future internet

MDPI

Article

Malicious Cognitive User Identification Algorithm in Centralized Spectrum Sensing System

Jingbo Zhang, Lili Cai * and Shufang Zhang

Information Science and Technology College, Dalian Maritime University, Dalian 116026, China; zhang_jingbo@dlmu.edu.cn (J.Z.); sfzhang@dlmu.edu.cn (S.Z.)

* Correspondence: cai_lili@dlmu.edu.cn; Tel.: +86-0411-84723118

Received: 30 September 2017; Accepted: 6 November 2017; Published: 8 November 2017

Abstract: Collaborative spectral sensing can fuse the perceived results of multiple cognitive users, and thus will improve the accuracy of perceived results. However, the multi-source features of the perceived results result in security problems in the system. When there is a high probability of a malicious user attack, the traditional algorithm can correctly identify the malicious users. However, when the probability of attack by malicious users is reduced, it is almost impossible to use the traditional algorithm to correctly distinguish between honest users and malicious users, which greatly reduces the perceived performance. To address the problem above, based on the β function and the feedback iteration mathematical method, this paper proposes a malicious user identification algorithm under multi-channel cooperative conditions (β-MIAMC), which involves comprehensively assessing the cognitive user's performance on multiple sub-channels to identify the malicious user. Simulation results show under the same attack probability, compared with the traditional algorithm, the β-MIAMC algorithm can more accurately identify the malicious users, reducing the false alarm probability of malicious users by more than 20%. When the attack probability is greater than 7%, the proposed algorithm can identify the malicious users with 100% certainty.

Keywords: collaborative spectrum sensing; spectrum-sensing false data; β function; feedback iteration; false alarm probability of malicious users

1. Introduction

Spectrum sensing is a key link of cognitive radio and the perceived performance will directly affect the performance of the whole cognitive radio system [1]. At present, the commonly-used spectrum sensing technologies can be divided into three categories: single-user spectrum sensing, distributed collaborative spectrum sensing, and centralized collaborative spectrum sensing. Single-user spectrum sensing technology can only rely on its own perception results, and thus the problems of hidden terminals exist [2]. Distributed collaborative spectrum sensing technology can rely on the perception results of neighboring cognitive users to achieve an increased sensing accuracy, but the method will greatly increase the complexity of the terminal design [3]. The centralized collaborative spectrum sensing technology can greatly improve the perceived precision because it can obtain the perceived result of all the cognitive users in the data fusion center. Furthermore, the demands of the sensing terminal design are not high, [3] and therefore centralized collaborative spectrum sensing technology has drawn more extensive attention.

In the centralized collaborative spectrum sensing system, the multi-user perceptual architecture of spectrum resources can greatly improve the sensing accuracy of the data fusion center. However, malicious users will seriously affect the reliability of the system, so the real-time monitoring of the reliability of multi-users is a key problem that the centralized collaborative spectrum sensing system needs to solve.

The malicious cognitive users can usually be divided into two categories according to the probability of the malicious cognitive user sending a wrong perceived result. The first category malicious users (I-MUs) refers to those which are caused by equipment failure, causing them to send a wrongly perceived result at a large probability. The second category of malicious users (II-MUs) refers to the cognitive users, who want to deliberately interfere with the normal operations of the system. In order to enhance their own concealment, II-MUs usually send tampered perceived results with a smaller probability. This behavior is called Spectrum Sensing Data False (SSDF) attacks [4]. In order to interfere with the main user or exclusive bands, these cognitive users tamper with their own perceived results, report tampered spectrum sensing information to the data fusion center, disturb the centralized cooperative spectrum sensing algorithm to determine the true spectral state and reduce the perceived performance.

The traditional fusion algorithm can identify the first category of malicious cognitive users (I-MU) with high attack probability, but can hardly identify the second category of malicious cognitive users (II-MU). In order to improve the reliability of the centralized collaborative spectrum sensing system, it is necessary to solve the SSDF problem. A study [5] proposed a "stripping onion" approach to combat SSDF attacks, in which the central node of the cognitive radio network compares the suspicious degree of the cognitive user with the detection threshold to identify the malicious cognitive user and rejects the perceived result of the malicious cognitive user from the decision. The algorithm needs prior master knowledge of the channel usage rules, or the ability to detect malicious cognitive users will be severely reduced. However, prior knowledge of channel usage is not readily available in reality. Reference [6] proposed a weighted order probability ratio test method based on prestige in order to detect malicious cognitive users and achieve reliable spectrum sensing in the joint spectrum sensing process. However, the algorithm needs to know the prior probabilities of each cognitive user's perceived results, resulting in the computational complexity and communication overhead being too large. Reference [7] proposed a confidence-based colony multi-ant random walk (CARW) algorithm to identify the malicious cognitive users. This method combines the game theory to establish the behavioral game model between honest cognitive users and malicious cognitive users, and based on this model quantitatively calculating the caution of the microblogging users, this method strengthens the microblogging user behavior characteristics' ability to distinguish honest users and malicious users. Reference [8] proposed a single channel centralized spectrum sensing algorithm based on the β-reputation (β-SCCSA) system [9]. This algorithm determines the cognitive user's reputation and weight by knowing the cognitive user's historical performance and can react effectively against malicious cognitive users. However, when a malicious user reduces the attack probability (to improve chances of remaining undetected), the algorithm takes a long time to identify malicious users, or simply cannot identify malicious users.

Based on existing research results and the characteristics of collaborative spectrum sensing, we propose using the β-MIAMC algorithm to solve the problem of malicious user identification when the malicious user attack probability is small. By analyzing the simulation results in the case of a small attack probability, the proposed algorithm can reduce the false alarm probability of malicious users by more than 20%. When the attack probability is greater than 7%, the proposed algorithm can distinguish malicious users with 100% certainty.

2. System Model

In order to deal with the problem of SSDF attack in the centralized collaborative spectrum sensing architecture, we propose a malicious cognitive user identification algorithm based on β function and feedback iterative method. Addressing the shortcomings of the prestige evaluation system under the traditional single channel condition and combining them with the characteristics of multiple sub-channels of collaborative sensing, we propose a prestige evaluation system based on multi-channel cooperation.

2.1. Centralized Collaborative Spectrum Sensing System Model

In cognitive radio systems, centralized collaborative spectrum sensing has drawn extensive attention due to its high perceived accuracy and low complexity of perceived terminals. As shown in Figure 1, the centralized collaborative spectrum sensing system consists of multiple cognitive users and a data fusion center.

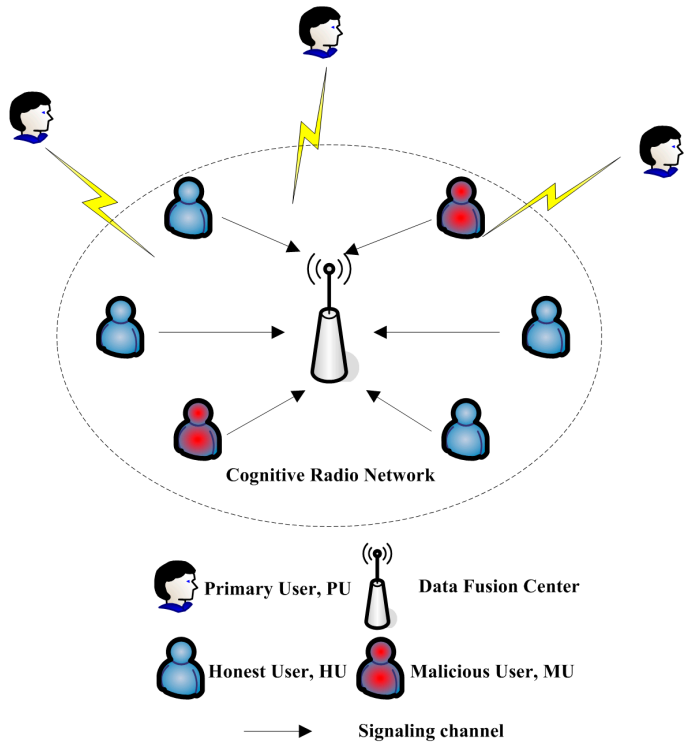


Figure 1. Centralized collaborative spectrum sensing system model.

In the cognitive wireless communication system, the available frequency band B is usually divided into N copies of non-overlapping sub-channels. During the period of spectrum sensing, K primary users randomly occupy different sub-channels for communicating (K is much smaller than N). In the stage of spectrum sensing, cognitive users typically use the energy detection method [10] to sense the spectral state and send the perceived results to the data fusion center, before the system enters into the centralized fusion stage.

According to the authenticity of the data transmitted by the cognitive user, we will divide the cognitive users into honest cognitive users (HUs) and malicious cognitive users (MUs). Malicious cognitive users tamper with local perceived results to the data fusion center and with the development of the perceived technology, the malicious cognitive users increase its degree of concealment by reducing the attack probability. This makes it difficult to quickly and correctly identify malicious cognitive users, thereby reducing the perceived performance [11,12]. Therefore, it is an urgent problem to identify malicious cognitive users accurately and efficiently in the case of high concealment of malicious cognitive users.

2.2. β Reputation System

By building a reputation system for all the cognitive users in the system, it is possible to effectively identify the hidden malicious users based on their historical data.

In order to mathematically model the system, we define the cognitive user sending to the fusion center as a dichotomy process with two possible outcomes $\{x, y\}$, where x indicates that the cognitive

user sends the true local perceived result to the data fusion center and y indicates that the cognitive user performs a SSDF attack.

Considering that the β-probability density function is usually used to describe the probability distribution properties of the two events and the dichotomy process [13], we use this mathematical model to construct the β-reputation system. We supposed that r represents the number of occurrences of the result x observed and s represents the number of occurrences of result y. For the probability of x (p_x) produced by the dichotomy following the β distribution, the probability density function can be expressed as:

$$f(p_x|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p_x^{\alpha-1}(1-p_x)^{\beta-1} \tag{1}$$

where $p_x \in [0,1]$; $\Gamma(\cdot)$ represents Gamma function; while β-distribution's parameters are $\alpha = r+1$, $\beta = s+1$ and $r \geq 0$, $s \geq 0$. The expectation of the β-distribution is:

$$E[p_x] = \frac{\alpha}{\alpha+\beta} \tag{2}$$

where $E[p_x]$ represents the average probability of the occurrence of the result x in the future after the number of occurrences of r and s of the observed results x and y are given. Since the first order variable p_x is continuous, for any given value of $p_x \in [0,1]$, the second order variable $f(p_x|\alpha,\beta)$ is negligible and meaningless. Therefore, the expected $E[p_x]$ of p_x is usually used to calculate the prestige.

2.3. Prestige Evaluation System in Spectrum Sensing

In order to effectively identify the second type of malicious users hidden in the centralized collaborative spectrum sensing system model, the β reputation evaluation system is usually used to analyze the cognitive users' reliability in the data fusion center. Currently, the cognitive user prestige building algorithm based on single channel decision is used and the system model of this algorithm is shown in Figure 2.

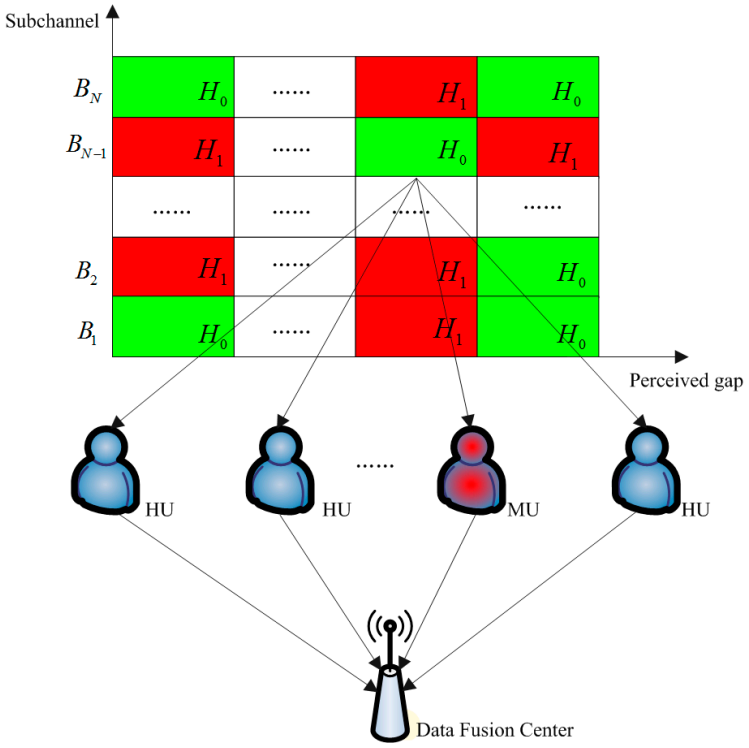


Figure 2. Single channel spectral sensing system model based on β-reputation system.

Figure 2 shows for the specific channel B_{N-1}, the data fusion center analyzes each cognitive users' perceived results of the channel in the system, before obtaining the confidence model of the cognitive users' perceived results for this channel. This method is more effective for finding the type of malicious users who interfere with a particular channel, although it is difficult to use this to accurately identify malicious users who are highly concealed.

SSDF attacks can be divided into three forms: false alarm attack, missed detection attack and probability attack in the process of centralized collaborative spectrum sensing [14]. In practice, the malicious cognitive users with the purpose of interfering with the sensing system usually use probabilistic attacks. In order to increase their concealment, malicious cognitive users generally attack with a method that randomly selects the channels. Broadband cognitive wireless communication systems typically divide spectrum resources into several independent sub-channels. In the same perceived interval, each cognitive user's perceived result on the different sub-channel should be correlated. Therefore, it is possible to more accurately distinguish hidden malicious cognitive users by comprehensively assessing the perceived results of cognitive users on multiple sub-channels. We propose a cognitive user reputation-building algorithm based on multi-channel collaboration. The algorithm uses the β-function and the feedback iteration for calculating, before integrating the perceived results of each cognitive user on each sub-channel. We modelled the reliability of cognitive user perceived results as a whole, using the system model of the algorithm shown in Figure 3.

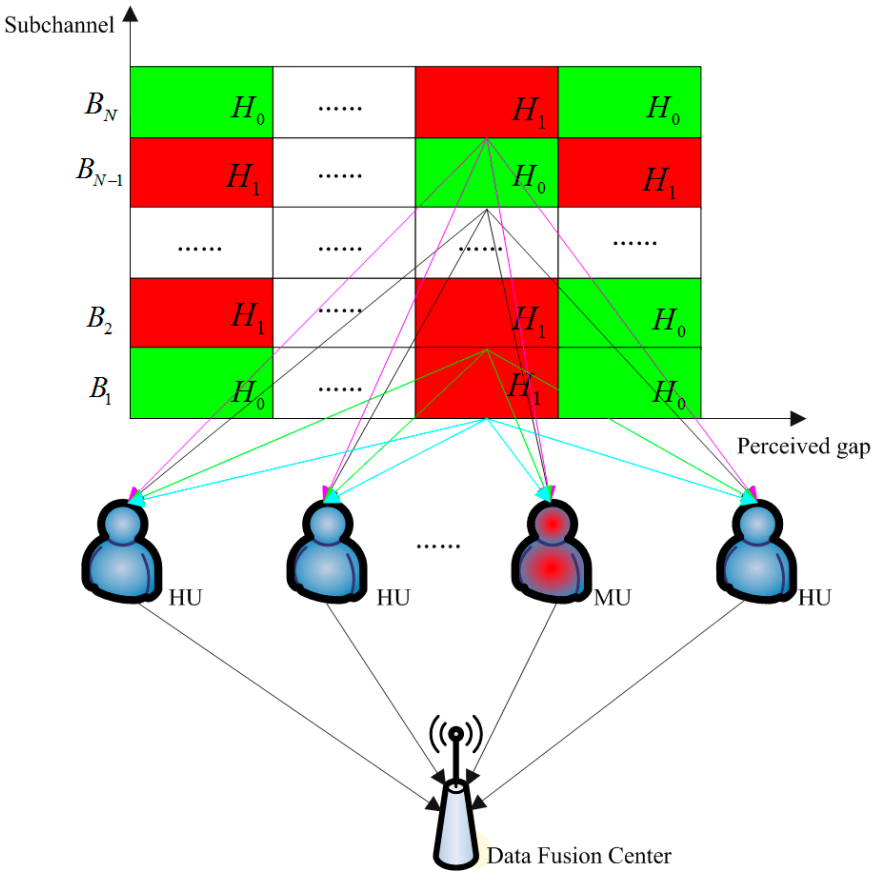


Figure 3. Multi-channel collaborative spectrum sensing system model based on β-reputation system.

In this system model, the data fusion center carries out the information fusion according to the plurality of cognitive users' perceived results on each sub-channel in order to calculate the optimal estimate of the occupied state of different sub-channels. After this, we adjust the reputation value of cognitive users by comparing the data provided by each cognitive user with the optimal estimate

value. After the data accumulates for a certain period of time, the data fusion center can distinguish the hidden malicious cognitive users.

3. Malicious User Identification Algorithm

We used the calculated prestige value to determine whether the cognitive user is a malicious cognitive user. Before discussing the malicious cognitive user identification algorithm based on multi-channel collaboration, we defined that the number of cognitive users in the system is J; the data fusion center assigning data depth to each cognitive user is L; and the initial reputation value of each cognitive user on each sub-channel is $R_{jn}(1) = \frac{1}{2}$ (where j represents a cognitive user and n represents a sub-channel).

Taking the lth spectrum sensing interval as an example, the algorithm is calculated as follows:

The reputation value of the cognitive user j on the nth sub-channel is $R_{jn}(l)$. According to Equation (3) we can calculate the weight of cognitive user j on the nth sub-channel:

$$\omega_{jn}(l) = \frac{R_{jn}(l)}{\sum_{j=1}^{J} R_{jn}(l)}, j = 1, \ldots, J; n = 1, \ldots, N \tag{3}$$

We combined this with the prestige value of the cognitive user on the sub-channel and the local perceived result of each cognitive user $d^{(j)}(l) \in \{0,1\}^{N\times 1}$ at this perceptual interval. Using Equation (4), we calculate the estimated state of each sub-channel:

$$\hat{d}_n(l) = \sum_{j=1}^{J} \omega_{jn}(l) d_n^{(j)}(l) \tag{4}$$

where $d_n^{(j)}(l)$ is the perceived result of the cognitive user j to the state of the sub-channel n. Comparing the estimated state $\hat{d}_n(l)$ of the sub-channel n on the perceived gap l with the majority decision threshold $d_{th} = \frac{1}{2}$ to obtain the actual state $d_n(l)$ of the sub-channel n on the perceived gap l, we obtain:

$$d_n(l) = \begin{cases} 0, \hat{d}_n(l) < d_{th} \\ 1, \hat{d}_n(l) \geq d_{th} \end{cases} \tag{5}$$

This $d_n(l)$ is used as the element to get the perceived vector $d(l) \in \{0,1\}^{N\times 1}$. Calculating the sum of the difference between the perceived results of the cognitive users on the sub-channels and the real state of the sub-channels, we obtain:

$$\Delta d_j(l) = \sum_{n=1}^{N} \left| d_n^{(j)}(l) - d_n(l) \right| \tag{6}$$

Using the mean of the sum of the perceived deviation of the cognitive users on all sub-channels as the threshold of the perceived deviation, we obtain:

$$\Delta \bar{d}(l) = \frac{1}{J} \sum_{n=1}^{N} \sum_{j=1}^{J} \Delta d_n^{(j)}(l) \tag{7}$$

By comparing the perceived result's deviation of the cognitive user with the deviation threshold, it is possible to obtain a positive or negative evaluation $r_j(l)$ of the cognitive user at this perceived gap as follows:

$$r_j(l) = \begin{cases} 0, \Delta d_j(l) \geq \Delta \bar{d}(l) \\ 1, \Delta d_j(l) < \Delta \bar{d}(l) \end{cases} \tag{8}$$

In this equation, $r_j(l) = 1$ indicates that the cognitive user j has made a positive contribution in the process of determining the channel state. On the contrary, $r_j(l) = 0$ indicates that the cognitive user j has made a negative effect in the process of determining the channel state.

It has been assumed that the data fusion center's maximum storage length to the cognitive user evaluation history record $r_j(l)$ is L. Essentially, the data fusion center can only store the cognitive users' evaluations that are obtained from L perceived gaps. Using the historical evaluation of cognitive users to calculate the positive total evaluation $P_j(l)$ and the negative total evaluation $N_j(l)$ at the perceived gap l, we obtain:

$$P_j(l) = \begin{cases} \sum_{l'=1}^{l} r_j(l')\lambda^{(l-l')}, l < L \\ \sum_{l'=l-L+1}^{l} r_j(l')\lambda^{(l-l')}, l \geq L \end{cases} \tag{9}$$

$$N_j(l) = \begin{cases} \sum_{l'=1}^{l} (1 - r_j(l'))\lambda^{(l-l')}, l < L \\ \sum_{l'=l-L+1}^{l} (1 - r_j(l'))\lambda^{(l-l')}, l \geq L \end{cases} \tag{10}$$

where λ is the forgetting factor used to reflect the dynamic characteristics of the prestige system [15]. $\lambda \in (0, 1]$ controls the forgotten rate of the historical evaluation. A smaller λ indicates a smaller influence of historical evaluation on the total evaluation and vice versa. The reputation value of the honest cognitive user that occasionally makes wrong sensing can be gradually returned to normal by the later good performance. The prestige parameters $\alpha_j(l)$ and $\beta_j(l)$ of the prestige system can be expressed as:

$$\alpha_j(l) = P_j(l) + 1 \tag{11}$$

$$\beta_j(l) = N_j(l) + 1 \tag{12}$$

Based on the prestige parameters of the cognitive user j on sub-channel n, the reputation value of the cognitive user j on the sub-channel n can be updated to $R_j(l + 1)$:

$$R_j(l + 1) = \frac{\alpha_j(l)}{\alpha_j(l) + \beta_j(l)} \tag{13}$$

This reputation value is used to calculate the weight parameter $\omega_j(l + 1)$ of the cognitive user j on each sub-channel in the next perceived gap.

The pseudo-code of this algorithm can be expressed as follows:

Algorithm Malicious user identification algorithm under multi-channel cooperative conditions

```
For l = 1 to G                          /*G is the perceived depth*/
  do  For j = 1 to J
    do  For n = 1 to N
      do  Calculate the weight value of the user on different channels
          Consolidate the user's perceived results
          if  d̂_n(l) < d_th
              d_n(l) = 0
          else
              d_n(l) = 1
          end if
          Calculate the deviation of the cognitive user on all subchannels
          Calculate the mean of all cognitive user deviations
          if  Δd_j(l) ≤ Δd̄(l)
              r_j(l) = 1
          else
              r_j(l) = 0
          end if
          Calculate the reputation parameter
          Calculate the user's reputation at the next interval
      end for
    end for
end for
```

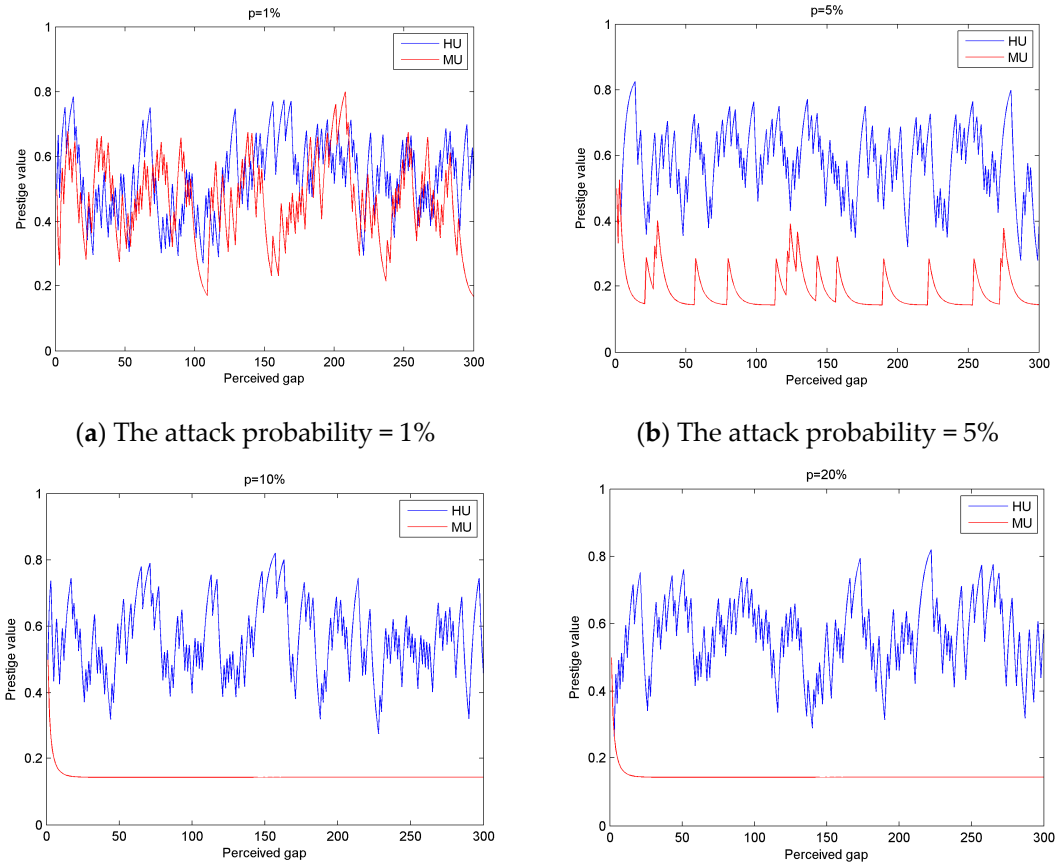
4. Algorithm Simulation and Performance Analysis

4.1. β-MIAMC Algorithm Availability Validation

In order to verify the availability of the proposed algorithm with different probabilities of attack from malicious users, the Monte Carlo simulation method is used. The experimental parameters are set as follows:

(1) The total available bandwidth is divided into N = 100 subchannels and the number of main users is K = 10 (that is, the occupied proportion of the spectrum is 10%);
(2) Cognitive radio networks include a data fusion center and J = 20 cognitive users, which contain honest cognitive users and malicious cognitive users;
(3) At the initial stage, the reputation value of the cognitive user is set to 0.5;
(4) The false alarm probability of honest cognitive users $p_f = 10\%$;
(5) In the data fusion center, the memory depth of each cognitive user prestige evaluation is L = 200 and the forgetting factor $\lambda = 0.8$;
(6) In order to strengthen the privacy of malicious users, set the number of malicious cognitive users $J_A = 1$.

Figure 4 depicts that in different attack probabilities, the reputation judgement results of the algorithm represent those of malicious users and one of the honest users at different perceived intervals in this paper.



(**a**) The attack probability = 1%

(**b**) The attack probability = 5%

(**c**) The attack probability = 10%

(**d**) The attack probability = 20%

Figure 4. The change in reputation value of cognitive users with different attack probabilities with sensing intervals.

As can be seen from the Figure 4:

1. With an increase in malicious user attack probability, the gap between the honest user reputation and malicious user reputation becomes larger. Essentially, with an increase in malicious user attack probability, honest users and malicious users can be more easily distinguished;
2. From Figure 4c,d, we can see that when the malicious user attack probability is large, the honest user's reputation fluctuates widely and the malicious user's reputation is gradually stabilized. This is because in this experiment, the honest user's false alarm probability is set to 10%, which creates an illusion of attack. However, in the subsequent judgment, the good performance of honest users will return the prestige value back to normal so the reputation of honest users with the perception of the interval will produce changes. When the attack probability is large, the use of feedback iterative mathematical algorithm results in the malicious users being basically in the attack state, so the popularity of malicious users tends to be fixed.

In order to verify the relationship between the convergent reputation value of the honest users and the malicious users at the different attack probabilities, we carried out 2000 Monte Carlo simulations and the concrete results are shown in Figure 5. It can be seen that as the attack probability increases, the reputation value of honest users gradually increases and tends to be stable, while the reputation value of malicious users is gradually reduced and tends to be fixed. Therefore, we set the median of the reputation value of the honest users and malicious users to the decision threshold. We can see that with this median as the decision threshold, we can accurately distinguish honest users and malicious users.

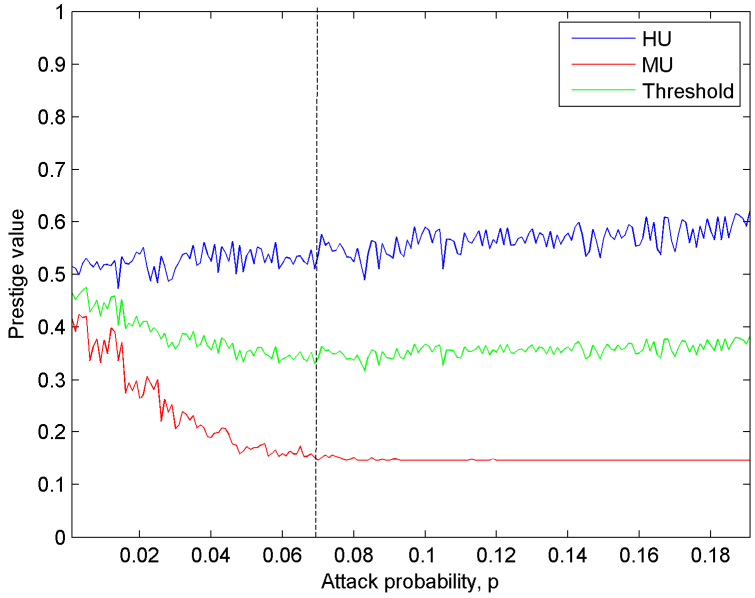


Figure 5. Reputation value of cognitive users under different attack probabilities.

It can be seen from Figure 5 that when the probability of attack is greater than 7%, the reputation value of malicious users tends to be stable. Combined with Figure 4, the malicious users with an attack probability greater than 7% can be defined as Class II malicious users, while the malicious users with an attack probability less than 7% can be defined as Class I malicious users.

4.2. Algorithm Performance Comparison

We created a simulation in order to compare the difference of the reputation convergence value of honest users and malicious users between the β-MIAMC algorithm proposed in this paper and the traditional β-SCCSA algorithm with the same attack probability. This used the situation of the probability of the malicious user attack being p = 0–50%, with the results shown in Figure 6:

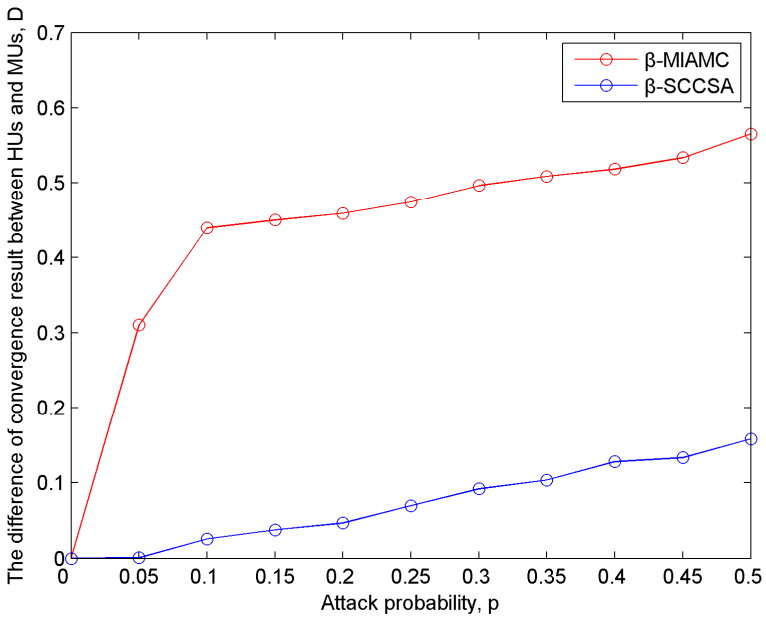


Figure 6. The difference between the honest user and the malicious user convergence results under different attack probabilities.

As seen from the Figure 6:

1. As the attack probability increases, the difference between the reputation value of honest users and malicious users gradually increases, essentially, a greater attack probability means that it is easier to accurately distinguish honest users and malicious users;
2. Under the same attack probability, the reputation value difference calculated by the β-MIAMC algorithm is obviously larger than the reputation value difference calculated by the β-SCCSA algorithm. It can be seen that the algorithm proposed in this paper can better and faster distinguish between honest users and malicious users.

Correctly distinguishing malicious users is the key for improving the performance of spectrum sensing. After performing 10,000 Monte Carlo experiments on the basis of the above experiment set, the analysis of the changes in the false alarm probability of malicious users under different attack probability are shown in this paper. As shown in Figure 7,

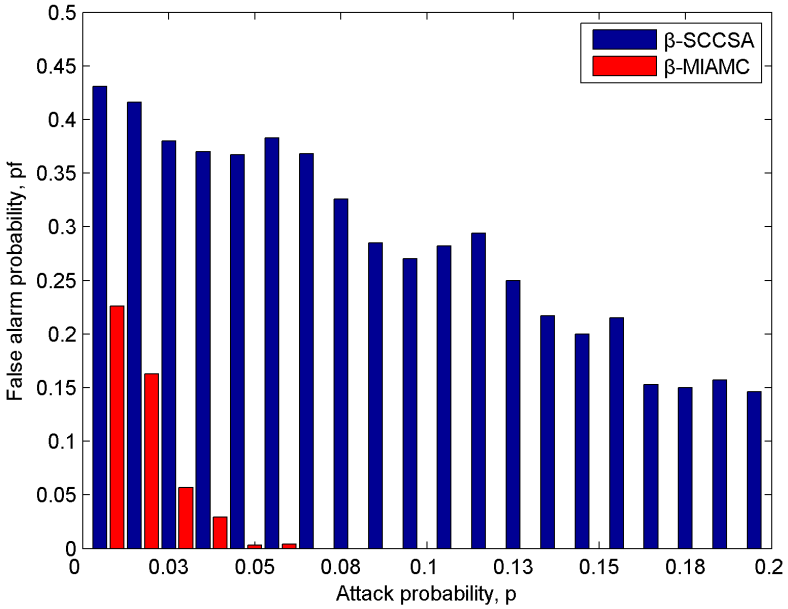


Figure 7. The false alarm probability under different attack probabilities.

Analysis of the above figure shows that with an increase in the attack probability of malicious users, the false alarm probability of malicious users decreases. This is due to the greater attack probability of malicious users, which makes it more difficult for them to hide. We compared the false alarm probability of the malicious users of the proposed β-MIAMC algorithm and the traditional β-SCCSA algorithm with the same attack probability and the trend of the false alarm probability of malicious users calculated under the change in attack probability. From this, we can see that with the same attack probability, the false alarm probability of the malicious user obtained by the β-MIAMC algorithm is reduced by at least 20% compared with the β-SCCSA algorithm. With an increase in the attack probability, the false alarm probability of the malicious user under the β-MIAMC algorithm is gradually reduced. When the attack probability is 6%, the false alarm probability of the malicious user is reduced to 3%. When the attack probability is 7%, the false alarm probability of malicious user converges to 0. It can be seen that the β-MIAMC algorithm proposed in this paper can distinguish malicious users better and faster.

5. Conclusions

We mainly studied the security problem of centralized collaborative spectrum sensing under SSDF attacks. In order to solve this problem, we established a model of a malicious user identification system

with multi-channel cooperation. The model uses the characteristics of cognitive users having the same performance on the different sub-channels in the same perceived gap. This model then collaborates the cognitive user's perceived results on multi-channels and reduces the probability of misjudgment.

On this basis, we propose a malicious user identification algorithm under multi-channel cooperative conditions that are based on the β-function and the feedback iteration mathematical method. The cognitive user's prestige value is updated by feedback iterations and the malicious user is distinguished according to the prestige value. The simulation results show that when the attack probability is the same, the β-MIAMC algorithm proposed in this paper can identify the malicious users more accurately than the traditional algorithms. The proposed algorithm reduces the false alarm probability of malicious users by more than 20%. When the attack probability is greater than 7%, the proposed algorithm can distinguish the malicious users with 100% certainty.

Acknowledgments: This work was supported by the Chinese National Science Foundation under Grants 61501078 and 61231006, the Fundamental Research Funds for the Central Universities under Grants 3132016208.

Author Contributions: Jingbo Zhang designed the maritime cognitive radio communication system model, the dynamic spectrum allocation algorithm based on the Cournot game and the organization of the paper, Lili Cai carried out the simulations and was responsible for the writing and editing of the manuscript and Shufang Zhang supervised the work and contributed to the writing of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, P.; Qi, W.; Yuan, E.; Wei, L.; Zhao, Y. Full-Duplex Cooperative Sensing for Spectrum-Heterogeneous Cognitive Radio Networks. *Sensors* **2017**, *17*, 1773. [CrossRef] [PubMed]
2. Chen, X.; Chen, H.H.; Meng, W. Cooperative Communications for Cognitive Radio Networks—From Theory to Applications. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1180–1192. [CrossRef]
3. Shinde, S.C.; Jadhav, A.N. Centralized Cooperative Spectrum Sensing with Energy Detecion in Cognitive Radio and Optimization. In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016; pp. 1002–1006. [CrossRef]
4. Ye, F.; Zhang, X.; Li, Y. Comprehensive Reputation-Based Security Mechanism against Dynamic SSDF Attack in Cognitive Radio Networks. *Symmetry* **2016**, *8*, 147. [CrossRef]
5. Wang, W.; Li, H.; Sun, Y.; Han, Z. CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing. In Proceedings of the 2009 IEEE Global Telecommunications Conference (GLOBECOM 2009), Honolulu, HI, USA, 30 November–4 December 2009; pp. 1–6. [CrossRef]
6. Chen, R.; Park, J.M.; Bian, K. Robust Distributed Spectrum Sensing in Cognitive Radio Networks. In Proceedings of the IEEE 27th Conference on Computer Communications (INFOCOM 2008), Phoenix, AZ, USA, 13–18 April 2008. [CrossRef]
7. Zhuo, J. Micro Blogging Malicious User Identification. Master's Thesis, Beijing Jiaotong University, Beijing, China, 2016.
8. Li, H.; Guo, Q. Research on Wind-Band Spectrum Sensing Based on Compression Sensing. *J. Harbin Inst. Technol.* **2014**, *5*, 80–94.
9. Arshad, K.; Moessner, K. Robust collaborative spectrum sensing in the presence of deleterious users. *IET Commun.* **2013**, *7*, 49–56. [CrossRef]
10. Bae, S.; So, J.; Kim, H. On Optimal Cooperative Sensing with Energy Detection in Cognitive Radio. *Sensors* **2017**, *17*, 2111. [CrossRef]
11. Fragkiadakis, A.G.; Tragos, E.Z.; Askoxylakis, I.G. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 428–445. [CrossRef]
12. Sumathi, A.C.; Vidhyapriya, R. Security in Cognitive Radio Networks—A Survey. In Proceedings of the 12th International Conference on Intelligent Systems Design and Applications (ISDA), Kochi, India, 27–29 November 2012; pp. 114–118. [CrossRef]
13. Ahmed, A.H. Characterization of beta, binomial, and Poisson distributions. *IEEE Trans. Reliab.* **1991**, *40*, 290–295. [CrossRef]

14. Vosoughi, A.; Cavallaro, J.R.; Marshall, A. Robust Consensus-Based Cooperative Spectrum Sensing under Insistent Spectrum Sensing Data Falsification Attacks. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
15. Faradji, F.; Rezaie, A.H.; Ziaratban, M. A Morphological-Based License Plate Location. In Proceedings of the 2007 IEEE International Conference on Image Processing, San Antonio, TX, USA, 16 September–19 October 2007; pp. I-57–I-60. [CrossRef]