Journal of Southeast University (English Edition) Vol. 34, No. 4, pp. 423 - 429 Dec. 2018 ISSN 1003—7985

A game-theory approach against Byzantine attack in cooperative spectrum sensing

Wu Jun Song Tiecheng Yu Yue Hu Jing

(School of Information Science and Engineering, Southeast University, Nanjing 211189, China)

Abstract: In order to solve the Byzantine attack problem in cooperative spectrum sensing, a non-cooperative game-theory approach is proposed to realize an effective Byzantine defense. First, under the framework of the proposed non-cooperative game theory, the pure Byzantine attack strategy and defense strategy in cooperative spectrum sensing are analyzed from the perspective of the Byzantine attacker and network administrator. The cost and benefit of the pure strategy on both sides are defined. Secondly, the mixed attack and defense strategy are also derived. The closed form Nash equilibrium is obtained by the Lemke-Howson algorithm. Furthermore, the impact of the benefit ratio and penalty rate on the dynamic process of the non-cooperative game is analyzed. Numerical simulation results show that the proposed game-theory approach can effectively defend against the Byzantine attack and save the defensive cost.

Key words: cooperative spectrum sensing; Byzantine attack; game theory; non-cooperative game; Nash equilibrium

DOI: 10.3969/j.issn.1003-7985.2018.04.002

Cognitive radio (CR) has become a promising technique to solve spectrum scarcity issues. Spectrum sensing unit as an essential of a CR is exploited to identify those frequency bands unused by the primary users (PU), but without causing harmful interference to the primary network. However, the individual secondary user (SU) is unable to accurately detect the primary signal due to the factors such as noise uncertainty, multipath fading, shadowing, etc. Therefore, cooperative spectrum sensing is proposed as an elegant solution to exploiting spatial diversity gain to make a more accurate decision about the PU's status. Nevertheless, due to the open characteristics of cognitive radio networks (CRNs), security vulnerability can be exploited by different types of attacks[1] that is launched in the process of cooperative spectrum sensing, such as the primary user emulation attack (PUEA) and Byzantine attack.

PUEA, one of the most representative attack types in the aspect of PU, mimics incumbent signals in order to cause denial-of-service (DoS) attacks, especially in distributed networks. They can cooperate and transmit fake incumbent signals, thus making SUs hop from band to band and severely disrupting their operation[2]. A Byzantine attack, also called spectrum sensing data falsification (SSDF), was first proposed by Lamport et al[3]. It manifests in that the attacker sends false observations with the intention of confusing other SUs or the fusion center (FC). Their aims are to lead the FC or other users to falsely conclude whether there is an ongoing incumbent transmission or not[2]. Different from PUEA, the Byzantine attack in cooperative spectrum sensing is a typical example of SU attack.

Recently, game theory has become an important tool, which is ideal and essential in studying, modeling, and analyzing the interaction among independent, and self-interested players. Moreover, it has been extensively used in the communication field[4]. Hence, some research related to the game theory progressively permeates the security of cooperative spectrum sensing, whereas most research directions only focus on combatting PUEA[5-11] and seldom apply the game theory in addressing the Byzantine attack problem. Several methods, such as two attack-prevention mechanisms with direct and indirect punishments, and the credit weighting scheme[12], have been proposed to mitigate the adverse effects of a Byzantine attack on cooperative spectrum sensing, such as, a cooperative spectrum sensing scheme based on the evidence theory[13] and a two-stage credit threshold scheme[14]. Besides, Wang et al.[15] presented the evidential reasoning-cooperative spectrum sensing scheme in dealing with the spectrum sensing problems in the presence of a false alarm (FA) and false alarm and miss detection (FAMD) attacks (such attacks are still a Byzantine attack on essence) on CRNs. Wu et al.[16] proposed a robust data fusion scheme, named the robust weighted sequential probability ratio test, against various Byzantine attack probabilities. The comprehensive study on the recent advances in Byzantine attack and defense for cooperative spectrum sensing was also surveyed[17].

However, these Byzantine mitigation methods derive from defense or protection mechanisms, and the cost and

Received 2018-03-29, **Revised** 2018-08-25.

Biographies: Wu Jun (1988—), male, Ph. D. candidate; Song Tiecheng (corresponding author), male, doctor, professor, songtc@seu.edu.cn.

Foundation item: The National Natural Science Foundation of China (No. 61771126).

Citation: Wu Jun, Song Tiecheng, Yu Yue, et al. A game-theory approach against Byzantine attack in cooperative spectrum sensing[J]. Journal of Southeast University (English Edition), 2018, 34(4): 423 - 429. DOI: 10.3969/j.issn.1003-7985.2018.04.002.

benefit of both the attacker and defender can often be ignored. How often and when to defend against a Byzantine attack can satisfy the demand of the network security under cost management remains to be explored. Defending against the Byzantine attacker that acts in a tragic manner is relatively more complex and challenging. To tackle this challenge, in this paper, the malicious attack behavior of malicious SUs instead of PUs is our special concern. Both various Byzantine attacks and the defensive efficiency are considered by the game-theory approach, since a positive or negative defense will cause resource waste or insufficient protection when the network suffers from a Byzantine attack at different levels. A non-cooperative game with incomplete information is formulated between the attacker and the defender. Furthermore, the benefit ratio and penalty rate are designed to analyze the Nash equilibrium (NE) of the game. In addition, various attack strategies and the cost-benefit of defense are considered.

1 System Model

1.1 Network model

Consider an infrastructure-based network consisting of a PU networks and a CRN under the IEEE 802.22 network standard model. We focus on the CRN with one primary transmitter (regarded as PU in the CRN), one FC and several collaborative SUs, wherein some of them are assumed to be Byzantine attackers.

In the frame structure for the CRN with periodic spectrum, each frame consists of one sensing slot and one transmission slot. In the sensing slot, each SU individually employs local spectrum sensing techniques to detect the absence or presence of the PU. After SUs located in different sensing environments independently obtain sensing observations, each SU submits its own decision result about the PU activity to the FC. After receiving each SU's decision, the FC concludes with a final decision in one detection whether the channel is being exploited by the PU or not and broadcasts the status to all SUs.

In the transmission slot, SUs have an opportunity to operate the channel after the channel is announced as idle by the FC. If the channel is identified as being in a busy state, SUs are forbidden to access the busy channel which is already in use, in case of harmful interference in the primary network.

1.2 Byzantine attack model

In the process of cooperative spectrum sensing, attackers may hide in a latent place against discovery, but the local sensing ability and condition of detecting primary signals are similar to reliable SUs. When all SUs are required to send their own sensing results to the FC for global decision-making, attackers accompany in a cooperative manner. Through a Byzantine attack, in which the attacker will send falsified local spectrum interference to mislead the FC, the adversary can prevent reliable SUs from using the existing white space, or lure them to accessing the channel in use and cause excessive interference to the primary network, thereby undermining the premise of CR technology.

In previous research, a prerequisite that attackers are the minority of SUs is generally emphasized. Nevertheless, the extrema malicious behaviors imposed on the network should be predictable. Therefore, we propose three levels of Byzantine attack, valid attack (VA), invalid attack (IA) and no attack (NA), as shown in Fig. 1. VA denotes that the FC's final decision is distorted by attackers. In detail, when the inactive PU occurs, attackers advertise 0 as 1, which causes the FC to believe in the presence of the PU via a specific fusion rule, e.g., *K*-out-of-*N*. Consequently, reliable SUs are restricted to accessing the idle channel, meanwhile, attackers take advantage of the occupying channel, termed as denial SSDF (DS)[18], resulting in a false alarm. When the PU is active, attackers announce 1 as 0, thus causing harmful interference to the primary incumbent, termed as inducing SSDF (IS)[18], leading to the false alarm.

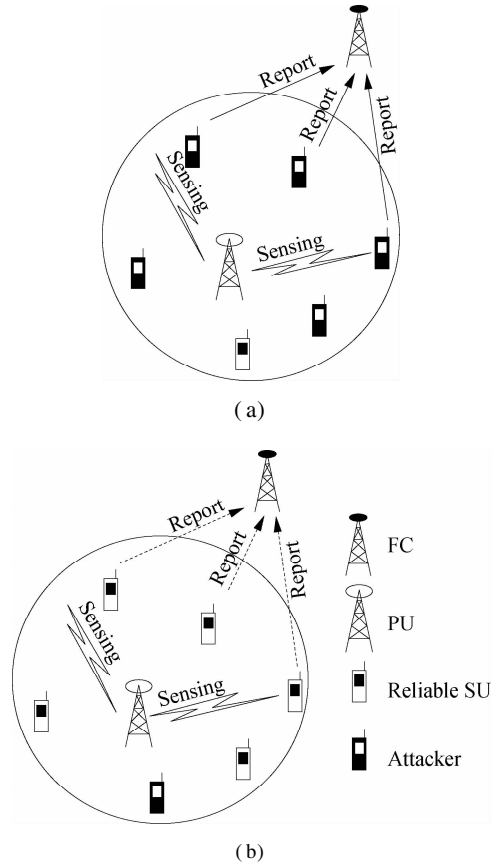


Fig. 1 Byzantine attack model. (a) Valid attack; (b) Invalid attack

Sometimes, attackers may be prone to carry out a milder attack IA rather than VA. The principle of such a strategic adjustment is based on whether a Byzantine attack makes the FC blind. We say that the FC is blind if

attackers can make the data that the FC receives from SUs such that no information is conveyed[19]. However, given the attack cost and the attack risk, attackers do not always make the FC blind (such as, a small percentage of attackers launch a Byzantine attack but are not able to compromise the FC, which is regarded as IA, while attackers still gain the attack gain since they participate in cooperative spectrum sensing). NA means that attackers sense the primary signal as well as the reliable SUs, and are unintentionally distorting their own sensing results. As a result, they truthfully submit own sensing results to the FC.

To simplify the analysis, we assume that all SUs have the same sensing capability, where some SUs are Byzantine attackers. The following assumptions of three conditional probabilities associated with a Byzantine attack and PU activity are made: When attackers launch VA under the inactive PU, the probability of which is donated by p_V; when attackers launch IA under the active PU, the probability of which is denoted by p_I; when attackers implement NA, the probability under the presence of the PU is p_N.

2 Game Formulation

2.1 Definition of players

There are two players, namely, the attacker and the defender. Attackers represent a set of attackers who participate in cooperative spectrum sensing. They sneak into reliable SUs and launch a Byzantine attack. As network administrators, defenders are responsible for suppressing Byzantine attacks in the network.

2.2 Attack and defense strategy

We characterize $S_a = \{S_{VA}, S_{IA}, S_{NA}\}$ and $S_d = \{S_D, S_{ND}\}$ as the strategy set of the attacker and defender, respectively.

2.2.1 Attack strategy analysis

In the Byzantine attack model, there are three actions VA, IA and NA, which can be performed by the attacker in the process of cooperative spectrum sensing. The concrete strategies must incorporate the spectrum sensing process and the PU activity.

In order to visually represent the attack strategy of the spectrum sensing process, we assume that X-Y means the attacker selects the action X in the sensing slot and Y in the transmission slot. When VA occurs, the attack strategy corresponding to the DS results in the false alarm concerning the PU state in the sensing slot, thereby Byzantine attackers selfishly occupy the idle channel to proceed with data transmission in the transmission slot. The whole process is denoted as VA-O. Otherwise, the strategy in connection with IS can be denoted by VA-I. Due to the miss detection, all the SUs proceed with data transmission in the transmission slot, thereby causing harmful interference in the normal communication of the primary network.

The attacker launches IA while the channel is being used by the PU. The FC's final decision is also accurate, and the attacker has to leave due to no benefits, and such a situation is denoted as IA-L. When the channel is unused, the attacker with IA can access it as well as the reliable SUs for transmitting data, which is denoted as IA-nO. After all SUs have sensed the active or inactive PU, since the attacker implements NA and operates like reliable SUs, the final decision is also idle or busy; therefore, both the attacker and reliable SUs access the unused channel or switch to another channel after the sensing slot. These two situations are respectively denoted as NA-L and NA-nO. Notably, NA-nO means no difference between the unintentional attacker and reliable SUs. Through the above analyses, the attack strategy is listed in Tab. 1

Tab. 1 Attack strategy

S_a	State of PU	
	Inactive	Active
S_{VA}	VA-O	VA-I
S_{IA}	IA-nO	IA-L
S_{NA}	NA-nO	NA-L

2.2.2 Defense strategy analysis

The strategy carried out by the defender is dependent on the decision result regarding the PU activity. To be specific, whether the FC broadcasts the busy or idle decision or not to SUs, the defender can select two actions: defense (D) and no defense (ND). D and ND, respectively, denotes that the defender adopts a defense mechanism or executes no defense policy. Which type of defense mechanism is implemented is of no interest, because a range of methods can be employed by the network defender. The defense strategy is listed in Tab. 2.

Tab. 2 Defense strategy

S_d	Decision result	
	Busy	Idle
S_D	D	D
S_{ND}	ND	ND

2.2.3 Mixed strategy

Given pure strategies for the attacker and defender, they will randomly propose a mixed strategy action in the following subsection, respectively.

2.3 Notation of cost and benefit

Before analyzing the non-cooperative game, we give some specific notations about the benefit and cost parameters of the Byzantine attack and defense strategy in the process of cooperative spectrum sensing .

For brevity of calculation, we assume that $G'_O = \gamma_1 G_O$, $G_I = \gamma_2 G_O$, $C'_O = \gamma_3 C_O$, $G'_D = \gamma_4 G_D$, where C_O refers to the cost that the idle channel is occupied by the attacker for data transmission under VA-O. G_O refers to the gain

of the attack strategy VA-O; C'_{O} represents the cost to that the attacker occupies the partial channel to transmit data at IA-nO; G'_{O} is the gain of IA-nO; G_{D} is the gain that the defender successfully captures the attacker with VA using the defense mechanism; G'_{D} is the gain of capturing the attacker when both the attacker with IA and reliable SUs access the idle channel in the transmission slot; G_{I} is the gain of interference which refers to that the attacker with IA has the negative effect on the primary network. $\gamma_1 \sim \gamma_4 (<1)$ rely on the framework of CRN, which is beyond the scope of this paper. Otherwise, C_{A} is the cost of VA or IA. ϕ is the penalty of the attacker being captured, such as, lower reputation value, pending sentence, etc. C_{D} denotes the cost of triggering the defensive mechanism.

Tab. 3 Payoff matrix of the Byzantine attack and the defense game

Strategy	S_{D}	S_{ND}
S_{VA}	$(U_{\mathrm{VA}}^{a1,d1}, U_{\mathrm{D}}^{a1,d1})$	$(U_{\mathrm{VA}}^{a1,d2}, U_{\mathrm{ND}}^{a1,d2})$
S_{IA}	$(U_{\mathrm{IA}}^{a2,d1}, U_{\mathrm{D}}^{a2,d1})$	$(U_{\mathrm{IA}}^{a2,d2}, U_{\mathrm{ND}}^{a2,d2})$
S_{NA}	$(U_{\mathrm{NA}}^{a3,d1}, U_{\mathrm{D}}^{a3,d1})$	$(U_{\mathrm{NA}}^{a3,d2}, U_{\mathrm{ND}}^{a3,d2})$

The payoff matrix of the Byzantine attack and defense game can be derived in Tab. 3. According to Ref. [20], the average payoffs of the defender and the attacker are computed as follows:

$$\left.\begin{aligned} U_{\mathrm{VA}} &= \sum_{j=1}^{2} U_{\mathrm{VA}}^{a1,dj} \\ U_{\mathrm{IA}} &= \sum_{j=1}^{2} U_{\mathrm{IA}}^{a1,dj} \\ U_{\mathrm{NA}} &= \sum_{j=1}^{2} U_{\mathrm{NA}}^{a1,dj} \end{aligned}\right\}, \quad \left.\begin{aligned} U_{\mathrm{D}} &= \sum_{i=1}^{3} U_{\mathrm{D}}^{ai,d1} \\ U_{\mathrm{ND}} &= \sum_{i=1}^{3} U_{\mathrm{ND}}^{ai,d2} \end{aligned}\right\} \tag{1}$$

Thus, by a simple mathematical investigation, the expected payoff of VA, IA and NA can be expressed as

$$\left.\begin{aligned} U_{\mathrm{VA}} &= -C_{\mathrm{A}} + p_{\mathrm{V}}(-C_{\mathrm{O}} + G_{\mathrm{O}}) + (1-p_{\mathrm{V}})\gamma_2 G_{\mathrm{O}} - \sigma_{\mathrm{d}}\phi \\ U_{\mathrm{IA}} &= -C_{\mathrm{A}} + (1-p_{\mathrm{I}})(-\gamma_3 C_{\mathrm{O}} + \gamma_1 G_{\mathrm{O}}) - \sigma_{\mathrm{d}}(1-p_{\mathrm{I}})\phi \\ U_{\mathrm{NA}} &= 0 \end{aligned}\right\} \tag{2}$$

where σ_{d} and σ_{nd} denote the probability of S_{D} and S_{ND}, respectively.

Likewise, the expected payoff of D and ND can be obtained by

$$\left.\begin{aligned} U_{\mathrm{D}} &= -C_{\mathrm{D}} + \sigma_{\mathrm{va}} G_{\mathrm{D}} + \sigma_{\mathrm{ia}}(1-p_{\mathrm{I}})\gamma_4 G_{\mathrm{D}} \\ U_{\mathrm{ND}} &= 0 \end{aligned}\right\} \tag{3}$$

where σ_{va} and σ_{ia} denote the probability of S_{VA} and S_{IA}, respectively.

3 Analysis of Equilibrium Points

In a non-cooperative game, the attacker and defender only focus on own benefit and choose the best response (BR) that can maximize the respective payoff function. Such an outcome of the non-cooperative game is termed as NE[20].

In the Byzantine attack model, given the occurrence of IA, the excessive defense is careless of the defender to evoke an expensive waste of resources, whereas the moderate defense for VA causes the network to be in a slight state of no protection. Our final purpose is to figure out how and when to select the economic and efficient defensive strategy for counteracting various Byzantine attacks in terms of the benefit and cost.

For this aim, we define two parameters from two players' perspectives, the penalty rate and benefit ratio. The penalty rate, denoted as $P_{\mathrm{r}} = \phi / G_{\mathrm{O}}$, makes the restrictive defense strategy unnecessary when the penalty is imposed on the attacker after being identified. The benefit ratio, denoted as $B_{\mathrm{r}} = G_{\mathrm{D}} / C_{\mathrm{D}}$, avoids unnecessary defense resource waste when the defender implements the defense mechanism unless the gain reaches a certain extent.

Due to its limited length, the proof of the NE will not be presented in this paper. Let $U'_{\mathrm{VA}} = p_{\mathrm{AC}}(-C_{\mathrm{O}} + G_{\mathrm{O}}) + (1-p_{\mathrm{AC}})G_{\mathrm{I}}$, $U'_{\mathrm{IA}} = (1-p_{\mathrm{AU}})(-C'_{\mathrm{O}} + G'_{\mathrm{O}})$, assume that B_{r}^{x} and P_{r}^{x} represent the penalty and benefit ratio thresholds in case x, respectively, where $x = 1, 2, 3$. By the Lemke-Howson algorithm, the three cases of the NE $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{\sigma_{\mathrm{va}}^*, \sigma_{\mathrm{ia}}^*, \sigma_{\mathrm{na}}^*\}, \{\sigma_{\mathrm{d}}^*, \sigma_{\mathrm{nd}}^*\}]$ are displayed as follows:

Case 1 $U_{\mathrm{VA}} > U_{\mathrm{IA}}$

If $C_{\mathrm{A}} \geqslant U_{\mathrm{VA}}$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{0,0,1\}, \{0,1\}]$

if $C_{\mathrm{A}} < U_{\mathrm{VA}}$,

when $B_{\mathrm{r}} \leqslant B_{\mathrm{r}}^1$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{1,0,0\}, \{0,1\}]$

when $B_{\mathrm{r}} > B_{\mathrm{r}}^1$,

when $P_{\mathrm{r}} > P_{\mathrm{r}}^1$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{\sigma_{\mathrm{va}}^*, 0, \sigma_{\mathrm{na}}^*\}, \{\sigma_{\mathrm{d}}^*, \sigma_{\mathrm{nd}}^*\}]$

when $P_{\mathrm{r}} \leqslant P_{\mathrm{r}}^1$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{1,0,0\}, \{1,0\}]$

where $\sigma_{\mathrm{va}}^* = \dfrac{C_{\mathrm{D}}}{G_{\mathrm{D}}}$, $\sigma_{\mathrm{na}}^* = 1 - \sigma_{\mathrm{va}}^*$, $\sigma_{\mathrm{d}}^* = \dfrac{U'_{\mathrm{VA}} - C_{\mathrm{A}}}{\phi}$, $\sigma_{\mathrm{nd}}^* = 1 - \sigma_{\mathrm{d}}^*$ and $B_{\mathrm{r}}^1 = 1$, $P_{\mathrm{r}}^1 = \dfrac{\phi(p_{\mathrm{V}} + \gamma_2 - \gamma_2 p_{\mathrm{V}})}{C_{\mathrm{A}} + C_O p_{\mathrm{V}} + \phi}$.

Case 2 $U_{\mathrm{VA}} = U_{\mathrm{IA}}$

If $P_{\mathrm{r}} > P_{\mathrm{r}}^2$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{0,0,1\}, \{\sigma_{\mathrm{d}}^*, \sigma_{\mathrm{nd}}^*\}]$

if $P_{\mathrm{r}} = P_{\mathrm{r}}^2$, $\sigma_{\mathrm{D}}^* = \{\sigma_{\mathrm{d}}^*, \sigma_{\mathrm{nd}}^*\}$,

when $1 \leqslant B_{\mathrm{r}} < B_{\mathrm{r}}^2$, then $\sigma_{\mathrm{ia}}^* = \dfrac{C_{\mathrm{D}} - \sigma_{\mathrm{va}}^* G_{\mathrm{D}}}{G'_{\mathrm{D}}(1-p_{\mathrm{I}})}$, $\sigma_{\mathrm{va}}^* \in \left[\dfrac{C_{\mathrm{D}} - (1-p_{\mathrm{I}})G'_{\mathrm{D}}}{G_{\mathrm{D}} - (1-p_{\mathrm{I}})G'_{\mathrm{D}}}, \dfrac{C_{\mathrm{D}}}{G_{\mathrm{D}}}\right]$, $\sigma_{\mathrm{na}}^* = 1 - \sigma_{\mathrm{va}}^* - \sigma_{\mathrm{ia}}^*$

when $B_{\mathrm{r}} \geqslant B_{\mathrm{r}}^2$, then $\sigma_{\mathrm{ia}}^* = \dfrac{C_{\mathrm{D}} - \sigma_{\mathrm{va}}^* G_{\mathrm{D}}}{G'_{\mathrm{D}}(1-p_{\mathrm{I}})}$, $\sigma_{\mathrm{va}}^* \in \left[0, \dfrac{C_{\mathrm{D}}}{G_{\mathrm{D}}}\right]$, $\sigma_{\mathrm{na}}^* = 1 - \sigma_{\mathrm{va}}^* - \sigma_{\mathrm{ia}}^*$ where $B_{\mathrm{r}}^2 = \dfrac{1}{\gamma_4(1-p_{\mathrm{I}})}$

if $P_{\mathrm{r}} < P_{\mathrm{r}}^2$, then $[\sigma_{\mathrm{A}}^*, \sigma_{\mathrm{D}}^*] = [\{\sigma_{\mathrm{va}}^*, 1 - \sigma_{\mathrm{va}}^*, 0\}, \{\sigma_{\mathrm{d}}^*,$

$\sigma_{nd}^*\}]$

where $\sigma_{va}^* \in [0,1]$, $\sigma_d^* = \dfrac{U_{VA} - U_{IA}}{p_I \phi}$, $\sigma_{nd}^* = 1 - \sigma_d^*$ and $P_r^2 = \dfrac{\phi(1-p_I)(\gamma_1 + \gamma_2 - \gamma_2 p_V - p_V)}{p_I C_A + (1-p_I)(\gamma_3 C_O - p_V C_O)}$.

Case 3 $U_{VA} < U_{IA}$

If $C_A \geqslant U_{IA}$, then $[\sigma_A^*, \sigma_D^*] = [\{0,0,1\}, \{0,1\}]$

if $C_A < U_{IA}$,

when $B_r \leqslant B_r^3$, then $[\sigma_A^*, \sigma_D^*] = [\{0,1,0\}, \{0,1\}]$

when $B_r > B_r^3$,

when $P_r > P_r^3$, then $[\sigma_A^*, \sigma_D^*] = [\{0, \sigma_{ia}^*, \sigma_{na}^*\}, \{\sigma_d^*, \sigma_{nd}^*\}]$

when $P_r \leqslant P_r^3$, then $[\sigma_A^*, \sigma_D^*] = [\{0,1,0\}, \{1,0\}]$

where $\sigma_{ia}^* = \dfrac{C_D}{C_D'(1-p_I)}$, $\sigma_{va}^* = 1 - \sigma_{ia}^*$, $\sigma_d^* = \dfrac{U_{IA}' - C_A}{\varphi(1-p_I)}$, $\sigma_{nd}^* = 1 - \sigma_d^*$ and $P_r^3 = \dfrac{\gamma_1 \phi(1-p_I)}{C_A + (\gamma_3 C_O + \phi)(1-p_I)}$.

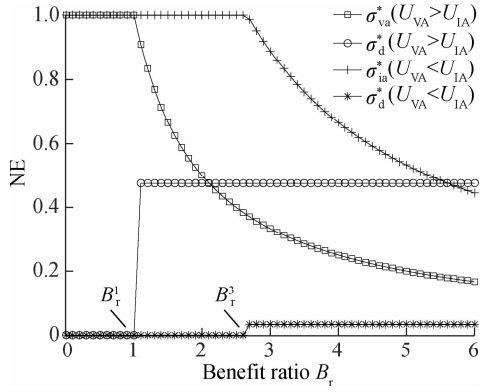
4 Simulation and Results

In this section, numerical simulations are shown to verify the efficiency of our proposed non-cooperative game to defend against various Byzantine attacks and the impact of the benefit ratio and penalty rate on the NE. The parameters are set as follows: $C_A = 10$, $p_V = p_I = 0.25$, $G_O = 3C_A$, $C_O = 0.3C_A$, $\phi = 0.5C_A$, $\gamma_1 = \gamma_3 = \gamma_4 = 0.5$, $\gamma_2 = 0.25$. Without loss of generality, the above selected parameters correspond to the most significant case $C_A = U_{VA}$ and $C_A = U_{IA}$.

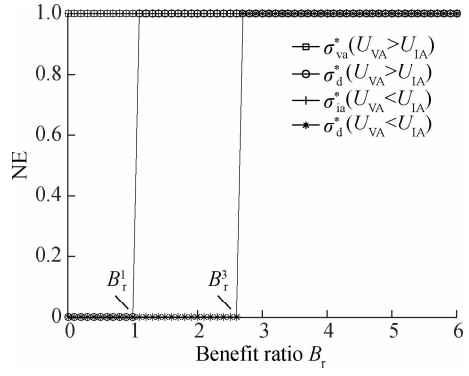
In Fig. 2, we plot the NE of the game for $U_{VA} > U_{IA}$ and $U_{VA} < U_{IA}$ under different benefit ratios B_r and penalty rates P_r. Observing $U_{VA} > U_{IA}$, we can see that unless the benefit ratio B_r exceeds threshold B_r^1, where $B_r^1 = 1$, it will not activate the defense mechanism since the defensive benefit and cost is judged and weighted, hence the defense strategy σ_D^* is $\{0,1\}$ when $B_r \leqslant B_r^1$. The consequent attack strategy is $\sigma_A^* = \{1,0,0\}$ due to the absence of the defense mechanism.

In terms of $B_r > B_r^1$, if the penalty rate P_r is lower than or equal to threshold P_r^1, where $P_r^1 = \phi(p_V + \gamma_2 - \gamma_2 p_V)/(C_A + C_O p_V + \phi) = 1$, both the better benefit and the smaller penalty obviously motivate the attacker to launch VA instead of IA and NA, ultimately, disregards whether the defender implements the defense mechanism or not. Subsequently, the attack strategy $\sigma_A^* = \{1,0,0\}$ is selected by the attacker in the NE. Concerning a higher penalty rate, e. g., $P_r > P_r^1$, the defender always keeps a constant defense level while the attacker has to decrease the attack rate to avoid being captured, and naturally the bilateral strategy is $[\sigma_A^*, \sigma_D^*] = [\{\sigma_{va}^*, 0, \sigma_{na}^*\}, \{\sigma_d^*, \sigma_{nd}^*\}]$.

In contrast to the simulation result of the case $U_{VA} > U_{IA}$, we can see the similar point of the NE but the lower level of defense in $U_{VA} < U_{IA}$. This happens since the benefit of IA is higher than that of VA, which is inclined to be launched by the attacker. Moreover, the weak strength attack requires sufficient benefits to attract defense ($B_r^3 > B_r^1$). There is no need to carry out rigorous defense, and a low defense level can tackle it (see Fig. 2 (a)). Consequently, such initiatives saves cost and secures the network.



(a)



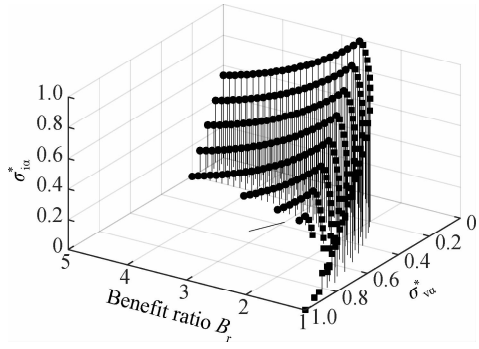
(b)

Fig. 2 NE of the game for $U_{VA} > U_{IA}$ and $U_{VA} < U_{IA}$. (a) $P_r > P_r^1$ or $P_r > P_r^3$; (b) $P_r \leqslant P_r^1$ or $P_r \leqslant P_r^3$

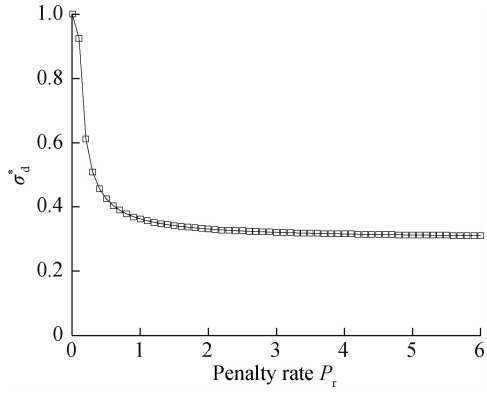
Similar to the simulations in $U_{VA} > U_{IA}$ and $U_{VA} < U_{IA}$, we also adopt the Lemke-Howson algorithm to verify our analysis on NE for $U_{VA} = U_{IA}$ in Fig. 3. It can certainly be affirmed that the mixed strategy for the defender is an obligatory choice to protect the network from Byzantine attacks. For various degrees of the penalty, the difference lies in the change of the attack strategy. For example, the attacker decides not to launch a Byzantine attack when the penalty is sufficiently high, i. e., $P_r < P_r^2$. However, the small penalty, i. e., $P_r > P_r^2$, will encourage malicious behaviors, such as, VA or IA.

As for $P_r = P_r^2$, the already selected parameters correspond to the most interesting case. In this case, as the attacker's mixed strategies, VA, IA and NA can be selected, where the circle and square dots represent mixed strategies of the attacker, they satisfy different relations and underline the boundary B_r^2 in Fig. 3(a). Apparently, we can see that the attacker also continuously adjusts its own strategy among VA, IA and NA against the defender's strategy, which satisfy a certain relationship

under various benefit ratios. To be specific, as shown in Fig. 3(a), compared with B_r varying from 1 to B_r^2, the region where σ_{ia}^* is selected is larger when $B_r \geqslant B_r^2$, which is reasonable, since the defense strategy σ_d^* is driven by the higher benefit.



(a)



(b)

Fig. 3 NE of the game for $U_{VA} = U_{IA}$. (a) Mixed attack strategy; (b) Mixed defense strategy

It also can be seen that the defense level decreases as the penalty rate P_r increases in Fig. 3(b). This is reasonable since the defender believes that sufficient penalty can frighten the attacker. In contrast, the deficiency of the attack transformation in Ref. [21] easily overprotects CRNs and wastes resources.

5 Conclusion

In this paper, we formulate a non-cooperative game with incomplete information between the Byzantine attacker and defender in the process of cooperative spectrum sensing. On the basis of bilateral practical actions, the opponent strategies are analyzed in detail. We propose individual cost-benefit from two players' perspective and derive the expected payoff over pure strategies. In addition, the closed form of the NE is obtained by the Lemke-Howson algorithm. Simulation results show that the benefit ratio and the penalty rate have a significant effect on NE, which demonstrates that the game-theory approach can take into account counteracting various Byzantine attacks and save the defensive cost.

References

[1] Nguyen-Thanh N, Ta D T, Nguyen V T. Spoofing attack and surveillance game in geo-location database driven spectrum sharing [J/OL]. *IET Communications*, 2018. http://digital-library.theiet.org/content/journals/10.1049/iet-com.2018.5266. DOI: 10.1049/iet-com.2018.5266.

[2] Li J W, Feng Z B, Feng Z Y, et al. A survey of security issues in cognitive radio networks[J]. *China Communications*, 2015, **12**(3): 132 − 150. DOI: 10.1109/cc.2015.7084371.

[3] Lamport L, Shostak R, Pease M. The byzantine generals problem[J]. *ACM Transactions on Programming Languages and Systems*, 1982, **4**(3): 382 − 401. DOI: 10.1145/357172.357176.

[4] Felegyhazi M, Hubaux J P. Game theory in wireless networks: A tutorial, No. LCA-REPORT-2006-002 [R]. 2006. https://infoscience.epfl.ch/record/79715.

[5] Le T N, Chin W L, Kao W C. Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks [J]. *IEEE Communications Letters*, 2015, **19**(5): 799 − 802. DOI: 10.1109/lcomm.2015.2399920.

[6] Borle K M, Chen B, Du W K. Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation[J]. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(10): 2225 − 2235. DOI: 10.1109/tifs.2015.2452893.

[7] Ahmed I K, Fapojuwo A O. Stackelberg equilibria of an anti-jamming game in cooperative cognitive radio networks[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2018, **4**(1): 121 − 134. DOI: 10.1109/tccn.2017.2769121.

[8] Karimi M, Sadough S M S. Efficient transmission strategy for cognitive radio systems under primary user emulation attack[J]. *IEEE Systems Journal*, 2017: 1 − 8. DOI: 10.1109/jsyst.2017.2747594.

[9] Ahmed I K, Fapojuwo A O. Nash equilibria of deception strategies in the IEEE 802.22 cognitive radio networks [C]// *IEEE 30th Canadian Conference on Electrical and Computer Engineering* (*CCECE*). Windsor, ON, Canada, 2017: 1 − 5. DOI: 10.1109/CCECE.2017.7946837.

[10] Kakalou I, Psannis K E. Coordination without collaboration in imperfect games: The primary user emulation attack example[J]. *IEEE Access*, 2018, **6**: 5402 − 5414. DOI: 10.1109/access.2018.2791519.

[11] Muthumeenakshi K, Radha S. Spectrum sensing in cognitive radios under noise uncertainty: Decision making using game theory[J]. *International Journal on Smart Sensing and Intelligent Systems*, 2017, **10**(1): 146 − 173. DOI: 10.21307/ijssis-2017-207.

[12] Du H, Fu S, Chu H N. A credibility-based defense SSDF attacks scheme for the expulsion of malicious users in cognitive radio[J]. *International Journal of Hybrid Information Technology*, 2015, **8**(9): 269 − 280. DOI: 10.14257/ijhit.2015.8.9.25.

[13] Wang H, Li Y M, Chang T C. An enhanced cooperative

spectrum sensing scheme for anti-SSDF attack based on evidence theory[J]. *Microsystem Technologies*, 2018, **24**(6): 2803 - 2811. DOI: 10.1007/s00542-018-3744-2.

[14] Wu J, Li X, Song T C, et al. Two-stage credit threshold on cooperative spectrum sensing to exclude malicious users in mobile cognitive radio networks [C]// *IEEE 85th Vehicular Technology Conference* (*VTC Spring*). Sydney, Australia, 2017: 1 - 6. DOI: 10.1109/VTCSpring.2017.8108221.

[15] Wang J P, Guo Q, Zheng W X, et al. Robust cooperative spectrum sensing based on adaptive reputation and evidential reasoning theory in cognitive radio network[J]. *Circuits, Systems, and Signal Processing*, 2018, **37**(10): 4455 - 4481. DOI: 10.1007/s00034-018-0774-z.

[16] Wu J, Song T C, Wang C, et al. Robust cooperative spectrum sensing against probabilistic SSDF attack in cognitive radio networks [C]// *IEEE 86th Vehicular Technology Conference* (*VTC-Fall*). Toronto, ON, Canada, 2017: 1 - 6. DOI: 10.1109/VTCFall.2017.8287979.

[17] Zhang L Y, Ding G R, Wu Q H, et al. Byzantine attack and defense in cognitive radio networks: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2015, **17**(3): 1342 - 1363. DOI: 10.1109/comst.2015.2422735.

[18] Bhattacharjee S, Sengupta S, Chatterjee M. Vulnerabilities in cognitive radio networks: A survey[J]. *Computer Communications*, 2013, **36**(13): 1387 - 1398. DOI: 10.1016/j.comcom.2013.06.003.

[19] Kailkhura B, Han Y S, Brahma S, et al. Distributed Bayesian detection in the presence of byzantine data[J]. *IEEE Transactions on Signal Processing*, 2015, **63**(19): 5250 - 5263. DOI: 10.1109/tsp.2015.2450191.

[20] Gibbons R. *Game theory for applied economists* [M]. Princeton, NJ, USA: Princeton University Press, 1992.

[21] Nguyen Thanh N, Ciblat P, Pham A T, et al. Surveillance strategies against primary user emulation attack in cognitive radio networks[J]. *IEEE Transactions on Wireless Communications*, 2015, **14**(9): 4981 - 4993. DOI: 10.1109/twc.2015.2430865.

一种对抗协作频谱感知中拜占庭攻击的博弈论方法

吴 俊 宋铁成 于 越 胡 静

(东南大学信息科学与工程学院, 南京 211189)

摘要:为了解决协作频谱感知中的拜占庭攻击问题,提出了一种非合作博弈论方法实现了对拜占庭攻击的有效防御. 首先,基于所提非合作博弈论方法,从拜占庭攻击者和网络管理员的角度分析了协作频谱感知中纯粹的拜占庭攻击和防御策略,并定义了双方纯粹策略的成本和收益. 其次,推导出双方的混合策略,利用 Lemke-Howson 算法得到闭合形式的纳什均衡,进一步分析了效益比和惩罚率对非合作博弈动态过程的影响. 仿真结果表明,所提出的博弈论方法能够有效地防御拜占庭攻击,并节省防御成本.

关键词:协作频谱感知; 拜占庭攻击; 博弈论; 非合作博弈; 纳什均衡

中图分类号:TN918