コグニティブ無線ネットワークでPUE攻撃に対するゼロサムゲームを用いる対策

郝　東† 櫻井 幸一†

†九州大学大学院システム情報科学府
{haodong, sakurai}@itslab.csce.kyushu-u.ac.jp

あらまし コグニティブ無線では、PUE攻撃という二次利用者に対するサービス拒否攻撃である。攻撃者が一次利用者と類似なシグナルを放送することで、特定な周波数帯域を占有する。二次利用者は攻撃者からのシグナルを感知したら、現在の周波数帯域が一次利用者に使用されていることを誤認識してしまい、この周波数帯域の使用を諦める。攻撃者と防御者の相互行為がゼロサムゲームと認められる。このゲームで、攻撃者がある確率で特定な周波数帯域にシグナルを送信する。同じように、防御者もある確率で特定な周波数帯域を感知する。本稿では、微分ゲーム理論を用い、攻撃—防御シナリオの分析に基づき、ナッシュ均衡により、最適な防御戦略を制定した。

A Zero-Sum Game based Approach for Primary User Emulation Attack in Cognitive Radio Network

Dong Hao†* Kouichi Sakurai†

†Graduate School of Information Science and Electrical Engineering, Kyushu University
{haodong, sakurai}@itslab.csce.kyushu-u.ac.jp

Abstract

In cognitive radio networks, primary user emulation (PUE) attack is a denial-of-service (DoS) attack on secondary users. It means that a malicious attacker send primary-user-like signals to jam certain spectrum channels during the spectrum sensing period. Sensing the signals, the legitimate secondary users will regard these channels are used by the primary users, therefore do not use the corresponding channels. The interaction between the PUE attacker and the secondary user (defender) can be seen as a two-player zero-sum game. The attacker (defender) randomly choose the probability for jamming (sensing) a certain set of spectrum channels. In the real case, the sensing will repeat every 6ms, so the attacking (sensing) can be viewed as a continuous time attack-defense process. We utilize differential game theory to analyze this time-continuous attack/defense scenario. The Nash equilibrium is deprived, and the optimal anti-PUE attack strategy is obtained.

1 Introduction

1.1 Background and Related Works

Cognitive radio is an innovative and promising technology that enables the intelligent ra-

*Dong HAO is a Ph.D candidate at Kyushu University and he is supported by the governmental scholarship from China Scholarship Council.

dios to sense and learn form their spectrum environments. The cognitive radio networks offers various technical to solve the conflict between the limited spectrum resources and the increasing demand for wireless services. This cognitive radio networks consist of two kinds of users: primary user and secondary user. Primary users are those who are licensed to access the spectrum channels, while the secondary users can opportunistically utilize the channels after they sensed the primary user is idle. Cognitive radio is a key technology that leading us to the next generation networks (xG).

In cognitive radio networks, to interrupt the spectrum sensing and using, the malicious attackers can launch various of attacks in different layers. Among these attacks, the *primary user emulation attack* is more dangerous. In primary user attack, the malicious attacker send jamming signals which have the same characteristic as the signals from the primary users. On detecting the jamming signals, the legitimate and selfish users can not distinguish them from the signals sent by the primary users, which is actually a false alarm. As a result, these normal users will quit the spectrum band, and choose other bands.

For mitigating primary user emulation attack, Chen and J.M Park proposed a proactive detection scheme[3]. The attacker is identified by comparing the received signal characteristic. Their approach is on the assumption that the attacker's transmission power is considerably less than the primary users. Beibei Wang, et.al proposed a stochastic game based spectrum sensing and reserving scheme[2]. Minimax-Q learning scheme is used for the secondary user to find their best strategies. Husheng Li and Zhu Han proposed a passive anti-PUE approach. In their approach, the strategy for the attacker (secondary) user is to randomly jam (sense) a subset of spectrum bands, and defender can avoid PUE attack by random frequency hopping. Their scheme is under the assumption that the attack will repeat limited times and there are not too many frequency bands.

In the previous PUE attack/defense games, the authors mostly assume the game is in discrete time horizon. However, in the real case, every 6ms, the secondary user will sense the spectrum[7]. On the contrary, the attacker will also attack the spectrum frequency every 6ms. As a result, the attack-defense game can be seen as a infinite round game in continuous time horizon.

1.2 Challenging Issues

*(1)*Most of the previous works on security issues in cognitive radio networks only provide qualitative analysis about countermeasures, but they neglect that the cognitive attacker has the capability to adjust their attacking strategy. When the attackers change their attack strategies, the situation will inevitably become more complicated and server.

*(2)*The the secondary user will sense the spectrum every 6ms[7]. With in a single day, the attack may happen tremendous times. As the time interval becomes so small, the long-term repeated attack/defense game can be seen as time continues. Previous game theory based solutions only focus on discrete time instance, however, how to deal with such continuous time case is a open problem.

1.3 Main Contribution

*(1)*Sticking to the first challenging issue, to properly analyze the changing attack strategy, we utilize game theory to construct the model for the interaction between the PUE attacker and the defender(secondary user). By using game theory, we derived the optimal attack and defense strategies(Nash equilibrium), and

indicate the best attack/defense strategy for both the attacker and the defender.

(2) We utilize the differential game to analyze this time continuous PUE attack. Based on the differential attack game model, we find the Nash equilibrium by optimal control theory. The advantage of our differential attack-defense game model is that it provides a general analyze framework, and can be well solved by existed theories.

2 One-Shot PUE Attack Game

We consider a cognitive radio network, which consists of one primary user (PU) and multiple secondary users (SUs). The secondary user can sense the spectrums, if the primary user is not busy, the SU can access the spectrum opportunistically. Besides the PU and SUs, suppose that there are multiple attackers. The attackers pretend to be the primary user, and send signals into various of channels. If the secondary use senses that the PU is busy in the channel i, it will give up using channel i.

We first consider the single round PUE attack. In this attack game, the players are the PUE attackers and the secondary users. We define Θ be the set of channels that are jammed by the attacker, and $|\Theta| \leq L$. We define Ω be the set of channels that are sensed by the secondary users. Since the attackers can not attack all the channel at the same time, and the secondary users can not sense all the channels at the same time, we define the attacker will attacker the set of channels $|\Theta|$ with probability $u(\Theta)$, and the secondary user will sense the channels Ω with probability $v(\Omega)$.

The probability for a certain channel i is sensed by the secondary users is $u(\Omega)$, while the probability for this channel i is not attacked by the attackers is $1-v(\Theta)$. Therefore, the total probability that channel i is sensed by the secondary users, and not attacked by the attacker is defined as:

$$(1 - v(\Omega)) \cdot u(\Theta)$$

Taking into consideration the probability for the primary user to appear tin the channel i is p_i, the overall probability that channel i can be well utilized by the secondary user is derived as:

$$p_{iI} \left(1 - v(\Omega)\right) \left(u(\Theta)\right)$$

Note that K is the total number of all the channels. Then taking into consideration of the probability above, we can define the utility for the secondary users as:

$$U_s(\sigma_A, \sigma_D) = \sum_{i=1}^{K} p_{iI} \left(1 - v(\Omega)\right) \cdot u(\Theta)$$

3 Equilibrium for One-Shot PUE Attack Game

In game theory, for the zero-sum two player game, the Nash equilibrium can be solved by using the min-max rule. The min-max rule, in the field of network security, is the defender first look the maximum damages that an attacker can cause, and then tries to minimum this maximum damages. For the attacker, it first look the maximum utility that the secondary user can reach, and then minimize this possible maximum utility.

The attacker's optimal strategy is derived by using:

$$\sigma_S^* = Arg \max_{\sigma_D} \min_{\sigma_A} R(\sigma_A, \sigma_S)$$

And the secondary user's optimal strategy is derived by using:

$$\sigma_A^* = Arg \min_{\sigma_A} \max_{\sigma_D} R(\sigma_A, \sigma_S)$$

To obtain the result of σ_S^* and σ_A^*, we can use similar approach. The secondary user's utility function is a linear function of its strategy $u(\Theta)$. Because the attacker wants to minimize the utility of the secondary user, it should

make some $1-v(\Omega)=0$, which means it should attack a certain set of channel Ω with probability 1. To minimize the value of $U_s(\sigma_A, \sigma_D$, the attacker should choose the set of channels which have the largest value of $u(\Theta)$. Because both the attackers and the secondary users are rational, and they can predict the possible strategies of the opponent. In the view of the secondary user, it can predict the fact that the attacker wants to attack those channels which have the largest value of $u(\Theta)$, therefore, its best strategy is to make the probability for sensing each channel equal. If not, the set of channels which has the largest value of $u(\Theta)$ will be definitely attacked.

According to the statement above, according to the min-max rules, the optimal strategy for the secondary user is:

$$u_i = \frac{C_1}{p_{iI}}$$

where C_1 is a constant.

Because the probability for sensing the different channels is a probability distribution over the different K channels, we have the following constrains:

$$\sum_{i=1}^{K} v_i = 1$$

.

Therefore, by combining the above two function, we can get the formalized strategy for the secondary user, which is denoted as:

$$u_i = \frac{\frac{C_1}{p_{iI}}}{\sum\limits_{i=1}^{K} \frac{C_1}{p_{iI}}}$$

On the contrary, by using the similar approach, we find the optimal strategy for the attacker, which is denoted as:

$$1 - \sum_{i \in \Theta} v(\Theta) = \frac{C_2}{p_{iI}}$$

.

And these u_i and v_i forms the Nash equilibrium for the single stage PUE attack game. In this equilibrium, neither the secondary user nor the attacker wants to unilaterally change its sense (attack) strategy. Because if it deviate from the Nash equilibrium, its utility will decrease. The Nash equilibrium is just the stable point of the one-shot primary user emulation attack.

4 Multi-Round PUE Attack Game

In the last section, we investigated the one-shot PUE attack. However, the one shot attack is not corresponding to the real scenario. According to the previous researches, in the real circumstances, the cognitive radio sensing may happen every 6ms. That mean within one day, the spectrum sensing may already repeats many times. Since the spectrum sensing repeats within very shot period, and it repeats many many times, it can be viewed as infinite times repetition of the spectrum sensing. On the other hand, for the PUE attackers, because the secondary user senses the spectrum every 6ms, to maximize its own attack effect, the attackers may also send jamming signals to the spectrum every 6ms. Therefore, the PUE attack game may repeat huge number of times within one day. It is better to see the attack game as time-continuous. And we will utilize the differential game to analyze the multi-roudn PUE attack.

We define the state of the game as : $\chi = (x_1, ..., x_t, ..., x_T)$, where each x_t is the states of the PUE attack game at time instance t. And we denote $\dot{x}_t$ as the changing rate of the variable x_t at time instance t. $\dot{x}_t$ is subject to:

(1) How many spectrums are not used by the secondary users: $K - x_t + \lambda$ Where K is the total number of channels. λ is the number of spectrum that released by some secondary users at time instance t. λ is with respect to

the Poisson process:

$$P[(N(t+dt)) - N(t) = k] = \frac{e^{-\lambda dt}(\lambda dt)}{k!}$$

(2) $\dot{x}_t$ is also subject to the strategies of the secondary users and the attacker. As we denoted before, $\sum_{i=1}^{N} u_i^m$ is the total probability for the channel m to be sensed by the secondary users. $\sum_{j=1}^{L} v_j^m$ is the total probability for the channel m to be attacked by the attacker. Therefore, the probability that channel m is sensed by the secondary user but not attacked buy the attacker, is defined as:

$$\sum_{i=1}^{N} u_i^m \times (1 - \sum_{j=1}^{L} v_j^m)$$

According to the above two conditions, the changing rate of x_t at time instance t, is defined as:

$$\dot{x}_t = \sum_{k=1}^{(M-x_t+\lambda)} [\sum_{i=1}^{N} u_i^m \times (1 - \sum_{j=1}^{L} v_j^m)];$$
$$x_0 = 0$$

This is the changing rate of the number of spectrum that is available to use for the secondary users. In the cognitive radio network, the most important resource is the availability of the spectrum. Thus, for the secondary users, this criteria can be viewed as its utility. The changing rate of x_t can be seen as the changing rate of the secondary user's utility at a certain time instance t. If we consider the life time of the cognitive radio network, between $[0, T]$, the long term overall spectrum availability for the secondary users can be defined as a integration of the changing rate of the availability of the spectrum, during time period $[0, T]$: $\int_0^T x_t dt$.

5 Equilibrium for Multi-Round PUE Attack Game

Based on this spectrum availability, we defined the overall utility for the secondary user as:

$$J_s(\mu, \omega) = \int_0^T x_t dt - \alpha \int_0^T \mu_t dt$$

where α is related to the power consuming for sensing the spectrums. The secondary user wants to maximize this utility function.

and we also define the overall utility of the attacker

$$J_a(\mu, \omega) = \int_0^T x_t dt + \beta \int_0^T \omega_t dt$$

where β is related to the power consuming for jamming a certain spectrums. The attacker want to minimize this function.

For analysis, we define a integrated utility function for the jamming attack game as:

$$G(\mu, \omega) = \int_0^T x_t dt - \alpha \int_0^T \mu_t dt + \beta \int_0^T \omega_t dt$$

Define Φ as the policies set of the secondary users, Ψ as the policies set of the attacker, then we define: $\mu^* \in \Phi$ and $\omega^* \in \Psi$ as the saddle point policies for the jamming attack game. For the secondary user, it wants to maximize the above utility function, and for the attacker, it wants to minimize the above utility function. Therefore, we come to another min-max problem:

$$\overline{V} = \max_{\mu \in \Phi} \min_{\omega \in \Psi} G(\mu, \omega)$$

$$\underline{V} = \min_{\omega \in \Psi} \max_{\mu \in \Phi} G(\mu, \omega)$$

From these two functions, we can get μ^* which is the optimal strategy for secondary users if $\max_{\mu \in \Phi} \min_{\omega \in \Psi} G(\mu^*, \omega)$ is satisfied; while ω^* is the optimal strategy for the attackers if the rule $\min_{\omega \in \Psi} \max_{\mu \in \Phi} G(\mu, \omega^*)$ is satisfied.

According to the utility function, and the changing rate of x_t, following the standard derivation of open-loop saddle point solution for Nash equilibrium, we have the single Hamiltonian:

$$H(u, v; x, p) = -\alpha u + \beta v + pu(1 - v)$$

which will be maximized over $u \in [0,1]$. Here p is called co-state coefficient, and it will satisfy the following equation:

$$\dot{p} = -\frac{\partial H}{\partial x} = pu(1-v),\ p(T) = 0$$

For the Hamiltonian function, the secondary user wants to maximize it, while the attacker wants to minimize it. If there exists a saddle point solution (u^*, v^*), which satisfy:

$$\max_{u\in[0,1]} H(u, v^*; x, p)$$
$$= \min_{v\in[0,1]} H(u^*, v; x, p) = H(u^*, v^*; x, p)$$

This saddle point is the Nash equilibrium of this differential game, which maximizes the value of $H(u, v; x, p)$ over $u \in [0,1]$ for each $v \in [0,1]$, and minimizes it over $v \in [0,1]$ for each $u \in [0,1]$, we get the final solution.

6 Conclusion

The primary user emulation attack put severe security threat to the secondary users in the cognitive radio networks. The primary user emulation attackers can intelligently choose various of channels to jam, trying to minimize the usability of the free spectrum. The secondary users can also adjust their strategies for sensing the spectrum. The interaction between the attackers and secondary users can be modeled as a two-player zero-sum game. We analyze the single round attack game, find the Nash equilibrium which is the stable point for both the attacker and and the secondary users. We also extend the single round attack game into time continuous multi-round attack game. By utilizing the differential game theory, we find the equilibrium of the multi-round PUE attack game. The result can be used to guide the secondary users to defend against the primary user emulation attack.

参考文献

[1] J. Mitola; "Cognitive radio: an integrated agent architecture for software defined radio" Ph.D. dissertation, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.

[2] B. Wang and K. J. R. Liu, "Advances in cognitive radios: a survey" to appear, IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, FEBRUARY 2011

[3] Ruiliang Chen; Jung-Min Park; Kaigui Bian; "Robust Distributed Spectrum Sensing in Cognitive Radio Networks" INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , vol., no., pp.1876-1884, 13-18 April 2008

[4] Husheng Li and Zhu Han; "Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems, part I: known channel statistics"; IEEE Trans. Wireless. Comm. 9, 11 (November 2010), 3566-3577. DOI=10.1109/TWC.2010.091510.100629

[5] Husheng Li, Zhu Han; "Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems"; Proceedings of the 28th IEEE conference on Global telecommunications, p.1511-1516, November 30-December 04, 2009, Honolulu, Hawaii, USA

[6] A. Bressan and F. Priuli, Infinite horizon noncooperative differential games, J. Differential Equations 227 (2006), pp. 230C257.

[7] Kelvin Lancaster; "The Dynamic Inefficiency of Capitalism"; The Journal of Political Economy Vol. 81, No. 5 (Sep. - Oct., 1973), pp. 1092-1109

[8] Y. Pei, Y.-C. Liang, K. Teh, and K. Li, How much time is needed for wideband spectrum sensing?, IEEE Trans. Wireless Commun., vol. 8, no. 11, pp. 5466C5471, Nov. 2009.

[9] R. Gibbons, *Game Theory for Applied Economics*, Princeton University Press. Princeton. NJ. 1992.

[10] T. Alpcan, T. Basar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, November 30, 2010