Surveillance Strategies against Primary User Emulation Attack in Cognitive Radio Networks

Nhan Nguyen-Thanh, Philippe Ciblat, Anh T. Pham and Van-Tam Nguyen

***Abstract*—We investigate the primary user emulation (PUE) attack which is a serious security problem in cognitive radio (CR) networks. There exist three types of PUE attackers: i) selfish one which aims at maximizing its selfish usage of channel resource, ii) malicious one which points for obstructing the operation of CR network, and iii) mixed between selfish and malicious PUE attacker. For combating a selfish PUE attacker, a channel surveillance process has to be implemented in order to determine active user's identification and so selfish PUE attacker. An extra-sensing process has to be implemented for observing new opportunities to access the channel and so for mitigating the malicious PUE attacker's effect. Relevant strategies for deploying the above processes are obtained through a game theory-based analysis and the exhibition of Nash equilibrium (NE). We show the NE strongly depend on the network demand, the availability of the spectrum resource, and the type of the attacker. We also show the proposed defensive strategies (surveillance and extra sensing) are efficient for combating the effects of PUE attackers.**

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

I. Introduction

COGNITIVE Radio (CR) has been proposed to be a promising solution for improving spectrum usage by enabling dynamic spectrum access. A prerequisite to this kind of secondary access is that there has no interference to primary or licensed system. This requirement makes spectrum holes exploration to be a key function in cognitive radio systems. Several approaches for determining spectrum holes such as spectrum sensing and spectrum access database service have been considered. Spectrum access database service-based methods enable to provide an accurate and reliable spectrum information service. However, the database-based approach is expensive and requires perfect knowledge of primary system including propagation models and locations of clients, and fast dissemination of spectrum updates [1]. On the other hand, spectrum sensing approaches provide a less accurate but cheaper and more flexible method for discovering spectrum holes for a wide range of network types. But, spectrum sensing suffers from two security threats [2]: primary user emulation (PUE) attack and spectrum sensing data falsification (SSDF) attack.

SSDF attack is the attacking case where malfunction CR users or malicious attackers may share incorrect sensing data causing a degradation on the accuracy of the collaborative spectrum sensing process, and hence on the operation of CR system. Several methods such as statistical reputation-based attacker elimination [3]–[7], and consensus-based mechanisms [8] have been proposed to counteract SSDF attack.

PUE attack is a more active attacking approach to the spectrum sensing process where attackers emulate and transmit a similar primary signal on the sensing period. The presence of an emulated primary signal may lead to a prohibition of secondary accessing to the sensed channel immediately. Several works have investigated PUE attack problem. In [9], the authors proposed localization-based transmitter verification scheme to defend against PUE attack. CR system will verify the location of primary transmitter through the received signal power to determine whether the primary signal is original or emulated. However, this method is inapplicable to mobile primary transmitter cases. Furthermore, the received power of PUE signal at CR users can be completely emulated by a revived transmission with an array antenna. In [10], frequency deviation feature of FM signal is utilized to distinguish between a primary wireless microphone signal and an emulated one to combat the PUE attack. However, recent achievements in hardware processing enable CR devices to generate a emulated primary signal perfectly, without too much effort. In [11], [12], another approach to defense against the PUE attack is to treat the PUE signal as the same as a jamming signal. Therefore, channel hopping is the proposed solution. However, there still have vulnerabilities if attackers conducts multiple channel attacks.

Notice that PUE attacks can be classified into two types: selfish and malicious PUE attacks. A selfish PUE attack aims at occupying attacked spectrum band for selfish use whereas a malicious one aims at obstructing operation of CR network. So selfish PUE is a security threat that affects the fairness of the secondary access of CR system, while malicious PUE is similar to the conventional Deny-of-Service (DoS) attack which is an irresistible problem in wireless systems.

Depending on the type of PUE attack, we can determine a good strategy to deal with. In the selfish PUE attack case, an attacker usually uses the attacked channel selfishly after succeeding in performing PUE attack at a sensing duration. Meanwhile, it is possible to determine the users' identifications in any communication links. Therefore, a channel surveillance process, which observes disallowed secondary-accessing channels on the data time after a sensing period, can help to detect the illegal occupation of the channel and identify the selfish PUE attacker. In the malicious PUE attack case, an attacker mostly targets to transmit PUE signal at sensing period to fool the spectrum sensing system of the CR network. Fortunately, it is possible to retrieve the opportunity of using the attacked

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Marie Curie Fellowship CORPA, from French industry ministry in Catrene CORTIF project, and from the NICT Foreign Researcher Invitation Program.

channel by re-sensing the attacked channel on the next data time. Therefore, an extra-sensing process which senses "busy"-declared channels at data duration can help to mitigate the bad effect of the malicious PUE attack.

However the concern is about when and how often the attacks and the channel surveillance or extra-sensing processes should be performed by the attacker and CR system defender, respectively. Since there are conflicting objectives and tradeoff between cost and benefit of both attacker and defender, game theory, which mathematically studies the interaction among independent, self-interested players [13] is well-adapted. Notice that game theory has already been used in many similar (but different) CR network problems [11], [14]–[16]. For example, [11] deals with PUE attack and game theory, but its authors focused on the optimization of the probabilities to sense or attack one channel among several ones through the derivations of the Nash equilibrium. In this paper, we do not deal with avoiding the attack but rather with catching the attacker and switching on the surveillance process as seen later.

Our problem is formulated as a non-zero-sum game with incomplete information [17] for the selfish, malicious and mixed (selfish and malicious) cases, and the corresponding actions, i.e., channel surveillance, channel extra-sensing and mixed processes. As the game is non-collaborative since each player would like to optimize its own objective without collaborating and so discussing with the other one, the "most" reasonable strategy for two players is to apply the strategy provided by the Nash equilibrium (NE) points [18]. Therefore, the main objective of the paper is to determine the NE of the formulated games.

The remainder of this paper is organized as follows. In section II, system model is provided. In section III, the game for one type of PUE attack (either selfish or malicious ones) is formulated. We especially exhibit closed-form expressions of the NE for both types of attacks. In section IV, the general surveillance game is investigated. In section V, some numerical results are shown. Conclusions are drawn in section VI.

II. System model

A. Network model

We consider a CR network which performs secondary access to a licensed band. In order to simplify the analysis and focus on the effects of the proposed surveillance approach on the PUE attack, we assume that the CR network includes two separated sets: network management entities, which are responsible to implement sensing and surveillance processes, and network utilization entities, which are users exploiting the services of the network.

As detailed in Fig. 1, time is divided into super-frames, each of which includes sensing frame and data frame. In sensing frame, dedicated sensing engines sense to detect primary signal, while all users must vacate the channel to ensure the accuracy of spectrum sensing process. The sensing engines can adopt various sensing techniques, which may also include cooperative sensing, as long as the sensing accuracy is as high as possible. Since the sensing system, through the network management set, is independent of network users set which may include adversaries or malicious users, the sensing results are assumed to be fair. So, before every data frame, the network management set provides its information about available channels by broadcasting the channel status to all users. In data frame, users may adopt multiple coordination or contention approaches to obtain channel access, if the channel is announced to be free according to the result of the sensing process. On the other hand, if the channel is announced to be occupied by primary user, all secondary users are prohibited to use the channel. Any secondary transmission on the disallowed channel is illegal and considered as a PUE attacker.

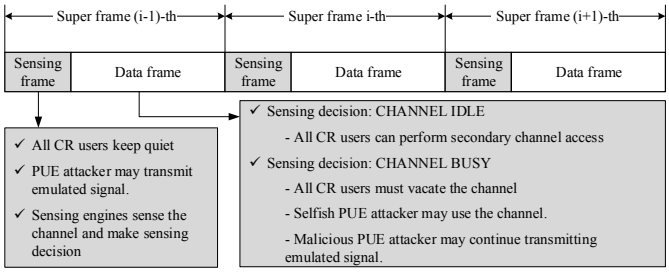

Figure 1. Timing frame for network operation

B. Attack and counter-action model

To a certain channel, a PUE attacker can either transmit or not transmit an emulated primary signal at a sensing frame. We assume that the sensing engines cannot distinguish the emulated and legitimate primary signals. Thus, the PUE attack will not be detected in the sensing frame. In addition, during PUE attack, the attacker cannot know the true status of primary signal on the attacked channel because it is busy to transmit an emulated primary signal in the same channel. This means that the PUE attacker conducts the attack in a blind information on the real primary signal's status.

Concerning the defense against selfish PUE attacker, we assume that a fixed format of data frame is used for exchanging data at all CR users including selfish users. The format contains the identifying information of a user such as medium access control (MAC) address. Therefore, CR users can be identified by observing transmitted signal in data frame. Channel surveillance process conducting on disallowed secondary access channels can determine selfish attackers if they are present. Once a selfish attacker has been detected, punishments such as a network isolation or a bandwidth limitation could be adopted to eliminate or penalize the attacker. This surveillance process is assumed to be implemented by network management entities. Concerning the defense against malicious PUE attacker, we propose to re-sense the channel before transmitting data to re-determine the true status of the channel by an extra-sensing process within the data frame.

C. The PUE attack and side information probabilities

At a sensing frame, there are three possible participators operating on the channel:

- The legitimate primary user which can have two following states: "***active***" and "***inactive***".
- The network management entity which always implements a sensing process for discovering the occupation

state of the channel, and returns two possible statuses: "***busy***", and "***idle***",
Notice that this response occurs when the spectrum sensing detects an channel occupation because of the presence of the primary user or of the attacker, or because of a false alarm.
- And the PUE attacker which may perform two actions: "***attack***" (*A*), and "***no attack***" (*NA*).

Let π_0 be the probability that the primary user is inactive. In the remainder of the paper, we also need the four additional probabilities associated with the above-mentioned states:

- Let p_A be the probability that the answer of the sensing engine is busy when the attacker's action is A. By noting $P_{F|A}$ and $P_{D|A}$ as the false alarm and detection probabilities of the spectrum sensing engine when the channel is attacked, one can easily check that $p_A = \Pr[busy|A] = \pi_0 P_{F|A} + (1-\pi_0) P_{D|A}$.
- Let p_N be the probability that the answer of the sensing engine is busy when the attacker's action is NA. Once again, by noting P_F and P_D as the false alarm and detection probabilities of the spectrum sensing engine when the channel is not attacked, we have $p_N = \Pr[busy|NA] = \pi_0 P_F + (1-\pi_0) P_D$.
- Let ρ_A be the probability that the channel is not used by the primary user while the sensing engine claims busy and the attacker attacks. Thus $\rho_A = \Pr[inactive|busy, A]$. Using Bayes's rule, we obtain $\rho_A = \pi_0 P_{F|A}/p_A$.
- Let ρ_N be the probability that the channel is not used by the primary user while the sensing engine claims busy and the attacker does not attack. Hence $\rho_N = \Pr[inactive|busy, NA]$. Similarly, we have $\rho_N = \pi_0 P_F/p_N$.

III. The Single Type of Attacker Case

In this section, we formulate the game where the PUE attacker has one of the two behaviors: the selfish case and the malicious case.

A. Elements of the game

The game for a single type of attacker is illustrated in Fig. 2.

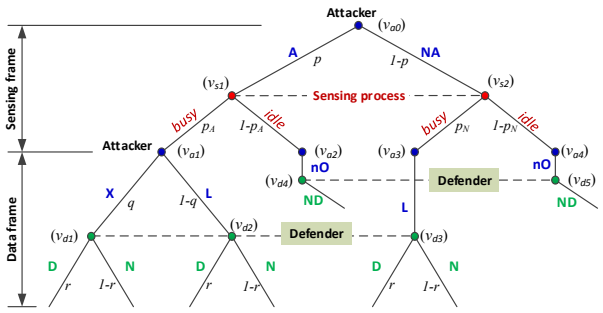

Figure 2. The common game for the single attacker type case

1) Player set: $\Gamma = \{Attacker, Defender\}$.

- ***Attacker*** who emulates a primary user in order to use the channel for its own interest.
- ***Defender*** who monitors the channel in order to defense against *Attacker*.

2) Pure strategy set: At a sensing frame, i.e., the beginning point v_{a0} in Fig. 2, an attacker may select action *A* or action *NA*. The sensing engine conducts the sensing process and returns either state "*busy*" or state "*idle*". Thus, there are four possible events $\{A, busy\}$, $\{A, idle\}$, $\{NA, busy\}$, and $\{NA, idle\}$ which define four corresponding information sets v_{a1}, v_{a2}, v_{a3}, and v_{a4}.

During the data frame, for each information set, the attacker can select the actions accordingly.

- At v_{a1}, i.e., $\{A, busy\}$ event, the attacker may select action ***Extra-action*** (*X*) to perform an extra-action on the attacked channel, or action ***Leave*** (*L*) to leave the attacked channel.
  Action *X* here depends on the type of *Attacker* type. If *Attacker* is a selfish one, *X* will be action ***Use*** (*U*) to use the channel selfishly. If *Attacker* is a malicious one, *X* will be action ***Attack*** (*A*) to continue attacking the channel for being sure that the network can not retrieve the channel by the extra sensing process.
  The reason to choose action *L* may be twofold: the attacker does not want to be caught by the defender or does not want to waste its resource if the channel is really occupied by an legitimate primary user.
- At v_{a2}, and v_{a4}, i.e., $\{A, idle\}$ and $\{NA, idle\}$ events, the attacker does the only action ***normal Operation*** (*nO*) which means the attacker behaves as the same as a normal user since the state "*idle*" is declared.
- At v_{a3}, the attacker does the action *L* because it does not perform attack at the sensing frame.

In summary, *Attacker* may have five possible combined actions: *A-X*, *A-L*, *A-nO*, *NA-L*, and *NA-nO*. Due to the uncontrollable impact of the sensing process, *Attacker* can have three pure combined strategies as follows.

i) Strategy $S_{a1} = [$*A-X,A-nO*$]$ where the attacker performs PUE attack at sensing frame. If sensing process declares "*busy*" state, then *Attacker* will perform an extra-action on the attacked channel at data frame. Otherwise, *Attacker* operates as the same as other normal users at data frame.

ii) Strategy $S_{a2} = [$*A-L,A-nO*$]$ where *Attacker* performs PUE attack at sensing frame. If sensing process declares "*busy*" state, then *Attacker* will leave the channel at data frame. Otherwise, *Attacker* operates as the same as other normal users at data frame.

iii) Strategy $S_{a3} = [$*NA-L,NA-nO*$]$ where *Attacker* does not perform PUE attack at sensing frame. At data frame, *Attacker* will do nothing on the channel if sensing process declares the state "busy". Otherwise, *Attacker* operates the same as a normal user.

The set of the strategies of *Attacker* is now denoted by $\mathbb{S}_a = \{S_{ai}\}$.

For *Defender*, there are two information sets $V_{busy} = \{v_{d1}, v_{d2}, v_{d3}\}$ and $V_{idle} = \{v_{d4}, v_{d5}\}$ corresponding to the

state "*busy*" and the state "*idle*" of the declared sensing result. Then, *Defender* may have the following actions:

- ***Defense*** (*D*) where *Defender* implements a defense process during the data frame.
  - If the game is formulated for the selfish attacker type, *D* will be a ***Surveillance*** (*S*) process, which can help to identify the selfish attacker.
  - If the game is formulated for the malicious attacker type, *D* will be an ***Extra sensing*** (*ES*) process, which can help to retrieve the true channel state by continually sensing the channel at the beginning of data frame.
- ***No action*** (*N*) where *Defender* does not implement any defensive action in the data frame
- ***No Defense*** (*ND*) where *Defender* does not consider defending the channel due to the return of state "*idle*" of the sensing process.

It can be seen that *ND* is the only option for defender when the state "*idle*" is declared, while the defender can randomly select *D* or *N* when the state "*busy*" is declared. Therefore, the defender may select randomly one of the two pure combined strategies:

i) Strategy $S_{d1} = [D,ND]$ where the defender implements a defensive action during the data frame if the state "*busy*" is declared and does not defend the channel otherwise.
ii) Strategy $S_{d2} = [N,ND]$ where the defender does not implement a defensive action during the data frame if "*busy*" is declared and does not defend the channel otherwise.

The set of the strategies of *Defender* is now denoted by $\mathbb{S}_D = \{S_{di}\}$.

3) Mixed and behavioral strategies: So far, the introduced game is a pure strategy game. Obviously, in practice, the players will choose randomly their actions. Then the game becomes a mixed-strategy game. Thus we define the mixed strategies of the attacker and defender by

$$\begin{cases} \sigma_A = \{\sigma_{a1}, \sigma_{a2}, \sigma_{a3}\} \\ \sigma_D = \{\sigma_{d1}, \sigma_{d2}\}, \end{cases} \tag{1}$$

where σ_{ai} is the probability of selecting the pure strategy S_{ai} of the attacker, σ_{di} is the probability of selecting the pure strategy S_{di} of the defender, i.e., $\sigma_{a1} + \sigma_{a2} + \sigma_{a3} = 1$ and $\sigma_{d1} + \sigma_{d2} = 1$.

The behavioral strategies, which are the mapping to give probabilities to the actions available at an information set [13], are defined for the attacker by

$$\begin{cases} \beta_A^{(v_{a0})} = \{p, 1-p\}, \\ \beta_A^{(v_{a1})} = \{q, 1-q\}, \\ \beta_A^{(v_{a2})} = \beta_A^{(v_{a3})} = \beta_A^{(v_{a4})} = \{1\}. \end{cases} \tag{2}$$

That is, in the information set v_{a0}, the attacker selects actions *A* with probability p and *NA* with probability $(1-p)$, and in the information set v_{a1}, the attacker performs action *X* with probability q and action *L* with probability $(1-q)$, etc. Similarly, the behavioral strategies for the defender are defined by

$$\begin{cases} \beta_D^{(V_{busy})} = \{r, 1-r\}, \\ \beta_D^{(V_{idle})} = \{1\}, \end{cases} \tag{3}$$

where r and $(1-r)$ are the probabilities of selecting action *D* and *N* in information set V_{busy}.

The game formulated in Fig. 2 is a game with perfect recall. Therefore, according to [19], the mixed and behavioral strategies are outcome-equivalent. This means that we can retrieve the behavioral strategies from the mixed strategies. Indeed, we have

$$\begin{cases} p = \sigma_{a1} + \sigma_{a2}, \\ q = \sigma_{a1}/(\sigma_{a1} + \sigma_{a2}), \\ r = \sigma_{d1}. \end{cases} \tag{4}$$

4) Payoffs and the induced normal form: Denote $P_a^{S_{ai};S_{dj}}$ and $P_d^{S_{ai};S_{dj}}$ are the payoffs for *Attacker* and *Defender* when *Attacker* plays S_{ai} and *Defender* plays S_{dj}. According to Table I which provides the normal form of the game in Fig. 2 (where *A-X* is replaced with *A-U* or *A-A* and *D* is replaced with *S* or *ES* with respect to selfish attacker type or malicious attacker type), we obtain the following payoff values:

$$\begin{cases} P_\pi^{S_{a1};S_{d1}} = p_A P_\pi^{\text{A-X;D}} + (1-p_A) P_\pi^{\text{A-nO;ND}} \\ P_\pi^{S_{a1};S_{d2}} = p_A P_\pi^{\text{A-X;N}} + (1-p_A) P_\pi^{\text{A-nO;ND}} \\ P_\pi^{S_{a2};S_{d1}} = p_A P_\pi^{\text{A-L;D}} + (1-p_A) P_\pi^{\text{A-nO;ND}} \\ P_\pi^{S_{a2};S_{d2}} = p_A P_\pi^{\text{A-L;N}} + (1-p_A) P_\pi^{\text{A-nO;ND}} \\ P_\pi^{S_{a3};S_{d1}} = p_N P_\pi^{\text{NA-L;D}} + (1-p_N) P_\pi^{\text{NA-nO;ND}} \\ P_\pi^{S_{a3};S_{d2}} = p_N P_\pi^{\text{NA-L;N}} + (1-p_N) P_\pi^{\text{NA-nO;ND}} \end{cases}, \tag{5}$$

where π is either a or d.

Table I
PAYOFF MATRIX OF THE INDUCED GAME

•	$S_{d1} = [D,ND]$	$S_{d2} = [N,ND]$
$S_{a1} = [A\text{-}X,A\text{-}nO]$	$[P_a^{S_{a1};S_{d1}}, P_d^{S_{a1};S_{d1}}]$	$[P_a^{S_{a1};S_{d2}}, P_d^{S_{a1};S_{d2}}]$
$S_{a2} = [A\text{-}L,A\text{-}nO]$	$[P_a^{S_{a2};S_{d1}}, P_d^{S_{a2};S_{d1}}]$	$[P_a^{S_{a2};S_{d2}}, P_d^{S_{a2};S_{d2}}]$
$S_{a3} = [NA\text{-}L,NA\text{-}nO]$	$[P_a^{S_{a3};S_{d1}}, P_d^{S_{a3};S_{d1}}]$	$[P_a^{S_{a3};S_{d2}}, P_d^{S_{a3};S_{d2}}]$

Let us define some intermediate costs/gains related to players' actions. Let us start with those associated with *Attacker*:

- C_A is the cost for implementing PUE attack. This cost may include many factors, in particular the transmitted energy and the processing cost.
- C_U is the cost for using the channel at the data frame. This is the cost that a selfish attacker pays for transmitting data.
- G_U is the benefit of using the channel for any CR users at one data frame. This is mainly the benefit on bandwidth utilization.
- ϕ_C is the penalty for being captured by *Defender* if *Attacker* is selfish. This penalty could be either a decrease in future allocated bandwidth resource or even an isolation from the network to the detected selfish attacker.
- G_M is the benefit of PUE attack if *Attacker* is malicious. This benefit is essentially equivalent to the degradation of the network due to malicious PUE attack.

Let us move on those associated with *Defender*:

- C_S is the cost for implementing the surveillance process at the data frame. This cost is paid for receiving and decoding the signal on the channel of interest to identify its owner.
- G_S is the benefit for capturing selfish attacker during the surveillance process of data frame. This benefit is the gain of having more bandwidth and more fairness for other users by punishing the selfish attacker.
- C_E is the cost for implementing extra spectrum sensing process in malicious attacker's case. This cost is used for receiving and detecting if a channel is occupied or not.
- G_E is the benefit of obtaining available channel by the extra spectrum sensing process in malicious attacker's case.. This benefit is the gain of having more bandwidth when the channel is detected to be free.

The payoffs for each pair of pure actions of *Attacker* and *Defender* are then defined in Table II in the next section. Notice that some action pairs in Table II are not defined yet since only related to the general case.

5) Expected payoff: The expected payoffs of the attacker and defender are determined by

$$\begin{cases} U_A(\sigma_A,\sigma_D) = \sum_{i=1}^{3}\sum_{j=1}^{2}\sigma_{ai}\sigma_{dj}P_a^{S_{ai};S_{dj}} = \sum_{i=1}^{3}\sigma_{ai}U_a^{S_{ai}}, \\ U_D(\sigma_A,\sigma_D) = \sum_{i=1}^{3}\sum_{j=1}^{2}\sigma_{ai}\sigma_{dj}P_d^{S_{ai};S_{dj}} = \sum_{j=1}^{2}\sigma_{dj}U_d^{S_{dj}}, \end{cases} \tag{6}$$

where

$$\begin{cases} U_a^{S_{ai}} = \sum_{j=1}^{2}\sigma_{dj}P_a^{S_{ai};S_{dj}}, \\ U_d^{S_{dj}} = \sum_{i=1}^{3}\sigma_{ai}P_d^{S_{ai};S_{dj}}. \end{cases} \tag{7}$$

B. Nash equilibrium for the selfish case

The Nash equilibrium (NE) is defined as the point where each player in a game has selected the best response (or one of the best responses) to the other players' strategies. The best response is the strategy (or strategies) playing on which a player gains the highest payoff given other players' strategies [18]. In the channel surveillance game for the selfish case, the NE is, therefore, defined by $\{\sigma_A^*,\sigma_D^*\}$, where

$$\begin{cases} U_A(\sigma_A^*,\sigma_D^*) \geq U_A(\sigma_A,\sigma_D^*), \forall\sigma_A, \\ U_D(\sigma_A^*,\sigma_D^*) \geq U_D(\sigma_A^*,\sigma_D), \forall\sigma_D. \end{cases} \tag{8}$$

In general, the NE of the game can be determined by searching all strategy profiles of both the defender and attacker that satisfy (8). Since the formulated game as shown in Table I is a bi-matrix (2-player) game with low number of pure strategies, we can obtain the closed-form of the mixed strategy NE by determining the intersection of the two best response (BR) function of each player. Then the NE behavioral strategies are computed based on (4).

The expected payoff of *Attacker* in the selfish case for playing each pure strategy S_{ai} over all *Defender*'s strategies are calculated according to (7), Table I, and Table II as follows.

$$\begin{cases} U_a^{S_{a1}} = p_A\rho_A(G_U - \sigma_{d1}\phi_C) - C_A - p_AC_U, \\ U_a^{S_{a2}} = -C_A, \\ U_a^{S_{a3}} = 0. \end{cases} \tag{9}$$

Similarly, the expected payoffs of *Defender* for playing each pure strategy are given by:

$$\begin{cases} U_d^{S_{d1}} = [p_A\rho_AG_S - (p_A-p_N)C_S]\sigma_{a1} \\ \qquad\qquad - (p_A-p_N)C_S\sigma_{a2} - p_NC_S, \\ U_d^{S_{d2}} = 0. \end{cases} \tag{10}$$

Based on (9) and (10), we obtain the detailed NE for the mixed strategies of the game given in Table I for the selfish case in ***Result*** 1.

Result 1. *The NE for the mixed strategies of the game given in Table I for the selfish case is computed as follows.*

1) *If* $C_A \geq B_U$ *then* $\sigma_A^* = \{0,0,1\}, \sigma_D^* = \{0,1\}$.
2) *If* $C_A < B_U$ *then*
   a) *If* $G_S \leq G_0$ *then* $\sigma_A^* = \{1,0,0\}, \sigma_D^* = \{0,1\}$,
   b) *If* $G_S > G_0$ *then*
      i) *if* $C_A > B_U^C \Rightarrow \begin{cases} \sigma_A^* = \{\sigma_{a1}^{(0)}, 0, \bar{\sigma}_{a1}^{(0)}\}, \\ \sigma_D^* = \{\sigma_{d1}^{(0)}, \bar{\sigma}_{d1}^{(0)}\}, \end{cases}$
      ii) *if* $C_A \leq B_U^C \Rightarrow \sigma_A^* = \{1,0,0\}, \sigma_D^* = \{1,0\}$,

where $G_0 = C_S/\rho_A$, $\begin{cases} B_U = p_A(\rho_AG_U - C_U), \\ B_U^C = B_U - p_A\rho_A\phi_C, \end{cases}$

$\begin{cases} \sigma_{a1}^{(0)} = \frac{p_NC_S}{p_A\rho_AG_S-(p_A-p_N)C_S}, \\ \bar{\sigma}_{a1}^{(0)} = 1-\sigma_{a1}^{(0)}, \end{cases}$ *and* $\begin{cases} \sigma_{d1}^{(0)} = \frac{B_U-C_A}{p_A\rho_A\phi_C}, \\ \bar{\sigma}_{d1}^{(0)} = 1-\sigma_{d1}^{(0)}. \end{cases}$

Proof. See Appendix A □

Substituting ***Result*** 1 into (4), we can determine the NE of the behavioral strategies, i.e., the probabilities p, q, and r. Hereafter, we interpret ***Result*** 1. When the PUE attacking cost C_A is too high, the NE says the attacker to stay inactive ($\sigma_{a3}^* = 1$). Then *Defender* does not have to monitor the channel ($\sigma_{d2}^* = 1$). Similarly, when the gain for capturing illegal attacker G_S is too low, *Defender* will not implement the surveillance process ($\sigma_{d1}^* = 0$). The derivations of the NE confirm the intuition but provide the thresholds for C_A and G_S. Moreover, in-between, the solution is not straightforward for the NE (see item 2(b)i in ***Result*** 1) and our result shows the values to choose.

When the attacker is captured, its punishment consists of banning it for the access to the radio resources. As a consequence, the saved radio resources will be beneficial for the rest of the network which implies that G_S depends on the being captured penalty ϕ_C and on the network demand k_b. For sake of simplicity, we assume $G_S = k_b\phi_C$. In addition, we assume $\phi_C = k_CG_U$ with k_C a non-negative penalty factor. Notice that the NE only depends on k_b and k_C when the using, attack, and surveillance costs and the probabilities of detection, false-alarm and presence of primary signal as well as the network are fixed. We also consider $C_A < B_U$ which corresponds to the non-trivial case and also to most networks. We then have the following remarks.

Remark 1. *Let* $C_A < B_U$. *If* k_C *is fixed, NE depends on* k_b, *and* ***Result*** *1 leads to*

1) *If* $k_b \leq K_0$ *then* $\sigma_A^* = \{0,0,1\}, \sigma_D^* = \{0,1\}$,
2) *If* $k_b > K_0$ *then*
   a) *if* $k_C > K_C^1$ *then* $\begin{cases} \sigma_A^* = \{\sigma_{a1}^{(0)}, 0, \bar{\sigma}_{a1}^{(0)}\}, \\ \sigma_D^* = \{\sigma_{d1}^{(0)}, \bar{\sigma}_{d1}^{(0)}\}, \end{cases}$

b) *if* $k_C \leq K_C^1$ *then* $\sigma_A^* = \{1,0,0\}, \sigma_D^* = \{1,0\}$,

where $K_0 = \frac{C_S}{k_C \rho_A G_U}$, $K_C^1 = \frac{B_U - C_A}{p_A \rho_A G_U}$.

Remark 2. *Let* $C_A < B_U$. *If* k_b *is fixed, NE depends on* k_C, *and* ***Result*** *1 leads to*

1) *If* $k_C \leq K_C^0$ *then* $\sigma_A^* = \{0,0,1\}, \sigma_D^* = \{0,1\}$,
2) *If* $k_C > K_C^0$ *then*
   a) *If* $k_b \leq K_1$ *then* $\begin{cases} \sigma_A^* = \{\sigma_{a1}^{(0)}, 0, \bar{\sigma}_{a1}^{(0)}\}, \\ \sigma_D^* = \{\sigma_{d1}^{(0)}, \bar{\sigma}_{d1}^{(0)}\}, \end{cases}$
   b) *If* $k_b > K_1$ *then*
      i) *if* $k_C > K_C^1 \Rightarrow \begin{cases} \sigma_A^* = \{\sigma_{a1}^{(0)}, 0, \bar{\sigma}_{a1}^{(0)}\}, \\ \sigma_D^* = \{\sigma_{d1}^{(0)}, \bar{\sigma}_{d1}^{(0)}\}, \end{cases}$
      ii) *if* $k_C \leq K_C^1 \Rightarrow \sigma_A^* = \{1,0,0\}, \sigma_D^* = \{1,0\}$,

with $K_1 = \frac{p_A C_S}{B_U - C_A}$, $K_C^0 = \frac{C_S}{k_b \rho_A G_U}$.

C. Nash equilibrium for the malicious case

In this subsection, we consider the game given in Table I for the malicious case. The expected payoff of *Attacker* and *Defender* for playing each pure strategy are calculated based on (7) and Table II by

$$\begin{cases} U_a^{S_{a1}} = p_A \rho_A G_M - C_A \left(1 + p_A\right), \\ U_a^{S_{a2}} = -C_A, \\ U_a^{S_{a3}} = 0, \end{cases} \tag{11}$$

and

$$\begin{cases} U_d^{S_{d1}} = -\sigma_{a1} p_A C_E + \sigma_{a2} p_A \left(\rho_A G_E - C_E\right) \\ \qquad\qquad + \sigma_{a3} p_N \left(\rho_N G_E - C_E\right), \\ U_d^{S_{d2}} = 0. \end{cases} \tag{12}$$

Result 2. *The NE for the mixed strategies of the game given in Table I for the malicious case is computed as follows.*

- *If* $G_M > G_M^{(0)}$ *then* $\sigma_A^* = \{1,0,0\}$ *and* $\sigma_D^* = \{0,1\}$.
- *If* $G_M = G_M^{(0)}$ *then* $\sigma_A^* = \{\alpha, 0, \bar{\alpha}\}$ *and* $\sigma_D^* = \{0,1\}$, *where* $\alpha \in [0,1]$ *and* $\bar{\alpha} = 1 - \alpha$.
- *If* $G_M < G_M^{(0)}$ *then*
  - *If* $G_E \leq G_E^{(0)}$ *then* $\sigma_A^* = \{0,0,1\}$ *and* $\sigma_D^* = \{0,1\}$,
  - *Otherwise,* $\sigma_A^* = \{0,0,1\}$ *and* $\sigma_D^* = \{1,0\}$.

where $G_M^{(0)} = \frac{C_A(1+p_A)}{p_A \rho_A}$ *and* $G_E^{(0)} = \frac{C_E}{\rho_N}$.

Proof. See Appendix B □

Result 2 shows that both the malicious attacker and the defender behave according to its own profit, i.e., G_M, G_E. G_M is equivalent to how much damage that a malicious attack could cause to the CR network. Therefore, it is proportional to how gain/benefit to use the channel and how necessary that the CR network needs to use that channel. Without lost of generality, we consider $G_M = k_b G_U$, where G_U and k_b are similar to those defined in the previous section. G_E is equivalent to how much benefit that the network can obtain if the extra-sensing process returns an availability of the channel. The extra-sensing process should be conducted when the network needs more channel resource for transmitting data. Hence, without lost of generality, we assume $G_E = G_U$.

Besides, since the extra-sensing cost C_E is normally smaller than the attacking cost C_A we also assume that $C_E < C_A$.

In next result, we analyze precisely the constraints on the introduced parameters and the corresponding NE points given in ***Result*** 2.

Remark 3. *Let* $\begin{cases} \pi_0^{(0)} = \frac{C_E P_D}{C_E P_D + (G_E - C_E) P_F}, \\ \pi_0^{(1)} = \frac{C_A(1+P_{D|A})}{G_U P_{F|A} k_b + C_A (P_{D|A} - P_{F|A})}, \end{cases}$ $G_U^{(0)} = C_A \left(1 + \frac{1}{P_{F|A}}\right)$, *and* $k_b^{(0)} = \frac{G_U^{(0)}}{G_U}$. *The NE points given in* ***Result*** *2 are equivalent to the following cases:*

- *If* $G_U \leq C_E$, *then* $\sigma_A^* = \{0,0,1\}$ *and* $\sigma_D^* = \{0,1\}$.
- *If* $C_E < G_U < G_U^{(0)}$, *then*
  - *If* $\pi_0 \leq \pi_0^{(0)}$, *then* $\sigma_A^* = \{0,0,1\}$ *and* $\sigma_D^* = \{0,1\}$,
  - *If* $\pi_0 > \pi_0^{(0)}$, *then* $\sigma_A^* = \{0,0,1\}$ *and* $\sigma_D^* = \{1,0\}$.
- *If* $G_U = G_U^{(0)}$, *then* $\sigma_A^* = \{\alpha, 0, \bar{\alpha}\}$ *and* $\sigma_D^* = \{0,1\}$, *where* $\alpha \in [0,1]$ *and* $\bar{\alpha} = 1 - \alpha$.
- *If* $G_U > G_U^{(0)}$, *then*
  - *If* $k_b < k_b^{(0)}$, *then*
    - *if* $\pi_0 \leq \pi_0^{(0)}$, *then* $\begin{cases} \sigma_A^* = \{0,0,1\}, \\ \sigma_D^* = \{0,1\}, \end{cases}$
    - *if* $\pi_0 > \pi_0^{(0)}$, *then* $\begin{cases} \sigma_A^* = \{0,0,1\}, \\ \sigma_D^* = \{1,0\}, \end{cases}$
  - *If* $k_b = k_b^{(0)}$, *then* $\begin{cases} \sigma_A^* = \{\alpha, 0, \bar{\alpha}\}, \\ \sigma_D^* = \{0,1\}, \end{cases}$
  - *If* $k_b > k_b^{(0)}$, *then*
    - *if* $\pi_0 \leq \pi_0^{(0)}$, *then* $\begin{cases} \sigma_A^* = \{0,0,1\}, \\ \sigma_D^* = \{0,1\}, \end{cases}$
    - *if* $\pi_0^{(0)} < \pi_0 < \pi_0^{(1)}$, *then* $\begin{cases} \sigma_A^* = \{0,0,1\}, \\ \sigma_D^* = \{1,0\}, \end{cases}$
    - *if* $\pi_0 = \pi_0^{(1)}$, *then* $\begin{cases} \sigma_A^* = \{\alpha, 0, \bar{\alpha}\}, \\ \sigma_D^* = \{0,1\}, \end{cases}$
    - *if* $\pi_0 > \pi_0^{(1)}$, *then* $\begin{cases} \sigma_A^* = \{1,0,0\}, \\ \sigma_D^* = \{0,1\}. \end{cases}$

IV. The general type of attacker case

In a general case, a CR network may suffer from various attackers of either selfish type or malicious one. Therefore, an attacker can know his own type but the defender cannot know exactly what type of the attacker is playing. And both of the players do not know the action of the opponent as well as the a prior probability of attacker's type. The game is therefore a simultaneous-move game with incomplete information or in other word a static Bayesian game.

In order to handle such a Bayesian game where player has many types, Harsanyi has proposed to add a move of a third player "***Nature***" at the beginning of the game [17] to decide the types of player based on a common prior assumption (CPA). In our game, the "***Nature***" assigns common prior probability of δ for selfish attacker type and $(1-\delta)$ for malicious attacker type. The value of δ may be estimated through a learning process [20] of the defender or the network management entity and becomes common owning to the inference of attackers based on management's messages exchanged on the network. The game for the general PUE attack case is illustrated in Fig. 3.

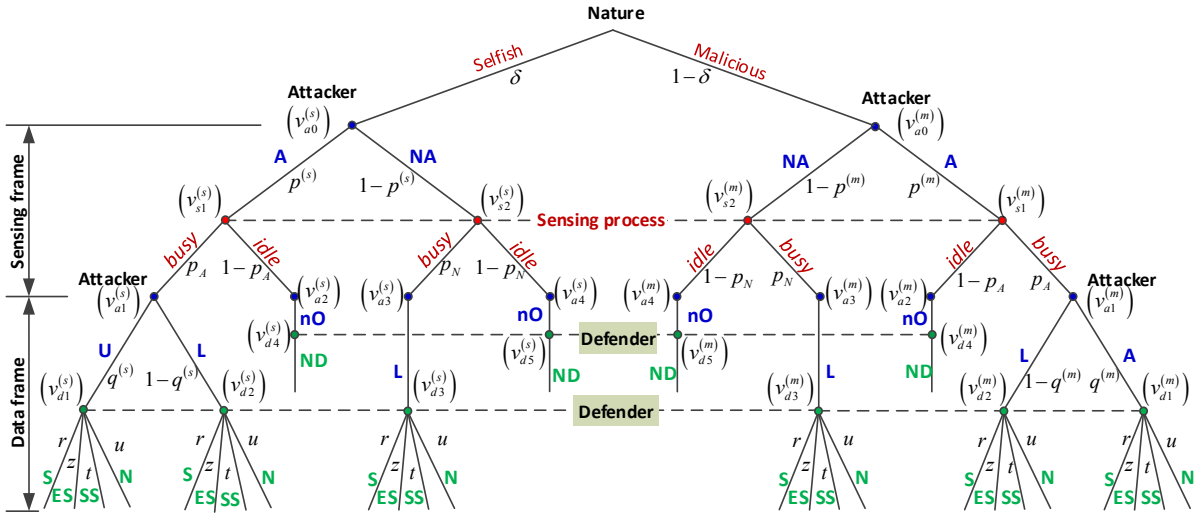

Figure 3. The channel surveillance game for the general case

A. Elements of the game

1) Player set: $\Gamma = \{Attacker, Defender\}$, with *Attacker* either a selfish or a malicious one.

2) Pure strategy set: At the data frame, the attacker has eight information sets (four for each type): $[\{v_{a1}^{(s)}\},\{v_{a2}^{(s)}\},\{v_{a3}^{(s)}\},\{v_{a4}^{(s)}\}]$, and $[\{v_{a1}^{(m)}\},\{v_{a2}^{(m)}\},\{v_{a3}^{(m)}\},\{v_{a4}^{(m)}\}]$. Due to the incomplete information, pure strategies of *Attacker* in the general case are formulated by combining the pure strategy sets of both attacker's types:

$$\mathbb{L}_a = \{L_{ai}\} = \{[S_{aj}^{(s)}, S_{ak}^{(m)}]\}. \tag{13}$$

where $i = 1, ..., 9$, and $[S_{aj}^{(s)}, S_{ak}^{(m)}], (j,k = 1,2,3)$ is a pure combined strategy of the general type attacker and means that *Attacker* will select $S_{aj}^{(s)}$ when it has selfish type and $S_{ak}^{(m)}$ when it has malicious type.

On the other hand, *Defender* has only two information sets at the data frame: I_{busy} and I_{idle} where $I_{busy} = \{v_{d1}^{(s)}, v_{d2}^{(s)}, v_{d3}^{(s)}, v_{d1}^{(m)}, v_{d2}^{(m)}, v_{d3}^{(m)}\}$ and $I_{idle} = \{v_{d4}^{(s)}, v_{d5}^{(s)}, v_{d4}^{(m)}, v_{d5}^{(m)}\}$.

- At I_{idle}, *Defender* performs action ***No Defense*** (*ND*) which has a similar meaning to the action *ND* described in the previous section.
- At I_{busy}, *Defender* chooses one of the four below actions:
  - ***Surveillance*** (*S*) which is equivalent to action *S* in the selfish attacking case
  - ***Extra Sensing*** (*ES*) which is equivalent to action *ES* in the malicious attacking case
  - ***Surveillance and Sensing*** (*SS*) which means that the defender performs both the surveillance and sensing processes simultaneously
  - ***No action*** (*N*) which is similar to the action *N* in the previous section

Therefore, there are four combined pure strategies for the defender in the game with general attacker case as follows.

$$\mathbb{L}_d = \{L_{di}\} = \left\{ \begin{array}{l} L_{d1} = [S,ND]; L_{d2} = [ES,ND]; \\ L_{d3} = [SS,ND]; L_{d4} = [N,ND] \end{array} \right\}. \tag{14}$$

3) Mixed and behavioral strategies: The mixed strategies of the attacker and defender are defined by

$$\left\{ \begin{array}{l} \lambda_A = \{\lambda_{ai}, i = 1, ..., 9, \} \\ \lambda_D = \{\lambda_{dj}, j = 1, ..., 4, \} \end{array} \right. \tag{15}$$

where λ_{ai} and λ_{di} are the probabilities of selecting the pure strategies L_{ai} and L_{di} for the attacker and the defender. This means that $\sum_{i=1}^{9} \lambda_{ai} = 1$ and $\sum_{i=1}^{4} \lambda_{di} = 1$.

The behavioral strategies of the attacker β_A in the cases of selfish type and malicious type are as the same as (2). The behavioral strategies of the defender are

$$\left\{ \begin{array}{l} \beta_D{}^{(I_{busy})} = \{r, z, t, u\} \\ \beta_D{}^{(I_{idle})} = \{1\} \end{array} \right. , \tag{16}$$

where r, s, t, u are the probabilities of performing *S*, *ES*, *SS*, *N*, respectively, and $r + z + t + u = 1$.

4) Payoffs and the induced normal form: The payoffs for each pair of actions are presented in Table II. Compare to the payoffs in the two previous game, there is a new action case *SS* that needs to be analyzed here. First we want to remind that the *SS* action is only performed after the "*busy*" state has been declared, and the action *SS* includes a surveillance and a sensing process conducted simultaneously. Typically, a sensing process is shorter and cheaper than a surveillance process. According to the true state of as well as the attacking operation of the attacker on the channel at the data frame, there are two values for the cost of this action as follows.

- If the channel is really empty, the action *SS* will be interrupted as soon as the sensing process detect the true state of the channel. Therefore, it can be considered that action *SS* is half-implemented, and the cost is $C_{SS}^{(h)} \approx C_{ES}$.
- If the channel is really occupied due to the presence of primary signal or the use of a selfish attacker, or the

transmission emulation signal of a malicious attacker, the action *SS* is fully performed. Thus, cost is $C_{SS}^{(f)} \approx C_S + C_{ES}$.

Table II
PAYOFFS IN GENERAL PUE ATTACK CASE

Type	Action pair $q_a; q_d$	Attacker payoff $(P_a^{q_a;q_d})$	Defender payoff $(P_d^{q_a;q_d})$
Selfish	*A-U;S*	$-C_A - C_U + \rho_A G_U - \rho_A \phi_C$	$-C_S + \rho_A G_S$
	A-U;ES	$-C_A - C_U + \rho_A G_U$	$-C_E$
	A-U;SS	$-C_A - C_U + \rho_A G_U$	$-C_{SS}^{(f)} + \rho_A G_S$
	A-U;N	$-C_A - C_U + \rho_A G_U$	0
	A-L;S	$-C_A$	$-C_S$
	A-L;ES	$-C_A$	$-C_E + \rho_A G_E$
	A-L;SS	$-C_A$	$-C_{SS}^{(h)} + \rho_A G_E$
	A-L;N	$-C_A$	0
	A-nO;ND	$-C_A$	0
	NA-L;S	0	$-C_S$
	NA-L;ES	0	$-C_E + \rho_N G_E$
	NA-L;SS	0	$-C_{SS}^{(h)} + \rho_N G_E$
	NA-L;N	0	0
	NA-nO;ND	0	0
Malicious	*A-A;S*	$-2C_A + \rho_A G_M$	$-C_S$
	A-A;ES	$-2C_A + \rho_A G_M$	$-C_E$
	A-A;SS	$-2C_A + \rho_A G_M$	$-C_{SS}^{(f)}$
	A-A;N	$-2C_A + \rho_A G_M$	0
	A-L;S	$-C_A$	$-C_S$
	A-L;ES	$-C_A$	$-C_E + \rho_A G_E$
	A-L;SS	$-C_A$	$-C_{SS}^{(h)} + \rho_A G_E$
	A-L;N	$-C_A$	0
	A-nO;ND	$-C_A$	0
	NA-L;S	0	$-C_S$
	NA-L;ES	0	$-C_E + \rho_N G_E$
	NA-L;SS	0	$-C_{SS}^{(h)} + \rho_N G_E$
	NA-L;N	0	0
	NA-nO;ND	0	0

The game formulated for general attacker case as shown in Fig. 3 can now be re-presented in the induced normal form of a 9×4 bi-matrix game matrix [13] as shown in Table III in which the payoffs of the defender and the attacker are determined by

$$\Pi_\pi^{L_{ai};L_{dn}} = \delta P_\pi^{S_{aj}^{(s)};L_{dn}} + (1-\delta)\, P_\pi^{S_{ak}^{(m)};L_{dn}}. \quad (17)$$

where π can be either a or d, $i = 1, ..., 9$, $j, k = 1, ..., 3$, and $n = 1, ..., 4$. The payoffs for the attacker and the defender of each pair of the pure strategies $P_\pi^{q_a;q_d}$ is computed by:

$$P_\pi^{q_a;q_d} = \begin{cases} p_A P_\pi^{A_1;B} + (1-p_A) P_\pi^{A_2;B} & \text{if} \quad q_a \in \{A-\} \\ p_N P_\pi^{A_1;B} + (1-p_N) P_\pi^{A_2;B} & \text{if} \quad q_a \in \{NA-\}, \end{cases} \quad (18)$$

where $q_a = [A_1, A_2], q_d = [B]$ represent the pure strategies of the attacker and the defender, where $\{A-\}$ and $\{NA-\}$ correspond to sub-strategy sets of the attacker where the action *A* and *NA* are played at the sensing frame, and where $P_\pi^{A_1;B}$ and $P_\pi^{A_2;B}$ are determined in Table II. For example, $\Pi_a^{L_{a1},L_{d1}}$ in Table III is calculated by:

$$\begin{aligned} \Pi_a^{L_{a1};L_{d1}} =& P_a^{\left[S_{a1}^{(s)},S_{a1}^{(m)}\right];L_{d1}} \\ =& \delta P_a^{S_{a1}^{(s)};L_{d1}} + (1-\delta)\, P_a^{S_{a1}^{(m)};L_{d1}} \\ =& \delta \left[p_A P_a^{\text{A-U;S}} + (1-p_A)\, P_a^{\text{nO;ND}}\right] \\ & + (1-\delta) \left[p_A P_a^{\text{A-A;S}} + (1-p_A)\, P_a^{\text{nO;ND}}\right]. \end{aligned} \quad (19)$$

B. Nash equilibrium

In the previous subsection, the game for general attacker case has been formulated in the induced normal form of 9×4 bi-matrix game. Finding a closed form of the NE for such a large bi-matrix is not trivial and necessary. Instead, it has been proven that any bi-matrix games have at least one NE point, and the NE point can be simply and effectively computed by Lemke and Howson (L-H) algorithm [21]–[23] or some other algorithms such as lrsnash and EEE [24]. Due to small scale computational requirement, in this paper, we propose to adopt L-H algorithm to find the NE for the game in the general attacking case.

V. SIMULATION RESULTS

In this section, we use numerical simulations to confirm the analytic results and to analyze more deeply the influence of some design parameters. Unless otherwise stated, the parameters are fixed as follows: $C_A = 10$, $C_S = .4C_A$, $C_E = .2C_A$, $C_U = .3C_A$, $G_U = 5C_A$, $k_C = 5$, $\pi_0 = .5$, $P_F = .1$, and $P_D = .9$. We assume that the sensing system adopts energy detection method and PUE attacker can perfectly emulate the primary signal, i.e., $P_{F|A} = P_D$ and $p_A = \pi_0 P_D + (1-\pi_0) P_{D|A} \geq P_D$. For the sake of simplicity, the channel between sensing device and both primary transmitter and PUE attacker are assumed to be AWGN channels, and the average SNR of the primary signal received at sensing engine is -10dB.

In order to verify the correctness of the analysis for the selfish attack case, numerical simulations of the NE have also been carried out with the L-H algorithm. Without loss of generality, the above selected parameters correspond to the most significant case $C_A < B_U$.

Fig. 4 shows the NE obtained by the theoretical analysis and the L-H algorithm with respect to values of network demand k_b for a low penalty factor ($k_C = 0.4 < K_C^1$), and a high penalty factor, ($k_C = 3 > K_C^1$) cases. We can see the perfect agreement between the theoretical analysis given in ***Remark*** 1 and simulated results. For low k_C (see Fig. 4(a)), the NE strategy of the attacker is to attack regardless of the operation of the defender which has to implement the surveillance process when the network demand k_b is higher than K_0. The reason is that the penalty is too low to enforce the attacker to avoid attack. For high k_C (see Fig. 4(b)), when $k_b < K_0$, the NE point is similar. However, when $k_b > K_0$, the defender just needs to maintain a low constant surveillance rate while the attacker has to decrease the attacking rate along with the increase of network demand since increasing network demand will increase the motivation for the defender to perform surveillance process.

In Fig. 5, we plot the NE obtained by the theoretical analysis and the L-H algorithm with respect to the penalty factor k_C for a high network demand ($k_b = 0.8 > K_1$) and a low network demand ($k_b = 0.2 < K_1$). As mentioned in ***Remark*** 2, we observe that the attack and the surveillance rates will be very low as soon as the penalty factor is large enough.

Similar to the simulations in the selfish case, we also adopt L-H algorithm to verify the NE analysis for the malicious attacking case. The already-selected parameters correspond to the most interesting case $G_U > G_U^{(0)}$.

Fig. 6 demonstrates the agreement of the analytic results and the numerical results. It can be seen that the NE point depends

Table III
PAYOFF MATRIX OF THE BAYESIAN CHANNEL SURVEILLANCE GAME FOR THE GENERAL PUE ATTACKER CASE

			L_{d1}=[*S*,*ND*] (λ_{d1})	L_{d2}=[*ES*,*ND*] (λ_{d2})	L_{d3}=[*SS*,*ND*] (λ_{d3})	L_{d4}=[*N*,*ND*] (λ_{d4})
$L_{a1}=$	$S_{a1}^{(s)}, S_{a1}^{(m)}$	- (λ_{a1})	$\Pi_a^{L_{a1};L_{d1}}, \Pi_d^{L_{a1};L_{d1}}$	$\Pi_a^{L_{a1};L_{d2}}, \Pi_d^{L_{a1};L_{d2}}$	$\Pi_a^{L_{a1};L_{d3}}, \Pi_d^{L_{a1};L_{d3}}$	$\Pi_a^{L_{a1};L_{d4}}, \Pi_d^{L_{a1};L_{d4}}$
$L_{a2}=$	$S_{a1}^{(s)}, S_{a2}^{(m)}$	- (λ_{a2})	$\Pi_a^{L_{a2};L_{d1}}, \Pi_d^{L_{a2};L_{d1}}$	$\Pi_a^{L_{a2};L_{d2}}, \Pi_d^{L_{a2};L_{d2}}$	$\Pi_a^{L_{a2};L_{d3}}, \Pi_d^{L_{a2};L_{d3}}$	$\Pi_a^{L_{a2};L_{d4}}, \Pi_d^{L_{a2};L_{d4}}$
$L_{a3}=$	$S_{a1}^{(s)}, S_{a3}^{(m)}$	- (λ_{a3})	$\Pi_a^{L_{a3};L_{d1}}, \Pi_d^{L_{a3};L_{d1}}$	$\Pi_a^{L_{a3};L_{d2}}, \Pi_d^{L_{a3};L_{d2}}$	$\Pi_a^{L_{a3};L_{d3}}, \Pi_d^{L_{a3};L_{d3}}$	$\Pi_a^{L_{a3};L_{d4}}, \Pi_d^{L_{a3};L_{d4}}$
$L_{a4}=$	$S_{a2}^{(s)}, S_{a1}^{(m)}$	- (λ_{a4})	$\Pi_a^{L_{a4};L_{d1}}, \Pi_d^{L_{a4};L_{d1}}$	$\Pi_a^{L_{a4};L_{d2}}, \Pi_d^{L_{a4};L_{d2}}$	$\Pi_a^{L_{a4};L_{d3}}, \Pi_d^{L_{a4};L_{d3}}$	$\Pi_a^{L_{a4};L_{d4}}, \Pi_d^{L_{a4};L_{d4}}$
$L_{a5}=$	$S_{a2}^{(s)}, S_{a2}^{(m)}$	- (λ_{a5})	$\Pi_a^{L_{a5};L_{d1}}, \Pi_d^{L_{a5};L_{d1}}$	$\Pi_a^{L_{a5};L_{d2}}, \Pi_d^{L_{a5};L_{d2}}$	$\Pi_a^{L_{a5};L_{d3}}, \Pi_d^{L_{a5};L_{d3}}$	$\Pi_a^{L_{a5};L_{d4}}, \Pi_d^{L_{a5};L_{d4}}$
$L_{a6}=$	$S_{a2}^{(s)}, S_{a3}^{(m)}$	- (λ_{a6})	$\Pi_a^{L_{a6};L_{d1}}, \Pi_d^{L_{a6};L_{d1}}$	$\Pi_a^{L_{a6};L_{d2}}, \Pi_d^{L_{a6};L_{d2}}$	$\Pi_a^{L_{a6};L_{d3}}, \Pi_d^{L_{a6};L_{d3}}$	$\Pi_a^{L_{a6};L_{d4}}, \Pi_d^{L_{a6};L_{d4}}$
$L_{a7}=$	$S_{a3}^{(s)}, S_{a1}^{(m)}$	- (λ_{a7})	$\Pi_a^{L_{a7};L_{d1}}, \Pi_d^{L_{a7};L_{d1}}$	$\Pi_a^{L_{a7};L_{d2}}, \Pi_d^{L_{a7};L_{d2}}$	$\Pi_a^{L_{a7};L_{d3}}, \Pi_d^{L_{a7};L_{d3}}$	$\Pi_a^{L_{a7};L_{d4}}, \Pi_d^{L_{a7};L_{d4}}$
$L_{a8}=$	$S_{a3}^{(s)}, S_{a2}^{(m)}$	- (λ_{a8})	$\Pi_a^{L_{a8};L_{d1}}, \Pi_d^{L_{a8};L_{d1}}$	$\Pi_a^{L_{a8};L_{d2}}, \Pi_d^{L_{a8};L_{d2}}$	$\Pi_a^{L_{a8};L_{d3}}, \Pi_d^{L_{a8};L_{d3}}$	$\Pi_a^{L_{a8};L_{d4}}, \Pi_d^{L_{a8};L_{d4}}$
$L_{a9}=$	$S_{a3}^{(s)}, S_{a3}^{(m)}$	- (λ_{a9})	$\Pi_a^{L_{a9};L_{d1}}, \Pi_d^{L_{a9};L_{d1}}$	$\Pi_a^{L_{a9};L_{d2}}, \Pi_d^{L_{a9};L_{d2}}$	$\Pi_a^{L_{a9};L_{d3}}, \Pi_d^{L_{a9};L_{d3}}$	$\Pi_a^{L_{a9};L_{d4}}, \Pi_d^{L_{a9};L_{d4}}$

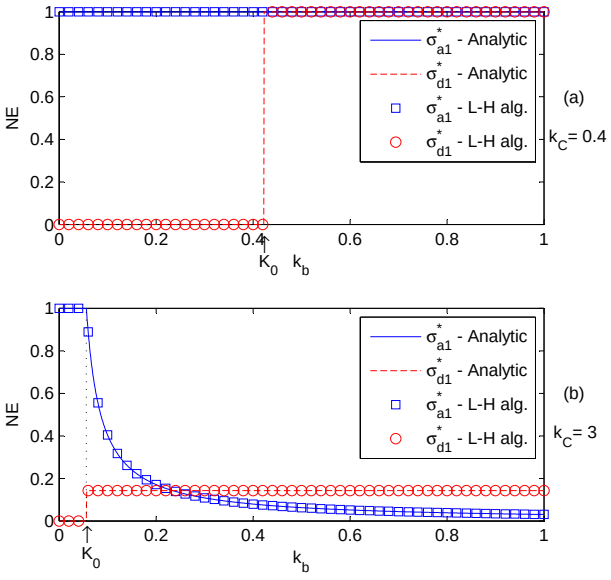

Figure 4. NE of the game in the selfish case vs. k_b when (a) $k_C = 0.4 < K_C^1$ or (b) $k_C = 3 > K_C^1$

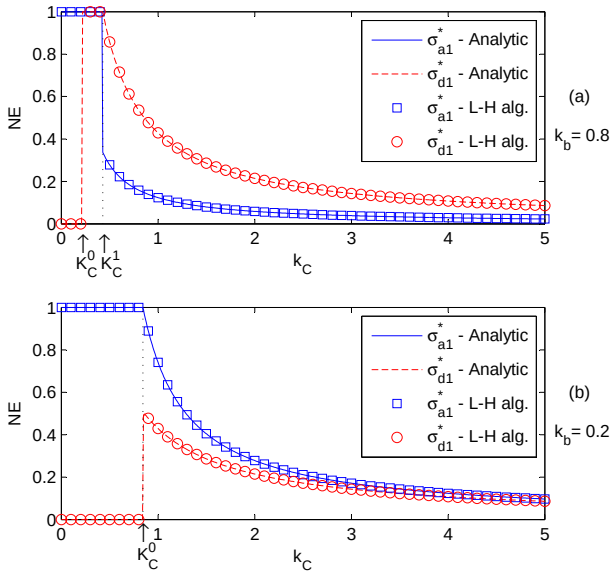

Figure 5. NE of the game in the selfish case vs. k_C when (a) $k_b = 0.8 > K_1$ or (b) $k_b = 0.2 < K_1$

on CR network's demand and the operation of primary users which are represented through k_b and π_0, respectively. When the operation of primary users on the channel is too high, i.e., $\pi_0 < \pi_0^{(0)}$, no benefit to perform the extra-sensing process as well as the PUE attack could be achieved. Thus, the best strategy is taking neither the extra-sensing process nor the attack. When the probability of channel's availability is higher, i.e., $\pi_0^{(0)} < \pi_0 < \pi_0^{(1)}$, the possible damage caused to the CR network by the attacker is still not large enough (compared to the possible cost) to motivate the attacker taking the PUE attack, whereas the benefit of increasing the probability of channel's usage is high enough to force the defender conducting the extra-sensing process. As a result, $\mu_{a1}^* = 0$ and $\mu_{d1}^* = 1$ in this region. Next, when the operation of primary users on the channel is very low, i.e., $\pi_0 > \pi_0^{(1)}$, the possible damage caused to the CR network by the attacker depends on k_b and π_0. If π_0 exceeds the threshold $\pi_0^{(1)}(k_b)$, or equivalently k_b exceeds a threshold $g_{k_b}(\pi_0) = \frac{C_A}{G_U}\left(\frac{P_{D|A}-P_{F|A}}{P_{F|A}} + \frac{1+P_{D|A}}{\pi_0 P_{F|A}}\right)$, the adverse impact of the malicious attack will be high enough to motivate an malicious PUE attack. Meanwhile, the defender will not select to perform the extra-sensing process since the benefit is not enough in this region. In summary, the results as shown in Fig. 6 illustrate the correctness of the results given in ***Result*** 2 and ***Remark*** 3.

For the game of the general attacking case as formulated in Section IV, we set $C_{SS}^{(h)} = C_E$, $C_{SS}^{(f)} = C_E + C_S$, and $\delta = 0.5$ for the simulation. Since it is a 9×4 bi matrix game, it is not easy to obtain the NE point manually. The L-H algorithm is adopted for finding NE point instead. Notice that the L-H algorithm in each tested set-up has always converged in a few iterations and its time of convergence was thus compatible with the coherence time of system parameters.

Firstly, we want to find the relation between parameters and the NE point. We set $k_C = 5$ which is large enough for this simulation. In addition, for attacker case, we only plot the non-zero NE strategies among the 9 attacking strategies.

Fig. 7 illustrates the relation between π_0 and the NE

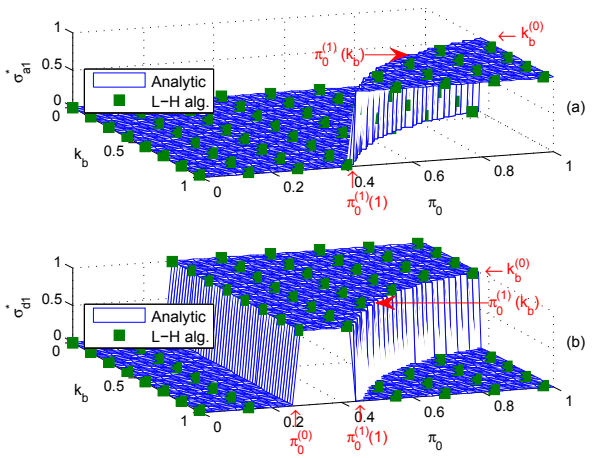

Figure 6. NE of the game in the malicious case vs. k_b and π_0: (a) Attacker's NE strategy σ^*_{a1}, and (b) Defender's NE strategy σ^*_{d1}

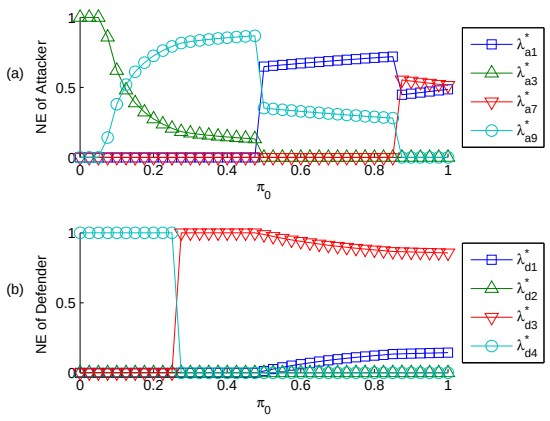

Figure 7. Attacker's and Defender's NE with respect to difference values of π_0, where $k_b = 0.5$, and $k_C = 5$

point. For attacker point of view (see Fig. 7(a)), it can be seen that there are only 4 non-zero mixed strategies including $\lambda^*_{a1}, \lambda^*_{a3}, \lambda^*_{a4}$, and λ^*_{a9} which correspond to $[S^{(s)}_{a1}, S^{(m)}_{a1}], [S^{(s)}_{a1}, S^{(m)}_{a3}], [S^{(s)}_{a3}, S^{(m)}_{a1}]$, and $[S^{(s)}_{a3}, S^{(m)}_{a3}]$. This means that the mixed strategies which contain either $S^{(s)}_{a2}$ or $S^{(m)}_{a2}$ are dominated. The NE point varies according to the value of π_0, and there are approximately three regions:

- the low π_0 region where the main attacking strategies should be *A-U* and *NA* for selfish attacker type and *NA* for malicious attacker type,
- the middle π_0 region where the main attacking strategies should be *A-U* and *NA* for selfish attacker type and *A-A* and *NA* for malicious attacker type,
- and the high π_0 region where the main attacking strategies should be *A-U* and *NA* for selfish attacker type and *A-A* for malicious attacker type.

For defender point of view (see Fig. 7(b)), it can be seen that the mixed strategy λ^*_{d2} is equal to zero for all cases of π_0. This means that the strategy *ES* is dominated. There are also three regions of NE points along with the increase of π_0:

- the low π_0 region where the defender does not perform the defensive strategies.
- the middle π_0 region where the defender only performs the strategy *SS*.
- the high π_0 region where the defender may perform either the strategy *SS* or the strategy *S*. However, it should be noted that the probability of performing the strategy *SS* is much larger than that of performing the strategy *S*.

This means that the defender only defends when π_0 is large enough, and the preferable defensive strategy is *SS*. The reason is that the cost for implementing *SS*, which is a combined strategy of *ES* and *S*, is more saving due to the flexibility by interrupting surveillance process if the channel is found to be empty after the sensing process.

Fig. 8 illustrates the relation between k_b and the NE point in the case where $\pi_0 = 0.5$. For attacker point of view (see Fig. 8(a)), it can be seen that there is the same behavior of the attacker with respect to the variation of k_b compared to the variation of π_0, i.e., there are also four regions of k_b having similar best response strategies. For defender point of view (see Fig. 8(b)), the strategy *SS* almost dominates other strategies. There is a very small probability of taking the strategy *S* when k_b is large ($k_b > 0.5$).

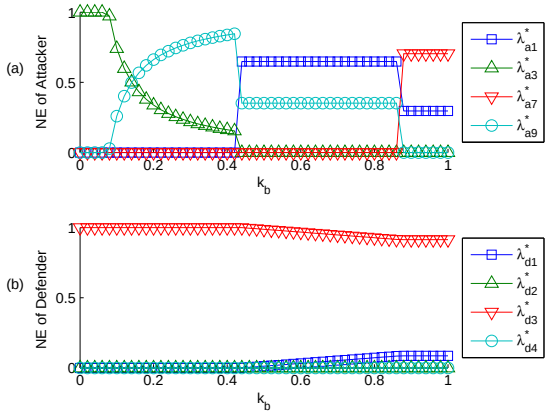

Figure 8. Attacker's and Defender's NE with respect to difference values of k_b, where $\pi_0 = 0.5$, and $k_C = 5$

Finally, we want to illustrate the robustness of the proposed defender strategies to the mismatch on the probability of attacker's type δ at both the defender's and the attacker's sides. It is worth reminding that the prior knowledge of the probability of attacker's type can be practically obtained through an estimation or a learning process. We denote the probability of attacker's type at the attacker side and at the defender side by δ_A and δ_D. Fig. 9 shows the utilities of the defender and the attacker with respect to different value of δ in the case where $\pi_0 = 0.5$, $k_b = 0.5$, and $k_C = 5$. For each case of δ, we depict the utilities of the defender and the attacker for all possible values of δ_D and δ_A, respectively. It can be seen that utility of the attacker decreases proportionally to the mismatch between δ and δ_A. Interestingly, utility of the defender is almost unchanged when δ_D is varied from δ. The reason is that the preferable NE strategy of the defender

as shown in previous simulations is the strategy *SS* which can counterpart either the types of attacker. The defender NE strategy thus is nearly independent of PUE attacker types.

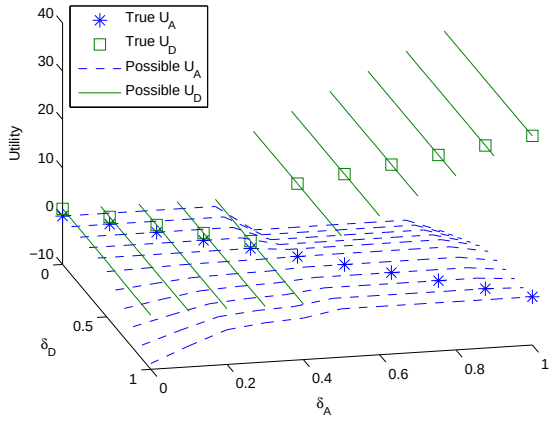

Figure 9. Attacker's and defender's utilities with imperfect knowledge of δ where $\pi_0 = 0.5$, $k_b = 0.5$, and $k_C = 5$

VI. Conclusion

We have discussed a game theory-based approach to counteract the serious security problem of PUE attack in CR networks. We have considered three types of PUE attacker: selfish, malicious, and mixed between selfish and malicious PUE attacker. We have determined the equilibrium points for the three games: channel surveillance game, extra-sensing game, and general game. The results exposed that for a known set of parameters, the equilibrium points strongly depend on the network demand which may vary according to network load and the available spectrum resource. For the general case of PUE attacker, i.e., the mixed selfish and malicious attacker, the equilibrium points also depend on the type of attacker. Though the equilibrium points are contingent on various parameters, they can be simply computed by Lemke and Howson algorithm. Particularly, by adopting a combined defensive strategy of extra-sensing and surveillance processes, the proposed method is a good candidate for combating the PUE attackers.

Appendix A
Proof of Result 1

It can be seen from (9) that $U_a^{S_{a2}} < U_a^{S_{a3}}, \forall \sigma_{d1}$ and $U_a^{S_{a3}}$ is equal to 0, hence the sign of $U_a^{S_{a1}}$, a first-order function with only one variable σ_{d1}, determines the BR of *Attacker*. In this case, the BR of *Attacker* is the selection between S_{a1} and S_{a3}. If $U_a^{S_{a1}} > 0$ the BR is S_{a1}. If $U_a^{S_{a1}} < 0$ the BR is S_{a3}. Otherwise, the BR is a mixed strategy between S_{a1} and S_{a3}. By some simple algebraic manipulations, we obtain the following BR function of *Attacker*:

$$\sigma_A^{BR} = \begin{cases} \{1,0,0\} & \text{if} \quad C_A \le B_U^C, \\ f(\sigma_{d1}) & \text{if} \quad B_U^C < C_A < B_U, \\ \{0,0,1\} & \text{if} \quad C_A \ge B_U, \end{cases} \tag{20}$$

where

$$f(\sigma_{d1}) = \begin{cases} \{1,0,0\} & \text{if} \quad \sigma_{d1} < \sigma_{d1}^{(0)}, \\ \{\sigma_{a1}, 0, 1-\sigma_{a1}\} & \text{if} \quad \sigma_{d1} = \sigma_{d1}^{(0)}, \\ \{0,0,1\} & \text{if} \quad \sigma_{d1} > \sigma_{d1}^{(0)}. \end{cases} \tag{21}$$

From (10), we can see that $U_d^{S_{d1}}$ is a first-order function with two variables σ_{a1} and σ_{a2} and $U_d^{S_{d2}}$ is equal to zero. Thus the BR of the defender is calculated by considering the sign of $U_d^{S_{d1}}$. If $U_d^{S_{d1}}$ is positive, negative or equal to zero, then the BR of the defender is S_{d1}, or S_{d2}, or a mixed strategy between S_{d1} and S_{d2}, respectively. The BR function of the defender is determined by

$$\sigma_D^{BR} = \begin{cases} \{0,1\} & \text{if} \quad G_S \le G_0, \\ g_1(\sigma_{a1}, \sigma_{a2}) & \text{if} \quad G_0 < G_S < G_1, \\ g_2(\sigma_{a1}, \sigma_{a2}) & \text{if} \quad G_S = G_1, \\ g_3(\sigma_{a1}, \sigma_{a2}) & \text{if} \quad G_S > G_1, \end{cases} \tag{22}$$

where $G_1 = (2p_A - p_N) C_S / (p_A \rho_A)$. Functions g_1, g_2, and g_3 are computed by

$$g_1 = \begin{cases} \{1,0\} & \text{if} \quad \sigma_{a1} > g(\sigma_{a2}), \sigma_{a2} < \sigma_{a2}^{(0)}, \\ \{\sigma_{d1}, 1-\sigma_{d1}\} & \text{if} \quad \sigma_{a1} = g(\sigma_{a2}), \sigma_{a2} \le \sigma_{a2}^{(0)}, \\ \{0,1\} & \text{if} \quad \begin{bmatrix} \forall \sigma_{a1}, \sigma_{a2} > \sigma_{a2}^{(0)}, \\ \sigma_{a1} < g(\sigma_{a2}), \sigma_{a2} \le \sigma_{a2}^{(0)}, \end{bmatrix} \end{cases} \tag{23}$$

$$g_2 = \begin{cases} \{1,0\} & \text{if} \quad \sigma_{a1} > g(\sigma_{a2}), \sigma_{a2} < \sigma_{a2}^{(0)}, \\ \{\sigma_{d1}, 1-\sigma_{d1}\} & \text{if} \quad \sigma_{a1} = g(\sigma_{a2}), \\ \{0,1\} & \text{if} \quad \sigma_{a1} < g(\sigma_{a2}), \end{cases} \tag{24}$$

and

$$g_3 = \begin{cases} \{1,0\} & \text{if} \quad \sigma_{a1} > g(\sigma_{a2}), \\ \{\sigma_{d1}, 1-\sigma_{d1}\} & \text{if} \quad \sigma_{a1} = g(\sigma_{a2}), \\ \{0,1\} & \text{if} \quad \sigma_{a1} < g(\sigma_{a2}), \end{cases} \tag{25}$$

where the function $g(\sigma_{a2})$ is given by

$$g(\sigma_{a2}) = \frac{(p_A - p_N) C_S \sigma_{a2} + p_N C_S}{p_A \rho_A G_S - (p_A - p_N) C_S}, \tag{26}$$

and $\sigma_{a2}^{(0)}$ is the the root of the equation $g(\sigma_{a2}) = 1$ obtained as

$$\sigma_{a2}^{(0)} = \frac{p_A \rho_A G_S - p_A C_S}{(p_A - p_N) C_S}. \tag{27}$$

Finding the intersection between the best response functions (20) and (22), we obtain the NE in Result 1 for the mixed strategies of the game in Table I for the selfish case.

Appendix B
Proof of Result 2

It can be seen from (11) that $U_a^{S_{a2}} < U_a^{S_{a1}}$ and $U_a^{S_{a1}} < U_a^{S_{a3}}$ for all σ_{d1} and σ_{d2}. Thus, S_{a2} is dominated. This means that $\sigma_{a2} = 0, \forall \sigma_{d1}, \sigma_{d2}$. We can obtain the following BR for attacker

$$\sigma_A^{BR} = \begin{cases} \{1,0,0\} & \text{if} \quad G_M > G_M^{(0)}, \\ \{\sigma_{a1}, 0, 1-\sigma_{a1}\} & \text{if} \quad G_M = G_M^{(0)}, \\ \{0,0,1\} & \text{if} \quad G_M < G_M^{(0)}. \end{cases} \tag{28}$$

Considering the game in Table I given that S_{a2} is dominated, we can compute the following BR functions for defender:

$$\sigma_D^{BR} = \begin{cases} \{0,1\} & \text{if} \quad G_E \leq G_E^{(0)}, \\ h\left(\sigma_{a1}\right) & \text{if} \quad G_E > G_E^{(0)}. \end{cases} \tag{29}$$

where

$$h\left(\sigma_{a1}\right) = \begin{cases} \{0,1\} & \text{if} \quad \sigma_{a1} > \sigma_{a1}^{(0)}, \\ \{\sigma_{d1}, 1-\sigma_{d1}\} & \text{if} \quad \sigma_{a1} = \sigma_{a1}^{(0)}, \\ \{1,0\} & \text{if} \quad \sigma_{a1} < \sigma_{a1}^{(0)}, \end{cases} \tag{30}$$

and $\sigma_{a1}^{(0)} = p_N\left(\rho_N G_E - C_E\right)/(p_N \rho_N G_E + \left(p_A - p_N\right) C_E)$. Intersect (28) and (29), we obtain ***Result*** 2.

REFERENCES

[1] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189–203, Feb 2012.

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

[3] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE Conference on Computer Communications (INFOCOM)*, April 2008.

[4] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *IEEE International Conference on Communications (ICC)*, May 2008.

[5] N. Nguyen-Thanh and I. Koo, "A robust secure cooperative spectrum sensing scheme based on evidence theory and robust statistics in cognitive radio," *IEICE Transactions on communications*, vol. 92, no. 12, pp. 3644–3652, December 2009.

[6] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226–228, March 2010.

[7] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1806–1822, April 2012.

[8] H. Tang, F. Yu, M. Huang, and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," *IET Communications*, vol. 6, no. 8, pp. 974–983, May 2012.

[9] 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.

[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] 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.

[12] Q. Peng, P. Cosman, and L. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 903–911, April 2011.

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

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

[15] B. Wang, Y. Wu, and K. Ray Liu, "Game theory for cognitive radio networks: An overview," *Computer Networks*, vol. 54, no. 14, pp. 2537 – 2561, April 2010.

[16] M. Felegyhazi and J. Hubaux, "Game Theory in Wireless Networks: A Tutorial," *ACM Computing Surveys*, pp. 1–14, January 2006.

[17] J. Harsanyi, "Games with incomplete information played by "bayesian" players, i-iii," *Manage. Sci.*, vol. 50, no. 12, pp. 1804–1817, Dec. 2004.

[18] R. Gibbons, *Game theory for applied economists*. Princeton University Press, 1992.

[19] H. Kuhn, "Extensive games and the problem of information," *Annals of Mathematics Studies*, vol. 28, 1953.

[20] Y. Utsumi, "The characterization of the common prior assumption without common knowledge," *Keio economic studies*, vol. 41, no. 1, pp. 15–26, January 2004.

[21] C. Lemke and J. Howson Jr, "Equilibrium Points of Bimatrix Games," *Journal of the Society for Industrial and Applied Mathematics*, vol. 12, no. 2, pp. 413–423, June 1964.

[22] S. Gabriel, A. Conejo, J. Fuller, B. Hobbs, and C. Ruiz, "Equilibria and complementarity problems," in *Complementarity Modeling in Energy Markets*, ser. International Series in Operations Research & Management Science. Springer New York, 2013, vol. 180, pp. 127–179.

[23] P. Goldberg, C. Papadimitriou, and R. Savani, "The complexity of the homotopy method, equilibrium selection, and lemke-howson solutions," *ACM Transactions on Econ. Comput.*, vol. 1, no. 2, pp. 1–25, May 2013.

[24] D. Avis, G. Rosenberg, R. Savani, and B. von Stengel, "Enumeration of nash equilibria for two-player games," *Economic Theory*, vol. 42, no. 1, pp. 9–37, 2010.