secondary networks have been successfully attacked is given by (using the same reasoning given in Appendix I):

$$f_0(j) = \frac{\binom{n-h}{j}\binom{k-1}{j-1}}{\binom{k+n-h-1}{n-h-1}}. \tag{13}$$

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

$$E_0(j) = \begin{cases} \sum_{j=1}^{k} f_0(j) \cdot j, & k > 0 \\ 0, & k = 0 \end{cases} \tag{14}$$

Consolidating Eqns (10)–(14), we derive the net payoff for the malicious nodes in the general case, $U_0(p)$, as:

$$U_0(p) = g\left(\sum_{i=0}^{m-h-r}\sum_{k=0}^{i+r} Q_0(i)\cdot R_0(k)\cdot E_0(j) + h\right) - c\left(\sum_{i=0}^{m-h-r} Q_0(i)\cdot i + r\right). \tag{15}$$

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

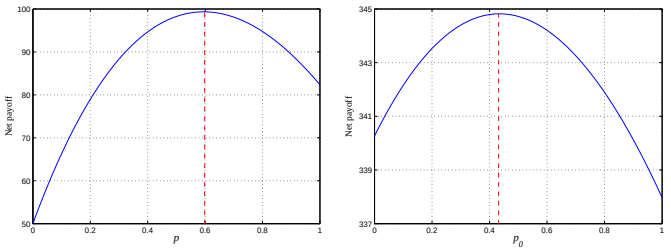
Similarly, the optimal switching probability, p_0^*, for the malicious nodes in the general case is given by:

$$p_0^* = \arg \max_{p_0 \in [0,1]} U_0(p) \tag{16}$$

C. Numerical Results

Both Eqn (9) and Eqn (16) can be solved numerically. We set the parameter values $g = 50$ and $c = 20$ as an example. With network parameters as: $N = 50$, $n = 30$ and $m = 20$, the numerical results for the special and general 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 general case respectively.



(a) (b)

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

VI. Markov Modeling of Multi-stage Case

In this section, we extend the coordinated DoS attack model to the multi-stage scenario. We incorporate the reaction of 802.22 secondary networks against the attacks and assume that malicious nodes will keep launching attacks for a long period.

A. Multi-stage System Model

We consider the time epochs in the IEEE 802.22 networks to be typically divided into discrete periods as shown in Fig. 2, in which each period consists of a quiet period for spectrum sensing, τ, and a transmission slot for communications, $t-\tau$ [28]. In each period, the secondary network measures the received signal power during the scheduled quiet period to identify the presence of the primary user. This slot is used to sense for the primaries and depending on the attack and the intelligence built into the secondary networks. After the spectrum sensing,

the secondary network will either switch to another band or stay in the same one. For example, if the secondary network decides that the transmission power is from the primary user, it will switch from the current spectrum band. On the other hand, if it suspects that a PUE attack is in progress, it will switch with some probability (related to the probability of successful PUE attack [18]). If the attack is a radio jamming type attack, which essentially results in very poor channel conditions, the secondary network will switch with a probability 1, upon detection of the strong jamming signal. In the multi-stage case, we still hold the assumption that the 802.22 secondary networks will follow exclusive spectrum sharing mechanism and transmit in a spectrum band free of interference of other secondary networks. It is noted that the attack timing depends on the specific type of DoS attack the malicious nodes will take. For example, for the PUE attack, the malicious nodes will emulate the primary user in the quiet period [11], whereas for the radio jamming attack, the malicious nodes would jam the spectrum band in the transmission slot [23].

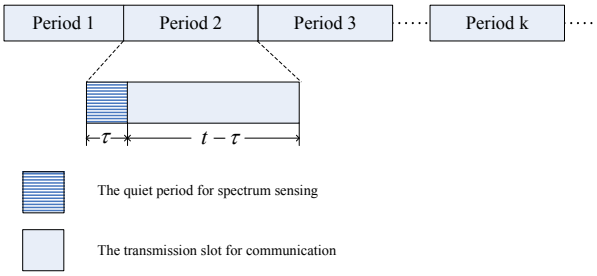


Fig. 2. Discrete periods with quiet periods and transmission slots in IEEE 802.22 networks.

B. Markov Model Analysis

Based on the system model of the multi-stage case, we know that both malicious nodes and secondary networks are dynamically switching around the spectrum bands to achieve their own goals. We model their dynamic switching between several states as a discrete-time Markov chain as shown in Fig. 3. The states of the Markov chain are described in Table I and correspond to activities in one typical spectrum band. Because of the inherent symmetry, the analysis on a single band can be extended to all the other bands.

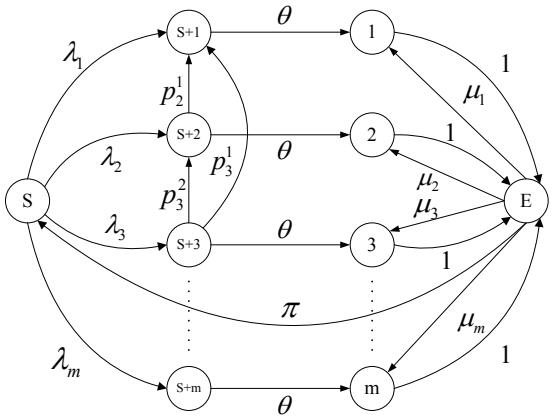


Fig. 3. The state transition diagram for one spectrum band.

TABLE I
THE STATES OF MARKOV CHAIN

State	Description
E	The spectrum band is empty
S	Only one secondary network is in this band
$S+i$	A secondary network and i malicious nodes are in this band
i	Only i malicious nodes are in this band

Without loss of generality, let us suppose that at a given slot, a spectrum band is in the state S. Upon i malicious nodes arriving in this band, its state will transit from S to $S+i$ with probability λ_i. As discussed in Section V, $i-1$ out of i malicious nodes will switch out with a certain optimal probability to maximize their net payoff. Thus, the spectrum band will transit from state $S+i$ to $S+j$ with probability p_i^j if $i-j$ malicious nodes actually choose to switch, where j could be any integer in $[1, i-1]$.

There are two outcomes after the malicious nodes launch the DoS attack: (i) The secondary network evacuates right away. In the case of the PUE attack, the secondary network falls victim to the attack. In case of a radio jamming attack, the secondary network switches out to avoid excessive interference; (ii) the secondary network continues to use the current band. This can happen if the PUE attack is either unsuccessful or the power in the jamming attack is too low to cause enough disruption to the secondary communication in that band. Let θ denote the probability that the secondary network moves out of the band, and so the transition probability from state $S+i$ to i would also be θ. When the malicious nodes find the absence of secondary activity in the spectrum band they stand, based on our assumption in Section V, they will definitely leave that band to search for another attack opportunity. Hence, the state transition from state i to E happens with probability 1. Next time a secondary network or i malicious nodes land in this band, the spectrum band transitions to state S or i with probability π or μ_i respectively.

The "flow-balance" and the normalization equation array governing the above Markov chain [29] are as follows:

$$
\begin{aligned}
&(\lambda_1+\lambda_2+\cdots+\lambda_{m-1}+\lambda_m)\Pi_S = \pi\Pi_E \\
&\theta\Pi_{S+1} = \lambda_1\Pi_S + p_2^1\Pi_{S+2} + p_3^1\Pi_{S+3} + \cdots + p_m^1\Pi_{S+m} \\
&(\theta+p_2^1)\Pi_{S+2} = \lambda_2\Pi_S + p_3^2\Pi_{S+3} + \cdots + p_m^2\Pi_{S+m} \\
&\vdots \\
&(\theta+p_{m-1}^1+\cdots+p_{m-1}^{m-2})\Pi_{S+m-1} = \lambda_{m-1}\Pi_S + p_m^{m-1}\Pi_{S+m} \\
&(\theta+p_m^1+p_m^2+\cdots+p_m^{m-1})\Pi_{S+m} = \lambda_m\Pi_S \\
&\Pi_1 = \theta\Pi_{S+1} + \mu_1\Pi_E \\
&\Pi_2 = \theta\Pi_{S+2} + \mu_2\Pi_E \\
&\vdots \\
&\Pi_{m-1} = \theta\Pi_{S+m-1} + \mu_{m-1}\Pi_E \\
&\Pi_m = \theta\Pi_{S+m} + \mu_m\Pi_E \\
&(\mu_1+\mu_2+\cdots+\mu_m+\pi)\Pi_E = \Pi_1+\Pi_2+\cdots+\Pi_m \\
&\Pi_S + \Pi_E + \sum_{i=1}^{m}\Pi_{S+i} + \sum_{i=1}^{m}\Pi_i = 1
\end{aligned}
\tag{17}
$$

where Π_{s_i} represents the stationary probability of being in

state s_i, $s_i \in \{E, S, S+i, i\}$.

Based on the state description, we know that when the spectrum band is in state $S+i$, the malicious nodes will try to attack the secondary networks.

We also assume that the attack gain g can be obtained by the malicious nodes if and only if the attack is successful. Thus, the probability of receiving an attack gain for the malicious nodes in state $S+i$ would be equal to transition probability θ. Moreover, since $i-1$ malicious nodes will switch out with a certain optimal probability, the costs $(i-j)c$ will be incurred if the spectrum band transits from state $S+i$ to $S+j$ with probability p_i^j. Furthermore, in state i, all i malicious nodes will switch out, incurring a cost of $i \cdot c$. Hence, given the stationary probability for each state, the net payoff for the m malicious nodes in one spectrum band is calculated as follows:

$$\begin{aligned} U_s^m &= g\theta(\Pi_{S+1} + \Pi_{S+2} + \cdots + \Pi_{S+m}) \\ &\quad - c(p_2^1\Pi_{S+2} + (2p_3^1 + p_3^2)\Pi_{S+3} + \cdots \\ &\quad + ((m-1)p_m^1 + (m-2)p_m^2 + \cdots + p_m^{m-1})\Pi_{S+m}) \\ &\quad - c(\Pi_1 + 2\Pi_2 + \cdots + m\Pi_m) \end{aligned} \tag{18}$$

The first term on the RHS of the equation represents the expected attack gain and the second and third terms represent the expected switching cost for the whole malicious nodes team. Since every spectrum band is equivalent, the net payoff of m malicious nodes for total N spectrum bands is simply obtained as $N \cdot U_s^m$.

Proposition: The net payoff of the malicious nodes for one typical spectrum band can be expressed as:

$$\begin{aligned} U_s^m &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \cdots + m\mu_m + \pi)\Pi_E) \\ &\quad - c(\lambda_2 + 2\lambda_3 + \cdots (m-1)\lambda_m)\Pi_S). \end{aligned} \tag{19}$$

Proof: We use mathematical induction to prove the above proposition. Note that all derivations below are on the basis of equation array (17).

(1) For $m = 1$

$$\begin{aligned} U_s^1 &= g\theta\Pi_{S+1} - c\Pi_1 = g(\Pi_1 - \mu\Pi_E) - c\Pi_1 \\ &= g((\mu_1 + \pi)\Pi_E - \mu\Pi_E) - (\mu_1 + \pi)\Pi_E \\ &= g\pi\Pi_E - c(\mu_1 + \pi)\Pi_E \end{aligned} \tag{20}$$

Thus, the *Proposition* holds for $m = 1$.

(2) For $m = 2$

$$\begin{aligned} U_s^2 &= g\theta(\Pi_{S+1} + \Pi_{S+2}) - cp_2^1\Pi_{S+2} - c(\Pi_1 + 2\Pi_2) \\ &= g(\Pi_1 + \Pi_2 - (\mu_1 + \mu_2)\Pi_E) - cp_2^1\Pi_{S+2} \\ &\quad - c((\mu_1 + \mu_2 + \pi)\Pi_E + \Pi_2) \\ &= g\pi\Pi_E - c(\mu_1 + \mu_2 + \pi)\Pi_E \\ &\quad - c(p_2^1\Pi_{S+2} + \theta\Pi_{S+2} + \mu_2\Pi_E) \\ &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \pi)\Pi_E \\ &\quad - c(p_2^1\Pi_{S+2} + \lambda_2\Pi_S - p_2^1\Pi_{S+2}) \\ &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \pi)\Pi_E - c\lambda_2\Pi_S \end{aligned} \tag{21}$$

Thus, the *Proposition* holds for $m = 2$.

(3) We assume the *Proposition* holds for $m = k$ and expand U_s^k by definition in Eqn (18) as:

$$\begin{aligned} U_s^k &= g\theta(\Pi_{S+1} + \Pi_{S+2} + \cdots + \Pi_{S+k}) \\ &\quad - c(p_2^1\Pi_{S+2} + (2p_3^1 + p_3^2)\Pi_{S+3} + \cdots \\ &\quad + ((k-1)p_k^1 + (k-2)p_k^2 + \cdots + p_k^{k-1})\Pi_{S+k}) \\ &\quad - c(\Pi_1 + 2\Pi_2 + \cdots + k\Pi_k) \\ &= g\pi\Pi_E - c(\theta\Pi_{S+1} + 2(\theta + p_2^1)\Pi_{S+2} - p_2^1\Pi_{S+2} + \cdots \\ &\quad + k(\theta + p_k^1 + \cdots + p_k^{k-1})\Pi_{S+k} \\ &\quad - (p_k^1 + 2p_k^2 + \cdots + (k-1)p_k^{k-1})\Pi_{S+k}) \\ &= g\pi\Pi_E - c(\lambda_1\Pi_S + p_2^1\Pi_{S+2} + \cdots + p_k^1\Pi_{S+k} \\ &\quad + 2(\lambda_1\Pi_S + p_3^2\Pi_{S+3} + \cdots + p_k^2\Pi_{S+k}) - p_2^1\Pi_{S+2} + \cdots \\ &\quad + k\lambda_k\Pi_S - (p_k^1 + 2p_k^2 + \cdots + (k-1)p_k^{k-1})\Pi_{S+k}) \\ &\quad - c(\mu_1 + 2\mu_2 + \cdots + k\mu_k)\Pi_E \end{aligned} \tag{22}$$

To simplify the expression, we define C_1 to be the sum of all terms associated with p_i^j in Eqn (22). Thus, U_s^k can be alternatively expressed as:

$$\begin{aligned} U_s^k &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \cdots + k\mu_k)\Pi_E \\ &\quad - c(\lambda_1\Pi_S + 2\lambda_2\Pi_S + \cdots + k\lambda_k\Pi_S) - C_1 \\ &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \cdots + k\mu_k + \pi)\Pi_E \\ &\quad - c(\lambda_2 + 2\lambda_3 \cdots + (k-1)\lambda_k)\Pi_S - C_1 \end{aligned} \tag{23}$$

Based on the induction hypothesis, U_s^k follows the Eqn (19), and so $C_1 = 0$. We now write U_s^{k+1} as:

$$\begin{aligned} U_s^{k+1} &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \cdots + k\mu_k + (k+1)\mu_{k+1})\Pi_E \\ &\quad - c(\lambda_1\Pi_S + p_2^1\Pi_{S+2} + \cdots + p_k^1\Pi_{S+k} + p_{k+1}^1\Pi_{S+k+1} \\ &\quad + 2(\lambda_2\Pi_S + p_3^2\Pi_{S+3} + \cdots + p_k^2\Pi_{S+k} + p_{k+1}^2\Pi_{S+k+1}) \\ &\quad - p_2^1\Pi_{S+2} + \cdots + k(\lambda_k\Pi_S + p_{k+1}^k) \\ &\quad - (p_k^1 + 2p_k^2 + \cdots + (k-1)p_k^{k-1})\Pi_{S+k} \\ &\quad + (k+1)\lambda_{k+1}\Pi_S - (p_{k+1}^1 + \cdots + kp_{k+1}^k)\Pi_{S+k+1}) \\ &= g\pi\Pi_E - c(\mu_1 + 2\mu_2 + \cdots + k\mu_k + (k+1)\mu_{k+1})\Pi_E \\ &\quad - c(\lambda_1\Pi_S + \cdots + k\lambda_k\Pi_S + (k+1)\lambda_{k+1}\Pi_S) - C_1 \\ &\quad - c(p_{k+1}^1\Pi_{S+k+1} + \cdots + kp_{k+1}^k\Pi_{S+k+1} \\ &\quad - (p_{k+1}^1 + 2p_{k+1}^2 + \cdots + kp_{k+1}^k)\Pi_{S+k+1}) \\ &= g\pi\Pi_E - c(\mu_1 + \cdots + k\mu_k + (k+1)\mu_{k+1} + \pi)\Pi_E \\ &\quad - c(\lambda_2 + 2\lambda_3 \cdots + (k-1)\lambda_k + k\lambda_{k+1})\Pi_S - C_1 \end{aligned} \tag{24}$$

Since, we have shown that $C_1 = 0$, U_s^{k+1} also follows Eqn (19) and *Proposition* has been proved. ■

From the state transition diagram in Fig. 3, we can see that the states E and S are not influenced by the transitions among the m states with index $S+i$. Hence, Π_E and Π_S are independent of p_i^j. Using standard Markov chain techniques [29], we obtain the expressions for Π_E and Π_S as follows:

$$\Pi_E = \frac{\theta(\sum_{i=1}^m \lambda_i)}{\theta\pi + (\pi + \theta + \theta\pi + \sum_{i=1}^m \theta\mu_i)(\sum_{i=1}^m \lambda_i)} \tag{25}$$

$$\Pi_S = \frac{\theta\pi}{\theta\pi + (\pi + \theta + \theta\pi + \sum_{i=1}^m \theta\mu_i)(\sum_{i=1}^m \lambda_i)} \tag{26}$$

The derivations of transition probabilities μ_i, λ_i and π are given in Appendix II. Based on the expressions of μ_i, λ_i and π, we can see that they are also independent of p_i^j. Thus,

according to Eqn (19), U_s^m is independent of p_i^j. That is, as the system reaches steady state, the net payoff of malicious nodes does not depend on their switching probabilities. Note that this conclusion holds only when the system reaches the steady state. The reason behind this observation is: from the malicious nodes' perspective, obtaining attack gains and consuming switch costs will become a dynamic balancing process in the steady system. In other words, more malicious nodes switching will incur more switch costs but at the same time acquire more opportunities to launch successful attacks that increases the attack gains.

On the other hand, from Eqns (19), (25) and (26), we see that the net payoff is related to the number, m, of malicious nodes participating in the attack. In the next section, we will conduct the numerical analysis to investigate how the number of malicious nodes influences the net payoff U_s^m.

Now we look at the transition probability θ for two different DoS attacks and take the preventive measures from the secondary networks into consideration.

(1) Radio Jamming Attack:

Radio jamming attack refers to the transmission of radio signals that disrupt communications by significantly decreasing the signal to noise ratio (SNR) of the frequency channel. This attack is easy to detect. We assume that the jamming signal is strong enough such that the communications in the frequency channel are completely interrupted. Hence, once being jammed, the best choice for the secondary network is to switch to another clear band. Thus, we set $\theta = 1$ for the radio jamming attack.

(2) PUE Attack:

The PUE attacker will effectively emulate the primary signal to make the protocol compliant 802.22 secondary network erroneously conclude that the primary user is active in the spectrum band and thus leave the band.

Because of the inherent randomness in the propagation characteristic and consequent randomness in the received signal, most spectrum sensing mechanism are probabilistic in nature. In Section II, we briefly reviewed several methods developed to mitigate the PUE attacks. Though the details of these prevention measures are beyond the scope of the paper, we include a parameter Pr(success) as the probability of a successful attack [18] and consider that the secondary networks will take some countermeasures against the PUE attack, thereby decreasing the Pr(success).

In the case of PUE attack, θ can be equated to Pr(success) because the secondary networks will only leave the current band when the attack is successful. In the following section, we will conduct the numerical analysis to investigate the performance under the countermeasures of secondary networks.

VII. Simulation and Numerical Results

In this section, we conduct simulations and numerical analysis for both one-stage and multi-stage scenarios. We consider $N = 50$ available spectrum bands and also set $g = 50$ and $c = 20$ as an example. The simulation results are averaged over 100,000 Monte Carlo simulations.

A. Simulations for the Special Case of the One-stage Game

We first conduct the simulation for the special case in the one-stage cooperative game where all malicious nodes start from the same busy band. Fig. 4 shows the theoretical and simulation results for the optimal switching probability, p^*, for $m-1$ malicious nodes. As evident from this figure, the simulation results are very close to the theoretical results. With the increase in the number of secondary networks, the probability of switching gradually converges to 1. This is because, as the number of secondary networks increases, the probability that the malicious nodes will land in a busy band increases. Note that the theoretical results are calculated from Eqn (9) by numerical analysis. Another point in Fig. 4 is that as the number of malicious nodes increases, the rate of convergence decreases. The reason behind this observation is that for certain number of secondary networks in the system, more malicious nodes can take relatively lower switching probability to achieve the maximum net payoff.

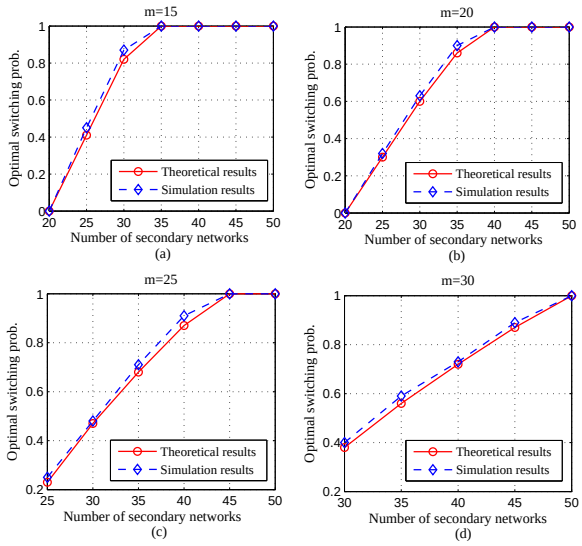


Fig. 4. The optimal switching probability, p^*, for the malicious nodes with varying number of malicious nodes, m, and secondary networks, n, under the special case that all malicious nodes start out in the same busy band (the special case is described in Section V).

The comparison of the net payoffs between the cooperative game and non-cooperative game is shown in Fig. 5, in which we fix the number of the malicious nodes at $m = 20$, and vary the number of secondary networks. As illustrated in this figure, the net payoff obtained by launching a cooperative attack results in approximately $10-15\%$ greater net payoff for the malicious nodes in comparison to the non-cooperative attack. Note that the strategy for the non-cooperative game is the Nash equilibrium strategy, which in our problem, is the switching probability for each independent malicious node (see details in Appendix II). Moreover, the malicious nodes following the optimal strategies can get greater net payoff as the number of secondary networks increases.

B. Simulations for the General Case of the One-stage Game

In the general case, we consider $m = 20$ malicious nodes. Many temporary states in this case are possible, but due to the

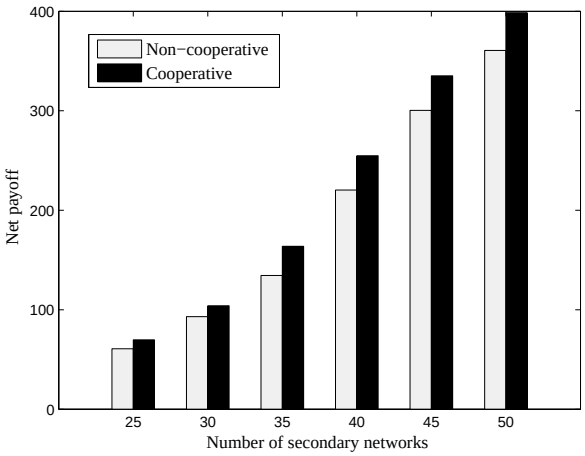


Fig. 5. The comparison of net payoff between the cooperative and non-cooperative game for the special case as described in Section V.

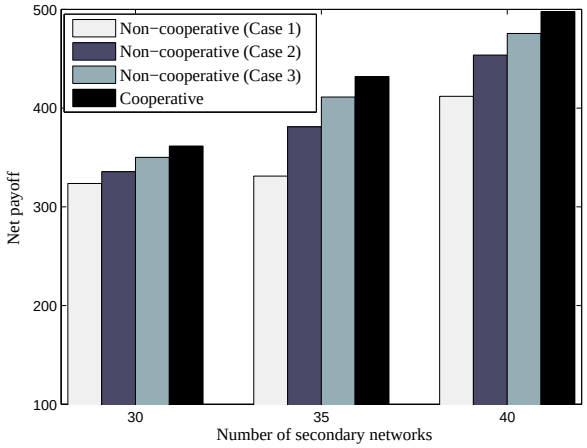


Fig. 6. The comparison of net payoff between the cooperative and non-cooperative game for the general case as described in Section V.

page limit, we choose the temporary state: $L = 10$, $h = 6$, $r = 6$ as an illustrative example. When comparing performances of the cooperative and non-cooperative attacks in the general case (where the malicious nodes are distributed in several spectrum bands), 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 we can calculate the Nash equilibrium for them. Hence, we consider three different 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 occupied 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 III.

Fig. 6 shows the simulation results of the comparison of net payoffs between the cooperative and non-cooperative attack for varying number of secondary networks. Note that the optimal strategy for the cooperative game is obtained from Eqn (15) by the numerical analysis. Similar to the special case, the cooperative attack in the general case also outperforms the non-cooperative attack in terms of the net payoff obtained by malicious nodes. Moreover, we notice that for the non-cooperative attack, the net payoffs for the three different cases are also different. That is because, with the decrease in the number of players sharing the attack gain, the malicious node's incentive to switch would decline, which consequently reduces the chance to attack more secondary networks.

C. Numerical Results for the Multi-stage Case

In the multi-stage case, without loss of generality, we focus on one typical spectrum band and still assume that $m \leq n < N$. Since we take into account the event that the malicious nodes will switch out when the secondary network leaves the spectrum band in the multi-stage scenario, the malicious nodes will frequently switch around the spectrum bands and consequently incur a huge cumulative switching cost. Hence, to incorporate this factor, we increase the difference between the attack gain and switching cost in the numerical analysis for the multi-stage scenario, e.g., $g = 100$ and $c = 20$. Otherwise, the final net payoff for the malicious nodes might be negative.

(1) Radio Jamming Attack:

For the radio jamming attack, we consider $\theta = 1$. Fig. 7 shows the net payoff in one typical spectrum band for the malicious nodes launching radio jamming attacks with varying number of the secondary networks, n, and malicious nodes, m. As shown in Fig. 7, it is evident that with increase in the number of secondary networks, the net payoff for the malicious nodes will increase as expected.

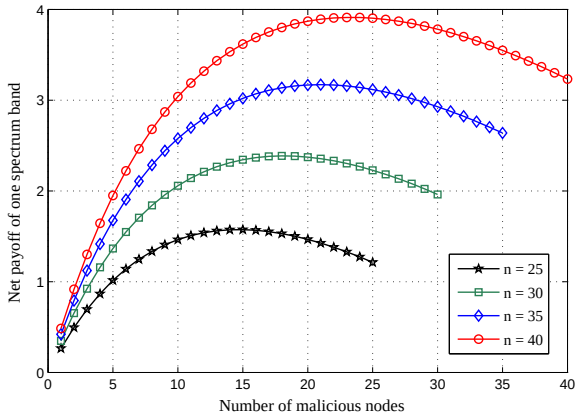


Fig. 7. The numerical results of the net payoff in one spectrum band for the malicious nodes launching radio jamming attacks with varying number of the secondary networks, n, and malicious nodes, m. ($g = 100$, $c = 20$)

(2) PUE Attack:

In the case of the PUE attack, since the secondary networks will take some mitigation measures, $Pr(\text{success})$ and θ will be less than 1. Fig. 8 shows the net payoff in one typical spectrum band for the malicious nodes launching PUE attacks with fixed

n, varying m and different values of θ. As shown, for certain number of secondary networks in the system, the malicious nodes can get less net payoff as the value of θ decreases. This is because, a smaller value of θ implies the smaller Pr(success). Thus, with the smaller successful probability for launching attacks, the malicious nodes will get less net payoff. This observation indicates that if the secondary networks can adopt effective preventive measures to decrease Pr(success), the impact of the PUE attack will be reduced.

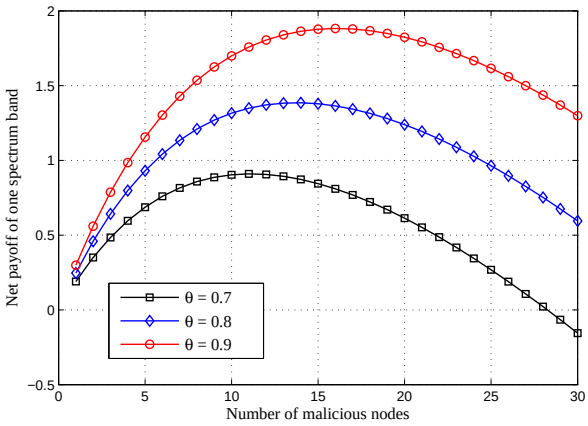


Fig. 8. The numerical results of the net payoff in one spectrum band for the malicious nodes launching PUE attacks with varying number of malicious nodes, m and different values of θ. Note that the number of secondary networks is fixed at $n = 30$. ($g = 100$, $c = 20$)

The common interesting point in Fig 7 and Fig. 8 is that there is a maximum for each curve, which indicates that there exists an optimal number of malicious nodes joining the coordinated attack. This observation reflects the importance of the tradeoff between increasing the attack gains and saving switching costs. More specifically, increasing the number of malicious nodes indefinitely, will result in a point of no returns because of the additional switching cost. Hence, it is important for the malicious nodes to adjust the number of attacking nodes based on the specific circumstances.

Furthermore, in order to investigate the impact of parameters on the numerical results, we use different sets of parameter values of g and c. Fig. 9 shows the net payoff in one typical spectrum band for the malicious nodes launching radio jamming attacks with different sets of parameter values of g and c with fixed number of secondary networks ($n = 30$). As illustrated, there always exists an optimal number of malicious nodes participating in the attacks. Another important observation from this figure is that as the difference between the value of g and c increases, the optimal number of malicious nodes for the attack also increases. This reason behind this result is: the net payoff for the malicious nodes is equal to the total attack gain minus the overall switching costs. Thus, as the switch cost decreases compared to the attack gain, it is rational to involve more malicious nodes in the attack because the additional attack gains obtained from more successful attacks will outweigh the increased switching costs due to more switching actions.

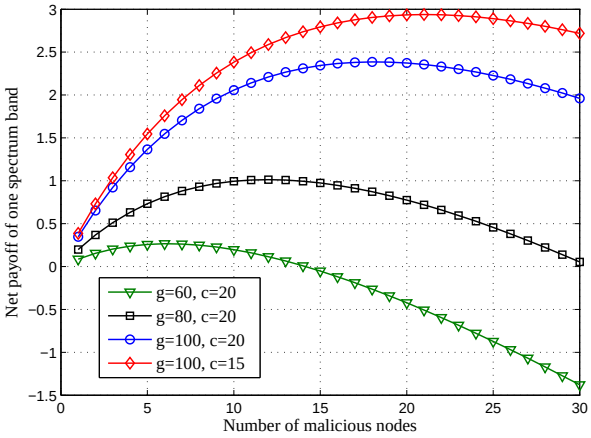


Fig. 9. The numerical results of the net payoff in one spectrum band for the malicious nodes launching radio jamming attacks with different sets of parameter values. Note that we fix $n = 30$ in this figure.

VIII. Conclusion

In this paper, we investigated the coordinated DoS attacks on IEEE 802.22 networks from the perspective of malicious nodes. We considered malicious nodes as a collaborative team that aims to maximize their net payoff by disrupting the communications of good 802.22 secondary networks. In the one-stage scenario, we considered the moves of malicious nodes and formulated the coordinated DoS attack as a cooperative game. The theoretical expressions of net payoff were derived and the optimal strategies for the malicious nodes (switching probability) were numerically obtained. In the multi-stage scenario, we incorporated the reactions of 802.22 secondary networks against the attacks and proposed a discrete-time Markov chain to model the change of states in a typical spectrum band. We further derived the expression for the net payoff as the system reaches steady state and proved it to be independent of the switching probabilities of the malicious nodes. Through simulation results in the one-stage case, we showed that by taking the coordinated approach, the malicious nodes can obtain as high as 10-15% more net payoff than when they do not cooperate. Moreover, the numerical results for the multi-stage case indicates that as the system reaches steady state, there exists an optimal number of malicious nodes participating in the attack to achieve the maximum net payoff.

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 the condition that $x_1 + x_2 + \cdots + x_j = k$, which is $\binom{k-1}{j-1}$ [30].

- 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 the condition that $x_1+x_2+\cdots+x_{n-1}=k$, which is $\binom{k+n-2}{n-2}$ [30].

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

$$f(j)=\frac{\binom{n-1}{j}\binom{k-1}{j-1}}{\binom{k+n-2}{n-2}}. \quad (27)$$

Appendix II
Derivations of μ_i, λ_i and π

In the Markov chain shown in Fig. 3, μ_i represents the transition probability from state E to state i, λ_i represents the transition probability from state S to state $S+i$ and π represents the transition probability from state E to state S.

(i) Expressions of μ_i and λ_i:

The transitions both from state E to state i and from S to state $S+i$ corresponds to the event that i malicious nodes switch to a certain spectrum band. Thus, based on the Markov property [29], we know that μ_i and λ_i simply follow the binomial distribution as:

$$\mu_i=\lambda_i=\binom{m}{i}(\frac{1}{N-1})^i(\frac{N-2}{N-1})^{m-i}, 1\le i\le m. \quad (28)$$

(ii) Expression of π:

Following the similar logic as Section V, we can calculate the probability that j secondary networks are under attack at a given time slot as:

$$Q^{'}(j)=\binom{m}{i}(\frac{n}{N-1})^i(\frac{N-n-1}{N-1})^{m-i}f^{'}(j), 0\le j\le i. \quad (29)$$

where $f^{'}(j)=\frac{\binom{n}{j}\binom{i-1}{j-1}}{\binom{i+n-1}{n-1}}$.

Moreover, since we denote θ to be the probability that the secondary network moves out of the band in state $S+i$, the probability that k out j secondary networks leave the spectrum band where they are transmitting, $R^{'}(k)$, is calculated as:

$$R^{'}(k)=\binom{j}{k}\theta^k(1-\theta)^{j-k}, 0\le k\le j. \quad (30)$$

Consolidating Eqns (29) and (30), we derive the expression of π as:

$$\pi=\sum_{i=0}^{m}\sum_{j=0}^{i}\sum_{k=0}^{j}Q^{'}(j)\cdot R^{'}(k)\cdot\frac{k}{N}. \quad (31)$$

Appendix III
The Mixed-strategy Nash Equilibrium for the Non-cooperative Game in 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 gets the average attack gain. For example, if 3 malicious nodes gather in the same busy band, each obtains $g/3$ attack gain. Without loss of generality, we consider one particular player, s.

(i) Expected payoff for the player s upon staying:

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

$$Q_{\text{stay}}(i)=\binom{m-1}{i}(1-\alpha)^i\alpha^{m-1-i},\ 0\le i\le m-1. \quad (32)$$

Hence, the expected payoff for the player s upon staying is calculated as:

$$E(\text{stay})=\sum_{i=0}^{m-1}Q_{\text{stay}}(i)\cdot\frac{g}{i+1}. \quad (33)$$

(ii) Expected payoff for the player s upon switching:

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

$$Q_{\text{switch}}(i)=\binom{m-1}{i}\alpha^i(1-\alpha)^{m-1-i},\ 0\le i\le m-1. \quad (34)$$

- Note that the probability that the player s will switch to the spectrum bands already being used by other 802.22 secondary networks exactly follows Eqn (4) and is given by $q=\frac{n-1}{N-1}$.
- Among the i switching nodes, we calculate the probability that exactly j nodes switch to the same band with player s, $H(j)$, as:

$$H(j)=\binom{i}{j}\frac{1}{(N-1)^j}\cdot(\frac{N-2}{N-1})^{i-j}. \quad (35)$$

Hence, the expected payoff for the player s upon switching is calculated as:

$$E(\text{switch})=\sum_{i=0}^{m-1}\sum_{j=0}^{i}Q_{\text{switch}}(i)\cdot q\cdot H(j)\cdot\frac{g}{j+1}-c. \quad (36)$$

Consolidating *(i)* and *(ii)*, the mixed-strategy Nash equilibrium, α^*, for the malicious nodes, is obtained by imposing E(stay)=E(switch), which can be solved numerically. For example, setting the network parameters to: $N=50$, $n=30$, $m=20$, gives α^* = 0.51. The expected payoff for the player s under this condition is shown in Fig. 10.

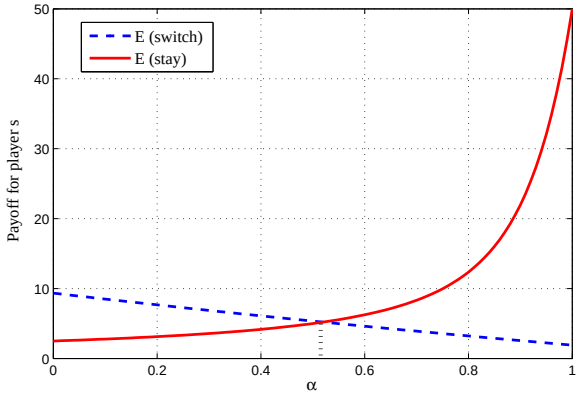


Fig. 10. The expected payoff for player s. The Nash equilibrium for player s is achieved at α = 0.51.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive comments which led to a significant improvement of the manuscript.

REFERENCES

[1] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Coordinated denial-of-service attacks in ieee 802.22 networks," *IEEE International Conference on Communications (ICC) 2010*, pp. 1 –5, May 2010.

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

[3] F. C. C., "In the matter of unlicensed operation in the TV broadcast bands," *Second Report and Order and Memorandum Opinion and Order*, no. FCC-08-260A1, Nov. 2008.

[4] C. Bazelon, "Licensed or unlicensed: The economic considerations in incremental spectrum allocations," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, pp. 1–8, Oct. 2008.

[5] I. Mitola, J. and J. Maguire, G.Q., "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, Aug 1999.

[6] 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.

[7] 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.

[8] IEEE 802.22 WG, "IEEE p802.22/d0.1 draft standard for wireless regional area networks part 22: Cognitive wireless ran medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the tv bands," *IEEE docs*, May 2006.

[9] K. Bian and J.-M. J. Park, "Security vulnerabilities in IEEE 802.22," *WICON '08: Proceedings of the 4th Annual International Conference on Wireless Internet*, pp. 1–9, 2008.

[10] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, pp. 1–8, May 2008.

[11] 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.

[12] "http://bits.blogs.nytimes.com/2009/08/11/here-we-go-again-twitter-is-back-down/."

[13] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," *Mob. Netw. Appl.*, vol. 13, no. 5, pp. 516–532, 2008.

[14] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 50–55, April 2008.

[15] J. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," *CrownCom 2008. 3rd International Conference on*, pp. 1 –7, 15-17 2008.

[16] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *IEEE INFOCOM 2008.*, pp. 1876 –1884, 13-18 2008.

[17] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006.*, pp. 110–119, Sept. 2006.

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

[19] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," *IEEE International Conference on Communications, ICC 2009*, pp. 1–5, June 2009.

[20] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *Proceedings, IEEE DySPAN 2008*, Oct. 2008.

[21] A. Sampath, H. Dai, H. Zheng, and B. Zhao, "Multi-channel jamming attacks using cognitive radios," *Proceedings of 16th International Conference on Computer Communications and Networks, ICCCN 2007.*, pp. 352 –357, 13-16 2007.

[22] L. Ma and C.-C. Shen, "Security-enhanced virtual channel rendezvous algorithm for dynamic spectrum access wireless networks," *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, pp. 1–9, Oct. 2008.

[23] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," pp. 1 –6, Nov. 2009.

[24] D. Grandblaise and W. Hu, "Inter base stations adaptive on demand channel contention for IEEE 802.22 WRAN self conexistance," *IEEE docs: IEEE 802.22-07/0024r0*, Jan. 2007.

[25] S. Sengupta, R. Chandramouli, S. Brahma, and M. Chatterjee, "A game theoretic framework for distributed self-coexistence among IEEE 802.22 networks," *In proceedings of IEEE Global Communications Conference (GLOBECOM)*, Dec. 2008.

[26] R. B. Myerson, *Game Theory: Analysis of Conflict*. Harvard University, 1997.

[27] J. Nash, "Two-person cooperative game," *Econometrica*, vol. 21, no. 1, pp. 763–772, 1953.

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

[29] V. Kulkarni, *Modeling and Analysis of Stochastic System*. CRC Press, 1995.

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

Yi Tan received the B.E. in Electrical Engineering from the Huazhong University of Science and Technology, China in 2007. Since Fall 2007, he has been a Ph.D. student in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey, where he works in the MSyNC lab under the guidance of Prof. K.P. Subbalakshmi. His research interests include quantization based data hiding, dynamic spectrum access networks, cognitive radio security and game theory. He was a technical program committee (TPC) member for the 6th International Wireless Communication & Mobile Computing conference, IWCMC 2010.

Shamik Sengupta is an Assistant Professor in the Department of Mathematics and Computer Science, John Jay College of Criminal Justice of the City University of New York. Shamik Sengupta received his B.E. degree in Computer Science from Jadavpur University, India in 2002 and the Ph.D. degree from the School of Electrical Engineering and Computer Science, University of Central Florida, Orlando in 2007. His research interests include cognitive radio, dynamic spectrum access, game theory, security in wireless networking. Shamik Sengupta serves as the Vice-Chair of Mobile Wireless Network (MobIG) special interest group of the IEEE COMSOC Multimedia Communications Technical Committee. He is in the organizing and technical program committee of several IEEE conferences. He is the recipient of an IEEE Globecom 2008 best paper award.

PLACE PHOTO HERE

K. P. (Suba) Subbalakshmi is an Associate Professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests are in cognitive radio network security, wireless security, steganography and stag-analysis as well as Internet forensics. Her research is supported by US NSF, US AFRL, US Army and other DoD agencies. Her research has led to the development of several digital forensic software tools that have been delivered to government agencies and industry. She is the Chair of the Security Special Interest Group, IEEE Multimedia Communications Technical Committee, COMSOC. She is the organizing chair of the Cognitive Networks track of the Symposium on Selected Areas of Communications, IEEE International Conference on Communications, 2009. She has chaired several conferences and serves on the editorial board of several journals. Suba is a Co-Founder as well as co-CTO of inStream Media, LLC, an interactive media company. Further information can be found at: http://personal.stevens.edu/ ksubbala