Journal of Southeast University (English Edition) Vol. 34, No. 4, pp. 439 - 443 Dec. 2018 ISSN 1003—7985

Cooperative spectrum sensing algorithm based on bilateral threshold selection against Byzantine attack

Zhu Hancheng Song Tiecheng Wu Jun Li Xi Hu Jing

(National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

Abstract: To deal with Byzantine attacks in 5G cognitive radio networks, a bilateral threshold selection-based algorithm is proposed in the spectrum sensing process. In each round, secondary uses (SUs) first submit the energy values and instantaneous detection signal-to-noise ratios (SNRs) to the fusion center (FC). According to detection SNRs, the FC conducts normalization calculations on the energy values. Then, the FC makes a sort operation for these normalized energy values and traverses all the possible mid-points between these sorted normalized energy values to maximize the classification accuracy of each SU. Finally, by introducing the recognition probability and misclassification probability, the distributions of the normalized energy values are analyzed and the bilateral threshold of classification accuracy is obtained via a target misclassification probability. Hence, the blacklist of malicious secondary users (MSUs) is obtained. Simulation results show that the proposed scheme outperforms the current mainstream schemes in correct sensing probability, false alarm probability and detection probability.

Key words: cognitive radio; Byzantine attack; bilateral threshold; misclassification probability; recognition probability

DOI: 10.3969/j.issn.1003-7985.2018.04.004

Recently, cognitive radio (CR) has been proposed to overcome the problem of limited available spectrum[1]. CR enables secondary users (SUs) to randomly access the spectrum. Due to the time-varying of the wireless channel, the signal-to-noise ratio (SNR) may become too low to obtain a reliable spectrum sensing. Hence, cooperative spectrum sensing (CSS) is proposed to deal with this issue[2]. In existing CSS, SUs need to send their local sensing information to the fusion center (FC), and then the FC makes a global decision[3]. However, this fusion scheme provides more opportunities for malicious secondary users (MSUs) to launch Byzantine attacks[4].

Nowadays, a series of solutions have been made to recognize MSUs. A reliable reference algorithm was proposed to reduce the influence of MSUs on spectrum sensing[5]. A trust node-assisted reference algorithm was put forward, in which the trust node was applied to screen out MSUs[6].

The traditional MSU detection scheme usually achieves a poor detection performance in a massive MSU and the low-SNR region. To enhance the performance in a relatively hash environment, a bilateral threshold detection scheme is put forward to resist Byzantine attacks.

1 System Model

1.1 Cooperative spectrum sensing

In this paper, an IEEE 802.22 wireless access network is considered, as shown in Fig. 1. It consists of a CRN with one PU, one FC, and N SUs. Each SU performs the estimation of the energy value from the PU and sends it to the FC. Then, the FC decides the availability/unavailability of the PU. Therefore, each SU performs the energy detection for a time duration τ_0. If we denote the sampling rate by f_s, the energy value of SU_i is given by

$$y_i = \begin{cases} \dfrac{2}{\sigma_i^2}\displaystyle\sum_{j=1}^{f_s\tau_0}[n_i(j)]^2 & \text{PU is available} \\ \dfrac{2}{\sigma_i^2}\displaystyle\sum_{j=1}^{f_s\tau_0}[h_i S(j)+n_i(j)]^2 & \text{PU is unavailable} \end{cases} \tag{1}$$

where h_i denotes the channel gain from PU to SU_i; $S(j)$ and $n_i(j)$ represent the signal of PU and background noise around SU_i, respectively. The noise power $\sigma_i^2 = E[|n_i(j)|^2]$. For a large $f_s\tau_0$, the energy value that SU_i received approximates the Gaussian distribution,

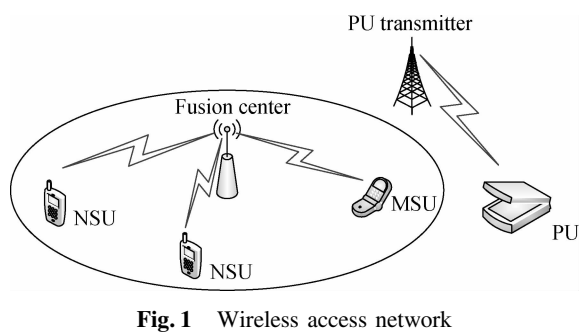

Fig. 1 Wireless access network

Received 2018-04-19, **Revised** 2018-09-16.

Biographies: Zhu Hancheng (1993—), male, graduate; Song Tiecheng (corresponding author), male, doctor, professor, songtc@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 61771126, 61372104), the Science and Technology Project of State Grid Corporation of China (No. SGRIXTKJ[2015]349).

Citation: Zhu Hancheng, Song Tiecheng, Wu Jun, et al. Cooperative spectrum sensing algorithm based on bilateral threshold selection against Byzantine attack. [J]. Journal of Southeast University (English Edition), 2018, 34(4): 439 - 443. DOI: 10.3969/j.issn.1003-7985.2018.04.004.

$$y_i \sim \begin{cases} N(2f_s\tau_0, 4f_s\tau_0) & \text{PU is unavailable} \\ N(2f_s\tau_0(1+\gamma_i), 4f_s\tau_0(1+2\gamma_i)) & \text{PU is available} \end{cases} \tag{2}$$

where $\gamma_i = E[\,|h_i S(j)|^2]$ represents the SNR from PU to SU_i. We assume that the FC has acquired the detection SNR γ_i and this can be realized by contacting the SUs[7].

1.2 Attack model

In order to efficiently carry out attacks, MSUs need to predict their own local decisions. By comparing the energy value y_m with a local threshold φ_m, the local decision of MSU_m can be reached. A PU is considered available if $y_m > \varphi_m$; otherwise, PU is considered unavailable.

After spectrum sensing, the individual sensing report d_m of each MSU is generated as

$$d_m = \begin{cases} 1 & y_m > \varphi_m \\ 0 & y_m \leqslant \varphi_m \end{cases} \tag{3}$$

In this paper, the following Byzantine attack model is employed. Here, MSUs use their local decisions to perform attacks. It first makes a local decision. Then, it generates an abnormal Gaussian distribution value with the attack probability β_m.

When the MSU_m does not launch an attack, the energy value he/she submits is $Y_m = y_m$. That is, he/she submits the energy value received in the energy detection phase. However, when the MSU_m launches the attack, the Byzantine attack model is denoted as follows:

$$Y_m \sim \begin{cases} N(2f_s\tau_0 + \Lambda, 4f_s\tau_0) & d_m = 0 \\ N(2f_s\tau_0(1+\gamma_m) - \Lambda, 4f_s\tau_0(1+2\gamma_m)) & d_m = 1 \end{cases} \tag{4}$$

where Λ is a deviation resulting in a falsification of data.

2 Bilateral Threshold Selection Scheme

2.1 Data collection

The FC first picks up the energy values submitted by SUs in the history rounds. Hence, the FC can obtain the actual availability states of PU during the end of these history rounds[8] (e.g. by interacting with the PU station). The energy values submitted by SUs and PU states are listed in Tab. 1. After the pretreatment of energy values, the normalized energy values are shown in Tab. 2.

Tab. 1 Collected energy values and PU states

Round	SU_1	SU_2	…	SU_N	PU state
1	$Y_1(1)$	$Y_2(1)$	…	$Y_N(1)$	PU(1) = 0
⋮	⋮	⋮		⋮	⋮
R	$Y_1(R)$	$Y_2(R)$	…	$Y_N(R)$	PU(R) = 0

Tab. 2 Normalized energy values

Round	SU_1	SU_2	…	SU_N	PU state
1	$Z_1(1)$	$Z_2(1)$	…	$Z_N(1)$	PU(1) = 0
⋮	⋮	⋮		⋮	⋮
R	$Z_1(R)$	$Z_2(R)$	…	$Z_N(R)$	PU(R) = 0

Note: $\mathrm{PU}(k) = \begin{cases} 0 & \text{PU is inactive in the } k\text{-th round} \\ 1 & \text{otherwise} \end{cases}$.

2.2 Pretreatment of energy values

The distributions of energy values submitted by SU_i may change with the rounds. Therefore, formula (2) is revised as follows:

$$Y_i(k) \sim \begin{cases} N(2f_s\tau_0, 4f_s\tau_0) & \text{PU is unavailable} \\ N(2f_s\tau_0(1+\gamma_i(k)), \\ \quad 4f_s\tau_0(1+2\gamma_i(k))) & \text{PU is available} \end{cases} \tag{5}$$

Drawing on the reference of standard normal distribution, the energy values are pretreated as

$$Z_i(k) = \begin{cases} \dfrac{(Y_i(k) - 2f_s\tau_0)}{\sqrt{4f_s\tau_0}} & \mathrm{PU}(k) = 0 \\ \dfrac{[(Y_i(k) - 2f_s\tau_0(1+\gamma_i(k)))}{\sqrt{4f_s\tau_0(1+2\gamma_i(k))]}} + \varepsilon & \text{otherwise} \end{cases} \tag{6}$$

where ε is a positive data bias. Therefore, for NSU_n

$$Z_n(k) \sim \begin{cases} N(0,1) & \text{PU is unavailable} \\ N(\varepsilon,1) & \text{PU is available} \end{cases} \tag{7}$$

Formula (7) describes the distributions of the normalized energy values of NSUs. However, due to the existence of the attack rounds, the normalized distributions of MSUs under two hypotheses will generate additional changes. The variations of the normalized distributions between NSUs and MSUs will be identified by our bilateral threshold selection scheme.

2.3 Classification accuracy for normalized energy values

After treatment, Tab. 2 can be obtained, and then the FC needs to analyze the normalized energy values in R rounds. The FC uses a rated value evaluation method to obtain the decision results of SU_i in R rounds:

$$H_i(k, S_i^{\mathrm{v}}) = U(Z_i(k) - S_i^{\mathrm{v}}) \tag{8}$$

where $H_i(k, S_i^{\mathrm{v}})$ represents a decision result of SU_i in the k-th round. S_i^{v} denotes the rated value of SU_i in R rounds. $U(\cdot)$ is the step function. For SU_i, the selection of the rated value S_i^{v} is shown in Definition 1.

Definition 1 The selection of the rated value S_i^{v} should minimize the deviation between the result vector $\{H_i(k, S_i^{\mathrm{v}})\}_{k=1,2,\cdots,R}$ and PU state vector $\{\mathrm{PU}(k)\}_k = 1, 2, \cdots, R$ in R rounds.

Hence, S_i^{v} is calculated as

$$S_i^{\mathrm{v}} = \underset{s}{\operatorname{argmin}} \sum_{k=1}^{R} [\mathrm{PU}(k) \oplus H_i(k,s)] \tag{9}$$

where $\oplus$ denotes exclusive-or logic. Therefore, the classification accuracy of SU_i is

$$C_i^{\mathrm{v}} = 1 - \frac{\sum_{k=1}^{R} [\mathrm{PU}(k) \oplus H_i(k,S_i^{\mathrm{v}})]}{R} \tag{10}$$

Owing to the fact that there are only R rounds used in Eqs. (8) and (9), a traversal algorithm is presented to find the rated value S_i^{v} and classification accuracy C_i^{v}, which is described as follows:

Step 1 Conduct an ascending sort to the normalized energy values. That is, $\{Z_i(1), Z_i(2), \cdots, Z_i(R)\} \xrightarrow{\text{sort}} \{Z_i(l_1), Z_i(l_2), \cdots, Z_i(l_R)\}$, where $Z_i(l_1) \leqslant Z_i(l_2) \leqslant \cdots \leqslant Z_i(l_R)$.

Step 2 Construct a candidate set of the rated value $\{S_i^{\mathrm{v}}(1), S_i^{\mathrm{v}}(2), \cdots, S_i^{\mathrm{v}}(R+1)\}$, where $S_i^{\mathrm{v}}(1) = Z_i(l_1) - 1$; $S_i^{\mathrm{v}}(R+1) = Z_i(l_R) + 1$; $S_i^{\mathrm{v}}(k) = (Z_i(l_{k-1}) + Z_i(l_k))/2 (k = 2, 3, \cdots, R)$.

Step 3 Traverse all the values of the candidate set, and select a value $S_i^{\mathrm{v}}(k) (k = 1, 2, \cdots, R+1)$ which minimizes Eq. (9). Therefore, the rated value $S_i^{\mathrm{v}} = S_i^{\mathrm{v}}(k)$ and the classification accuracy C_i^{v} of SU_i can be calculated by Eq. (10).

2.4 Bilateral threshold for normalized energy values

Here, two probabilities are introduced: recognition probability and misclassification probability. Recognition probability is the probability that MSUs are correctly recognized, while misclassification probability is the probability that a NSU is mistaken for a MSU.

For SU_i, the distributions of the normalized energy values obtained by the FC satisfy (7). According to the law of large numbers, the theoretical rated value S_i^{F} of SU_i is calculated as

$$P_0 P_i(z = S_i^{\mathrm{F}} \mid H_0) = P_1 P_i(z = S_i^{\mathrm{F}} \mid H_1; \varepsilon) \tag{11}$$

where $P_i(z \mid H_0)$ and $P_i(z \mid H_1; \varepsilon)$ are the distributions under H_0 and H_1 in (7). P_1 and P_0 denote the probabilities that PU is present and absent, respectively. Solving the above gives

$$S_i^{\mathrm{F}} = \frac{\varepsilon}{2} + \frac{1}{\varepsilon} \ln\left(\frac{P_0}{P_1}\right) \tag{12}$$

Hence, the theoretical classification probability $p(\varepsilon)$ of SU_i is

$$p(\varepsilon) = 1 - P_0 P_i(z > S_i^{\mathrm{F}} \mid H_0) - P_1 P_i(z \leqslant S_i^{\mathrm{F}} \mid H_1; \varepsilon) \tag{13}$$

Then, a random variable is introduced:

$$Q_i^{\mathrm{F}}(k) = \begin{cases} 0 & \text{The } k\text{-th sample is misclassified} \\ 1 & \text{Otherwise} \end{cases} \tag{14}$$

It is clear that $P(Q_i^{\mathrm{F}}(k) = 1) = p(\varepsilon)$. Therefore, the theoretical classification accuracy C_i^{F} of SU_i is

$$C_i^{\mathrm{F}} = \sum_{k=1}^{R} Q_i^{\mathrm{F}}(k)/R \tag{15}$$

Given the misclassification probability τ, the fluctuating range Δ can be calculated as

$$P(p(\varepsilon) - \Delta < C_i^{\mathrm{F}} < p(\varepsilon) + \Delta) \geqslant 1 - \tau \tag{16}$$

According to the central limit theorem, we can derive from the above expression that

$$\Delta \geqslant \sqrt{2p(\varepsilon)(1 - p(\varepsilon))/R}\ \operatorname{erfc}^{-1}(\tau) \tag{17}$$

Clearly, the recognition probability is a monotone decreasing function of Δ. To maximize the recognition probability, we write formula (17) as an equation. Therefore,

$$u_{i\mathrm{L}} = p(\varepsilon) - \Delta = p(\varepsilon) - \sqrt{2p(\varepsilon)(1 - p(\varepsilon))/R}\ \operatorname{erfc}^{-1}(\tau) \tag{18}$$

$$u_{i\mathrm{H}} = p(\varepsilon) + \Delta = p(\varepsilon) + \sqrt{2p(\varepsilon)(1 - p(\varepsilon))/R}\ \operatorname{erfc}^{-1}(\tau) \tag{19}$$

Eqs. (18) and (19) describe the relationship between the misclassification probability and the bilateral threshold of classification accuracy C_i^{F}. As can be seen from the above expressions and (15), with the increase of R, the bilateral threshold $\{u_{i\mathrm{L}}, u_{i\mathrm{H}}\}$ and the theoretical classification accuracy C_i^{F} both converge to $p(\varepsilon)$ and the convergence rate of $\{u_{i\mathrm{L}}, u_{i\mathrm{H}}\}$ is geometric. In addition, owing to the pretreatment of the energy values, each SU has the same bilateral threshold in the FC. With the increase of R, for NSU_n, its classification accuracy C_n^{v} is coincident with C_n^{F}. Therefore, it will fall into the $[u_{n\mathrm{L}}, u_{n\mathrm{H}}]$. However, for MSU_m, owing to the attack rounds, its classification accuracy C_m^{v} is not consistent with C_m^{F}. Therefore, it will fall outside $[u_{m\mathrm{L}}, u_{m\mathrm{H}}]$ as the number of samples R increases.

3 Description of the Bilateral Threshold Selection Scheme

In this part, the steps of the selection algorithm are introduced.

Step 1 Initialize $P_0 = \frac{\sum_{k=1}^{R} (\mathrm{PU}(k) \oplus 1)}{R}$, $P_1 = \frac{\sum_{k=1}^{R} (\mathrm{PU}(k) \oplus 0)}{R}$.

Step 2 For each SU_i, the FC converts the energy values $Y_i(k)$ into $Z_i(k)$ via (6).

Step 3 FC calculates $p(\varepsilon)$ and $\{u_{iL}, u_{iH}\}$ by (17), (22) and (23).

Step 4 Calculate C_i^v through the traversal algorithm

Step 5 If $C_i^v \notin [u_{iL}, u_{iH}]$, then add SU_i to the blacklist.

In order to demonstrate the effectiveness of the selection scheme, a simple likelihood ratio scheme is adopted to achieve the PU state as follows:

Step 1 Pick out the energy values $Y_{U_j}(k)$ of the SUs not included in the blacklist.

Step 2 Calculate likelihood ratio

$$L_r = \prod_{j=1}^{M} \frac{P_{U_j}(y = Y_{U_j}(k) \mid H_1)}{P_{U_j}(y = Y_{U_j}(k) \mid H_0)}$$

Step 3 If $L_r > 1$, then PU is available. Otherwise PU is unavailable.

As is shown from the scheme, P_1 and P_0 are counted by the actual state of the PU from Tab. 2. $P_{U_j}(y \mid H_v)(v = 0, 1)$ are the original distributions of the energy values in (5). $\{U_j\}_{j=1,2,\cdots,M}$ are the SU indices not belonging to the blacklist in the selection algorithm.

4 Simulation Results

If the parameters are not listed explicitly in the figures, parameters are set by default as follows. The number of SUs is 50. The number of samples R is 100. The sampling frequency f_s is 10 kHz. The sensing duration τ_0 is 5 ms, the noise power $\sigma_i^2 = \sigma^2 = 1$. The misclassification probability τ is 0.05, and the signal to noise ratio $\gamma_i(k)$ fluctuates between -10 and -5 dB. The data bias ε is 1, and the deviation Λ is $2f_s\tau_0\gamma_m$.

Fig. 2 shows the MSUs screened out by our selection algorithm. Owing to the normalization of the energy values, SUs with different SNRs have the same bilateral thresholds. In Fig. 2, a NSU is misclassified as a MSU (Its index is 7), and two MSUs are not screened out (Their indices are 20 and 21).

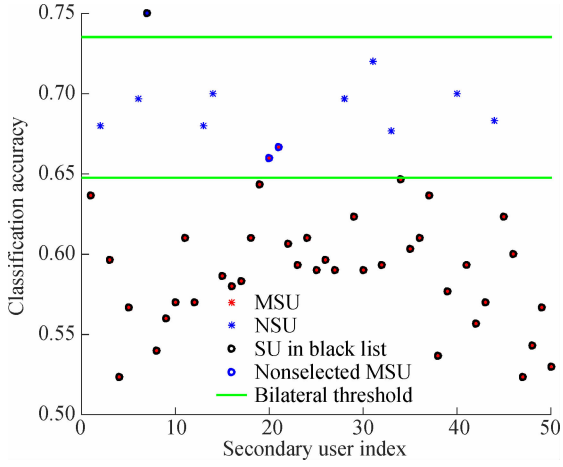

Fig. 2 The filter result of MSUs in selection algorithm ($\beta_m \in [0.2, 0.4]$)

Fig. 3 describes the correct sensing probabilities of our selection algorithm and the SVDD algorithm[9] with the rounds increasing. Due to the users' mobility, the proportion of MSUs will change. The variations of the percentage of MSUs are marked with red circles. From Fig. 3, our scheme achieves better performance than the SVDD algorithm. Besides, a large R has a positive impact on sensing performance, which is coincident with Eqs. (18) and (19).

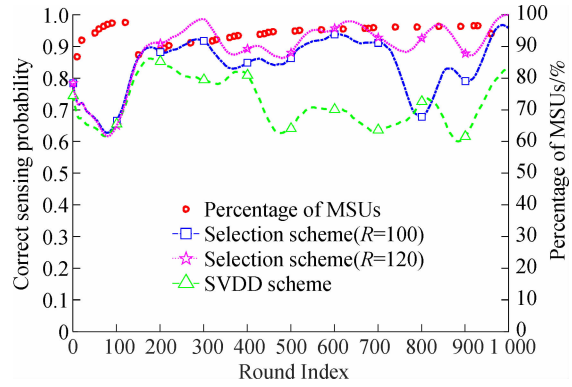

Fig. 3 The variation of correct sensing probability with rounds ($\beta_m \in [0.1, 0.3]$)

Fig. 4 shows the detection probability with the increase in the percentage of MSUs. In this figure, the traditional trust scheme[10] and the critical learning scheme[11] are the worst, while the sensing guard scheme[12] is better than them. This is due to the fact that the sensing guard scheme will impose severe punishments on the SUs who submit false sensing energy values frequently. However, our proposed scheme screens out most MSUs, which ensures excellent detection probability in scenarios with massive MSUs.

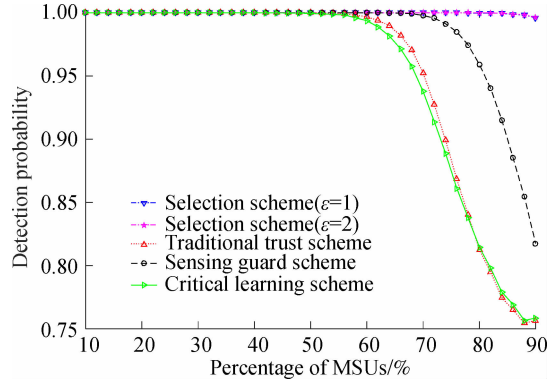

Fig. 4 The variation of detection probability with percentage of MSUs ($\beta_m \in [0.2, 0.4]$)

Fig. 5 describes the impact of the percentage of MSUs on false alarm probability. We compare our selection scheme with the above algorithms. From Fig. 5, we can see that the data bias ε has a modest impact on the sensing performance of the selection algorithm. Hence, the appropriate value of all data bias is allowed in our scheme.

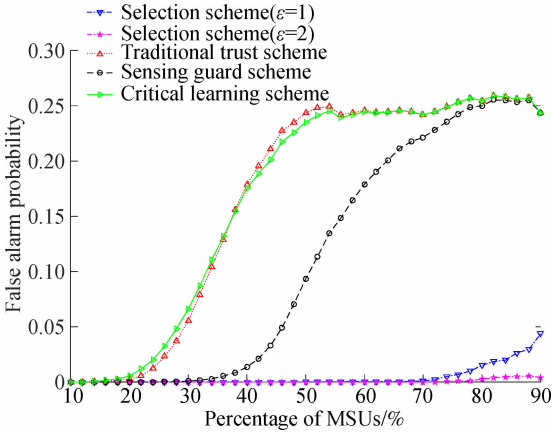

Fig. 5 The variation of false alarm probability with percentage of MSUs($\beta_m \in [0.2, 0.4]$)

5 Conclusion

In this paper, we design a bilateral threshold selection scheme for MSU detection. Besides, we analyze the relationship between misclassification probability and the bilateral threshold. In simulation, we verify the performance of the algorithm in terms of a series of parameters. Hence, the proposed scheme can deal with the byzantine attacks in CSS to improve the robustness of the system.

References

[1] Haykin S. Cognitive radio: Brain-empowered wireless communications[J]. *IEEE Journal on Selected Areas in Communications*, 2005, **23**(2): 201 - 220. DOI: 10.1109/jsac.2004.839380.

[2] Guo H Y, Reisi N, Jiang W, et al. Soft combination for cooperative spectrum sensing in fading channels [J]. *IEEE Access*, 2017, **5**: 975 - 986. DOI: 10.1109/access.2016.2628860.

[3] Peng T, Chen B, Xiao J, et al. Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks [C]//2016 *International Conference on Computer, Information and Telecommunication Systems*. Kunming, China, 2016: 1 - 5.

[4] Shen J, Liu S, Zeng L, et al. Optimization of cooperative spectrum sensing in cognitive radio network[J]. *IET Communications*, 2009, **3**(7): 1170. DOI: 10.1049/iet-com.2008.0177.

[5] Zhang L, Ding G, Song F, et al. Defending against byzantine attack in cooperative spectrum sensing relying on a reliable reference [C]//2016 *International Conference on Communications in China*. Chengdu, China, 2016: 1 - 6.

[6] He X F, Dai H Y, Ning P. A Byzantine attack defender in cognitive radio networks: The conditional frequency check[J]. *IEEE Transactions on Wireless Communications*, 2013, **12**(5): 2512 - 2523. DOI: 10.1109/twc.2013.031313.121551.

[7] Zeng F, Li J, Xu J, et al. A trust-based cooperative spectrum sensing scheme against SSDF attack in CRNs [C]//2016 *IEEE Trustcom/BigDataSE/ISPA*. Tianjin, China, 2016: 1167 - 1173.

[8] Hyder C S, Grebur B, Xiao L, et al. ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks [J]. *IEEE Transactions on Mobile Computing*, 2014, **13**(8): 1707 - 1719. DOI: 10.1109/tmc.2013.26.

[9] Farmani F, Abbasi-Jannatabad M, Berangi R. Detection of SSDF attack using SVDD algorithm in cognitive radio networks [C]//2011 *Third International Conference on Computational Intelligence, Communication Systems and Networks*. Bali, Indonesia, 2011: 201 - 204.

[10] Pei Q Q, Yuan B B, Li L, et al. A sensing and etiquette reputation-based trust management for centralized cognitive radio networks[J]. *Neurocomputing*, 2013, **101**: 129 - 138. DOI: 10.1016/j.neucom.2012.08.005.

[11] Chen H F, Zhou M, Xie L, et al. Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack[J]. *IEEE Transactions on Vehicular Technology*, 2016, **65**(11): 9181 - 9191. DOI: 10.1109/tvt.2016.2520983.

[12] Jing Y F, Yu Q Z, Guang Y L. Securing cooperative spectrum sensing against rational SSDF attack in cognitive radio networks[J]. *KSII Transactions on Internet and Information Systems*, 2014, **8**(1): 1 - 17. DOI: 10.3837/tiis.2014.01.001.

基于双边阈值的抗 Byzantine 攻击协作频谱感知算法

朱翰宬　宋铁成　吴　俊　李　茜　胡　静

(东南大学移动通信国家重点实验室,南京 210096)

摘要:为了解决 5G 认知无线网络中的 Byzantine 攻击,在频谱感知过程中提出了一种双边阈值筛选方案. 在每个回合中,从用户首先将感知能量值和检测信噪比提交给融合中心. 根据检测信噪比,融合中心对能量值进行归一化. 然后,对归一化能量值进行排序并遍历这些归一化能量值的中点,以最大化从用户的分类准确率. 此外,通过引入识别概率和误筛概率,分析了归一化能量值的分布,从而推导了给定误筛概率情况下的恶意用户双边筛选阈值. 最后,通过该双边筛选阈值获得恶意用户名单. 仿真结果表明:所提方案的主用户正确感知率、虚警和检测概率均要优于当前主流方案.

关键词:认知无线电;Byzantine 攻击;双边阈值;误筛概率;识别概率

中图分类号:TN915