Journal of Systems Engineering and Electronics
Vol. 31, No. 2, April 2020, pp.243 – 251

An algorithm based on evidence theory and fuzzy entropy to defend against SSDF

YE Fang, BAI Ping, and TIAN Yuan*

College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China

Abstract: In cognitive radio networks, spectrum sensing is one of the most important functions to identify available spectrum for improving the spectrum utilization. Due to the open characteristic of the wireless electromagnetic environment, the wireless network is vulnerable to be attacked by malicious users (MUs), and spectrum sensing data falsification (SSDF) attack is one of the most harmful attacks on spectrum sensing performance. In this article, an algorithm based on the evidence theory and fuzzy entropy is proposed to resist SSDF attacks. In this algorithm, secondary users (SUs) obtain the corresponding degree of membership function and basic probability assignment function based on the local energy detection result. The new conflicting coefficient is calculated based on the evidence distance and classical conflicting coefficient, and the conflicting weight of the evidence is obtained. The fuzzy weight is calculated by the fuzzy entropy. The credibility weight is obtained by updating the credibility. On this basis, the probability assignment function of the evidence is corrected, and the final result is obtained by using the fusion formula. Simulation results show that the proposed algorithm has a higher detection probability and lower false alarm probability than other algorithms. It can effectively defend against SSDF attacks and improve the performance of spectrum sensing.

Keywords: cooperative spectrum sensing, evidence theory, fuzzy entropy, spectrum sensing data falsification (SSDF).

DOI: 10.23919/JSEE.2020.000002

1. Introduction

With the rapid development of wireless communication technology, the conventional static spectrum management policy cannot satisfy the demand for the wireless spectrum resources [1,2]. As the most proposed solution to the spectrum resources problem, cognitive radio (CR) has attracted widespread attention [3]. Spectrum sensing enables opportunistic spectrum usage of white spaces under the premise of not causing harmful interference to the primary user (PU) [4,5].

Spectrum sensing is the premise of the successful implementation of CR [6,7]. Among various spectrum sensing techniques, energy detection is widely used due to its low implementation complexity and without any prior knowledge about signal features [8]. Due to the influence of multipath fading and shadowing in the wireless channel, it is difficult for single user sensing to ensure the accuracy of spectrum sensing [9 – 11]. In order to solve this problem, scholars use the cooperative spectrum sensing technology, which enables numerous users to participate in the sensing at the same time and make the final judgment about the primary user information [12 – 14]. Cooperative spectrum sensing is confronted by spectrum sensing data falsification (SSDF) attacks by which malicious users (MUs) intentionally report fake sensing results to mislead decision-making [15 – 17].

In order to resist the SSDF attack, plenty of algorithms based on the Dempster-Shafer (D-S) theory of evidence have been proposed. In [18], a new method based on decision making trial and evaluation laboratory (DEMATEL) is proposed to take the weight of each evidence into consideration. Zhang et al. proposed a spectrum sensing algorithm based on an improved D-S evidence theory in [19], and improved spectrum sensing performance by using improved D-S evidence theory fusion rules. In [20], a cooperative spectrum sensing algorithm based on a weighted D-S evidence theory is used to resist SSDF attacks, in which the weight is a function of the energy and position. Peng et al. proposed a spectrum sensing algorithm based on trust and the D-S evidence theory in [21]. Due to the different environments of the secondary users (SUs), the reliability of the detection results is inconsistent. Evidence theory is introduced to solve the final decision problem of the trust value. Nie et al. proposed a cooperative spectrum sensing algorithm based on dynamic double threshold and the D-S

Manuscript received January 14, 2019.

*Corresponding author.

This work was supported by the National Natural Science Foundation of China (61701134; 51809056), the Fundamental Research Funds for the Central Universities of China (HEUCFM180802), the National Key Research and Development Program of China (2016YFF0102806), and the Natural Science Foundation of Heilongjiang Province, China (F2017004).

evidence theory in [22] to reduce the network overhead and the computational of the fusion center. In [23], Feng et al. proposed a trust evaluation mechanism based on the D-S evidence theory — HardGuard, which took preprocessing measures to filter false perceptual data before fusion and avoided the influence of MUs. In [24], Men et al. proposed an evaluation method which considers the sensor node reliability and the mutually supportive degree among different sensor nodes. In [25], Yu et al. used the similarity degree to calculate the reliability of evidence to defend against SSDF attacks.

The above several security spectrum sensing schemes based on the evidence theory only consider the difference of the similarity of user's evidence, and ignore the distance between the data and the degree of determination. To target the aforementioned problems and improve the detection accuracy in the spectrum sensing, this paper proposes an algorithm against SSDF attacks based on the evidence theory and fuzzy entropy.

The rest of this article is organized as follows. Section 2 introduces the system model and the SSDF attack mode. In Section 3, an algorithm against SSDF attack based on the evidence theory and fuzzy entropy is described in detail. Section 4 verifies the performance of the algorithm in different SSDF attack modes. Section 5 depicts the final conclusions.

2. System description

Due to the shadowing and multipath fading, multiple SUs perform cooperative spectrum sensing in this paper to solve the problem of inaccurate estimation of the spectral holes by a single SU [26,27]. Considering a cognitive radio network shown in Fig. 1, there is a PU, a fusion center (FC) and several SUs. SUs use energy detection to obtain energy values x_{E_i} and make decisions d_i by being compared with thresholds. Then the users transfer the local decision through the control channel to the FC to make the final decision d through certain fusion criteria.

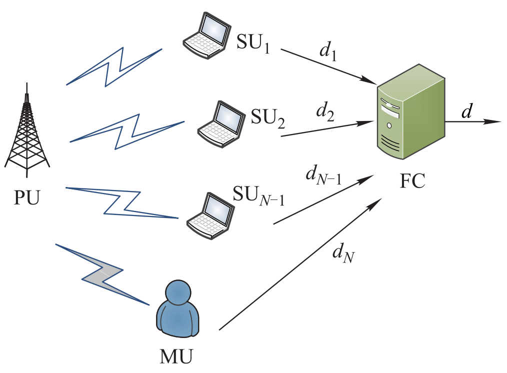


Fig. 1 System model

There are three main types of SSDF attacks in the process of cooperative spectrum sensing [28].

Always busy (AB) attack: regardless of the result of the judgment, the MUs determine the result as 1 so as to achieve the purpose of monopolizing the specific frequency band.

Always free (AF) attack: regardless of the result of the judgment, the MUs will set the judgment as 0 so as to cause more interference to the PU.

Always opposite (AO) attack: the MUs tamper the decision result 0 to 1, and tamper the result 1 to 0. The first two attacks can be seen as a special form of AO attack.

3. Algorithm based on evidence theory and fuzzy entropy to resist SSDF attacks

From the perspective of cognition, the greater the uncertainty of the evidence is, the worse the credibility is, and the worse the decision would be, vice versa. Aiming at the uncertainties of perceptual results, the fuzzy entropy is used to represent the uncertainties, which improves the reliability of the results. The D-S evidence theory is a mathematical theory which can deal with uncertain information effectively. In this paper, it is used as a fusion algorithm for cooperative spectrum sensing. This paper combines the fuzzy entropy and evidence distance to express the uncertainty of the evidence and define the weights of the evidence.

3.1 Energy detection

Assuming that $s(t)$ denotes the signal transmitted by a PU, $n_i(t)$ denotes the additive white Gaussian noise on the authorized frequency band, $h(t)$ is the channel gain on the authorized band, $x_i(t)$ represents the received signal at the ith SU $(i = 1, 2, \dots, N)$, where N is the number of SUs participating in cooperative spectrum sensing.

$$x_i(t) = \begin{cases} n_i(t), & H_0 \\ h_i \cdot s(t) + n_i(t), & H_1 \end{cases} \tag{1}$$

In this paper, the local spectrum sensing is realized by the energy detection method. The detection statistics of the energy detection is as follows:

$$x_{E_i} = \sum_{k=1}^{N} |x_i(k)|^2 \tag{2}$$

where k denotes the kth sampling point and $N = 2TW$, T and W are the product of the signal duration and signal bandwidth. According to the central limit theorem, x_{E_i} is approximately subject to the Gaussian distribution when N is large enough.

3.2 Distribution and correction of basic probability assignment (BPA)

Consider a subset A on the domain X, and for any x belonging to X, we specify a number $\mu_A(x) \in [0,1]$ to denote the degree of x belonging to A, it can be expressed as $A = \{(x, \mu_A(x) | x \in X\}$. $\mu_A(x)$ is called the membership function (generalized characteristic function) of A. Membership functions can be approximated by some common functions which are in accordance with the essential characteristics of fuzzy variables.

There are two possible outcomes of the spectrum sensing: H_1 and H_0. Θ indicates that the result might be H_1 or H_0. For a subset H_0 of the decision result domain of spectrum sensing, a number $\mu_{H_0}(x_{E_i})$ is assigned to any detection statistic x_{E_i} to denote the degree of x_{E_i} belonging to H_0. $\mu_{H_0}(x_{E_i})$ is called the membership function of H_0. When the number of sampling points is large enough, the membership function is Gauss-type because x_{E_i} obeys the Gaussian distribution in the two cases of H_1 and H_0.

$$\begin{cases} H_0 : \mu_{H_0}(x_{E_i}) = \exp\left(-\dfrac{(x_{E_i} - \mu_0)^2}{a\sigma_0^2}\right) \\ H_1 : \mu_{H_1}(x_{E_i}) = \exp\left(-\dfrac{(x_{E_i} - \mu_1)^2}{a\sigma_1^2}\right) \end{cases} \tag{3}$$

The degree of x_{E_i} belonging to Θ can be expressed as

$$\mu_\Theta(x_{E_i}) = 1 - \max(\mu_{H_0}(x_{E_i}), \mu_{H_1}(x_{E_i})).$$

As the values of the adjustment factor increase, the downward trend of the membership function curve in (3) becomes slower and the opening range becomes larger. The probability that the random variable x_{E_i} falls outside $(\mu - 3\sigma, \mu + 3\sigma)$ is less than three-thousandths, which is the "3σ" principle of the normal distribution. Consider that the majority of x_{E_i} can be assigned a reasonable degree of membership, the adjustment factor a is set to 9.

Assuming that there is a decision problem, we can recognize that the set of all possible outcomes is denoted by $\varOmega$ which is called the recognition framework. The function is called BPA when the following conditions are satisfied:

$$\boldsymbol{m}(\varPhi) = 0 \tag{4}$$
$$\sum_{A \subseteq \varOmega} \boldsymbol{m}(A) = 1.$$

For any A belonging to $\varOmega$, $\boldsymbol{m}(A)$ is called the BPA of proposition A.

In spectrum sensing, the recognition framework $\varOmega$ is composed of H_1, H_0 and Θ. The sum of the BPSs under the same recognition frame $\varOmega$ is 1 [29]. The BPA functions of H_1, H_0 and Θ are shown as follows.

$$\boldsymbol{m}_{H_1}(A_i) = \frac{\mu_{H_1}(x_{E_i})}{\mu_{H_1}(x_{E_i}) + \mu_{H_0}(x_{E_i}) + \mu_\Theta(x_{E_i})}$$

$$\boldsymbol{m}_{H_0}(A_i) = \frac{\mu_{H_0}(x_{E_i})}{\mu_{H_1}(x_{E_i}) + \mu_{H_0}(x_{E_i}) + \mu_\Theta(x_{E_i})}$$

$$\boldsymbol{m}_\Theta(A_i) = \frac{\mu_\Theta(x_{E_i})}{\mu_{H_1}(x_{E_i}) + \mu_{H_0}(x_{E_i}) + \mu_\Theta(x_{E_i})} \tag{5}$$

When an MU launches an AO, AF or AB attack, there is a difference between the data reported to the FC and the data reported by the honest user. The classical conflict coefficient is usually used to describe the degree of non-inclusion of the focal elements, but when the data are completely in conflict, the correct result cannot be obtained. Later, the distance function was proposed to solve the above problems. The distance and the conflict in the representation of evidence are complementary. In order to better describe the conflicts of different user data, this paper combines the two and defines a new conflict coefficient to accurately identify MUs.

For the decision results H_1 and H_0 of spectrum sensing, the BPAs are $\boldsymbol{m}_{H_1}$ and $\boldsymbol{m}_{H_0}$, respectively. The distance between the propositions H_1 and H_0 can be expressed as

$$d_{\mathrm{BPA}}(\boldsymbol{m}_{H_1}, \boldsymbol{m}_{H_0}) = \sqrt{\frac{1}{2}(\boldsymbol{m}_{H_1} - \boldsymbol{m}_{H_0})^{\mathrm{T}} \boldsymbol{D} (\boldsymbol{m}_{H_1} - \boldsymbol{m}_{H_0})} \tag{6}$$

where $\boldsymbol{D}$ is a positive definite matrix, and the elements in the matrix satisfy $\boldsymbol{D}(A_i, A_j) = \dfrac{|A_i \cap A_j|}{|A_i \cup A_j|}$, $\cap$ and $\cup$ represent intersection and union, respectively.

The distance between focal elements $\boldsymbol{m}_{H_1}$ and $\boldsymbol{m}_{H_0}$ is a function of $\boldsymbol{D}$. $|A_i \cap A_j|$ denotes the similarity between A_i and A_j. If $|A_i \cap A_j| = 0$, it shows that there is no common element between A_i and A_j, and the similarity is 0. Thus, we can use the distance of evidence to express the degree of difference between evidence. The greater the distance is, the greater the difference between them will be, and vice versa.

In addition, the expression of the classical conflicting coefficient for the two basic probability functions is

$$k = \sum_{A_i \cap A_j = \emptyset} \boldsymbol{m}_{H_1}(A_i) \cdot \boldsymbol{m}_{H_0}(A_j) \tag{7}$$

where $i = 1, 2, \dots, n$ (or $j = 1, 2, \dots, n$) represents the ith (or jth) evidence.

We define the new conflicting cf_{ij} between users i and j as follows, and $cf_{ij} \in [0,1]$.

$$cf_{ij} = \sqrt{\sqrt{k \cdot d_{\mathrm{BPA}}} \cdot \frac{k + d_{\mathrm{BPA}}}{2}} \tag{8}$$

After obtaining the degree of conflicting between SUs, a matrix of the degree of conflicting can be constructed:

$$\mathbf{CONF} = \begin{bmatrix} 0 & cf_{12} & \cdots & cf_{1n} \\ cf_{21} & 0 & \cdots & cf_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ cf_{n1} & cf_{n2} & \cdots & 0 \end{bmatrix}_{n \times n}. \tag{9}$$

The similarity can be calculated according to the new conflicting coefficient between the uers:

$$\mathrm{sim}(i,j)=1-cf_{ij}. \tag{10}$$

The similarity matrix $\boldsymbol{S}$ of the evidence can be obtained:

$$\boldsymbol{S}=\begin{bmatrix} 1 & 1-cf_{12} & \cdots & 1-cf_{1n} \\ 1-cf_{21} & 1 & \cdots & 1-cf_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1-cf_{n1} & 1-cf_{n2} & \cdots & 1 \end{bmatrix}_{n\times n}. \tag{11}$$

Calculate the degree of the ith user presented by other users:

$$\mathrm{Sup}(m_i)=\sum_{j=1,j\neq i}^{n}\mathrm{sim}(i,j),\quad i=1,2,\dots,n. \tag{12}$$

Normalize the support degree of the user to obtain the conflicting weight:

$$\sigma_i=\mathrm{Sup}(\boldsymbol{m}_i)/\sum_{j=1}^{n}\mathrm{Sup}(\boldsymbol{m}_j). \tag{13}$$

In the energy detection algorithm, the selection of the threshold value is very important, and it will have a great influence on the final sensing performance. When the detection value is near the threshold value, there is some uncertainty in the spectrum sensing results. The fuzzy entropy is a measure of fuzziness proposed by Bandemer. It can be represented by the fuzzy entropy in view of the uncertainty of sensing results. Let A be a fuzzy set, then its fuzzy entropy can be expressed as

$$H(A)=-\sum_{i=1}^{n}\mu_A(y_i)\log_2\mu_A(y_i) \tag{14}$$

where y_i is the element of the fuzzy set A, and $\mu_A(y_i)$ indicates the degree of y_i belonging to the set A.

For the three decision results H_1, H_0 and Θ, the fuzzy entropy of the evidence in the spectrum sensing system can be expressed as

$$H(\boldsymbol{m}_i)=-(\boldsymbol{m}_{H_0}(A_i)\log_2\boldsymbol{m}_{H_0}(A_i)+$$

$$\boldsymbol{m}_{H_1}(A_i)\log_2\boldsymbol{m}_{H_1}(A_i)+\boldsymbol{m}_{\Theta}(A_i)\log_2\boldsymbol{m}_{\Theta}(A_i)). \tag{15}$$

The larger the fuzzy entropy of the evidence is, the greater the uncertainty of the evidence is, the more intractable decision-making could be [30]. When the fuzzy entropy is large, it is given a small weight, which reduces its impact on the final result [31]. Therefore, the fuzzy weight of the user is defined as a negative exponential form of the constant, i.e.,

$$\rho_i=\frac{\exp(-H(\boldsymbol{m}_i))}{\sum\limits_{i=1}^{n}\exp(-H(\boldsymbol{m}_i))}. \tag{16}$$

The evidence weights based on users' data are obtained by combining the conflicting weight based on the new conflicting coefficient with the fuzzy weight based on the fuzzy entropy. The calculation method is as follows:

$$\omega_1^i=\sigma_i\cdot\rho_i^{-\Delta\sigma_i} \tag{17}$$

where $\Delta\sigma_i=\sigma_i-\dfrac{1}{n}\sum\limits_{j=1}^{n}\sigma_j$.

In cooperative spectrum sensing, the global decision result obtained by the FC is taken as a reference to judge whether the SU's local decision is correct or not, and the credibility of the user is updated. The calculation method of credibility is defined as follows:

$$r_i(k)=(-1)^{d_i(k)+d_0(k)}\cdot\tau^{\theta},\quad k=1,2,\dots \tag{18}$$

where d_i denotes the local sensing results of SU_i, and d_0 represents the global decision result of the FC. If d_i is consistent with d_0, the credibility of SU_i is increased by 1; otherwise, the credibility of SU_i is subtracted by τ. τ is a constant greater than 1, which is used to increase the credibility slowly but decreases rapidly. The calculation of θ is as follows:

$$\theta=\begin{cases}1, & d_i(k)\neq d_0(k)\\ 0, & d_i(k)=d_0(k)\end{cases}. \tag{19}$$

The weight of credibility ω_2^i is calculated as follows:

$$\omega_2^i=\begin{cases}\dfrac{r_i(k)}{\max\limits_i(r_i(k))}, & r_i(k)>0\\ 0, & r_i(k)\leqslant 0\end{cases}. \tag{20}$$

The comprehensive weight ω^i of SU_i is obtained by combining the evidence weight ω_1^i with the weight of credibility ω_2^i.

$$\omega^i=\begin{cases}\dfrac{\omega_1^i+\omega_2^i}{\max\limits_i(\omega_1^i+\omega_2^i)}, & \omega_2^i>0\\ 0, & \omega_2^i=0\end{cases} \tag{21}$$

The honest users and MUs are distinguished according to their credibility weights. MUs are not allowed to participate in subsequent evidence fusion when they launch AO, AF or AB attack. For the honest users, the BPA function is modified by using the above comprehensive weight, that is $\boldsymbol{m}'_{H_0}(A_i)$ and $\boldsymbol{m}'_{H_1}(A_i)$.

$$\boldsymbol{m}'_{H_0}(A_i)=\omega^i\cdot\boldsymbol{m}_{H_0}(A_i)$$

$$\begin{aligned} \boldsymbol{m}'_{H_1}(A_i) &= \omega^i \cdot \boldsymbol{m}_{H_1}(A_i) \\ \boldsymbol{m}'_{\Theta}(A_i) &= \omega^i \cdot \boldsymbol{m}_{\Theta}(A_i) \end{aligned} \tag{22}$$

3.3 Evidence fusion and judgment

Finally, two or more BPA functions are orthogonal and calculated by using the D-S fusion formula to get the total BPA function which is used to be compared with the threshold λ to get the final decision result d_0.

$$\boldsymbol{m}_{H_0} = \frac{\sum\limits_{B \cap C = H_0} \boldsymbol{m}'_B(A_i)\boldsymbol{m}'_C(A_i)}{1 - \sum\limits_{B \cap C = \emptyset} \boldsymbol{m}'_B(A_i)\boldsymbol{m}'_C(A_i)} \tag{23}$$

$$\boldsymbol{m}_{H_1} = \frac{\sum\limits_{B \cap C = H_1} \boldsymbol{m}'_B(A_i)\boldsymbol{m}'_C(A_i)}{1 - \sum\limits_{B \cap C = \emptyset} \boldsymbol{m}'_B(A_i)\boldsymbol{m}'_C(A_i)} \tag{24}$$

where B and C can be H_1, H_0 or Θ.

$$d_0 = \begin{cases} 1, & \dfrac{\boldsymbol{m}_{H_1}}{\boldsymbol{m}_{H_0}} > \lambda \\ 0, & \dfrac{\boldsymbol{m}_{H_1}}{\boldsymbol{m}_{H_0}} \leqslant \lambda \end{cases} \tag{25}$$

Given the above discussion, the procedures of the algorithm based on the evidence theory and fuzzy entropy to resist SSDF attacks is given in the following.

(i) Each user obtains the local sensing result through energy detection.

(ii) The degree of membership function and BPA function are assigned to SUs according to the sensing result.

(iii) The new conflicting coefficient and the conflicting weight are obtained according to the evidence distance and classical conflicting coefficient.

(iv) The fuzzy weight of evidence is obtained by the fuzzy entropy.

(v) The credibility is updated to obtain the credibility weight.

(vi) The BPA of the evidence is corrected based on the above weight.

(vii) The final result is obtained by using the fusion formula.

4. Simulation results and analysis

The simulation experiments are provided to evaluate the performance of the algorithm based on the evidence theory and fuzzy entropy. The algorithm is compared with the following methods, the single-user detection method (denoted as SIN in the figures), a method for evaluating the reliability of sensor nodes and the degree of mutual support between different sensor nodes proposed by Men et al. [24]. Yu et al. used the similarity of the evidence to calculate the reliability of users [25]. The simulation parameters are set as follows: there is a PU and an FC in the system, the number of SUs participating in cooperative spectrum sensing is 6, and the time bandwidth product u is 10. The probability that the PU exists is 0.5, so is the absence. τ's value is 2. The intensity of AF attack is 0.5, and the strength of AB attack is 2. The credibility threshold is 0.7, and the number of simulations is 10 000. Assuming that the transmission channel is not affected by shadow fading, the channel gain is a constant.

Figs. 2–4 show the receiver operating characteristic (ROC) curve of two MUs who launch the same attack type. Fig. 2 shows that there are two AO attack users in the system, and the proportion of MUs is 33%. It can be seen that the performance of the proposed algorithm is obviously better than that of the other two algorithms. When two users simultaneously launch AO attacks, the data similarity is small, and the method based on user similarity and mutual support cannot be accurately sensed, so the performance is not good.

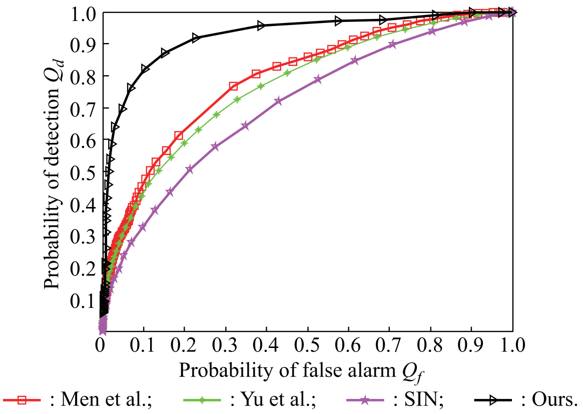


Fig. 2 ROC of two users launching AO attack

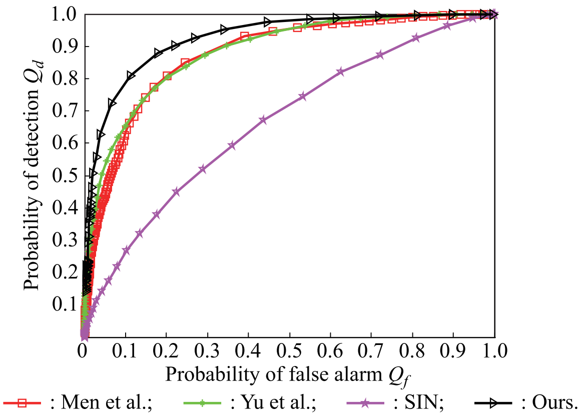


Fig. 3 ROC of two users launching AB attack

Fig. 3 shows that there are two AB attack users in the system. It can be seen that the performance of the proposed algorithm is the best. Because the other two algorithms have a worse ability to distinguish honest users from MUs when the number of MUs increases, and MUs constantly report the results of the existence of the main user signal, resulting in a small difference in the detection statistics of the users. Therefore, the performance of the algorithms proposed in [25] and [24] are similar, but they are better than the single-user detection algorithm.

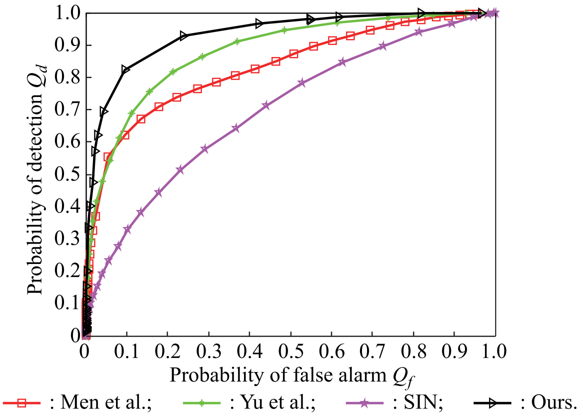


Fig. 4 ROC of two users launching AF attack

Fig. 4 shows that there are two AF attack users in the system. It can be seen that the performance of the proposed algorithm is the best. The performance of the algorithm proposed by Yu et al. is slightly worse. Then it is the algorithm based on the degree of mutual support of users proposed by Men et al. The worst performance is the method of single-user detection.

Figs. 5–7 show that there are two MUs, but the two users adopt different types of attacks, the proportion of MUs is 33%. Fig. 5 shows that there is an AB attack user and an AF attack user in the system. It can be seen that the proposed algorithm is superior to the other two algorithms.

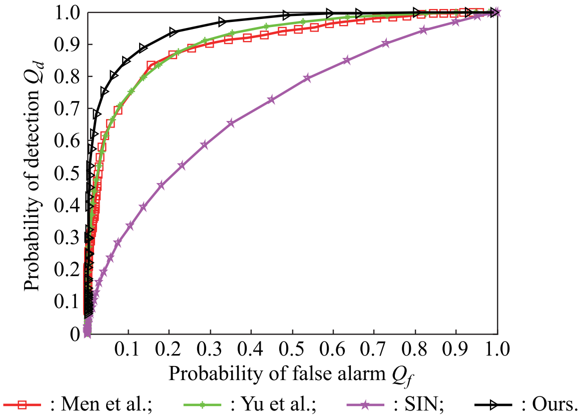


Fig. 5 ROC of a user launching AF attack and a user launching AB attack

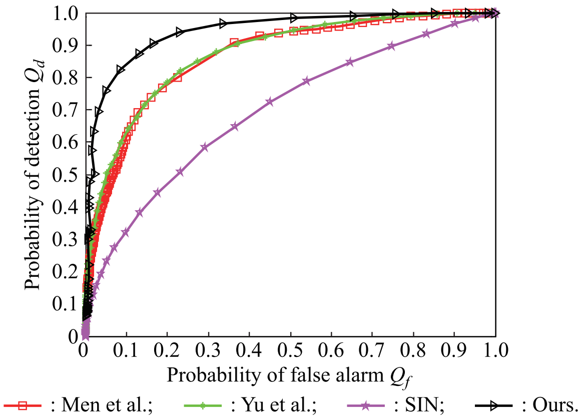


Fig. 6 ROC of a user launching AO attack and a user launching AB attack

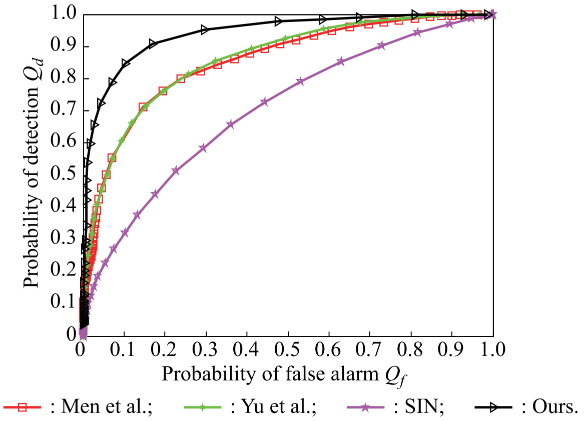


Fig. 7 ROC of a user launching AF attack and a user launching AO attack

Because of the large gap between the AB attack and the AF attack data, the user data is recognized. The similarity between the two is low, and the algorithm proposed by Yu et al. can play a better role, and the performance is the second. Since the data reported to the FC is quite different, honest users cannot judge whether the results are correct, so the performance of Men's algorithm based on user mutual support is affected, which is slightly lower than that of other algorithms.

Fig. 6 shows the ROC curves for an AO attack user and Fig. 7 shows an AB attack user, an AO attack user and an AF attack user. Because the new conflict coefficient is quoted and the influence of evidence distance on data similarity is considered, the detection accuracy of the proposed algorithm is higher, while the other two algorithms cannot identify MU data accurately, so the performance of the proposed algorithm is obviously better than that of other algorithms.

Figs. 8–10 show the ROC curve of the system under AF, AO and AB attacks, where there are four MUs in cognitive wireless networks, and the proportion of MUs is 66%.

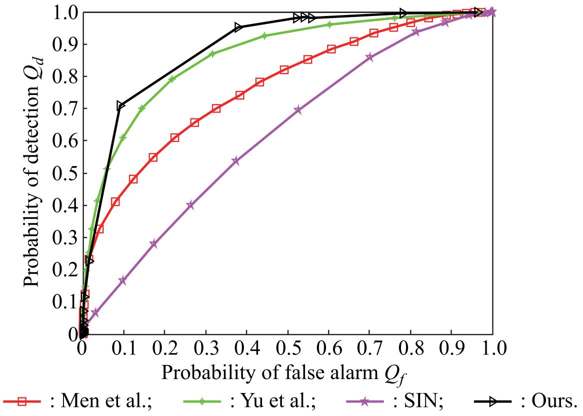


Fig. 8 ROC of four users launching AF attack

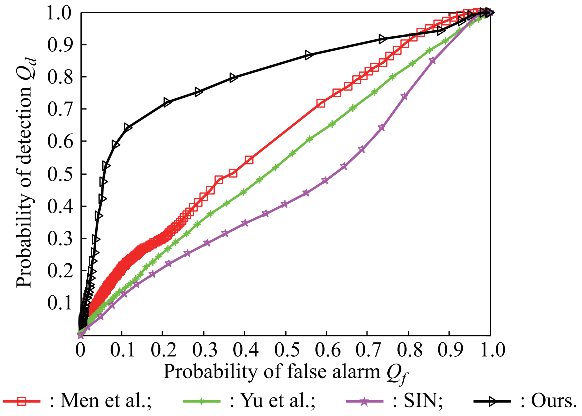


Fig. 9 ROC of four users launching AO attack

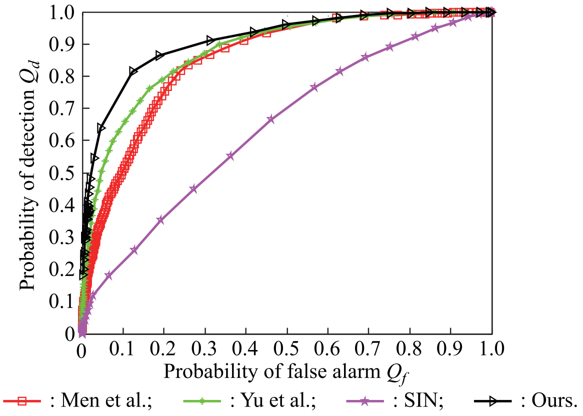


Fig. 10 ROC of four users launching AB attack

As can be seen from Fig. 8, for the case of four AF attacks, the proposed algorithm performs the best, the algorithm proposed by Yu et al. the second, and the algorithm proposed by Men et al. the third, and the worst performance comes from the single-user detection method. Since the conflict coefficient is redefined in this paper and is used as a part of the weight coefficient, the conflict between data is described more accurately, so the optimal detection performance is obtained.

As can be seen from Fig. 9, when there are four AO attack users in the system, the detection performance decreases due to the high proportion of malicious data. Because the Jousselme distance of evidence is introduced to distinguishing the data better, the performance of this algorithm is better than that of other algorithms.

As can be seen from Fig. 10, when there are four AB attack users in the system, the detection probability is higher because the users keep reporting the results of the presence of the PU signal. The performances in [25] and [24] are close. The algorithm introduces the fuzzy weight of evidence and provides an approximate result when the FC cannot completely determine the sensory data, which improves the detection performance.

Figs. 11 – 13 show that four MUs launch different attacks, and the proportion of MUs is 66%. It can be seen from Fig. 11 that the proposed algorithm performs the best when there are two AF attack users and two AO attack users, followed by the algorithm proposed by Men et al., then the algorithm proposed by Yu et al., and finally the single-user sensing algorithm.

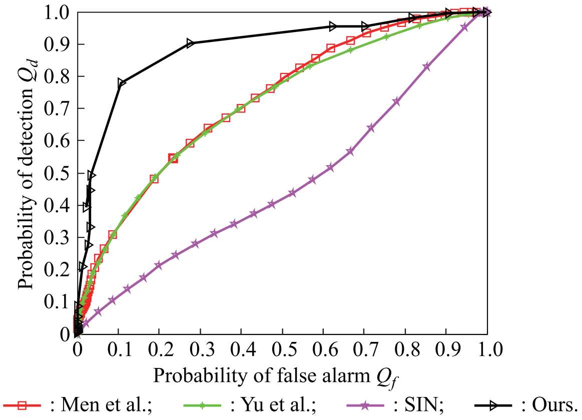


Fig. 11 ROC of two user launching AF attack and two user launching AO attack

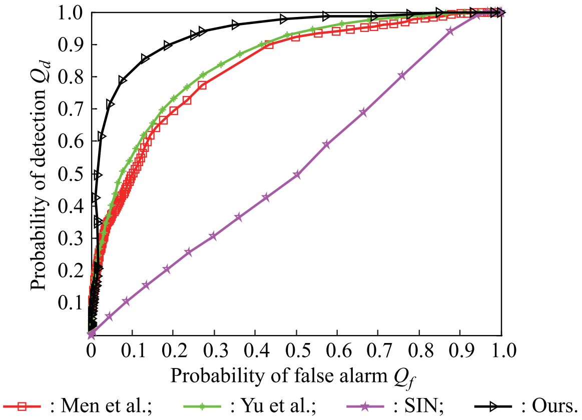


Fig. 12 ROC of two user launching AB attack and two user launching AO attack

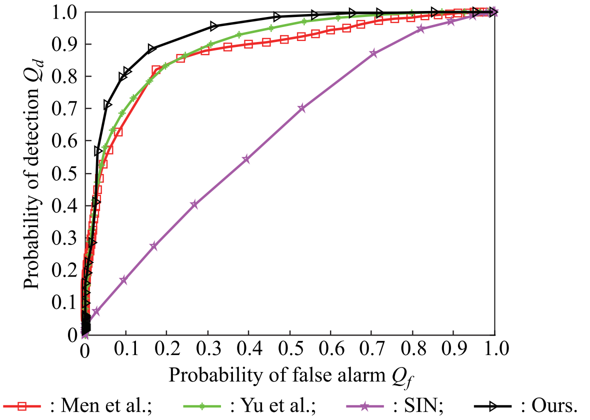


Fig. 13 ROC of two user launching AB attack and two user launching AF attack

Compared with the result in Fig. 12, it can be seen that the algorithm proposed in [25] is more suitable for AB attack, and the algorithm proposed in [24] is more suitable for AF attack.

When there are two AB attack users and two AF attack users, the data reported by the users are quite different, and the detection performance of the three algorithms is similar. However, the algorithm in this paper considers both data similarity and uncertainty, so it has the best detection effect.

5. Conclusions

In order to solve the problem of SSDF attacks by MUs, an algorithm based on the evidence theory and fuzzy entropy is proposed in this paper. The SUs obtain the degree of membership function and BPA function according to the local result by energy detection. The new conflicting coefficient is calculated based on the evidence distance and classical conflicting coefficient, and the conflicting weight of the evidence is obtained. The fuzzy entropy is used to obtain the fuzzy weight. The credibility weight is obtained by updating the credibility. The BPA function of the evidence is corrected based on the above weight. The final result is obtained by using the fusion formula. Simulation results show that the proposed algorithm can maintain a good performance under different attack modes of the MUs. Compared with other algorithms, the proposed algorithm has a good robustness and can effectively resist SSDF attacks.

References

[1] HAYKIN S. Cognitive radio: brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications, 2005, 23(2): 201 – 220.

[2] SUN Q, TIAN Y, DIAO M. Cooperative localization algorithm based on hybrid topology architecture for multiple mobile robot system. IEEE Internet of Things Journal, 2018, 5(6): 4753 – 4763.

[3] MITOLA J, MAGUIRE G Q. Cognitive radio: making software radios more personal. IEEE Personal Communications, 1999, 6(4): 13 – 18.

[4] NIU C, LI Y, HU R Q, et al. Fast and efficient radio resource allocation in dynamic ultra-dense heterogeneous networks. IEEE Access, 2017, 5(99): 1911 – 1924.

[5] ALTHUNIBAT S, DENISE B J, GRANELLI F. Secure cluster-based cooperative spectrum sensing against malicious attackers. Proc. of the IEEE Globecom Workshops, 2015: 1284 – 1289.

[6] XIE J, CHEN J, WU D. Cooperative spectrum sensing for cognitive radios over fading channels. Proc. of the International Conference on Computer Science and Network Technology, 2012: 1962 – 1966.

[7] SHARIFI A A, NIYA J M. Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks. Wireless Personal Communications, 2016, 90(1): 1 – 17.

[8] SHINDE S C, JADHAV A N. Centralized cooperative spectrum sensing with energy detecion in cognitive radio and optimization. Proc. of the IEEE International Conference on Recent Trends in Electronics, 2017: 1002 – 1006.

[9] ZHOU M, SHEN J, CHEN H, et al. A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks. Proc. of the IEEE Wireless Communications and Networking Conference, 2013: 614 – 619.

[10] DO N, AN B. A soft-hard combination-based cooperative spectrum sensing scheme for cognitive radio networks. Sensors, 2015, 15(2): 4388 – 4407.

[11] MUSTAPHA I, MOHD ALI B, RASID M F, et al. A weighted hard combination scheme for cooperative spectrum sensing in cognitive radio sensor networks. Proc. of the IEEE Malaysia International Conference on Communications, 2016: 12 – 17.

[12] AKYILDIZ I F, LEE W Y, CHOWDHURY K R. CRAHNs: cognitive radio ad hoc networks. Ad Hoc Networks, 2009, 7(5): 810 – 836.

[13] BI Y, JING X, SUN S, et al. Hierarchical fusion-based cooperative spectrum sensing scheme in cognitive radio networks. Proc. of the International Symposium on Communications and Information Technologies, 2016: 579 – 583.

[14] SHEN B, CUI T P, KWAK K, et al. An optimal soft fusion scheme for cooperative spectrum sensing in cognitive radio network. Proc. of the IEEE Wireless Communications and Networking Conference, 2009: 1 – 5.

[15] PEI Q Q, YUAN B B, LI L, et al. A sensing and etiquette reputation-based trust management for centralized cognitive radio networks. Neurocomputing, 2013, 101(3): 129 – 138.

[16] ZHANG J, CAI L, ZHANG S. Malicious cognitive user identification algorithm in centralized spectrum sensing system. Future Internet, 2017, 9(4): 79.

[17] FENG J Y, ZHANG M, XIAO Y, et al. Securing cooperative spectrum sensing against collusive SSDF attack using XOR distance analysis in cognitive radio networks. Sensors, 2018, 18(2): 370.

[18] ZHANG W Q, DENG Y. Combining conflicting evidence using the DEMATEL method. Soft Computing, 2019, 23(17): 8207 – 8216.

[19] ZHANG X, TANG X, TIAN F. A spectrum sensing algorithm based on improved D-S evidence theory. Computer Technol-

ogy and Development, 2014, 24(6): 44 – 48.

[20] GHOSH S, BHOWMICK A, NALLAGONDA S, et al. Performance of weighted fusion based spectrum sensing under double threshold in cognitive radio network. Proc. of the IEEE International Conference on Microelectronics, Computing and Communications, 2016: 1 – 4.

[21] PENG Q, ZENG K, WANG J, et al. A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context. Proc. of the IEEE International Symposium on Personal Indoor and Mobile Radio Communications, 2006: 1 – 5.

[22] NIE M, SHAO J, LI B. Cooperative sensing algorithm based on dynamic double threshold and D-S evidence theory. Journal of Nanjing Normal University (Engineering and Technology Edition), 2014, 14(2): 43 – 48. (in Chinese)

[23] FENG J Y, LI J L, LU G Y. Evaluating uncertainty behaviors of cognitive users against SSDF attack for cooperative spectrum sensing. Telecommunications Science, 2015, 31(2): 97 – 102.

[24] MEN S, CHARGÉ P, PILLEMENT S. A robust cooperative spectrum sensing method against faulty nodes in CWSNs. Proc. of the IEEE International Conference on Communication Workshop, 2015: 334 – 339.

[25] YU M T, ZHAO L J, LI Z. Improved cooperative spectrum sensing scheme based on Dempster-Shafer theory in cognitive radio network. Journal on Communications, 2014, 35(3): 168 – 173.

[26] ZHANG L, DING G, WU Q, et al. Defending against byzantine attack in cooperative spectrum sensing: defense reference and performance analysis. IEEE Access, 2016, 4: 4011 – 4024.

[27] LI Y B, YANG R, YE F, et al. Improved spectrum sharing algorithm based on feedback control informationin cognitive radio networks. Systems Engineering and Electronics, 2013, 24(4): 564 – 570. (in Chinese)

[28] KIM H, RYU E. Delegation based user authentication framework over cognitive radio networks. Journal of Sensor & Actuator Networks, 2017, 6(4): 29.

[29] SUN R, DENG Y. A new method to identify incomplete frame of discernment in evidence theory. IEEE Access, 2019, 7: 15547 – 15555.

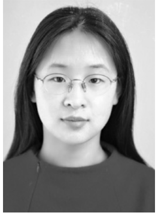
[30] LI Y, DENG Y. Generalized ordered propositions fusion based on belief entropy. International Journal of Computers Communications & Control, 2018, 13(5): 792 – 807.

[31] LIU Y T, PAL N R, MARATHE A R, et al. Weighted fuzzy Dempster – Shafer framework for multimodal information integration. IEEE Trans. on Fuzzy Systems, 2018, 26(1): 338 – 352.

Biographies

YE Fang was born in 1980. She received her B.S. and Ph.D. degrees in electrical information engineering from Harbin Engineering University in 2002 and 2006, respectively. During 2007-2008, she worked as a visiting scholar in University of Southampton. At present, she is an associate professor in Harbin Engineering University. Her research interests include cognitive radio network and radio resource management.
E-mail: yefang0923@126.com

BAI Ping was born in 1994. She received her B.S. and M.S. degrees from Harbin Engineering University in 2016 and 2019, respectively. During her postgraduate period, she concentrated on cognitive radio spectrum sensing. At present, she is an algorithm engineer in Huawei company.
E-mail: baiping0325@126.com



TIAN Yuan was born in 1978. She received her B.S and M.S. degrees from Harbin Engineering University in 2000 and 2006, respectively. At present, she is a lecturer in Harbin Engineering University. Her research interests include cognitive radio network and radio resource management.
E-mail: tianyuan347@126.com