Extra-sensing game for malicious primary user emulator attack in cognitive radio network

Ta Duc-Tuyen, Nhan Nguyen-Thanh, Philippe Ciblat, van Tam Nguyen, Ta Duc-Tuyen

Extra-Sensing Game for Malicious Primary User Emulator Attack in Cognitive Radio Network

Ta Duc-Tuyen[1], Nhan Nguyen-Thanh[1], Philippe Ciblat[1], and Van-Tam Nguyen[1,2]
[1]Department of Communications and Electronics, Telecom ParisTech, France
[2]Department of EECS, University of California at Berkeley, USA
Email: {duc-tuyen.ta, nhan.nguyen-thanh)@telecom-paristech.fr, philippe.ciblat@enst.fr, vantamnguyen@berkeley.edu

***Abstract*—Primary User Emulation (PUE) attack is a serious security problem in cognitive radio (CR) network. A PUE attacker emulates a primary signal during sensing duration in order the CR users not to use the spectrum. The PUE attacker is either selfish if it would like to take benefit of the spectrum, or malicious if it would like to do a Deny of Service of the CR network. In this paper, we only consider malicious PUE. We propose to perform sometimes an additional sensing step, called extra-sensing, in order to have a new opportunity to sense the channel and so to use it. Obviously the malicious PUE may still perform an attack during this extra-sensing. Therefore, our problem can be formulated as a zero-sum game to modeling and analyzing the strategies for two players. The equilibrium is expressed in closed-form. The results show that the benefit ratio and the probability of channel's availability strongly influence the equilibrium. Numerical results confirm our claims.**

I. Introduction

In the context of interweave cognitive radio (CR), the spectrum sensing which enables to discover the spectrum hole is a key issue. A lot of efficient methods for sense the spectrum has been proposed in the literature (see [1] and references therein). However, these methods may be subject to attack in order to disturb the CR network. Therefore, the security for the spectrum sensing operation has received recently a lot of attention [2]–[12].

The spectrum sensing attack can be twofold: the first type of attack is the *spectrum sensing data falsification* (SSDF) in the context of cooperative spectrum sensing [3]–[8] in which malicious attackers may share incorrect sensing data leading to a degradation on the accuracy of the collaborative spectrum sensing process, and hence of the CR system. The second type of attack is *primary user emulation* (PUE) in which the attacker emulates the characteristics of a primary user to obtain exclusive spectrum usage. If the attacker wants to occupy the attacked spectrum band for its own usage, it is called *selfish* PUE. Otherwise, if the attacker wants to prevent the network operation, it is called *malicious* PUE. In this paper, we focus on the PUE attack.

To overcome the PUE attack, several solutions have been proposed. Some works focused on surveillance algorithms usually based on some network knowledge, such as the location of both primary user and secondary user as in [9] or the primary signal feature as in [10]. But as the attacker does not want to be caught, it can not always play. Therefore according to the cost to play (for the attacker) and the cost to monitor (for the defender), the trade-off between attacker and defender strategies can be formulated through the game theory tool. Some papers already took benefit of game-theoretic approach for analyzing some PUE attack schemes. In [11], the so-called dog-fight spectrum scheme corresponding to random frequency hopping was analyzed. In [13], a multistage anti-jamming scheme was considered. In [14], the nature of the PUE attack was taken in account. Actually, the authors considered a selfish PUE attack. In that case, they proposed to monitor the channel randomly in order to identify the selfish PUE attacker. They formulated the problem as a non-zero sum game with incomplete information (see [15]–[17] for more information on game theory), and they found the best strategies for both attacker and defender.

In this paper, we focus on the malicious PUE attack. In such a type of attack, the goal is to foll the spectrum sensing step by sending signals coming from PUE during the spectrum sensing step. We propose to add an extra-sensing process into the part of the frame devoted to data transmission if the channel was declared "busy" in order to have the opportunity to observe free channel (since not used for data since the PUE attack succeeds but not used by the PUE attack since it is malicious) and so to use it in the remainder of the frame. Assuming the payoffs of the attacker and defender are opposite, we formulate the extra-sensing problem as a zero-sum game. The main purpose of the paper is to find the relevant strategy for each player by exhibiting equilibrium points of the formulated game.

The remainder of this paper is organized as follows: The system model is introduced in Section II. The extra-sensing zero-sum game is described in Section III and solved in Section IV. Numerical results are provided in Section V. Concluding remarks are drawn in Section VI.

II. System Model

We consider a CR network with secondary users accessing to a licensed band while malicious PUE attacker may operate. In order to simplify the analysis, we assume that the CR network consists in two separated sets of nodes: i) the network operator managing the spectrum sensing and the extra sensing process, and ii) the network users exploiting the network services.

The network operator firstly collects the result of the spectrum sensing devices and declares the status of the channel (present or absent primary user). Then its broadcasts this information to all network users. If the status of the channel is busy, the network operator may decide to apply defense mechanism or not within the part of the frame devoted to data transmission. The defense mechanism corresponds to re-sense the channel in order to re-determine the *true* status of the channel.

The attacker can either transmit or not transmit the PUE signal in order to fool the spectrum sensing and to deny the service of the network. The attacker is assumed not to know the true status of the primary signal during PUE attack. So it can attack the network unsuccessfully if the primary is already present. Therefore, a re-attack may be performed within the part of the frame devoted to data transmission if the sensing result was busy. In contrast, if the sensing result was idle, re-attack mechanism is never applied.

Let P_F and P_D be the false alarm and detection probabilities of the spectrum sensing engine respectively when the channel is not attacked. Let $P_{F|A}$ and $P_{D|A}$ be the false alarm and detection probabilities of the spectrum sensing engine respectively when the channel is attacked. Let π_0 be the probability that the primary user is inactive. In the remainder of the paper, we also need the following four probabilities:

- p_A is the probability that the answer of the sensing engine is busy when the attacker attacks.
- p_N is the probability that the answer of the sensing engine is busy when the attacker does not attack.
- ρ_A is the probability that the channel is not used by the primary user while the sensing engine claims busy and the attacker attacks.
- ρ_N is the probability that the channel is not used by the primary user while the sensing engine claims busy and the attacker does not attack.

III. The Game Formulation

A. Players

There are two players: the **Attacker** who emulates a PU, and the **Defender** who monitors the channel in order to mitigate the bad effect of the malicious PUE attack.

B. Strategies

During the sensing step, the attacker may perform two possible actions: **Attack** (**A**) or **No Attack** (**NA**). The sensing engine senses the network environment and returns the status of primary user signal by two state "*busy*" or "*idle*". Therefore, there are four possible cases: (A,"*busy*"), (NA, "*busy*"), (A, "*idle*") and (NA,"*idle*").

During the data transmission step, according to the sensing result, the attacker takes one of three possible actions: **Attack** (**A**) to re-attack the channel, **Leave** (**L**) not to attack the channel or **No Operation** (**nO**) to act as normal secondary user. Meanwhile, the defender chooses one of three possible actions: **Extra-Sensing** (**ES**) to re-sense the busy channel, **No Extra-Sensing** (**NE**) not to re-sense the busy channel or **No Defense** (**ND**) not to defense when the channel is idle.

Therefore. the game tree for malicious PUE attack can be illustrated as Figure 1.

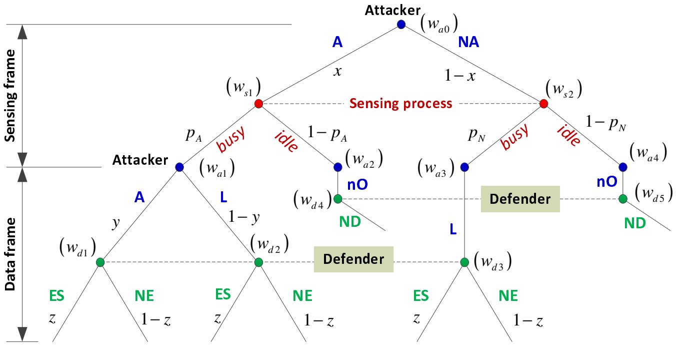

Fig. 1: The extra-sensing game

The attacker has three pure combined actions leading to its pure strategy set M_A:

$$\begin{aligned} M_A &= \{M_{a1}, M_{a2}, M_{a3}\} \\ &= \{[AA, AnO], [AL, AnO], [NAL, NAnO]\}. \end{aligned}$$

Similarly, the defender has two pure combined actions leading to its pure strategy set M_D:

$$\begin{aligned} M_D &= \{M_{d1}, M_{d2}\} \\ &= \{[ES, ND], [NE, ND]\} \end{aligned}$$

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 μ_a and μ_d, as follows

$$\begin{cases} \mu_a = & \{\mu_{a1}, \mu_{a2}, \mu_{a3}\} \\ \mu_d = & \{\mu_{d1}, \mu_{d2}\} \end{cases} \tag{1}$$

where μ_{ai}, $i = 1, 2, 3$ are the probabilities of action M_{ai} and μ_{dj}, $j = 1, 2$ are the probabilities of action M_{dj}.

In Figure 1, we denote by x the probability that the attacker takes the action **A** at the beginning of game. Similarly, we denote by y the probability that the attacker performs the action **A** when the sensing result shows that the attacked channel is busy. In addition, we denote by z the probability that the defender performs the extra-sensing action. The relationship between the three parameters x, y, and z with the mixed strategies of the formulated game is as follows

$$\begin{cases} x = & \mu_{a1} + \mu_{a2} \\ y = & \mu_{a1}/(\mu_{a1} + \mu_{a2}) \\ z = & \mu_{d1} \end{cases} \tag{2}$$

The objective is now to find the values of x, y, and z or equivalently, the values of μ_{a1}, μ_{a2}, and μ_{d1} that lead to the equilibrium point.

C. Payoffs

For the formulated game, the benefits of the attacker and defender are assumed to be completely opposite, which means that the payoff of the attacker is given by the negative of the payoff of the defender. Consequently, the game corresponds to a so-called zero-sum game. We first introduce the payoff of each defender's action as below:

- C_E is the cost for implementing the extra-sensing process.
- G_E is the benefit for retrieving the attacked channel during the extra-sensing step.

Notice that G_E is also the benefit for attacker to re-attack the channel

In Table I, we provide the payoffs for each pair of actions of the defender and the attacker. The payoff of the attacker is obtained by taking the opposite of those of the defender.

TABLE I: Action's payoffs for Defender and Attacker

	Defender's Payoff $P_D^{a;d}$	**Attacker's Payoff** $P_A^{a;d}$
AA-ES	$-C_E + \rho_A G_E$	$C_E - \rho_A G_E$
AA-NE	$-\rho_A G_E$	$\rho_A G_E$
AL-ES	$-C_E + \rho_A G_E$	$C_E - \rho_A G_E$
AL-NE	0	0
NAL-ES	$-C_E + \rho_N G_E$	$C_E - \rho_N G_E$
NAL-NE	0	0
AnO-ND	0	0
NAnO-ND	0	0

In Table II, we define the payoff matrix for the considered game.

TABLE II: Payoff Matrix of the malicious PUE attack game

	$M_{d1} = [ES, ND]$	$M_{d2} = [NE, ND]$
$M_{a1} = [AA, AnO]$	$(U_D^{a1,d1}, U_A^{a1,d1})$	$(U_D^{a1,M_{d2}}, U_A^{a1,d2})$
$M_{a2} = [AL, AnO]$	$(U_D^{a2,d1}, U_A^{a2,d1})$	$(U_D^{a2,M_{d2}}, U_A^{a2,d2})$
$M_{a3} = [NAL, NAnO]$	$(U_D^{a3,d1}, U_A^{a3,d1})$	$(U_D^{a3,M_{d2}}, U_A^{a3,d2})$

According to the game's tree displayed in Figure 1, the defender's payoff for each pair of actions is as follows

$$\begin{aligned}
U_D^{a1,d1} &= p_A P_D^{AA;ES} + (1-p_A) P_D^{AnO;ND} \\
U_D^{a1,d2} &= p_A P_D^{AA;NE} + (1-p_A) P_D^{AnO;ND} \\
U_D^{a2,d1} &= p_A P_D^{AL;ES} + (1-p_A) P_D^{AnO;ND} \\
U_D^{a2,d2} &= p_A P_D^{AL;NE} + (1-p_A) P_D^{AnO;ND} \\
U_D^{a3,d1} &= p_N P_D^{NAL;ES} + (1-p_N) P_D^{NAnO;ND} \\
U_D^{a3,d2} &= p_N P_D^{NAL;NE} + (1-p_N) P_D^{NAnO;ND}
\end{aligned}$$

and the attacker's payoff of each pair of actions is

$$U_A^{ai,dj} = -U_D^{ai,dj}, \quad i = 1,2,3; j = 1,2. \tag{3}$$

Finally, the average payoffs of the defender and the attacker are computed as follows:

$$\begin{cases} U_D(\mu_a, \mu_d) = & \sum\limits_{i=1}^{3} \sum\limits_{j=1}^{2} \mu_{ai} \mu_{dj} U_D^{ai,dj} \\ U_A(\mu_a, \mu_d) = & -U_D(\mu_a, \mu_d) \end{cases} \tag{4}$$

For instance, one can easily check that

$$\begin{aligned} U_D(\mu_a, \mu_d) = -(1-\mu_{d1}) p_A \rho_A G_E \mu_{a1} + [p_A C_E + p_N \rho_N G_E \\ - p_N C_E - p_A \rho_A G_E] \mu_{d1} \mu_{a3} + [p_A \rho_A G_E - p_A C_E] \mu_{d1}. \end{aligned} \tag{5}$$

IV. The Equilibrium Points

In [15], it has showed that a two-player zero-sum game admits a solution in mixed strategies and the solution (saddle point) is be obtained by solving the following primal-dual linear programming problems:

$$\mu_d^* = \arg \max_{\mu_d} \min_{\mu_a} U_D(\mu_a, \mu_d) \tag{6}$$

$$\mu_a^* = \arg \min_{\mu_a} \max_{\mu_d} U_D(\mu_a, \mu_d) \tag{7}$$

where (μ_a^*, μ_d^*) is the equilibrium point.

Hereafter, we discuss only about μ_d^* since μ_a^* can be obtained similarly. Since Eq. (5) is a linear function of μ_{d1}, the Linear Programming (LP) method can be used to solve the problem. The basic idea here is that, from the series of linear constraints of the variables, we find the feasible region of the possible values for those. This region is a convex simple polygon. The problem now is to find the vertex of this convex polygon with the highest (lowest) possible value [18].

Therefore, the analytic solution for *maximin* problem in Eq. (6) is to find the minimum value of $U_D(\mu_a, \mu_d)$ with variable μ_a. By replacing μ_{a2} with $(1 - \mu_{a1} - \mu_{a3})$, this can be expressed in the canonical form:

$$\begin{aligned} &\textbf{minimize}_{\mu_{a1}, \mu_{a3}} && U_D(\mu_a, \mu_d) \\ &\textbf{subject to:} && \mu_{a1} + \mu_{a3} \leq 1 \\ & && 0 \leq \mu_{a1}, \mu_{a3} \leq 1 \end{aligned} \tag{8}$$

The solutions of Eq. (8) with respect to variables μ_{a1} and μ_{a3} are used to find the *maximum* of $U_D(\mu_a, \mu_d)$ with respect to variable μ_{d1} and μ_{a2} in Eq. (6). Once again replacing μ_{d1} with $(1 - \mu_{d1})$, we obtain two cases. The optimal μ_{d1} is that maximizing either $U_D^{(1)}$ or $U_D^{(2)}$ defined as follows

Case 1:

$$\begin{aligned} &\textbf{maximize}_{\mu_{d1}} && U_D^{(1)}(\mu_d) \\ &\textbf{subject to} && U_D^{(0)}(\mu_d) \geq 0 \\ & && 0 \leq \mu_{d1} \leq 1 \end{aligned} \tag{9}$$

Case 2:

$$\begin{aligned} &\textbf{maximize}_{\mu_{d1}} && U_D^{(2)}(\mu_d) \\ &\textbf{subject to} && U_D^{(0)}(\mu_d) < 0 \\ & && 0 \leq \mu_{d1} \leq 1 \end{aligned} \tag{10}$$

with

$$\begin{aligned} U_D^{(0)}(\mu_d) &= \mu_{d1}[p_A C_E + p_N \rho_N G_E - p_N C_E - 2 p_A \rho_A G_E] \\ &\quad + p_A \rho_A G_E, \\ U_D^{(1)}(\mu_d) &= (2 p_A \rho_A G_E - p_A C_E)\, \mu_{d1} - p_A \rho_A C_E, \\ U_D^{(2)}(\mu_d) &= (p_N \rho_N G_E - p_N C_E)\, \mu_{d1}. \end{aligned}$$

Similarly, the solutions μ_a^* to obtain the *minimax* in Eq. (7) will be achieved by analysis the highest/lowest possible value in the feasible region of $U_D(\mu_a, \mu_d)$.

Due to the page limitation, we have skipped the details of the derivations (based on LP method) for obtaining next Result which corresponds to the closed-form expression of the equilibrium point (EP) μ_d^*, μ_a^*.

Result 1. *The EP for the mixed strategy zero-sum game given in Table II is as follows:*

$$
\begin{array}{lll}
\textit{If} \quad (p_A - p_N)C_E - (p_A\rho_A - p_N\rho_N)G_E \geq 0 & & \\
\quad \textit{If} \quad 2G_E < C_E/\rho_A; \mu_{d1}^* = 0, & & \\
\qquad G_E - C_E/\rho_N < 0; \mu_{a1}^* = 1, \mu_{a3}^* = 0; & & \text{(11a)} \\
\qquad G_E - C_E/\rho_N \geq 0; \mu_{a1}^* = \mu_{a1}^{(0)}, \mu_{a3}^* = \mu_{a3}^{(0)}; & & \text{(11b)} \\
\quad \textit{If} \quad 2G_E \geq C_E/\rho_A; \mu_{d1}^* = 1, \mu_{a1}^* = 1, \mu_{a3}^* = 0; & & \text{(11c)} \\
\textit{If} \quad (p_A - p_N)C_E - (p_A\rho_A - p_N\rho_N)G_E < 0 & & \\
\quad \textit{If} \quad G_E < C_E/\rho_A & & \\
\qquad 2G_E < C_E/\rho_A; \mu_{d1}^* = 0, \mu_{a1}^* = 1, \mu_{a3}^* = 0; & & \text{(11d)} \\
\qquad 2G_E \geq C_E/\rho_A; \mu_{a1}^* = 1, \mu_{a3}^* = 0; & & \\
\qquad\quad G_E - C_E/\rho_N < 0; \mu_{d1}^* = \mu_{d1}^{(0)}; & & \text{(11e)} \\
\qquad\quad G_E - C_E/\rho_N \geq 0; \mu_{d1}^* = 1; & & \text{(11f)} \\
\quad \textit{If} \quad G_E \geq C_E/\rho_A & & \\
\qquad G_E - C_E/\rho_N < 0; \mu_{a1}^* = \mu_{a1}^{(0)}, \mu_{a3}^* = \mu_{a3}^{(0)}; & & \\
\qquad\quad 2G_E > C_E/\rho_A; \mu_{d1}^* = \mu_{d1}^{(0)} & & \text{(11g)} \\
\qquad G_E - C_E/\rho_N \geq 0; \mu_{a1}^* = 0, \mu_{a3}^* = 1 & & \\
\qquad\quad 2G_E > C_E/\rho_A; \mu_{d1}^* = 1 & & \text{(11h)}
\end{array}
$$

with

$$
\begin{aligned}
\mu_{d1}^{(0)} &= \frac{p_A\rho_A G_E}{2p_A\rho_A G_E + p_N C_E - p_A C_E - p_N\rho_N G_E}, \\
\mu_{a1}^{(0)} &= \frac{p_N\rho_N G_E - p_N C_E}{p_A C_E + p_N\rho_N G_E - p_A C_E - 2p_A\rho_A G_E}, \\
\mu_{a3}^{(0)} &= \frac{p_A C_E - 2p_A\rho_A G_E}{p_A C_E + p_N\rho_N G_E - p_A C_E - 2p_A\rho_A G_E}.
\end{aligned}
$$

Substituting Eq. (11) into Eq. (7) leads to the EP for the probabilities x, y, and z.

Hereafter, we interpret Result 1. When implementing cost of extra-sensing to retrieve the attacked channel is too high (Eqs. 11a, 11b, 11d, 11e, and 11g), the defender will not perform the defense process ($\mu_{d1}^* = 0$). When the extra-sensing cost is higher, the network operator will take the defense action. However, depending the transmission medium, the EP is not straightforward (see Eqs. 11e, 11g). Since the payoff of the attacker is completely opposite, the attacker's strategy also is the inverse of the defender's actions. If the cost of implementing extra-sensing is too high, the attacker will attack the network. Similar to the defender's case, the EP is not obtained directly (see Eqs. 11b, 11g). Our solution shows the values to choose for both attacker and defender.

The gain of the extra-sensing process (G_E) shows the benefit that CR network can earn by performing defense action or lost when the attacked channel is extra-sensed. In analytic results, there is a strong relation between the gain and the cost of extra-sensing actions with the player's strategy. Therefore, we introduce the benefit ratio k_b which is computed by

$$k_b = G_E/C_E. \tag{12}$$

The analysis shows that, the strategy of attacker (resp. defender) in the zero-sum extra-sensing game depends on both benefit ratio k_b and the availability of primary user's channel (here given by the probability that the primary user is inactive π_0). We then have the following result.

Result 2: *Assuming fixed probability of channel's availability π_0, Eqs. (11) are equivalent to the following ones depending only on the benefit ratio k_b.*

$$
\begin{array}{ll}
\textit{If}\, k_b \leq \pi^{(0)}; \mu_{d1}^* = 0, \mu_{a1}^* = 1, \mu_{a3}^* = 0 & \text{(13a)} \\
\textit{If}\, \pi^{(0)} \leq k_b \leq \pi^{(*)}; \mu_{d1}^* = 1, \mu_{a1}^* = 1, \mu_{a3}^* = 0 & \text{(13b)} \\
\textit{If}\, \pi^{(0)} < k_b \leq \pi^{(1)}; \mu_{d1}^* = \mu_{d1}^{(0)}, \mu_{a1}^* = \mu_{a1}^{(0)}, \mu_{a3}^* = \mu_{a3}^{(0)} & \text{(13c)} \\
\textit{If}\, \pi^{(1)} < k_b \leq \pi^{(2)}; \mu_{d1}^* = \mu_{d1}^{(0)}, \mu_{a1}^* = \mu_{a1}^{(0)}, \mu_{a3}^* = \mu_{a3}^{(0)} & \text{(13d)} \\
\textit{If}\, k_b > \pi^{(2)}; \mu_{d1}^* = 1, \mu_{a1}^* = 0, \mu_{a3}^* = 1 & \text{(13e)}
\end{array}
$$

with $\pi^{(0)} = 1/2\rho_A$, $\pi^{(1)} = 1/\rho_A$, $\pi^{(2)} = 1/\rho_N$ and $\pi^{(*)} = (p_A - p_N)/(p_A\rho_A - p_N\rho_N)$.

V. Numerical Results

Numerical simulations are run to confirm the analytic results and to analyze more deeply the influence of some design parameters. Unless the otherwise stated, the parameters are fixed as follows: $C_E = 3$, $p_D = 0.9$ and $p_F = 0.1$. We also assume that the sensing engine uses energy detection method and the average Signal-to-Noise Ratio (SNR) of the primary signal received at sensing engine is -10dB. In order to verify the correctness of the analysis, numerical simulations of the EP have also been carried out with the Lemke-Hawson (L-H) algorithm [19].

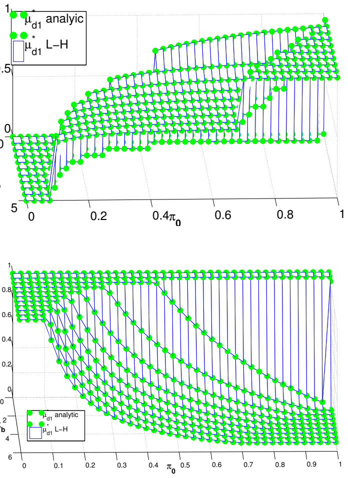

Fig. 2: Analytic results and L-H algorithm: (top) defender's strategy, (bottom) attacker's strategy

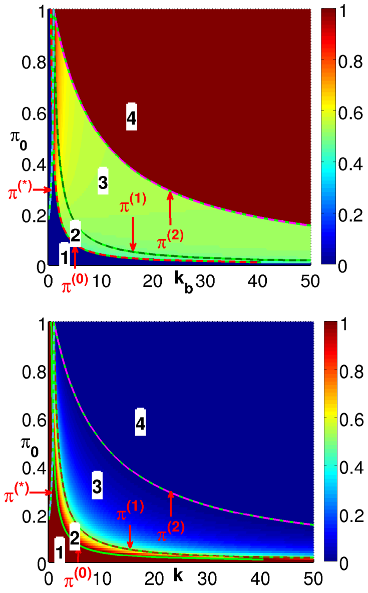

Fig. 3: Value regions of the players' strategies vs. benefit ratio k_b and probability that primary user is inactive π_0: (top) defender, (bottom) attacker

Figure 2 demonstrates the agreement between the theoretical analysis and the L-H algorithm with respect to the benefit ratio k_b and the probability that primary user is inactive π_0.

Figure 3 illustrates the relationship between k_b, π_0 and the equilibrium point in **Result 2**. For the defender point of view (see Figure 3.a), the EP varies according to the relationship between k_b and π_0 and there are approximately four regions, bounded by the line $\pi^{(*)}, \pi^{(0)}$, $\pi^{(1)}$ and $\pi^{(2)}$, respectively. Similarly, for the attacker point of view, the attacker's strategy also exhibits four regions (see Figure 3.b), bounded by the line $\pi^{(*)}, \pi^{(0)}$, $\pi^{(1)}$ and $\pi^{(2)}$. When benefit ratio is high, the main strategy of the attacker is not to perform attack when the defender performs defense. In contrast, the strategies of defender and attacker are reverse when benefit ratio is low. Moreover, the attacker always takes the attack action while the defender takes the extra-sensing action in the cross region between $\pi^{(*)}$, $\pi^{(0)}$, and $\pi^{(1)}$.

VI. Conclusion

We have proposed a game theory-based approach to counteract the serious security problem of malicious PUE attack in CR networks. By implementing the extra-sensing process within data period, the bad effect of malicious PUE attack can be mitigated. The good strategy for both attacker and defender is analyzed by finding the equilibrium of the considered zero-sum game. The equilibrium point has been determined in closed form. The results showed that for a known set of parameters, the equilibrium point strongly depends on the benefit ratio and the availability of primary user channel.

Acknowledgment

This work has been supported by French ministry of industry and European CATRENE in CORTIF project (Coexistence Of RF Transmissions In the Future).

References

[1] E. Axell, G. Leus, E. Larsson, and H. Poor, "Spectrum sensing for cognitive radio : State-of-the-art and recent advances," *IEEE Signal Processing Magazine*, vol. 29, no. 3, pp. 101–116, May 2012.

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

[3] 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, 2009.

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

[5] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and Counteracting Statistical Attacks in Cooperative Spectrum Sensing," *Signal Processing, IEEE Transactions on*, vol. 60, no. 4, pp. 1806–1822, April 2012.

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

[7] R. Chen, J. M. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008.

[8] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," in *Communications, 2008. ICC '08. IEEE International Conference on*, May 2008, pp. 3406–3410.

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

[10] S. Chen, K. Zeng, and P. Mohapatra, "Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space," *Mobile Computing, IEEE Transactions on*, 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," *Wireless Communications, IEEE Transactions on*, 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," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 4, pp. 903–911, April 2011.

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

[14] N. Nguyen-Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, "Attack and Surveillance Strategies for Selfish Primary User Emulator in Cognitive Radio Network," in *GlobalSIP14*, 2014.

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

[16] 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, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001064

[17] M. Felegyhazi and J. Hubaux, "Game Theory in Wireless Networks: A Tutorial," *Computing Surveys, ACM*, 2006.

[18] G. B. Dantzig and M. N. Thapa, *Linear Programming 1: 1: Introduction*. Springer Science & Business Media, 1997, vol. 1.

[19] 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, 1964. [Online]. Available: http://dx.doi.org/10.2307/2946376