Attack and Surveillance Strategies for Selfish Primary User Emulator in Cognitive Radio Network

Nhan Nguyen-Thanh[1], Philippe Ciblat[1], Anh T. Pham[2], and Van-Tam Nguyen[1,3]
[1] Department of Communications and Electronics, Telecom ParisTech, France
[2] Laboratory of Computer Communications, University of Aizu, Aizu-Wakamatsu, Japan
[3] Department of EECS, University of California at Berkeley, USA
Email: nhan.nguyen-thanh@telecom-paristech.fr, philippe.ciblat@telecom-paristech.fr,
pham@u-aizu.ac.jp, vantamnguyen@berkeley.edu

***Abstract*—Primary user emulation (PUE) attack is a serious security problem in cognitive radio (CR) networks. In PUE attack, attacker transmits an emulated primary signal during a spectrum sensing interval to fool the CR system causing a prohibition in the secondary access on the attacked channel. An attacker is called selfish attacker if it performs the PUE attack for its selfish own purpose. Since it is obligate to reveal the user's identification in any communication link, a channel surveillance process can help to identify the selfish PUE attacker. In this paper, we formulate a non-zero-sum game with incomplete information for analyzing and modeling the selfish PUE attack and surveillance strategies simultaneously. Nash Equilibrium (NE) is figured out in closed form. The results show that the network demand and the penalty factor strongly influence the NE. Numerical simulations confirm our claims based on our analytic results.**

I. Introduction

Determining spectrum hole is a key function for implementing cognitive radio (CR) which is a promising technology for improving spectrum utilization by enabling secondary spectrum access. Although the accuracy and the reliability of the spectrum database service make it to be proposed as a interesting solution for providing spectrum resource information, its high cost, its low flexibility and its dependence on perfect knowledge of primary system including propagation models and locations of clients prevents to use it alone [1]. Therefore the spectrum sensing (SS) approach continues to be an elegant solution since it is superior for future applications where flexibility of discovering spectrum holes for a wide range of spectrum band and network types is the most important factor. Nevertheless, SS suffers from two important security threats [2]: primary user emulation (PUE) attack and spectrum sensing data falsification (SSDF) attack.

On the one hand, SSDF attack occurs due to the presence of malfunction or malicious terminals sharing incorrect SS data which causes a degradation on accuracy of the cooperative SS process. Several works have considered this security threat [3]–[8]. On the other hand, PUE attack influences actively the SS process by transmitting an emulated primary signal on the sensing duration. The presence of an emulated primary signal is more dangerous since it may lead to a prohibition of secondary accessing to the channel immediately. Therefore we focus on this type of attack. Several solutions to counteract PUE attack such as localization-based transmitter verification [9], primary signal feature verification [10], or channel hopping communication [11], [12] have been proposed. However, a verification of transmitter position or signal feature requires the knowledge of the locations of both primary transmitter and CR users or the information of primary signal characteristics, which are not always available or applicable, whereas channel hopping method can not resist multi-channel attacking cases.

PUE attacks are classified into malicious PUE attacks and selfish PUE attacks. A malicious PUE attack aims at obstructing operation of CR network, whereas a selfish PUE attack aims at occupying the attacked spectrum band for selfish use purpose. The malicious PUE attack is essentially similar to the conventional denial-of-service or jamming attack, which is an irresistible issue in wireless systems, whereas the selfish PUE attack is a novel security threat, which considerably influences on the fairness of the CR network operation. Therefore, counteracting PUE selfish attack is crucial and so our purpose.

In selfish PUE attack, a successful PUE attack in sensing duration is usually followed by a selfish use of the attacked channel by the attacker. Meanwhile, it is possible to determine user's identification in any communication link. Therefore, a channel surveillance process, which observes prohibited secondary-accessing channels after sensing duration, can help to detect illegal channel occupation, and identify selfish PUE attacker. However the concern is about when and how often the PUE selfish attack as well as the channel surveillance process 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 player [13] and has been adopted in many similar CR network problems [14], [15], can be adopted to formulate this problem as a game between PUE attacker and CR system defender.

In this paper, we formulate a non-zero-sum game with incomplete information [16] for the selfish PUE attack and the

This work has been supported by French ministry of industry and ENIAC Joint Undertaking in ARTEMOS project, by French ministry of industry in AppsGate project, and by French Ministry of defense in DGA-ERE program.

surveillance process. It has been proven that the best strategy for all player of a certain game is the Nash equilibrium (NE) points [17]. Therefore, the main objective of the paper is to determine the NE of the formulated game.

II. System model

We consider a CR network performing secondary access to a licensed band, and operating in an adversarial environment where exists selfish users who want to use more spectrum resource by performing PUE attack. We assume that the CR network includes two separated sets: the network manager set which are entities being responsible to manage the network operations including the implementation of sensing and surveillance processes, and the network user set which are users exploiting the services of the network manager set.

The operation time is divided into super frames, each of which includes a sensing frame following by a data frame. In the sensing frame, dedicated sensing engines sense to detect primary signal, while all non-primary users must vacate the channel to ensure the accuracy of the sensing process. After sensing duration, two possible results of the channel state could be provided: state "*busy*" or state "*idle*" which means that the channel is declared to be occupied or to be free, respectively. The attacker is assumed to know nothing about the true status of primary signal during PUE attack. In data frame, if the state "*busy*" is declared, all CR users should not use the channel; any secondary transmission on that channel will be considered to be done by a PUE attacker. We also assume that any CR user could be recognized by observing its transmitted data since the identifying information is contained.

III. The game formulation

There are two players: ***Attacker*** who emulates a PU in order to use the channel for its own interest, and ***Defender*** who monitors the channel to catch the attacker.

At the sensing frame, an attacker takes one of two possible actions: ***Attack*** (*A*) to transmit an emulated primary signal or ***No Attack*** (*NA*) not to transmit any emulated signal.

At the data frame, depending on the sensing result (*busy* or *idle*), the attacker takes one of three possible actions: ***Use*** (*U*) to use the channel selfishly, ***Leave*** (*L*) to leave the channel, or ***normal Operation*** (*nO*) to operate as a normal user. Meanwhile, for a defender, three possible actions are: ***Surveillance*** (*S*) to implement a surveillance algorithm, ***No Surveillance*** (*NS*) to do no surveillance on the channel, or ***No Defense*** (*ND*) to do no defense on the channel.

The game can be summarized in Fig. 1. According to Fig. 1, an attacker has three pure combined strategies leading to its pure strategy set S_A.

$$\begin{aligned} S_A &= \{s_{a1}, s_{a2}, s_{a3}\} \\ &= \{[AU,AnO], [AL,AnO], [NAL,NAnO]\} \end{aligned} \quad (1)$$

where $[XY_1, XY_2]$ means that the attacker performs action X at the sensing frame and then Y_1 or Y_2 at the data frame depending on "*busy*" or "*idle*" state of the channel. Similarly, the pure strategy set S_D of a defender is as follows

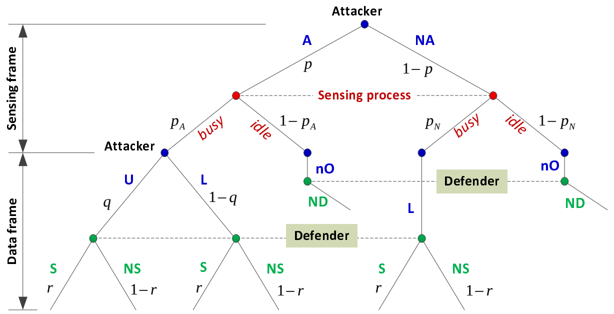

Fig. 1. The channel surveillance game

$$S_D = \{s_{d1}, s_{d2}\} = \{[S,ND], [NS,ND]\} \quad (2)$$

where $[X, Y]$ means that the defender implements action X or Y at data frame depending on "*busy*" or "*idle*" state of the channel.

In practice, the players choose their actions based on a so-called mixed-strategy. For an attacker, it is defined by

$$\sigma_A = \{\sigma_{a1}, \sigma_{a2}, \sigma_{a3}\} \quad (3)$$

where σ_{ai} is the probability of selecting the pure strategy s_{ai}. For a defender, we have

$$\sigma_D = \{\sigma_{d1}, \sigma_{d2}\} \quad (4)$$

where σ_{di} is the probability of selecting the pure strategy s_{di}.

In Fig. 1, we introduce p and q the probabilities of action A and action U of the attacker, and r the probability of the action S of the defender. As the game in Fig. 1 is the game with perfect recall, we have [18]

$$\begin{cases} p = \sigma_{a1} + \sigma_{a2}, \\ q = \sigma_{a1}/(\sigma_{a1} + \sigma_{a2}), \\ r = \sigma_{d1}. \end{cases} \quad (5)$$

The objective of the paper is to find the values of p, q, and r, or equivalently, of σ_{a1}, σ_{a2}, and σ_{d1} leading to NE.

To calculate the NE, we need to introduce payoffs for each player's action as below:

- C_A: cost for implementing PUE attack
- C_U: cost for transmitting data at data frame
- G_U: benefit/gain for using the channel at one data frame
- ϕ_C: penalty for being captured by the defender.
- C_S: cost for implementing the surveillance process
- G_S; benefit/gain for capturing illegal attacker during the surveillance process of data frame

In addition, three probabilities, already displayed in Fig. 1, have to be defined as follows:

- p_A: probability the answer of the sensing engine is busy when the attacker's action is A.
- p_N: probability the answer of the sensing engine is busy when the attacker's action is NA.

TABLE I
ACTIONS PAYOFFS FOR ATTACKER AND DEFENDER

Actions	**Attacker payoff**	**Defender payoff**
$a;d$	$P_A^{a;d}$	$P_D^{a;d}$
AU;S	$-C_A - C_U + \rho_A G_U - \rho_A \phi_C$	$-C_S + \rho_A G_S$
AU;NS	$-C_A - C_U + \rho_A G_U$	0
AL;S	$-C_A$	$-C_S$
AL;N	$-C_A$	0
AnO;ND	$-C_A$	0
NAL;S	0	$-C_S$
NAL;NS	0	0
NAnO;ND	0	0

TABLE II
STRATEGIES PAYOFF MATRIX OF THE INDUCED NORMAL GAME

	$s_{d1} = [\mathit{S,ND}]$	$s_{d2} = [\mathit{NS,ND}]$
$s_{a1} = [\mathit{AU,AnO}]$	$[P_A^{s_{a1};s_{d1}}, P_D^{s_{a1};s_{d1}}]$	$[P_A^{s_{a1};s_{d2}}, P_D^{s_{a1};s_{d2}}]$
$s_{a2} = [\mathit{AL,AnO}]$	$[P_A^{s_{a2};s_{d1}}, P_D^{s_{a2};s_{d1}}]$	$[P_A^{s_{a2};s_{d2}}, P_D^{s_{a2};s_{d2}}]$
$s_{a3} = [\mathit{NAL,NAnO}]$	$[P_A^{s_{a3};s_{d1}}, P_D^{s_{a3};s_{d1}}]$	$[P_A^{s_{a3};s_{d2}}, P_D^{s_{a3};s_{d2}}]$

- ρ_A: probability primary user is inactive while the sensing engine claims busy and the attacker attacks.

Payoffs for each pair of attacker and defender actions are given on Table I. According to Eqs. (1)-(2) and Fig. 1, the game can be seen as a game with two players whose the normal form is provided by Table II, where the payoffs for each strategy can be derived from the payoffs of each action as follows:

$$\begin{aligned}
P_X^{s_{a1};s_{d1}} &= p_A P_X^{\mathit{AU;S}} + (1-p_A) P_X^{\mathit{AnO;ND}} \\
P_X^{s_{a1};s_{d2}} &= p_A P_X^{\mathit{AU;NS}} + (1-p_A) P_X^{\mathit{AnO;ND}} \\
P_X^{s_{a2};s_{d1}} &= p_A P_X^{\mathit{AL;S}} + (1-p_A) P_X^{\mathit{AnO;ND}} \\
P_X^{s_{a2};s_{d2}} &= p_A P_X^{\mathit{AL;NS}} + (1-p_A) P_X^{\mathit{AnO;ND}} \\
P_X^{s_{a3};s_{d1}} &= p_N P_X^{\mathit{NAL;S}} + (1-p_N) P_X^{\mathit{NAnO;ND}} \\
P_X^{s_{a3};s_{d2}} &= p_N P_X^{\mathit{NAL;NS}} + (1-p_N) P_X^{\mathit{NAnO;ND}}
\end{aligned}$$

with X equal to either A for attacker or D for defender.

Finally, their expected payoffs, also called utilities, are

$$\begin{aligned}
U_A(\sigma_A, \sigma_D) &= \sum_{i=1}^{3}\sum_{j=1}^{2} \sigma_{ai}\sigma_{dj} P_A^{s_{ai};s_{dj}} = \sum_{i=1}^{3} \sigma_{ai} U_A^{s_{ai}} \\
U_D(\sigma_A, \sigma_D) &= \sum_{i=1}^{3}\sum_{j=1}^{2} \sigma_{ai}\sigma_{dj} P_D^{s_{ai};s_{dj}} = \sum_{j=1}^{2} \sigma_{dj} U_D^{s_{dj}}
\end{aligned}$$

where $U_A^{s_{ai}}$ and $U_D^{s_{dj}}$ are the expected payoff for each pure strategy of the attacker and the defender over all of the opponent's strategies respectively.

IV. NASH EQUILIBRIUM

The Nash equilibrium (NE) is the point where each player in a game has selected the best response (BR) (or one of the BRs) to the other players' strategies. The BR is the strategy on which a player gains the highest payoff given other players' strategies [17]. If $\{\sigma_A^*, \sigma_D^*\}$ is a NE of our game, then

$$\begin{cases} U_A(\sigma_A^*, \sigma_D^*) \geq U_A(\sigma_A, \sigma_D^*), \forall \sigma_A \\ U_D(\sigma_A^*, \sigma_D^*) \geq U_D(\sigma_A^*, \sigma_D), \forall \sigma_D \end{cases} \tag{6}$$

To find the NE, we first need to calculate $U_A^{s_{ai}}$. One can easily check that

$$\begin{cases} U_A^{s_{a1}} = B_U - C_A - p_A \rho_A \sigma_{d1} \\ U_A^{s_{a2}} = -C_A \\ U_A^{s_{a3}} = 0 \end{cases} \tag{7}$$

where $B_U = p_A(\rho_A G_U - C_U)$. As $U_A^{s_{a2}} < U_A^{s_{a3}}$, the BR of the attacker can only be a selection between s_{a1} and s_{a3}. Thanks to simple algebraic manipulations, we obtain the following BR function for the attacker:

$$\sigma_A^{BR} = \begin{cases} s_{a3} & \text{if} \quad C_A \geq B_U \\ f(\sigma_{d1}) & \text{if} \quad B_U^C < C_A < B_U \\ s_{a1} & \text{if} \quad C_A \leq B_U^C \end{cases} \tag{8}$$

where $B_U^C = B_U - p_A \rho_A \phi_C$ and

$$f(\sigma_{d1}) = \begin{cases} s_{a1} & \text{if} \quad \sigma_{d1} < \sigma_{d1}^{(0)} \\ \sigma_{a1} s_{a1} + (1-\sigma_{a1}) s_{a3} & \text{if} \quad \sigma_{d1} = \sigma_{d1}^{(0)} \\ s_{a3} & \text{if} \quad \sigma_{d1} > \sigma_{d1}^{(0)} \end{cases}, \tag{9}$$

and $\sigma_{d1}^{(0)} = (B_U - C_A)/(p_A \rho_A \phi_C)$. The second row in Eq. (9) means that the BR is a mixed strategy with probability σ_{a1} for action s_{a1}. Similar derivations can be done for obtaining σ_D^{BR} in closed-form. Then by finding the intersection between both BR functions (σ_A^{BR}, σ_D^{BR}), we obtain the NE of the proposed game.

Result 1. *The NE for the mixed strategies of the game given in Table II is computed as follows:*

$$\begin{aligned}
&\mathit{If}\ C_A \geq B_U, && \sigma_{a1}^* = 0, \sigma_{a2}^* = 0, \sigma_{d1}^* = 0 && \text{(10a)} \\
&\mathit{If}\ C_A < B_U, && && \\
&\qquad G_S \leq G_0 \Rightarrow && \sigma_{a1}^* = 1, \sigma_{a2}^* = 0, \sigma_{d1}^* = 0 && \text{(10b)} \\
&\qquad G_S > G_0 \Rightarrow && \sigma_{a1}^* = \sigma_{a1}^{(0)}, \sigma_{a2}^* = 0, \sigma_{d1}^* = \sigma_{d1}^{(0)} && \text{(10c)} \\
& && (\mathit{if}\ C_A > B_U^C) && \\
& && \sigma_{a1}^* = 1, \sigma_{a2}^* = 0, \sigma_{d1}^* = 1 && \text{(10d)} \\
& && (\mathit{if}\ C_A \leq B_U^C) &&
\end{aligned}$$

where $\sigma_{a1}^{(0)} = p_N C_S/(p_A \rho_A G_S - (p_A - p_N) C_S)$.

Substituting Eq. (10) into Eq. (5) leads to the NE of the probabilities p, q, and r.

Hereafter, we interpret Result 1. When the implementing PUE attack cost C_A is too high (Eq. (10a)) , the NE says the attacker to stay inactive ($s_{a3}^* = 1$). Then the defender does not have to monitor the channel ($\sigma_{d2}^* = 1$). Similarly, when the gain for capturing illegal attacker G_S is too weak, the 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 Eq. (10c)) and our result shows the values to choose.

When the attack 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 $\phi_C = k_C G_U$ 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, the NE depends on the network demand k_b, and Eqs. (10) are equivalent to*

$$\begin{array}{lll}
\text{If } k_b \le K_0, & & \sigma^*_{a1} = 1, \sigma^*_{a2} = 0, \sigma^*_{d1} = 0 \\
\text{If } k_b > K_0, & & \\
\quad k_C > K^1_C & \Rightarrow & \sigma^*_{a1} = \sigma^{(0)}_{a1}, \sigma^*_{a2} = 0, \sigma^*_{d1} = \sigma^{(0)}_{d1} \\
\quad k_C \le K^1_C & \Rightarrow & \sigma^*_{a1} = 1, \sigma^*_{a2} = 0, \sigma^*_{d1} = 1
\end{array}$$

with $K_0 = C_S/(k_C \rho_A G_U)$, $K^1_C = (B_U - C_A)/(p_A \rho_A G_U)$.

Remark 2. *Let $C_A < B_U$. If k_b is fixed, the NE depends on the penalty factor k_C, and Eqs. (10) are equivalent to*

$$\begin{array}{lll}
\text{If } k_C \le K^0_C, & & \sigma^*_{a1} = 1, \sigma^*_{a2} = 0, \sigma^*_{d1} = 0 \\
\text{If } k_C > K^0_C, & & \\
\quad k_b \le K_1 & \Rightarrow & \sigma^*_{a1} = \sigma^{(0)}_{a1}, \sigma^*_{a2} = 0, \sigma^*_{d1} = \sigma^{(0)}_{d1} \\
\quad k_b > K_1 & \Rightarrow & \sigma^*_{a1} = \sigma^{(0)}_{a1}, \sigma^*_{a2} = 0, \sigma^*_{d1} = \sigma^{(0)}_{d1} \\
 & & (\text{if } k_C > K^1_C) \\
 & & \sigma^*_{a1} = 1, \sigma^*_{a2} = 0, \sigma^*_{d1} = 1 \\
 & & (\text{if } k_C \le K^1_C)
\end{array}$$

with $K_1 = p_A C_S/(B_U - C_A)$, $K^0_C = C_S/(k_b \rho_A G_U)$.

V. Simulation Results

In order to confirm the correctness of the above analysis, numerical simulations of the NE have also been carried out with the Lemke-Howson (L-H) algorithm [19]–[21]. Without loss of generality, we only consider the most interesting case ($C_A < B_U$). Actually, $C_A = 10$, $C_S = 0.4C_A$, $C_U = 0.3C_A$, and $G_U = 5C_A$. The probabilities of false alarm and detection of the system are 0.1 and 0.9 respectively. The presence probability of primary signal is 0.5.

Fig. 2 shows the NE obtained by the theoretical analysis and the L-H algorithm with respect to network demand k_b for a low penalty factor $k_C = 0.4 < K^1_C$, and a high penalty factor $k_C = 3 > K^1_C$. We observe the perfect agreement between the theoretical analysis given in Remark 1 and simulated results. For low k_C (see Fig. 2(a)), the NE strategy of the attacker is to select 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. 2(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.

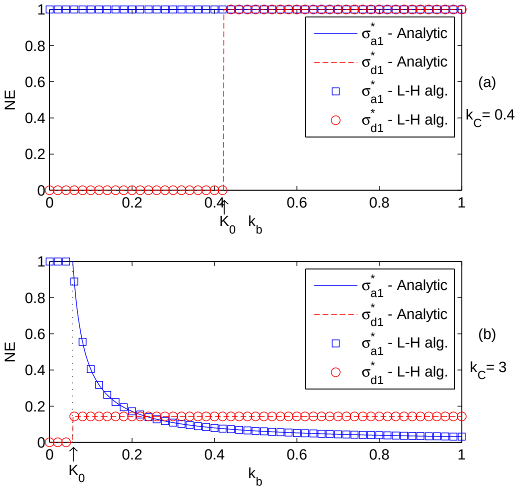

Fig. 2. NE vs. k_b when (a) $k_C = 0.4 < K^1_C$ or (b) $k_C = 3 > K^1_C$

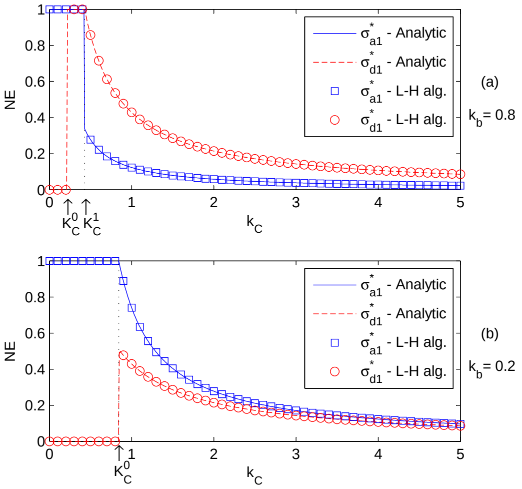

Fig. 3. NE vs. k_C when (a) $k_b = 0.8 > K_1$ or (b) $k_b = 0.2 < K_1$

In Fig. 3, 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.

VI. Conclusion

We have discussed a game theory-based approach to counteract the security problem of selfish PUE attack in CR networks. The formulated game was a non-zero-sum game with incomplete information for the selfish PUE attack and surveillance process. Nash Equilibrium (NE) has been expressed in closed form. The results showed a close relationship between the network demand and the penalty ratio at NE. Numerical simulations confirmed our claims.

REFERENCES

[1] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, ”Senseless: A database-driven white spaces network,” IEEE Symposia on New Frontiers in Dynamic Spectrum Access Networks, DySpan, 2011.

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

[3] R. Chen, J.M. Park, and K. Bian, “Robust Distributed Spectrum Sensing in Cognitive Radio Networks,” IEEE Conference on Computer Communications, INFOCOM, pp.1876-1884, April 2008.

[4] P. Kaligineedi, M. Khabbazian, and V.K. Bhargava, “Secure cooperative sensing techniques for cognitive radio systems, IEEE International Conference on Communications, ICC, pp.34063410, 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. E92.B, pp. 3644-3652, 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.R. 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.H. 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] 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, Mar. 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, Nov. 2010.

[12] Q. Peng, P.C. Cosman, and L.B. 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, 2009.

[14] E. Hossain, et al., Dynamic Spectrum Access and Management in Cognitive Radio Networks: Cambridge University Press, 2009.

[15] B. Wang, et al., ”Game theory for cognitive radio networks: An overview,” Computer Networks, vol. 54, pp. 2537-2561, 2010.

[16] J.C. Harsanyi, ”Games with Incomplete Information Played by ”Bayesian” Players, I-III,” Manage. Sci., vol. 50, pp. 1804-1817, 2004.

[17] R. Gibbons, “Game Theory for Applied Economics,” Princeton University Press, Princeton, 1992.

[18] H.W. Kuhn, “Extensive Games and the Problem of Information” Contributions to the Theory of Games, vol. II, pp. 193-216, 1953; reprinted in H.W. Kuhn (ed.) Classics in Game Theory, Princeton University Press, 1997.

[19] C. E. Lemke and J. T. Howson, “Equilibrium Points of Bimatrix Games,” Journal of the Society for Industrial and Applied Mathematics, vol. 12, pp. 413-423, 1964.

[20] S. Gabriel, et al., “Equilibria and Complementarity Problems,” in Complementarity Modeling in Energy Markets. vol. 180, ed: Springer New York, pp. 127-179, 2013.

[21] P. W. Goldberg, et al., “The Complexity of the Homotopy Method, Equilibrium Selection, and Lemke-Howson Solutions,” ACM Trans. Econ. Comput., vol. 1, pp. 1-25, 2013.