Strategic Surveillance Against Primary User Emulation Attacks in Cognitive Radio Networks

Duc-Tuyen Ta, Nhan Nguyen-Thanh, Patrick Maillé, van Tam Nguyen

Strategic Surveillance Against Primary User Emulation Attacks in Cognitive Radio Networks

Duc-Tuyen Ta, Nhan Nguyen-Thanh, Patrick Maillé, and Van-Tam Nguyen

***Abstract*—Selfish primary user emulation (PUE) is a serious security problem in cognitive radio networks. By emitting emulated incumbent signals, a PUE attacker can selfishly occupy more channels. Consequently, a PUE attacker can prevent other secondary users from accessing radio resources and interfere with nearby primary users. To mitigate the selfish PUE, a surveillance process on occupied channels could be performed. Determining surveillance strategies, particularly in multi-channel context, is necessary for ensuring network operation fairness. Since a rational attacker can learn to adapt to the surveillance strategy, the question is how to formulate an appropriate modeling of the strategic interaction between a defender and an attacker. In this paper, we study the commitment model in which the network manager takes the leadership role by committing to its surveillance strategy and forces the attacker to follow the committed strategy. The relevant strategy is analyzed through the Strong Stackelberg Equilibrium (SSE). Analytical and numerical results suggest that, by playing the SSE strategy, the network manager significantly improves its utility with respect to playing a Nash equilibrium (NE) strategy, hence obtains a better protection against selfish PUEs. Moreover, the computational effort to compute the SSE strategy is lower than to find a NE strategy.**

***Index Terms*—cognitive radio, game theory, primary emulation attack, spectrum sensing, security**

I. Introduction

SECURITY issues have attracted plenty of attention in wireless communication, particularly in cognitive radio networks (CRNs). One of the serious threats to CRNs is the *Primary User Emulation* (PUE), originally investigated in [1]–[4]. Unlike the well-known attack method-known as the spectrum sensing data falsification attack (or the Byzantines attack) [5]–[8] where the malicious terminals share incorrect spectrum sensing results and cause a degradation of accuracy of the cooperative spectrum sensing process, the PUE attack influences actively the spectrum sensing process by transmitting an emulated primary signal on the sensing duration. The presence of an emulated primary signal is more dangerous since it leads to the presumptuously occupied state on the attacked channels (i.e., the spectrum sensing engine perceives the channels as being occupied) and then the prohibition of secondary access to the channel immediately. Consequently, this kind of attack reduces the spectrum access of the CRNs and thus severely degrades their operations.

Depending on goals, PUE attacks can be categorized into two types: selfish and malicious. The malicious attack targets at preventing the secondary users from identifying and using vacant spectrum bands, similar to the Denial-of-Service or jamming attack. The selfish attack, however, aims at illegitimately occupying channel resource. Consequently, it can prevent other secondary users from accessing. In that sense, the selfish PUE attack is associated with an illegal benefit while creating an unfair obstruction to the CRNs and possible unnecessary interferences to the nearby primary users (PUs). Therefore, combating the selfish PUE attack is crucial and so the purpose of our paper.

Recently, several techniques have been presented to mitigate selfish PUE. In [3], [9], the authors proposed to use the location of PUs to detect PUE attacks. The primary signal characteristics [10] and the difference between communication channels of PUE attackers and the PUs [11] are used to identify the emulated primary signal and then detect the PUE. A physical layer authentication scheme by adding the authentication tag at the primary signal to identify and mitigate PUE is studied in [12]. Unfortunately, these techniques are only applicable when information about the location of the PUs, the channel characteristics or the authentication tag is available. However, there still is a vulnerability if an attacker conducts multi-channel attacks. Another approach to defend against the PUE is to treat the PUE signal as a jamming signal by adopting the channel hopping method [13], [14]. Typically, a successful selfish PUE in the sensing duration is followed by a selfish use of the attacked channel by the attacker. Meanwhile, it is possible to determine user's identification in any communication link [12]. Thus, in [15], we propose to perform a channel surveillance process in the network manager (i.e., the secondary system manager) to monitor the prohibited secondary accessed channels in the data duration. The channel surveillance process can help to detect illegal channel occupation and identify the selfish PUE attacker. Since CRNs usually work on multiple frequency bands, and because of the rapid expansion of software-defined radio, the attacker can launch a multichannel selfish PUE attack. For such a case, by considering each channel separately, a sequential monitoring plan can be used, however, at the cost of long surveillance time. Therefore, in [16], we extended the single-channel surveillance process to a multi-channel surveillance process. A game-theoretic analysis is employed to determine the optimal surveillance strategy as a Nash Equilibrium (NE) [17] of the game.

All the studies discussed above are considered when the attacker and the network manager implement the attack and the surveillance process simultaneously without information regarding the other's strategy. However, a rational attacker can

Duc-Tuyen Ta, Nhan Nguyen-Thanh, and Van-Tam Nguyen are with LTCI, CNRS, Télécom ParisTech, Université Paris Saclay, 75013, Paris, France. E-mail: {duc-tuyen.ta, nhan.nguyen-thanh, van-tam.nguyen}@telecom-paristech.fr.

Patrick Maille is with IMT Atlantique, Institut Mines-Telecom, Rennes, France. E-mail: patrick.maille@imt.fr.

learn to adapt to the surveillance strategy by conducting a fixed period of monitoring before performing a selfish PUE [18]. In this case, a NE may not be an efficient strategy for the defender. Instead of simply playing a NE strategy, the network manager can leverage its position of leader by committing to a defense strategy and forcing the attacker as the follower to play its best response regarding the observed surveillance strategy. The leadership and commitment are remarkably close to real-life security problems, such as patrolling scenarios, for which these types of commitments by the security agent are necessary [19], [20]. For example, security personnel patrolling an infrastructure decides on a patrolling strategy first, before their adversaries act taking this committed strategy into account. It has been shown that Stackelberg games appropriately model these commitments [21], [22]. Therefore, analyzing an appropriate modeling of the strategic interaction between a defender and an attacker in the multi-channel PUE attack context as well as the corresponding benefit/lost of both players are our main challenge.

In this paper, we extend our previous works from [15], [16] and provide means for taking into account leadership and commitment in the game model. The relevant strategies for the attacker and the network manager are analyzed through the NE for the non-commitment model (which is presented in our previous work [16]) and the Strong Stackelberg Equilibrium (SSE) [23] for the commitment model. We then analyze the benefits/losses of both players and the comparison with the non-commitment model.

The rest of the paper is organized as follows. Section II introduces the system model of surveillance process to mitigate selfish PUEs. Regarding the primary user signal status, two scenarios of selfish PUE attack are considered: the selfish PUE attack without the fallow set (i.e., the set of channels on which the PU is not active) and the selfish PUE attack with the fallow set. For the first scenario, Section III then formulates the relationship between the attacker and the defender as an extensive-form game while the commitment model and the corresponding comparison with the conventional model are considered in Section IV. A game formulation and the methodology to investigate the commitment model of the surveillance process for the second scenario are presented in Section V. Numerical results are presented in Section VI and the concluding remarks are finally discussed in Section VII.

II. System Model

A. Network Model

We consider a half-duplex, sensing-based CRN which allows secondary access to multiple licensed bands. In order to simplify the analysis and focus on the effects of the surveillance process to mitigate the selfish PUE attack, we assume that the CRN contains two separate sets: the network manager and the CR users. The network manager is responsible for providing sensing and surveillance services, while CR users exploits these services for opportunistic data transmission. Note that the selfish PUE attacker is also a CR user.

In the presence of several selfish PUE attackers, the damage to the CRN will be at the highest level if they collude in a joint attack. Therefore, to be conservative, we assume that the joint PUE attack by an attacker set is conducted by only one equivalent attacker. We denote by *attacker* the representative of the selfish attacker set and *defender* the representative of the network manager.

Naturally, both the attacker and the network manager have a partial observation on the probability of the primary user activity after the fixed sensing period. Also, the probability of detection (P_d) and the probability of false alarm (P_f) of the spectrum sensing in each channel are the prior knowledge for both attacker and network manager. Before each time slot, the network manager ignores whether the PU is active or not. In contrast, the attacker can know whether the PU is active or not. Thus, the following scenarios are considered for the attacker:

- **Selfish PUE attack without the fallow set**: the attacker conducts a selfish PUE attack without information on the status of the primary user signal before the sensing duration of each time slot[1]. Instead, the attacker has information on the probability of the primary user activity.
- **Selfish PUE attack with the fallow set**: the attacker conducts a selfish PUE attack with the *fallow* set before sensing duration of each time slot[2] and only performs the selfish PUE attack on channels in this set.

B. Attack and Surveillance Process

The network operation is divided into super-frames, each of which includes a sensing duration and a data duration. We assume the sensing engine cannot distinguish the emulated and legitimate incumbent signals, hence the PUE will not be detected during the sensing duration.

During sensing (Fig.1a), the network manager estimates the available channels. Due to the inherently unreliable nature of the wireless medium, there are two possible sensing results for each channel: "*unoccupied*", e.g., the network manager estimates that the channel is not occupied by the licensed users, and "*occupied*", e.g., the network manager estimates that the channel is occupied by the licensed users [3]. The selfish PUE attacker, however, emits the emulated primary user signal to prevent other secondary users from competing for that band.

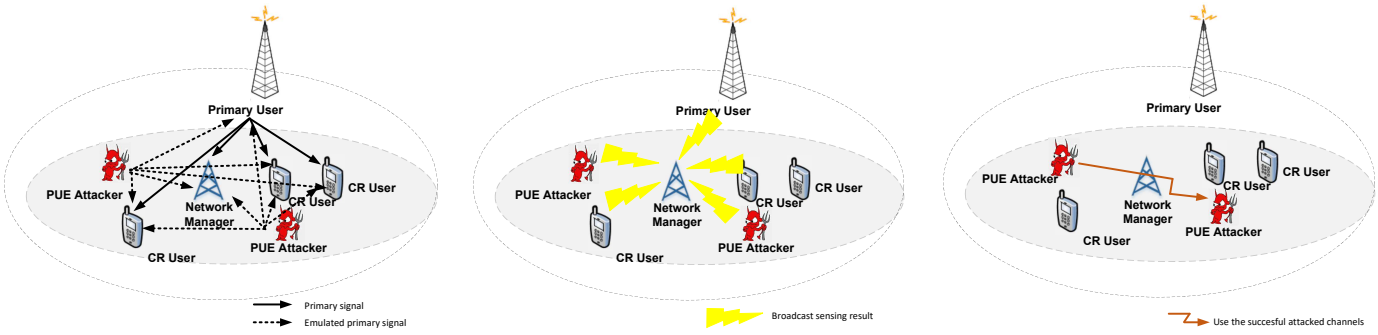
After that (Fig.1b), the network manager provides the decision on the available channels by broadcasting it to all CR users, including the PUE attacker.

At data duration (Fig.1c), if the channel is announced to be unoccupied[3], users may adopt multiple coordination or contention approaches to obtain channel access. On the contrary, if the channel is announced to be occupied, all CR users are prohibited to use the channel. Any secondary accessing the prohibited channel is illegal and considered as an attack. Hence, if the attacked channel is announced to be unoccupied,

[1]This assumption is considered in some studies as [13]–[16].

[2]This assumption is considered in some studies as [3], [4], [24].

[3]Note that because of sensing errors, a PU can be undetected and then undergo interference from CR users. This problem is well-known in the CRN literature [3], [25], [26]. We do not solve it in this paper, but rather focus on defending against PUEs which have negative effects even without sensing errors. Also, the details of the data transmission like channel coding and modulation are irrelevant to the discussion in this paper.



(a) At sensing duration (b) After sensing duration (c) At data duration

Fig. 1: The surveillance process to mitigate selfish PUE attack in a CRN: a) the attackers emits the emulated primary signal while the network manager provides sensing service to the network, b) the network manager broadcasts the sensing result to all CR users, including PUE attackers, c) the attackers use the attacked and occupied channels to transmit data while the network manager monitors a subset of occupied channels to detect the illegal occupation.

the attackers then act as normal CR users. Conversely, if the attacked channel is announced to be occupied, the attackers use this channel to transmit data selfishly[4]. Concerning the defense against a selfish PUE attacker, we assume that a fixed format of the data frame is used to exchange data with all CR users, including selfish users. The format contains the identification of the user, e.g., the *medium access control* address. Consequently, CR users can be identified by observing the transmitted signals during the data time. The defender then performs the channel surveillance process on prohibited secondary access channels to detect an illegal occupation, hence the selfish attacker. Once the attacker has been detected, punishments such as bandwidth limitation can be adopted to penalize the attacker.

C. Notations

For the t^{th} channel ($t = 1, \ldots, N$), we suppose the presence probability of the PU is π_t. Other specific notations used throughout the paper are defined as follows:

- p_N^t is the probability that the channel is detected as occupied if the attacker does not attack the channel. Denoting by p_d^t and p_f^t the probability of detection and the probability of false alarm when the attacker does not attack the channel, one can easily check that $p_N^t = \pi_t p_d^t + (1-\pi_t)p_f^t$.
- p_A^t is the probability that the attacked channel is detected as occupied. Denoting by $p_{d|A}^t$ and $p_{f|A}^t$ the probability of detection and the probability of false alarm[5] when the attacker attacks on the channel, one can easily check that $p_A^t = \pi_t p_{d|A}^t + (1-\pi_t)p_{f|A}^t$. Note that if t is in the fallow set, in the scenario of selfish PUE attack with the fallow set, $p_A^t = p_N^t$.
- ρ_N^t is the probability that the t^{th} channel is not used by the PU when the sensing engine notifies as occupied and the attacker does not attack. Using Bayes rule, we obtain that $\rho_N^t = (1-\pi_t)p_f^t / p_N^t$.
- ρ_A^t is the probability that the t^{th} channel is not used by the PU when the sensing engine notifies as occupied and the attacker attacks. Using Bayes rule, we have $\rho_A^t = (1-\pi_t)p_{f|A}^t / p_A^t$. If t is in the fallow set, in the scenario of selfish PUE attack with the fallow set, $\rho_A^t = \rho_N^t$.

III. Selfish PUE Attack Without The Fallow Set: Game Formulation

In this section, we formulate the relationship between the selfish PUE attacker which conducts a selfish PUE attack without the fallow set and the defender as an extensive-form game with incomplete information. We consider a CRN with N channels. At a time, the attacker can select up to M channels to implement a selfish PUE attack while the defender can select up to L channels to perform the surveillance process. Typically, we have $M \leq N$, $L \leq N$[6]. An example of the channel surveillance game for a CRN with $(N, M, L) = (2, 1, 1)$ is illustrated in Fig. 2.

A. Game Elements

Below we introduce the elements of the game, including the player set, the strategy set, the payoff and the expected payoff for each player.

1) Players: $\Gamma = \{Attacker, Defender\}$

- **Attacker** who emulates the primary signal to implement the selfish PUE for a selfish purpose.
- **Defender** who monitors the occupied channels to catch the attacker.

[4]The attacker could also attack and leave the attacked channel if it is announced to be occupied [15], [16]. However, such an "attack and leave" strategy is strictly dominated by a "do not attack" strategy, hence we can assume it will never be played.

[5]Suppose that the energy detection is adopted for spectrum sensing. If the threshold value for the energy detection is not changed, one can easily to find the value of $p_{d|a}^t$ and $p_{f|a}^t$ from p_d^t and p_f^t. Suppose that the attacker emits the emulated primary signal at the same power as PU. For the scenario of selfish PUE attack without the fallow set, $p_{f|a}^t = p_d^t$. For the scenario of selfish PUE attack with the fallow set, however, $p_{d|a}^t = p_d^t$ and $p_{f|a}^t = p_f^t$.

[6]The case $M > N$ (or $L > N$) is equivalent to $M = N$ (or $L = N$). Moreover, if $M = L = N$ the considered scheme would turn out to be the same as a single channel surveillance problem, that has already been studied in the literature [15]. Therefore, we assume that $M \leq N$ and $L \leq N$.

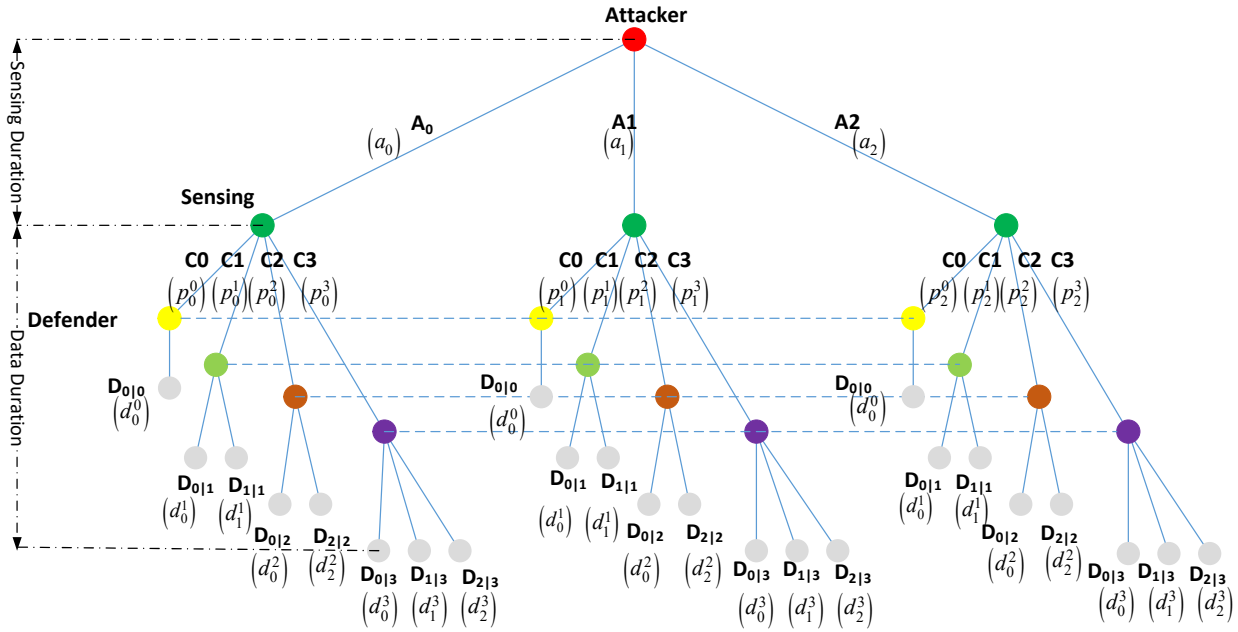


Fig. 2: The multi-channel surveillance game for a CRN with two available channels where the attacker/defender can attack/monitor one channel at a time. The attacker conducts a selfish PUE attack without the fallow set. We denote by p_m^n the probability of the m^{th} sensing result when the attacker plays A_n.

2) Pure Strategy Set: We denote by A_i the action to transmit an emulated primary signal on a non-empty subset of available channels and A_0 the action not to transmit any emulated signal. The strategy set of the attacker is given by

$$\Sigma_A = \{A_0, A_1, A_2, \ldots, A_{K_1-1}\}, \tag{1}$$

where the total number of pure strategies is the total number of channel subsets with less than M elements, i.e.,

$$K_1 = \sum_{i=0}^{M} \binom{N}{i}, \tag{2}$$

and $\binom{}{}$ is the binomial coefficient.

For N available channels, there are 2^N possible sensing results. Let $\mathbf{C}$ be the set of sensing results. For the k^{th} element $C_k \in \mathbf{C}$ $(k = 0, \ldots, 2^N - 1)$, we denote by $s(C_k)$ the number of occupied channels. Hence, the defender can take the action $D_{j|k}$ $(j \neq 0)$ to implement a surveillance algorithm on the j^{th} subset of occupied channels of C_k or $D_{0|k}$ not to monitor any channel. Given C_k, let Σ_D^k be the corresponding strategy set of the defender. Hence, the size of Σ_D^k is given by

$$\sum_{j=0}^{min(L,s(C_k))} \binom{s(C_k)}{j}. \tag{3}$$

Due to the incomplete information, pure strategies of the defender are formulated by combining the action sets of each sensing result, e.g., $(D_{\emptyset|0}, D_{\emptyset|1}, D_{\emptyset|2}, D_{\emptyset|3})$, $(D_{\emptyset|0}, D_{\emptyset|1}, D_{\emptyset|2}, D_{1|3})$, etc. The pure strategy set of the defender is written as

$$\Sigma_D = \{S_0, S_1, \ldots, S_{K_2-1}\}|_{S_j \in \Sigma_D^0 \times \Sigma_D^1 \times \ldots \Sigma_D^{2^N-1}} \tag{4}$$

The size of Σ_D is given by

$$K_2 = \prod_{k=0}^{2^N-1} \sum_{j=0}^{min(L,s(C_k))} \binom{s(C_k)}{j}. \tag{5}$$

3) Payoff: We first introduce the payoff related to player's actions at each channel: for the attacker of the t^{th} channel

- C_A^t is the cost for implementing selfish PUE.
- G_A^t is the benefit of using the channel for any CR user at one data frame.
- P_A^t is the penalty value for being captured by the defender.

For the defender

- C_S^t is the cost for implementing the surveillance process of the data frame.
- G_S^t is the benefit for capturing the attacker during the surveillance process of the data frame.

For each channel, if the PU was active in the data duration then the PU signal would interfere with the attacker's data transmission. Without loss of generality, we assume that the PU signal would be well in that case. Consequently, the attacker will gain nothing from the selfish PUE attack. Also, the defender cannot distinguish the PU signal from the attacker's signal[7]. We hence obtain the payoff of each player for a pair of actions regarding the presence of the PU at the t^{th} channel as given in Table I. The corresponding expected payoffs (w.r.t. PU presence and sensing results) for the attacker and the defender are shown in Table II.

4) Expected Payoff: To compute the corresponding expected payoff for each player, we consider the game tree described in Fig. 2. In the game theory framework, terminal

[7]Due to the interference between the PU's signal and the attacker's signal, the defender cannot identify the ID (i.e., the identification) of the attacker.

TABLE I: The relationship between the player payoffs and the presence of the PU for a pair of actions at the t^{th} channel in the scenario of selfish PUE attack without the fallow set.

PU	Attacker	Sensing	Defender	Payoff (Attacker, Defender)
Inactive	Attack	Occupied	Surveillance	$\left(-C_A^t - P_A^t, -C_S^t + G_S^t\right)$
			No Surveillance	$\left(-C_A^t + G_A^t, 0\right)$
		Unoccupied	No Surveillance	$\left(-C_A^t, 0\right)$
	No Attack	Occupied	Surveillance	$\left(0, -C_S^t\right)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$
Active	Attack	Occupied	Surveillance	$\left(-C_A^t, -C_S^t\right)$
			No Surveillance	$\left(-C_A^t, 0\right)$
		Unoccupied	No Surveillance	$\left(-C_A^t, 0\right)$
	No Attack	Occupied	Surveillance	$\left(0, -C_S^t\right)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$

TABLE II: Action payoffs for the attacker (left) and the defender (right) at the t^{th} channel in the scenario of selfish PUE attack without the fallow set.

Attacker	Defender	
	Surveillance (when occupied)	No surveillance
Attack	$p_A^t\left(-C_A^t - \rho_A^t P_A^t\right)$; $p_A^t\left(-C_S^t + \rho_A^t G_S^t\right)$	$-C_A^t + p_A^t \rho_A^t G_A^t$; 0
No Attack	0; $-p_N^t C_S^t$	0; 0

states are states at which the game ends. By imagining a game as a finite, rooted tree, each leaf in the game tree represents a terminal state. We denote by Z the set of terminal states where $\theta_a(z)$ and $\theta_d(z)$ are the corresponding actions of the attacker and the defender that lead to a terminal state $z \in Z$. Let $\delta_a(z)$ and $\delta_d(z)$ be the corresponding probabilities of the action $\theta_a(z)$ and $\theta_d(z)$.

For the pair of strategies $(\theta_a(z), \theta_d(z))$, the payoff of the attacker $U_A(\theta_a(z), \theta_d(z))$ is given by

$$U_A(\theta_a(z), \theta_d(z)) = \sum_{t \in \theta_a(z)} U_A^{t,\theta_d(z)}, \tag{6}$$

where $U_A^{t,\theta_d(z)}$ is the payoff of the attacker at channel $t \in \theta_a(z)$ when the defender plays strategy $\theta_d(z)$.

Similarly, the payoff of the defender for the strategy pair $\{\theta_a(z), \theta_d(z)\}$ is given by

$$U_D(\theta_a(z), \theta_d(z)) = \sum_{k \in \theta_d(z)} U_D^{\theta_a(z),k}, \tag{7}$$

where $U_D^{\theta_a(z),k}$ is the payoff of the defender at channel $k \in \theta_d(z)$ when the attacker plays strategy $\theta_a(z)$.

Let $P(z)$ be the probability of the sensing result on the path from the root to z, the expected payoffs of the attacker and the defender are given by

$$\Omega_A = \sum_{z \in Z} P(z)\, \delta_a(z)\, \delta_d(z)\, U_A(\theta_a(z), \theta_d(z)), \tag{8}$$

$$\Omega_D = \sum_{z \in Z} P(z)\, \delta_a(z)\, \delta_d(z)\, U_D(\theta_a(z), \theta_d(z)). \tag{9}$$

B. Equilibrium Point

In a game, the rational player always adapts to the other's strategy by playing the best response (or one of the best responses). In our previous work, called the non-commitment model [16]), the best strategy of the defender is the NE. Consequently, the best response strategy for the attacker in the non-commitment model is the NE.

IV. Selfish PUE Attack Without The Fallow Set: Commitment Model

Our goal is to compute the optimal mixed strategy for the defender and the attacker, as well as to compare the corresponding performance of the surveillance strategy in both models (commitment and non-commitment). Hereafter, we present the elements of the Stackelberg multi-channel surveillance game.

A. Game Formulation

The defender acts as the *Leader* by monitoring the occupied channels to catch the illegal occupations while committing to a (mixed) surveillance strategy. In contrast, the attacker acts as the *Follower* by optimizing its outcome regarding the committed surveillance strategy.

1) Pure Strategy Set: In the Stackelberg game, the strategy of each player is the set of its' actions in the path from the root to each terminal state. As defined above, Z is the set of terminal states, whose size is given by

$$K_3 = K_1 \sum_{k=0}^{2^N - 1} \sum_{j=0}^{min(L, s(C_k))} \binom{s(C_k)}{j}. \tag{10}$$

Thus, there are K_3 pure strategies, so we can write the pure strategy set of the defender as follows:

$$\Theta_D = \{\theta_d(z)\}_{z \in Z}. \tag{11}$$

Similarly, there are K_3 pure strategies, so we can write the pure strategy set of the attacker as follows:

$$\Theta_A = \{\theta_a(z)\}_{z \in Z}. \tag{12}$$

For example, the game illustrated in Fig.2 contains $K_3 = 3 \times 8 = 24$ terminal states. For each terminal state, we have a pure strategy of the attacker and a corresponding pure strategy of the defender (e.g. $(A_\emptyset, D_{\emptyset|0})$, $(A_\emptyset, D_{\emptyset|1})$, $(A_\emptyset, D_{1|1})$.).

2) Mixed Strategy Set: The mixed strategies for the defender and the attacker are respectively defined by

$$\Delta_D = \{\delta_d(z)\}_{z \in Z}, \tag{13}$$

$$\Delta_A = \{\delta_a(z)\}_{z \in Z}. \tag{14}$$

3) Expected Payoff: The expected payoffs of each player are computed as given in (8) and (9), respectively.

B. Strong Stackelberg Equilibrium

In the commitment model, the best strategy for the defender is the Strong Stackelberg Equilibrium (SSE) [27], which is defined as follows:

Definition 1: A pair of strategies $(\gamma_a(\delta_d), \delta_d)$ forms a Strong Stackelberg Equilibrium (SSE) if it satisfies the following:

1) *The follower plays a best response*

$$\Omega_A(\gamma_a(\delta_d), \delta_d) \geq \Omega_A(\delta_a, \delta_d) \, \forall \delta_a \in \Delta_A, \delta_d \in \Delta_D,$$

2) *The leader plays a best response*

$$\Omega_D(\gamma_a(\delta_d), \delta_d) \geq \Omega_D\left(\gamma_a(\delta_d^{'}), \delta_d^{'}\right) \forall \delta_d^{'} \in \Delta_D,$$

3) *If the follower has the choice of best response, then it advantages the leader*

$$\Omega_D(\gamma_a(\delta_d), \delta_d) \geq \Omega_D\left(\delta_a^{'}, \delta_d\right) \forall \delta_a^{'} \in \Delta_A^*(\delta_d), \delta_d \in \Delta_D,$$

where $\gamma_a(\cdot)$ denotes the follower's response function and $\Delta_A^*(\delta_d)$ denotes the set of the follower's best responses to δ_d.

Consequently, the attacker is forced to adapt by playing the best response regarding the committed surveillance strategy. We observe that the defender's SSE expected payoff is always at least as high as the defender's expected payoff in any NE profile [27]. The reason is in the commitment model, the leader can at the very least choose to commit to its NE strategy. If it does so, then among its best responses the follower will choose one that maximizes the utility of the leader due to the tie-breaking assumption. In the NE, however, the follower will choose from his best responses to this defender strategy but not necessarily the ones that maximize the leader's utility.

We observe that, for a given defender's mixed strategy, the best pure strategy of the attacker belongs to its set of best-mixed strategies because *its expected payoff is a linear function* [23], [27]–[29]. Therefore, we restrict the attacker's pure strategies to find out the optimal strategy of the defender. The *Multiple Linear Programs* (MLP) [28] method is adopted to determine the SSE equilibrium of the game. Specifically, this solves a set of linear programs for *each pure strategy* of the attacker as follows.

Typically, MLP is a natural divide-and-conquer approach. The main idea is to consider each pure strategy of the follower in turn by solving the corresponding linear program. For each linear program, given a pure strategy of the attacker, we must find the corresponding mixed strategy of the defender that satisfies: (i), the given pure strategy of the attacker is a best response, and (ii), the expected payoff of the defender is maximized. By solving all separated linear programs, we can determine the optimum mixed strategy for the defender. In particular, for the multi-channel surveillance game, we must consider K_1 linear programs, each for a pure strategy of the attacker as presented by (15)-(18). Each linear program works as follows: the first constraint (16) says the given attacker strategy must be a best response to the defender's strategy. Other constraints (17), (18) provide the bound for the defender's strategy. The objective (15) ensures the defender's expected payoff is maximal. In general, the MLP algorithm is implemented as follows

for *each pure strategy of the attacker* $\delta_a^*(z)$ **do**
  Compute the best response of the defender $\delta_d^*(z)$ by using MLP;
  Store the expected payoff $U_D\left(\delta_a^*(z), \delta_d^*(z)\right)$
end
Compare the expected payoff for each pair of $\left(\delta_a^*(z), \delta_d^*(z)\right)$;
Determine the SSE strategy

Algorithm 1: MLP Algorithm

Since there is at least one feasible solution for each linear program, the SSE strategy is achieved by choosing one with the highest optimal solution value in the solutions of K_1 linear program. Because each of the linear programs can be solved in polynomial time, the MLP gives a *polynomial time algorithm* to calculate the SSE strategy of the game.

C. Commitment vs. Non-commitment

Hereafter we analyze the expected payoffs associated with the attacker and the defender, as well as the time required to determine the equilibrium strategies in two considered models, allowing for a clear comparison between non-commitment and commitment strategies for the network manager. We first state two straightforward corollaries

Corollary 1: In the multi-channel surveillance game, the defender's expected payoff obtained from optimally committing to a mixed strategy is at least as high as its expected payoff in any NE equilibrium.

Proof: It is direct consequence of Definition 1. ■

Corollary 2: In the multi-channel surveillance game, finding the NE strategy in the non-commitment case is approximately 2^N time more complex than computing the SSE strategy in the commitment case.

Proof: To determine the NE strategy in the non-commitment case, the computational algorithms must consider all possible mixed strategies of both players. It means that we must solve at least $K_4 = 1 + K_1 \times \left(2^N + 1\right)$ linear programs, each with K_2 variables, through the sequence-form representation [16]. However, to determine the SSE strategy, the MLP algorithm considers only K_1 linear program of a smaller number of variables ($K_3 \ll K_2$) for each attacker's pure strategy. Since $K_4 \approx 2^N \times K_1$, we conclude that the computational algorithm to determine the NE strategy in the non-commitment case is approximately 2^N times more complex

Multiple Linear Program (MLP)

$$\max_{\delta_d} \sum_{z\in Z} P(z)\,\delta_a(z)\,\delta_d(z)\,U_D(z) \tag{15}$$

$$s.t \sum_{z\in Z|\sigma_a(z)=A_j} P(z)\,\delta_a(z)\,\delta_d(z)\,U_A(z) \geq \sum_{z'\in Z|\sigma_a(z')=A_k} P(z')\,\delta_a(z')\,\delta_d(z)\,U_A(z') \tag{16}$$

$$\sum_{z\in Z|C_k \text{leads to } z} \delta_d(z) = 1, \forall C_k \in C \tag{17}$$

$$0 \leq \delta_d(z) \leq 1, \forall z \in Z \tag{18}$$

than the MLP algorithm to determine the SSE strategy in the commitment case. Thus we obtain Corollary 2. ■

Remark 1: Two corollaries suggest that the commitment model leading to the SSE defense strategy, is a better candidate to mitigate selfish PUE in CRNs than the non-commitment approach (leading to the NE defense strategy).

V. Selfish PUE Attack With Fallow Set: Commitment Model

In this section, we formulate the relationship between the defender and the PUE attacker, which has known the fallow set, as an extensive-form game with incomplete information. We consider a CRN with N channels which is contained P ($P \leq N$) fallow channels. Let Λ_P be the fallow set. At a time, the attacker can select up to M channels in Λ_P to attack while the defender can select up to L occupied channels to perform the surveillance process. Typically, we have $M \leq P$, $L \leq N$. An example of the channel surveillance game for a CRN with $(N, \Lambda_P, M, L) = (2, \{2\}, 1, 1)$ is illustrated in Fig. 3.

A. Game Formulation and Commitment Model

In this scenario, the defender plays as the *Leader* white the attacker plays as the *Follower*.

The corresponding strategy set of the attacker is given by

$$\Sigma_A = \{A_0, A_1, A_2, \ldots, A_{K_1^{'}-1} | A_i \subset \{P\}\}, \tag{19}$$

where $K_1^{'}$ is the total number of channel subsets with less than M elements in the fallow set, i.e

$$K_1^{'} = \sum_{i=0}^{P} \binom{M}{i}. \tag{20}$$

The strategy set of the defender is defined as same as in (4).

The payoff of each player for a strategy pair (w.r.t PU presence and sensing results) is given in Table I, except the case that the attacker attacks when the PU is active.

For the Stackelberg game, the size of the terminal states set $Z^{'}$ is given by

$$K_3^{'} = K_1^{'} \times \sum_{k=0}^{2^N-1} \sum_{j=0}^{min(L,s(C_k))} \binom{s(C_k)}{j}, \tag{21}$$

Consequently, there are $K_3^{'}$ pure strategies in the pure strategy sets of the attacker and the defender as follows.

$$\Theta_A^{'} = \{\theta_a^{'}(z)\}_{z\in Z'}, \tag{22}$$

$$\Theta_D^{'} = \{\theta_d^{'}(z)\}_{z\in Z'}. \tag{23}$$

For example, the game in Fig. 3 contains $K_3^{'} = 2 \times 8 = 16$ terminal states. For each terminal state, we have a pure strategy of the attacker and a pure strategy of the defender. E.g., $(A_\emptyset, D_{\emptyset|0})$, $(A_\emptyset, D_{\emptyset|1})$, $(A_\emptyset, D_{1|1})$, …, $(A_2, D_{2|3})$.

The mixed strategies for the defender and the attacker are respectively defined by

$$\Delta_D^{'} = \{\delta_d^{'}(z)\}_{z\in Z'}, \tag{24}$$

$$\Delta_A^{'} = \{\delta_a^{'}(z)\}_{z\in Z'}. \tag{25}$$

Similar (6) and (7), the payoffs of the attacker and the defender for a strategy pair $\left(\theta_a^{'}(z), \theta_d^{'}(z)\right)$ are given by

$$U_A^{'}\left(\theta_a^{'}(z), \theta_d^{'}(z)\right) = \sum_{t\in\theta_a^{'}(z)} U_A^{'\,t,\theta_d^{'}(z)}, \tag{26}$$

$$U_D^{'}\left(\theta_a^{'}(z), \theta_d^{'}(z)\right) = \sum_{k\in\theta_d^{'}(z)} U_D^{'\,\theta_a^{'}(z),k}, \tag{27}$$

where $U_A^{'\,t,\theta_d^{'}(z)}$ is the payoff of the attacker at channel $t \in \theta_a^{'}(z)$ when the defender plays $\theta_d^{'}(z)$ and $U_D^{'\,\theta_a^{'}(z),k}$ is the payoff of the defender at channel $k \in \theta_d(z)$ when the attacker plays $\theta_a(z)$.

Similar (8) and (9), the expected payoffs of the attacker and the defender are given by

$$\Omega_A^{'} = \sum_{z\in Z'} P(z)\,\delta_a^{'}(z)\,\delta_d^{'}(z)\,U_A^{'}\left(\theta_a^{'}(z), \theta_d^{'}(z)\right), \tag{28}$$

$$\Omega_D^{'} = \sum_{z\in Z'} P(z)\,\delta_a^{'}(z)\,\delta_d^{'}(z)\,U_D^{'}\left(\theta_a^{'}(z), \theta_d^{'}(z)\right). \tag{29}$$

The same method (Algorithm 1-MLP) is adopted to determine the SSE strategy of the game by solving a set of linear programs for *each pure strategy* of the attacker.

B. Selfish PUE Attack With v.s. Without Fallow Set

Remark 2: Below are some interesting observations.

- First, Algorithm 1 can be adopted to determine the SSE strategy in both scenarios: selfish PUE attack with/without the fallow set.
- Second, from (10) and (21), the number of strategies in the scenario of selfish PUE attack without the fallow set is higher than with the fallow set. Thus, the computing time to determine the SSE strategy in the second scenario is smaller than the first one.
- Third, we still have the straightforward result that provided in Remark 1.

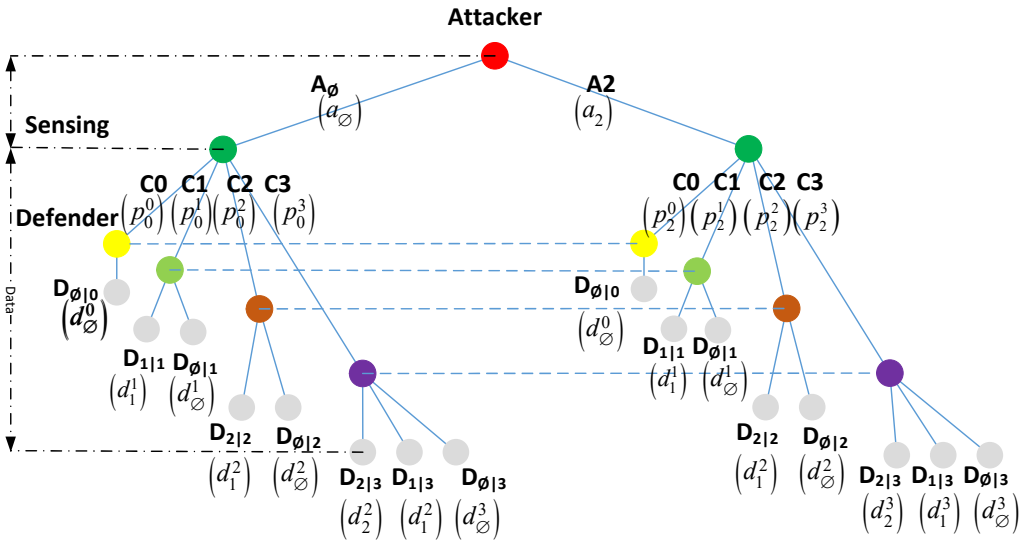


Fig. 3: The multi-channel surveillance game for a CRN with two available channels where the attacker conducts a selfish PUE attack with the fallow set (i.e., channel 2). The attacker/defender can attack/monitor one channel at a time.

VI. Numerical Results

To investigate the influence of system parameters on the equilibrium strategies, numerical simulations have been conducted in Matlab environment with CPLEX 12.4 [30] for optimization. We assume that the average SNR of the primary signal received at the spectrum sensor is -10 dB, the false alarm probability P_f is 0.1[8] and the number of samples is 1500 samples. The detection probability (P_d) is computed from the false alarm probability and the number of samples through the *Constant False Alarm Rate* (CFAR) criterion, where the threshold is determined by keeping the false alarm rate constant. Without loss of generality, we assume that the benefit of a successful attack exceeds the attack cost for the attacker, i.e., $C_A^t < G_A^t$. This assumption guarantees that the attacker has the incentive to attack the CRN.

When the attacker is captured, its punishment (penalty) consists of banning it from accessing the radio resources. Consequently, the saved radio resources will be beneficial for the rest of the network. In general, the gain of attack (G_A^t) and the gain of surveillance (G_S^t) depend on the being captured penalty (P_A^t). To simplify the problem, we assume that the cost/gain/penalty for the attack and the surveillance process are equal in all channels. To make the simulation results clear and easy to follow, we start with a CRN with two channels ($N = 2$) with a capture penalty $P_A = 100$. We first consider the case where the attacker can attack up to $M = 1$ channel and the defender can monitor up to $L = 1$ channel at a time. Other parameters are $C_A = 20$, $C_S = 10$, $\pi_1 = 0.2$ and $\pi_2 = 0.5$.

A. Scenario 1: Selfish PUE Attack Without Fallow Set

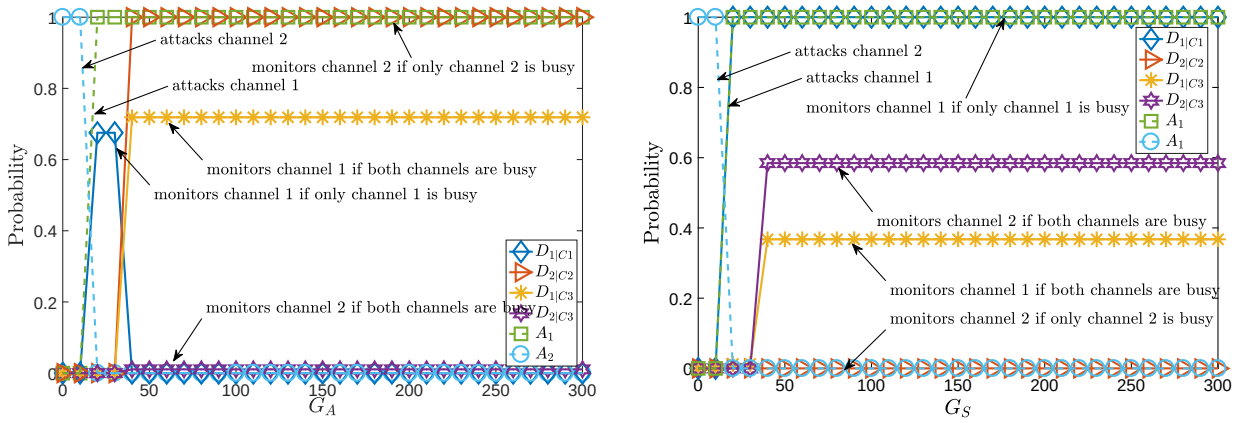
1) SSE strategy in the commitment model: Fig. 4 presents the SSE strategies of the defender and the attacker in the commitment case with low attack gain ($G_A = 100$) and high attack gain ($G_A = 300$), respectively. We observe that, for a fixed captured penalty value, the SSE strategy of both players depends on G_A and G_S. For both cases, if G_S is low, the defender gives a low effort to implement the surveillance process on the occupied channels. The attacker, however, will implement the selfish PUE on the CRN. If G_S is high, the defender will perform the following surveillance strategy on the occupied channel.

- For low G_A: the defender monitors *channel* 2 if only channel 2 is busy. If both channels are busy, the defender then monitors *channel* 1.
- For high G_A: the defender monitors *channel* 1 if only channel 1 is busy and *channel* 1 with a probability 0.58 and *channel* 2 with a probability 0.36 if both channels are busy.

Consequently, given any strategy of the defender, the best response of the attacker is to attack channel 1 since the presence probability of PU in channel 1 is smaller than in channel 2 ($\pi_1 = 0.2 < \pi_2 = 0.5$). This is based on the assumption that if the attacker has the choice of best response, then it advantages the defender.

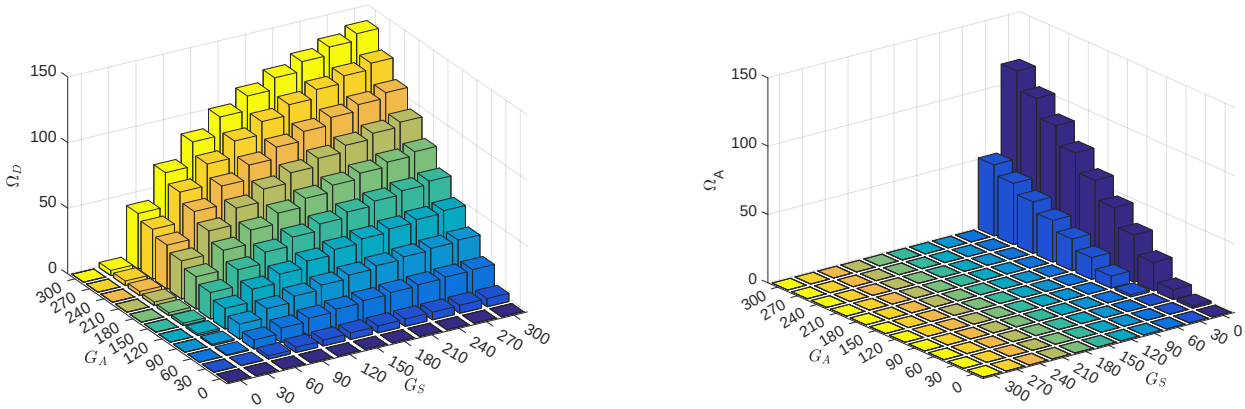
Fig. 5a and Fig. 5b display the obtained expected payoffs of the defender and the attacker by considering the SSE strategy, respectively. We observe the consistency between the SSE strategies and the expected payoffs of both players. When G_S is small, the defender gives a low effort to monitor the occupied channels. In such a case, the expected payoff of the defender is 0. The attacker, however, gets a positive expected payoff. When G_S increases, the expected payoff of the defender will increase along with the increase of the attack gain. In contrast, the expected payoff of the attacker decreases to 0. By setting a high monitoring gain, in the commitment case, the lowest expected payoff of the defender by playing the SSE strategy is 0, which corresponds to the case that the

[8]Based on the IEEE Standard for Cognitive Wireless RAN IEEE.802.22 [26]



(a) $G_A = 100$ (b) $G_A = 300$

Fig. 4: The SSE strategies of the attacker and the defender for (a) the low attack gain ($G_A = 100$) and (b) the high attack gain ($G_A = 300$) when the attacker conducts a selfish PUE attack without the fallow set.



(a) Defender (b) Attacker

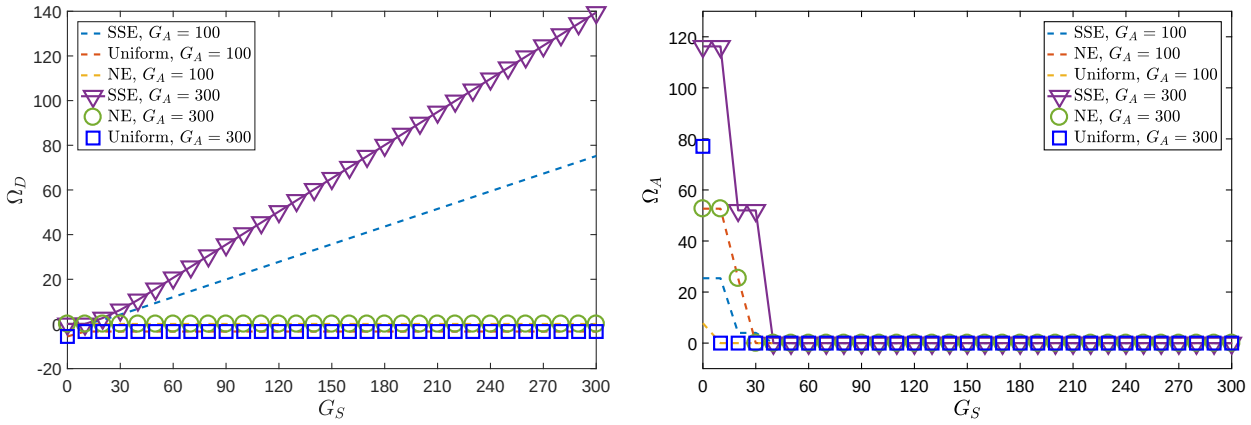
Fig. 5: The expected payoff of (a) the defender, and (b) the attacker in the commitment case when the attacker conducts an attack without the fallow set

attacker performs "No attack" on the CRN. Conversely, if the attacker chooses to attack, the defender's expected payoff will improve significantly. We conclude that the network manager must set a high monitoring gain to mitigate the influence of selfish PUE in CRN.

2) The benefits of the commitment model: To validate the benefits of the SSE strategy in the commitment model, we take into account the comparison between the expected payoffs of the defender and the attacker in three cases: 1) the commitment case where the defender and the attacker play their SSE strategy, 2) the non-commitment case where the defender and the attacker play their NE strategy, and 3) the commitment case where the defender plays the uniform strategy (i.e., the defender performs the same probability for every possible strategies) and the attacker plays its best response to the defender's strategy.

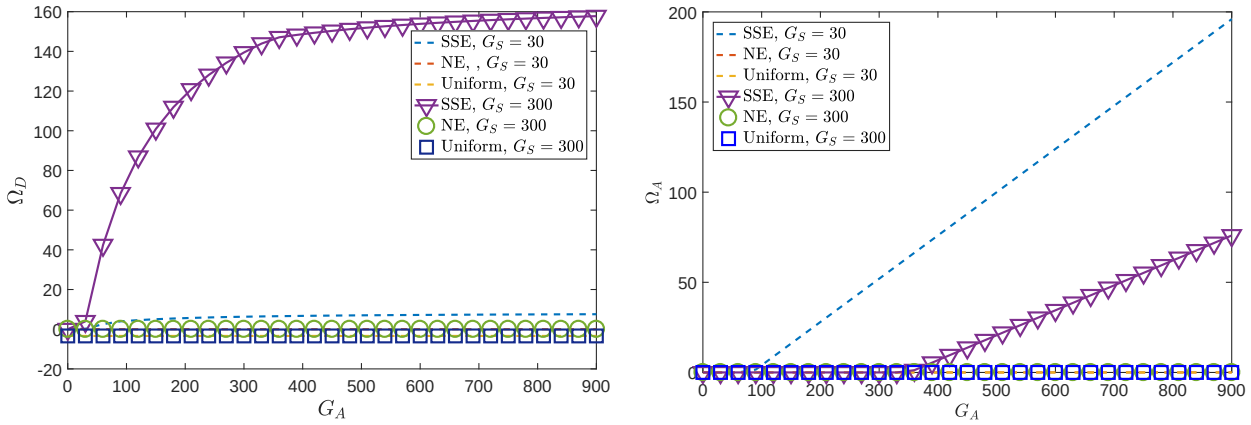
First, we consider the influence of the surveillance gain G_S on the expected payoffs of two players. Fig. 6a shows the expected payoffs of the defender when $G_A = 100$ and $G_A = 300$, respectively. We observe that, with the SSE strategy, the expected payoff of the defender is much higher than with the uniform strategy or the NE strategy. Similarly, Fig. 6b shows the expected payoffs of the attacker when $G_A = 100$ and $G_A = 300$, respectively. We observe that, for most G_S, the expected payoff of the attacker obtained with the SSE strategy is approximately the one with the NE strategy. For the low surveillance gain (G_S), the defender will not perform the monitoring on the occupied channel due to the low gain, then the attacker will implement the selfish PUE and achieve a positive expected payoff. In contrast, for the high surveillance gain (G_S), the expected payoff of the attacker in all considered cases will degrade to 0.

Next, we consider the influence of the attack gain (G_A) on the expected payoffs of two players. Fig. 7a shows the obtained expected payoffs of the defender when $G_S = 30$ and $G_S = 300$, respectively. We observe that, for a given surveillance gain (G_S), the expected payoff of the defender obtained with the SSE strategy is much higher than in the other cases. Similarly, Fig. 7b shows the obtained expected payoff of the attacker when the surveillance gain $G_S = 30$ and $G_S = 300$, respectively. We observe that, for a given G_S, the expected payoff of the attacker when both players play their



(a) Defender. (b) Attacker.

Fig. 6: The expected payoff of (a) the defender, and (b) the attacker in three considered cases for $G_A = 100$ and $G_A = 300$ when the attacker conducts a selfish PUE attack without the fallow set.



(a) Defender. (b) Attacker.

Fig. 7: The expected payoff of (a) the defender, and (b) the attacker in three considered cases for $G_S = 30$ and $G_S = 300$ when the attacker conducts a selfish PUE attack without the fallow set.

SSE strategy is approximately 0 when G_A is small ($G_A < 60$ for $G_S = 30$ and $G_A < 330$ for $G_S = 300$) and increases linearly as G_A increases.

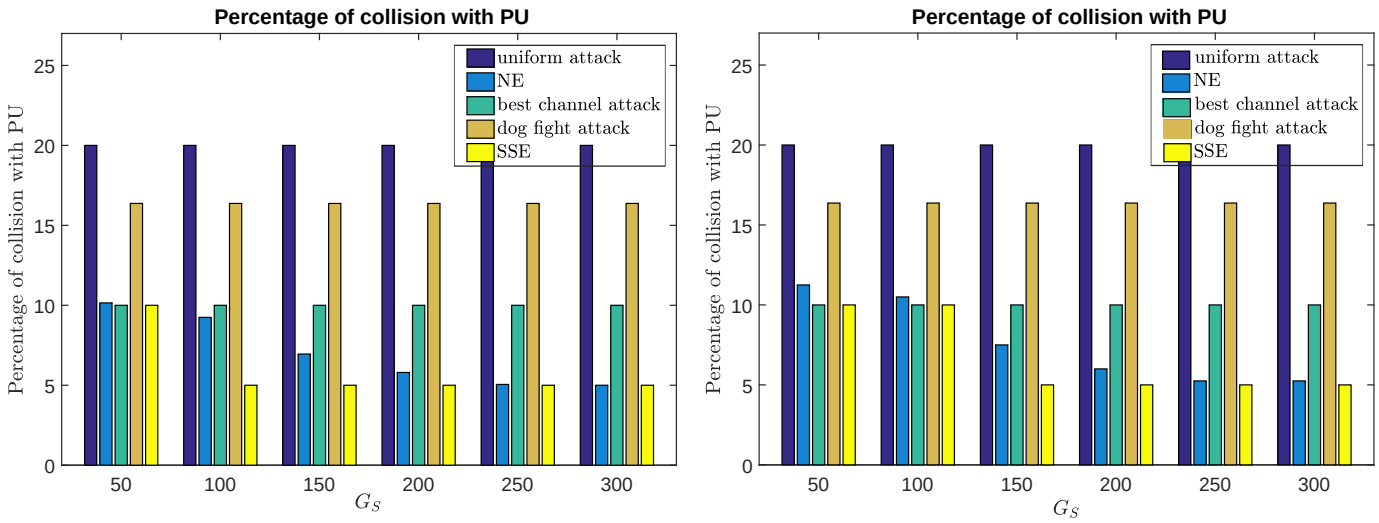
In summary, from Fig. 6 and Fig. 7, we conclude that, by exploiting the leader position by committing the surveillance strategy and forcing the attacker as the follower, the defender significantly improves its utility with respect to playing a NE strategy, hence obtains a better protection against selfish PUEs.

Next, we consider the computation time to find the equilibrium point (of the corresponding algorithms) in the multi-channel surveillance game. The simulations are conducted on a Dell Precision M6700 laptop with Intel Core i7 CPUs 2.6GHz. Table III shows the average computation time (through the Monte-Carlo simulation) to determine the SSE point by using the MLP and the NE point by the sequence-form representation method (which is presented in our previous work [16]). In these simulations, we assume that the attacker/defender can attack/monitor $M = L = 1$ channel at most. The results show that the MLP method to determine the equilibrium point in the commitment model is much faster than the sequential representation method to determine the NE strategy in the non-commitment model. Consequently, the MLP method can provide the solution for a large game which is infeasible by using the sequence-form representation method.

TABLE III: The average computation time required to determine the equilibrium point in the non-commitment case (sequence-form method) and commitment case (MLP method).

	$N = 2$	$N = 4$	$N = 6$	$N = 8$	$N = 10$
Sequence-form	2s	11564s	>12h	–	–
MLP	0.17 s	7.8s	84.05s	20min	2h

Next, we show the effectiveness of our proposed commitment model on reducing the number of collisions to PU due to PUE attacks through the following simulation. We consider a CRN with $N = 3$ channels, where the attacker/defender can attack/monitor one channel at most, i.e., $M = L = 1$. The common knowledge are the probability of PU activity at each channel $\pi_1 = 0.1$, $\pi_2 = 0.2$ and $\pi_3 = 0.3$, the probability of detection $P_d = 0.9$ and the probability of false alarm $P_f = 0.1$. A collision between the attacker and the PU happens



(a) $G_A = 100$ (b) $G_A = 300$

Fig. 8: The percentage of collision with the primary user of the attacker for different values of G_A and G_S when the attacker conducts a selfish PUE attack without the fallow set.

if the sensing results show that an attacked channel, where the PU is actually transmitting, is occupied (then is used by the attacker). The Monte-Carlo simulations with 10^6 samples is adopted to observe the collision between the attacker and the PU. Five scenarios are considered: i) the attacker follows its SSE strategy, ii) the attacker follows its NE strategy, iii) the attacker follows a uniform strategy (i.e., the attack probability is the same for all channels), iv) the attacker conducts attack on the channel with the lowest probability of PU activity (i.e., channel 1), and v) the attacker conducts attack as in the dog fight attack [14] (i.e., the attacker attack channel t with a probability $\frac{1}{\pi_t}/\sum_{i=1}^{N}\frac{1}{\pi_j}$). From the simulation results (Fig. 8), if the attacker follows the SSE strategy, the percentage of collision with primary users of the attacker is smallest. This conclusion confirms the added value of our proposed approach in order to mitigate the selfish PUE attack in CRNs.

3) The influence of N, M and L: Finally, we consider the influence of the different configurations in terms of the number of available channels (N), the maximal number of attacked channels (M) and the maximal monitored channels (L) on the system performance. A CRN system with $N = 4$, $M = \{1, 2, 3, 4\}$ and $L = \{1, 2, 3, 4\}$ is considered. In order to simplify the analysis and focus on the effects of (N, M, L) on the system performance, we assume that $G_A = G_S = P_A = 100$. In practice, this assumption is reasonable since these gains are equal to the gain for using the channel (for data transmission) at one data frame.

Fig. 9a presents the expected payoff of the defender for various values of L and M. We observe that, for a fixed value of L, the increase of M will lead to the increase of the defender's expected payoff. The reason is that the more channels will be attacked, the higher the probability of capture. Indeed, this is due to the leader position of the defender in the game. In contrary, increasing L with a fixed value of M only makes sense when M is larger than 1. If $M = 1$, the increase of L even leads to the degradation of the defender's expected payoff due to the increase of the surveillance cost.

Similarly, Fig. 9b presents the expected payoff of the attacker for various values of L and M. We observe that, if $M > L$, then the expected payoff of the attacker will be a positive value. Otherwise, the expected payoff of the attacker is approximately 0. Also, if $L = 1$, the attacker will get a higher expected payoff if it attacks on multiple channels.

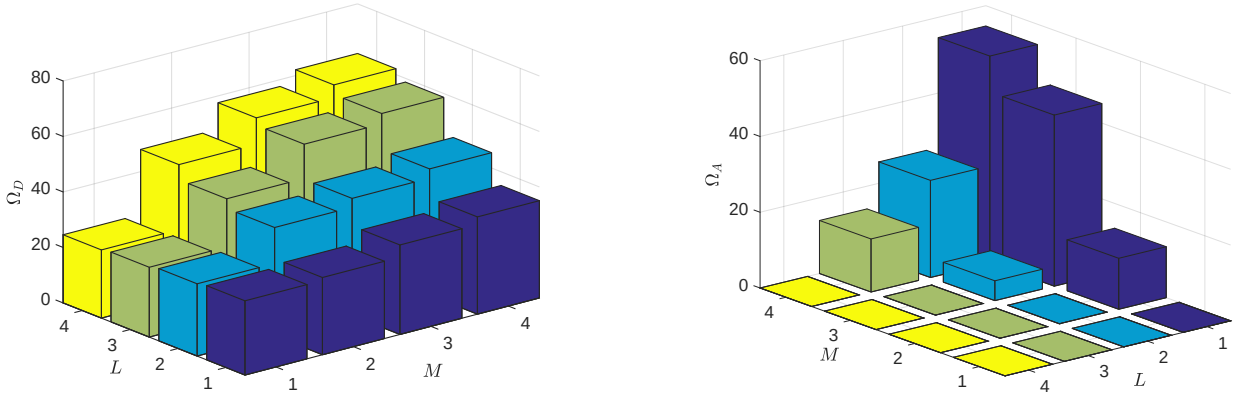
Since the performance of the surveillance process depends not only on (N, M, L) but also on the relationship between the penalty value (P_A), the attack gain (G_A) and the surveillance gain (G_S), it is difficult to provide an optimal value of N, L and M for an effective PUEA attack or an effective surveillance process. Instead, for the attacker, we can use a heuristics way as follows: if $G_S \gg P_A$ and/or $G_A \ll P_A$, it will be better to not perform the selfish PUE attack; otherwise, if $L < N$, it is better to set $M > L$, otherwise M is set smaller; if $L = N$, it is better to set $M = 1$. Similarly, for the defender, we can use a heuristics way as follows: if $M = 1$, it is better to set $L = 1$; otherwise L is set higher than M.

B. Scenario 2: Selfish PUE Attack With The Fallow Set

To investigate the SSE strategy in the commitment model when the attacker conducts a selfish PUE attack with the fallow set, we consider the CRN system where $(N, M, L) = (2, 1, 1)$. The fallow set $\{P\} = \{2\}$, i.e., the PU is not active in channel 2 and the attacker knows that. Other parameters are all set as in the scenario of selfish PUE attack without the fallow set.

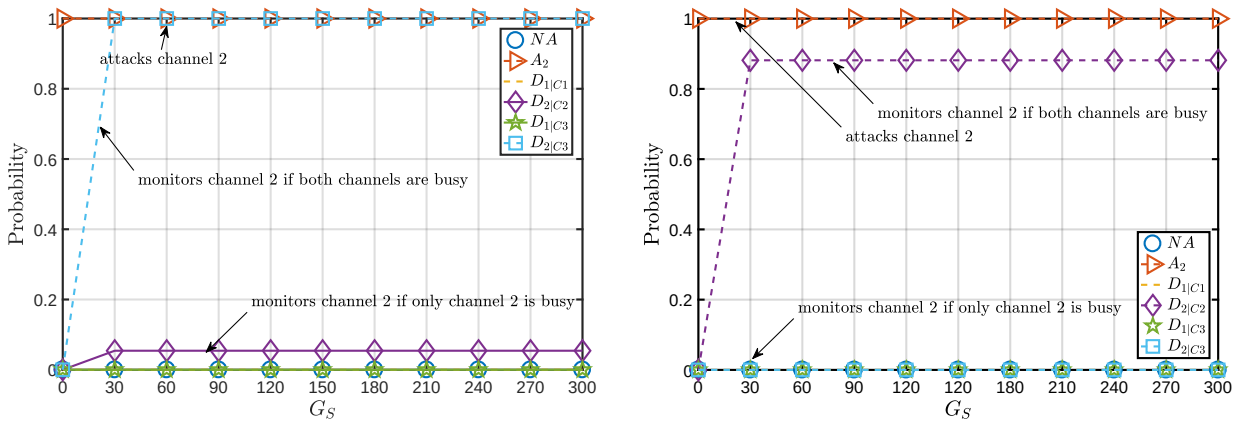
1) SSE strategy in the commitment model: Fig. 10 presents the surveillance strategy of the defender as well as the attack strategy of the attacker in the commitment case with low attack gain ($G_A = 100$) and high attack gain ($G_A = 300$), respectively. Similarly, Fig. 11 displays the obtained expected payoffs of the defender and the attacker by considering the SSE strategy, respectively. We observe that

- The defender monitors the fallow channel (channel 2) if it is busy with a low probability for the low attack gain



(a) Defender (b) Attacker

Fig. 9: The expected payoff of (a) the defender and (b) the attacker for different configurations of N, L and M while $G_A = G_S = P_A = 100$ when the attacker conducts an attack without the fallow set.



(a) $G_A = 100$ (b) $G_A = 300$

Fig. 10: The SSE strategies of the attacker and the defender for (a) the low attack gain ($G_A = 100$) and (b) the high attack gain ($G_A = 300$) in the scenario of selfish PUE attack with the fallow set.

G_A and with a high probability for the high attack gain G_A, respectively.

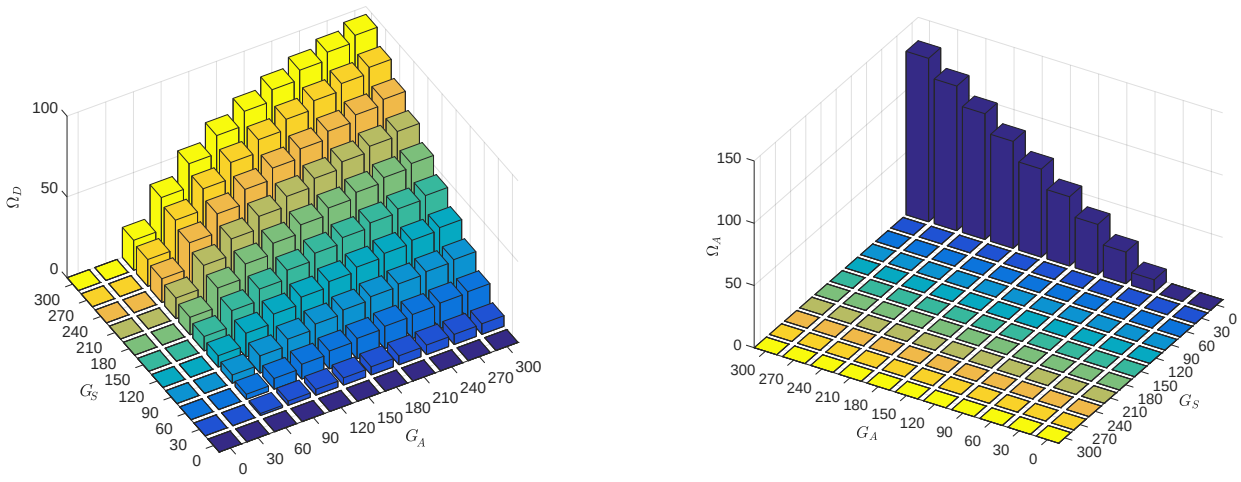
- If G_S is small, the defender will give a low effort to monitor the occupied channels. In such a case, the expected payoff of the defender is 0. The attacker, however, gets a positive expected payoff.
- When G_S increases, the expected payoff of the defender will increase along with the increase of G_A. In contrast, the expected payoff of the attacker decreases to 0.

In summary, by setting a high monitoring gain, the lowest expected payoff of the defender by playing the SSE strategy is 0, which corresponds to the case that the attacker performs "No attack" on the CRN. Conversely, if the attacker chooses to attack, the defender's expected payoff will improve significantly. We conclude that the network manager must set a high monitoring gain to mitigate the influence of selfish PUE attack.

2) The benefits of the commitment model: To validate the benefits of the SSE strategy in the commitment case when the attacker conducts a selfish PUE attack with the fallow set, a similar comparison is considered between the expected payoffs of the defender as well as the expected payoffs of the attacker in three cases where the defender plays: 1) its SSE strategy, 2) a uniform strategy and 3) its NE strategy.

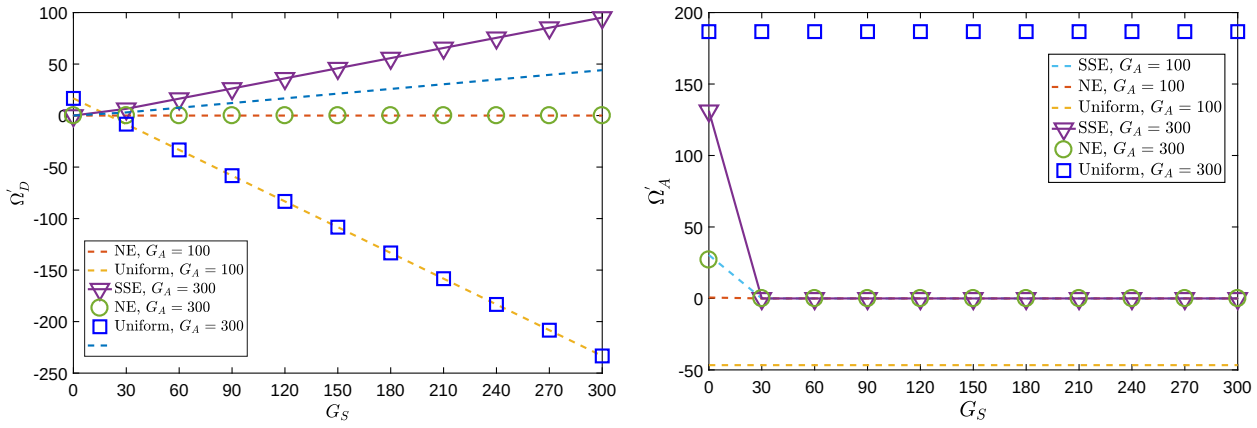
Fig. 12 shows the expected payoff of defender $\Omega_D^{'}$ and the one of the attacker $\Omega_A^{'}$ in the scenario of selfish PUE attack with the fallow set scenario where $G_A = 100$ and $G_A = 300$. Similar to the scenario of selfish PUE attack without the fallow set, for most G_S, the expected payoff of the attacker obtained with the SSE strategy is approximately the one with the NE strategy. For the low G_S, the defender will not perform the monitoring on the occupied channel due to the low gain, then the attacker will implement the selfish PUE and achieve a positive expected payoff. For the high G_S, the expected payoff of the attacker in all considered cases will degrade to 0. The attacker's expected payoff in the uniform case, however, will be a negative value for low G_A and a positive value for high G_S. Moreover, the expected payoff of the defender obtained by following the SSE strategy outperforms the ones in other cases. Also, in the scenario of selfish PUE attack with the fallow set, if the defender performs a uniform surveillance strategy then its expected payoff degrades sharply.

Fig. 13 shows the expected payoffs of two players in the



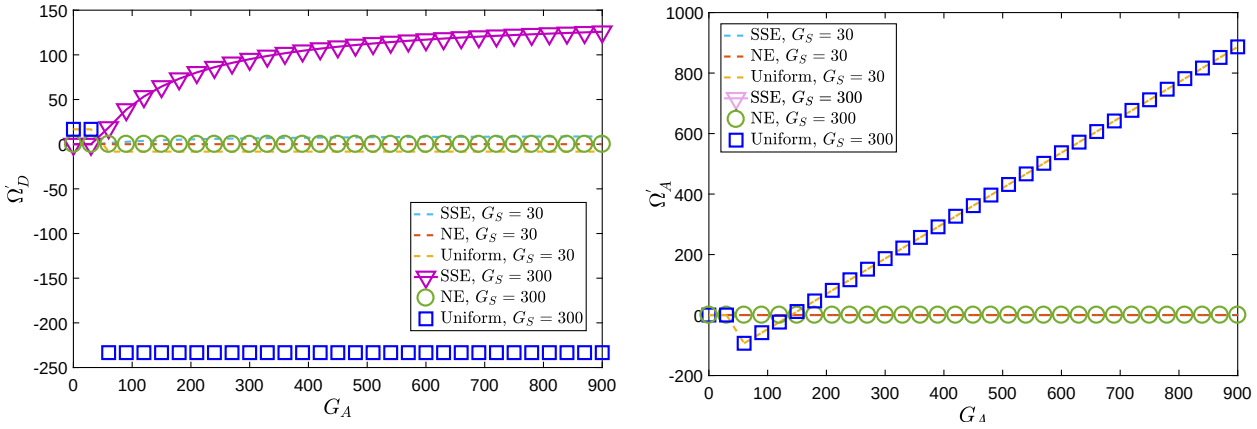
(a) Defender (b) Attacker

Fig. 11: The expected payoff of (a) the defender, and (b) the attacker in the commitment case when the attacker conducts a selfish PUE attack with the fallow set.



(a) Defender. (b) Attacker.

Fig. 12: The expected payoff of (a) the defender and (b) the attacker in three considered cases for $G_A = 100$ and $G_A = 300$ when the attacker conducts a selfish PUE attack with the fallow set.



(a) Defender. (b) Attacker.

Fig. 13: The expected payoff of (a) the defender and (b) the attacker in three considered cases for $G_S = 30$ and $G_S = 300$ when the attacker conducts a selfish PUE attack with the fallow set.

scenario of selfish PUE attack with the fallow set where G_S = 30 and G_S = 300. We observe that the expected payoff of the attacker obtained with the SSE strategy is approximately the one with the NE strategy while the expected payoff of the defender is much higher than the ones with the NE strategy and the uniform strategy.

In summary, we conclude that for the selfish PUE attack with the fallow set, by exploiting the leader position by committing to a surveillance strategy and forcing the attacker to act as the follower, the network manager significantly improves its utility with respect to playing a other strategies, hence obtains a better protection against selfish PUEs.

VII. Conclusion

We have discussed the surveillance process to mitigate multi-channel selfish PUE in cognitive radio networks. Two scenarios are considered: the selfish PUE attack with and without the fallow set. By monitoring the occupied channels, the network manager can detect the selfish attacker. The relationship between the selfish attacks and the surveillance process is analyzed by game-theoretic approaches. Through appropriate modeling of the strategic interaction between a defender and an attacker, we investigated the commitment model. In this model, the defender takes the lead by committing to a surveillance strategy. To maximize the expected payoff, the rational attacker is forced to become a follower responding to the strategy used by the defender. The relevant strategies of the surveillance process are invested through the SSE. Analytical and numerical results show that the defender's expected payoff is significantly improved when the defender commits to a surveillance strategy. Moreover, the computation time required to find the equilibrium point is lower in the commitment case than in the non-commitment case. We conclude that the defender should exploit the leader position in the game by committing to a defense strategy. This method can be generalized to address other types of PUEs such as malicious or unknown-attacking-type attacks.

References

[1] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. of 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2008.

[2] K. Bian and J.-M. J. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. of 4th Annual International Conference on Wireless Internet*. ICST, 2008.

[3] R. Chen, J. M. Park, and J. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, Jan 2008.

[4] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. of IEEE International Conference on Communications (ICC)*, June 2009.

[5] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," in *EEE International Conference on Communications (ICC)*, May 2008, pp. 3406–3410.

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

[7] A. Abrardo, M. Barni, K. Kallas, and B. Tondi, "A game-theoretic framework for optimum decision fusion in the presence of byzantines," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1333–1345, June 2016.

[8] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, Feb 2011.

[9] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," *IEEE Network*, vol. 29, no. 4, pp. 68–74, 2015.

[10] S. Chen, K. Zeng, and P. Mohapatra, "Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space," *IEEE Transactions on Mobile Computing,*, vol. 12, no. 3, pp. 401–411, March 2013.

[11] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Ráez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. of IEEE International Performance Computing and Communications Conference (IPCCC)*, 2009, pp. 208–215.

[12] K. M. Borle, B. Chen, and W. K. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2225–2235, Oct 2015.

[13] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach," *IET Communications*, vol. 6, no. 8, pp. 964–973, May 2012.

[14] H. Li and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3566–3577, November 2010.

[15] N. N. Thanh, P. Ciblat, A. Pham, and V.-T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4981–4993, Sept 2015.

[16] T. Duc-Tuyen, N. Nguyen-Thanh, P. Maille, P. Ciblat, and V. T. Nguyen, "Mitigating selfish primary user emulation attacks in multi-channel cognitive radio networks: A surveillance game," in *Proc. of IEEE Globecom*, December 2016.

[17] J. C. Harsanyi and R. Selten, *A general theory of equilibrium selection in games*. The MIT Press, 1988, vol. 1.

[18] M. Dabaghchian and et al, "Online learning-based optimal primary user emulation attacks in cognitive radio networks," *Proc. of IEEE Communications and Network Security (CNS)*, 2016.

[19] N. Agmon, V. Sadov, G. A. Kaminka, and S. Kraus, "The impact of adversarial knowledge on adversarial planning in perimeter patrol," in *Proc. of 7th international joint conference on Autonomous agents and multiagent systems-Volume 1*, 2008, pp. 55–62.

[20] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, "Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport," in *Proc. of 7th international joint conference on Autonomous Agents and Multiagent systems*, 2008, pp. 125–132.

[21] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing games for security: An efficient exact algorithm for solving bayesian stackelberg games," in *Proc. of International joint conference on Autonomous Agents and Multiagent systems*, 2008, pp. 895–902.

[22] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press, 2011.

[23] H. Von Stackelberg, *Market structure and equilibrium*. Springer Science & Business Media, 2010.

[24] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *The 27th Conference on Computer Communications. IEEE Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[25] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009.

[26] "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the tv bands," *IEEE Std 802.22-2011*, pp. 1–680, July 2011.

[27] B. Von Stengel and S. Zamir, "Leadership with commitment to mixed strategies," *CDAM Research Report, LSE-CDAM-2004-01*, 2004.

[28] V. Conitzer and D. Korzhyk, "Commitment to correlated strategies." in *AAAI*, 2011.

[29] Y. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. New York, NY, USA: Cambridge University Press, 2008.

[30] IBM. CPLEX Optimizer. [Online]. Available: http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/