Abnormal Information Identification and Elimination in Cognitive Networks

Ruowu Wu\textsuperscript{a}, Xiang Chen\textsuperscript{a}, Hui Han\textsuperscript{a}, Haojun Zhao\textsuperscript{b,\ast}, and Yun Lin\textsuperscript{b,\ast}

\textsuperscript{a}State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang, 471003, China
\textsuperscript{b}Harbin Engineering University, Harbin, 150001, China

Abstract

The electromagnetic spectrum is an important national strategic resource, and spectrum sensing data falsification (SSDF) is an attack method that destroys the cognitive network and makes it impossible to be used effectively. Malicious users capture the sensory nodes through cyber attacks, virus intrusions, etc., tampering with the perceived data and making the cognitive network biased or even completely reversed. In order to eliminate the negative effects caused by the identification and elimination of abnormal information in the electromagnetic spectrum in multi-user collaboration and to ensure the desired effect, this paper studies and constructs a robust cognitive user evaluation reference system based on improving the performance of cooperative spectrum sensing. The impact of attack behavior on the reference frame is greatly reduced. At the same time, the attacker’s identification and elimination algorithm are improved, and the influence of abnormal data on the perceived performance under the combined effect is eliminated.

Keywords: cognitive radio; cooperative spectrum sensing; spectrum sensing data falsification; defense reference

(Submitted on May 17, 2018; Revised on July 8, 2018; Accepted on August 17, 2018)

© 2018 Totem Publisher, Inc. All rights reserved.

1. Introduction

Secondary users in cognitive radio jointly explore spectrum holes through cooperative spectrum sensing, thereby effectively utilizing the idle spectrum and reducing the impact on primary users. This is an effective means to improve spectrum utilization and solve spectrum shortages. However, in cooperative spectrum sensing, malicious users pretend to be honest users, tamper with spectral data, and initiate Byzantine attacks, also known as Spectrum Sensing Data Falsification (SSDF). SSDF is the main threat of cooperative spectrum sensing \cite{1}. On the one hand, cooperative spectrum sensing needs to be able to discover spectrum holes to improve spectrum utilization. On the other hand, cooperative spectrum sensing should avoid missed detection of primary users and avoid interference with normal communication of primary users. However, spurious data severely affects the performance of cooperative spectrum sensing, resulting in reduced spectrum utilization and disruption of communication for authorized users.

Therefore, spectrum sensing data tampering has received widespread attention, and many researchers have proposed different identification and defense solutions from multiple perspectives. Literature \cite{2} proposed a sensing user anomaly detection scheme based on data mining. The biggest advantage of this scheme is that the Fusion Center (FC) does not need to know the user’s prior information in advance, and it more closely reflects our actual life. Literature \cite{3} analyzes the limit performance of cooperative spectrum sensing under Byzantine attack. This method identifies and removes the attacker before data fusion, which is easy to implement and can eliminate malicious users in a short time but also leads to users. The analysis of dynamic interactions with the fusion center is missing. In order to ensure the stability of spectrum sensing, literature \cite{4} studied a scheme of trusted node help based on the user’s reputation value. When the user’s reputation value reaches the set threshold value and thus improves the perceived stability, the user’s sentiment information will be uploaded to the Fusion Center for integration. In \cite{5}, the authors proposed a distributed scheme using spatial correlation and anomaly detection, which is used to receive signal strength between adjacent SUs to detect malicious users in cooperative spectrum sensing. The authors in \cite{6} studied the use of Bayesian methods to deal with methods for secondary user attacks to enhance...

* Corresponding author.
E-mail address: jeawray@hrbeu.edu.cn, linyun@hrbeu.edu.cn
the robustness of cooperative spectrum sensing. This method uses a statistical attack model, and each malicious node has a certain degree of attack probability. This method effectively solves the Bayesian estimation problem by using the belief propagation model on the factor graph. In addition, literature [7-11] have different views and research on the detection and identification of anomalous information in cognitive networks.

This paper combines the methods mentioned in different literatures to study the robust perception user evaluation reference system construction technology based on reputation value to effectively identify abnormal information. Then, the attacker identification and elimination algorithm are improved based on the proposed reference system, which eliminates the impact of abnormal data on the perceived performance under the combined effect.

2. Basic Theory

2.1. Perceptual Process

The working status of the licensed band can be divided into $H_0$ and $H_1$. $H_0$ indicates that the frequency band operates in an idle state, and $H_1$ indicates that the frequency band operates in a busy state. $r(t)$ is the received signal strength at time $t$, $n(t)$ is Gaussian white noise, $P_d(t)$ is the signal transmitted by the primary user, and $h(t)$ is the channel gain of the authorized user to the perceived user.

$$
\begin{align*}
H_0 &: r(t) = n(t) \\
H_1 &: r(t) = h(t)P_d(t) + n(t)
\end{align*}
$$

At the same time, two metrics are introduced, the detection probability $P_d$ and the false alarm probability $P_f$. $\lambda$ is the determine threshold.

$$
\begin{align*}
P_f &= P(v_i = 1 | H_0) = Q\left(\frac{\lambda - \mu_0}{\sigma_0}\right) \\
P_d &= P(v_i = 1 | H_1) = Q\left(\frac{\lambda - \mu_1}{\sigma_1}\right)
\end{align*}
$$

Among them, $\mu_0 = 2U$, $\sigma_0^2 = 4U$, $\mu_i = 2U(\beta + 1)$, $\sigma_i^2 = 4U(2\beta + 1)$, $\beta$ is the signal to noise ratio received by the SU, and $Q$ function is the complementary cumulative distribution function of the standard normal distribution.

2.2. SSDF and Data Reporting Process

In cooperative spectrum sensing, the local decision result of each secondary user $i$ is represented by the final FC global decision result. Considering the perceptual information of the upload error in the sensing process, the perceptual error probability $P_e$ is introduced here. Combined with formula (2), it is as follows:
Abnormal Information Identification and Elimination in Cognitive Networks

\[
\begin{align*}
\begin{cases}
    p_f' &= p_f \cdot (1-p_e) + (1-p_f) \cdot p_e \\
p_d' &= p_d \cdot (1-p_e) + (1-p_d) \cdot p_e
\end{cases}
\end{align*}
\]

(3)

To better analyze the impact on the sensing network, the attack probability is also introduced into the spectrum falsifying frequency. When the authorized band sensing result is idle, the probability that the malicious user reports as busy is \(P_a\); when the perceived frequency of the authorized band is busy, the probability that a malicious user reports as idle is \(P_b\). The relevant perceptual performance formulas of malicious users after passing SSDF are:

\[
\begin{align*}
\begin{cases}
    p_f^b &= p_f \cdot (1-p_b) + (1-p_f) \cdot p_b \\
p_d^b &= p_d \cdot (1-p_b) + (1-p_d) \cdot p_b
\end{cases}
\end{align*}
\]

(4)

Considering the probability of transmission errors in the data reporting process, the false alarm probabilities of the honest and malicious users and the detection probabilities are as follows.

For honest users, there are:

\[
\begin{align*}
\begin{cases}
    p_f^H &= p_f \cdot (1-p_e) + (1-p_f) \cdot p_e \\
p_d^H &= p_d \cdot (1-p_e) + (1-p_d) \cdot p_e
\end{cases}
\end{align*}
\]

(5)

For malicious users, there are:

\[
\begin{align*}
\begin{cases}
    p_f^M &= p_f^b \cdot (1-p_e) + (1-p_f^b) \cdot p_e \\
p_d^M &= p_d^b \cdot (1-p_e) + (1-p_d^b) \cdot p_e
\end{cases}
\end{align*}
\]

(6)

3. Robust Perceptual User Evaluation Reference System

3.1. Review of Existing Reference Systems

In order to eliminate the negative impact of abnormal information on the electromagnetic spectrum, the existing defense reference system can be roughly divided into:

Global decisions as a reference (GDaR) [3, 12]. The final judgment is obtained by data fusion of the reported results of all the sensing nodes. Therefore, after the proportion of malicious users is greater than that of the honest users, the reference system will be invalid.

Trusted sensor’s reports as a reference (TRaR) [13-14]. The reference system assumes that some honest user sensors are known to the primary user, and the reported results are approximated by the true spectrum state and used to assess the reported values of other sensors.

These reference systems focus on the processing of perceived user reporting results and determine the true state of the spectrum by obtaining reliable information. However, these are always susceptible to interference and influence by false or erroneous information. For example, the GDaR reference system is based on the processing of reported values for all users, but the actual perceived performance of each sensor is unknown, so the reliability of the reference system is difficult to guarantee. In addition, when the attacker is the majority, the efficiency of GDaR will be very low. In TRaR, a priori information of trusted nodes is difficult to obtain in some cases. Although trusted nodes do not provide forged perceived results, they may suffer from severe shadow fading, thereby reducing their spectrally perceived performance. Therefore, the wrong perception will lead to the loss of reliability of TRaR.

3.2. The Proposed Reference System

The entire testing process consists mainly of the learning phase and the decision phase. The learning phase consists of a large segment of perceptual time slots in which the reference system will evaluate the perceptual users and update their reputation values cumulatively. Specifically, when the user is perceived as an attacker at a certain moment, the reputation
value will be processed +1. In the subsequent judgment stage, the obtained reputation value is compared with the credit threshold to judge the attribute of the current cognitive user.

As shown in Figure 2, the sensing node reports the local sensing result, and the FC makes a decision \( F \) on the band status according to the result of the fusion. However, due to the limitations of its decision mode, the results of the global judgment alone are not reliable and cannot provide reference to other perceived users. Therefore, the proposed reference combines the feedback information of the transmission result and the sensing mechanism of the full time slot. Specifically, when the frequency band working state of the global decision is busy, that is, when the global decision result \( F=1 \), the SU or the FC continues to be perceived, because the sensing performance of the SU itself may greatly increase as the perceived time slot is extended. Thus, a moderate expansion in time can improve its perceived performance. When the global decision result \( F=0 \), that is, when the globally determined band operating state is idle, the SU will access the band to transmit data, and the following two situations often occur: the SU successfully accesses the licensed band, or the SU pair fails to access the licensed band. Ideally, if the SU successfully accesses the band, then the result \( F \) of the global decision is correct. Otherwise, the result \( F \) of the global decision is wrong.

As shown in Figure 2.2, it is clear that after the SU access grant band transmission, there is an inferred error probability: the probability of successful transmission when the band status is busy, and the probability of failure transmission when the band status is idle. For the sake of simplicity in the following, here are two probabilities:

\[
\begin{align*}
    P(\text{success} \mid F = 0, H_i) & = P_{i_0}^{\text{su}} \\
    P(\text{failure} \mid F = 0, H_i) & = P_{i_0}^{\text{fa}}
\end{align*}
\]  

(7)

4. Abnormal Data Elimination based on Proposed Reference System

4.1. Identification of Abnormal Data

As can be seen from Figure 2, the reference system will evaluate the sensing nodes in each time slot, update their reputation values cumulatively, and distinguish between honest data and malicious data according to the last obtained reputation value. Each sensing node is assigned a measured reputation worth indicator, indicating that the number of times the final decision \( A \) of the reference system in the \( T \)-slot is inconsistent with the reported result \( u \) of the node \( i \). The reputation value \( n_i \) of the perceived node can be shown as:

\[
n_i = \sum_{t=1}^{T} [1(F_t \neq u_i(t))]
\]

(8)

Where \( I \) is an indication function, and it can be found that the higher the reputation value of the sensing node, the more likely the uploaded sensing data is not adopted by the fusion center. Comparing the reputation value of the node \( n_i \) with the set threshold \( \eta \), we can finally identify the abnormal user or abnormal data.
Abnormal Information Identification and Elimination in Cognitive Networks

Table 1. Abnormal information culling algorithm based on the proposed reference system

<table>
<thead>
<tr>
<th>Algorithm 1 Abnormal information culling algorithm based on the proposed reference system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Initialization</strong>: The number of users participating in the CSS is N, the number of malicious users is Nm, the time slot is T, the weight of the user in the FC is k, and the threshold value when the fusion center performs global judgment is L. And the threshold value of the malicious user is marked. For ( \eta ), the reputation of the ( i )-th secondary user is ( n_i ).</td>
</tr>
<tr>
<td>2. <strong>For</strong> ( i = 1, 2, \ldots, T ) <strong>do</strong></td>
</tr>
<tr>
<td>3. <strong>For</strong> ( i = 1, 2, \ldots, N ) <strong>do</strong></td>
</tr>
<tr>
<td>4. The user performs cooperative spectrum sensing and reports the local result ( u_i ) to the FC</td>
</tr>
<tr>
<td>5. <strong>end for</strong></td>
</tr>
<tr>
<td>6. Fusion Center for data fusion</td>
</tr>
<tr>
<td>7. The fusion center conducts a global judgment:</td>
</tr>
<tr>
<td>8. If the local perception result is ( u &lt; L ), ( F = 0 ); otherwise ( F = 1 ).</td>
</tr>
<tr>
<td>9. When ( F = 0 ), the FC access band continues to transmit information. If the transfer fails, ( A = 1 ), otherwise ( A = 0 ).</td>
</tr>
<tr>
<td>10. When ( F = 1 ), FC access continues spectrum sensing. If the perceived result is that the band is idle, then ( A = 0 ), otherwise, ( A = 1 ).</td>
</tr>
<tr>
<td>11. <strong>For</strong> ( i = 1, 2, \ldots, N ) <strong>do</strong></td>
</tr>
<tr>
<td>12. If ( u_i \neq A ), then the reputation value ( n_i = n_i + 1 ).</td>
</tr>
<tr>
<td>13. <strong>end for</strong></td>
</tr>
<tr>
<td>// Judgment process</td>
</tr>
<tr>
<td>15. <strong>For</strong> ( i = 1, 2, \ldots, N ) <strong>do</strong></td>
</tr>
<tr>
<td>16. If ( n_i &gt; \eta ), then user ( i ) will be judged as a malicious user, whereas user ( i ) is judged to be an honest user.</td>
</tr>
</tbody>
</table>

4.2. Elimination of Abnormal Data

In order to measure the elimination of the anomaly data by the reference system, two indicators \( P_B^{iso} \) and \( P_H^{iso} \) are proposed here to measure the recognition and elimination of malicious users by the system. \( P_H^{iso} \) indicates the probability that an honest user is misjudged as a malicious user by the reference system after \( T \) time slots and is removed from the fusion center [3]:

\[
P_H^{iso} = P(n_i > \eta) = \sum_{j=\eta}^{T} \binom{T}{j} P_H^j (1-P_H)^{T-j}
\]  \hspace{1cm} (9)

\( P_B^{iso} \) represents the probability that the malicious user is identified and eliminated by the reference after \( T \) time slots:

\[
P_B^{iso} = P(n_i > \eta) = \sum_{j=\eta}^{T} \binom{T}{j} P_B^j (1-P_B)^{T-j}
\]  \hspace{1cm} (10)

\( P_B \) and \( P_H \) indicate the probability that the perceived data reported by the malicious user and the honest user are different from the FC decision results. In the eliminating process, the reputation value is used to identify the Byzantine attack user. By sensing the \( \eta \), comparison with the threshold \( \eta \), the sensory node whose reputation value is greater than the threshold is judged as a malicious node, and the reported data can be regarded as abnormal data. It is then removed from the cooperative spectrum perception.

4.3. Threshold and Efficient Purification Standards

For the threshold \( \eta \) in the proposed reference, the selection of \( \eta \) plays an important role in whether the system can efficiently complete data purification. If the threshold is low, some honest nodes will be mistakenly judged as malicious users, thus eliminating normal data. Conversely, if the threshold is set higher, it will make it difficult for a malicious user to
be identified, and eventually the elimination of the abnormal information cannot be completed. Mathematically, optimization tries to satisfy the following effects:

$$\max_{\eta} (P_{H}^{\text{iso}} - P_{H}^{\text{iso}})$$  \hspace{1cm} (11)$$

For the above problems, the optimal threshold obtained after optimization is as follows:

$$\eta_{opt} = \left[ T \frac{\ln\left(\frac{1 - P_{H}}{1 - P_{B}}\right)}{\ln\left(\frac{P_{H}(1 - P_{B})}{P_{B}(1 - P_{H})}\right)} \right]$$  \hspace{1cm} (12)$$

Among them, this $\lceil \cdot \rceil$ represents the rounding function, and the threshold is rounded up. A detailed derivation of the formula can be found in [15-17].

5. Performance Analysis

5.1. Simulation Parameter Settings

In the simulation, 100 cognitive nodes were set to participate in the process of cooperative spectrum sensing. The probability that the authorized band works in the busy state was set to 0.2, $P_{f}^{\text{Hi}} = 0.2$, $P_{d}^{\text{Hi}} = 0.8$, and $p_{b} = P_{\text{mal}} = 1$. The simulation results took the average of 2000 trials. To reflect the superior performance of the proposed reference, it is compared here with the Global decisions as a reference (GDaR) [18].

5.2. Analysis of Results

Figure 3 shows the probability of a malicious user and an honest user being identified and eliminated in two references with the change of malicious users proportion $\alpha$ as follows. It can be found that the proportion $\alpha$ has little effect on the proposed reference system, and it always maintains excellent performance. In contrast, with the increase of $\alpha$, the performance of GDaR began to become unstable. When $\alpha$ was greater than 0.4, the GDaR reference system was reversed, and when it was greater than 0.5, the GDaR reference system was completely ineffective.

Figure 4 shows the simulation curves for the two reference frames and the reported error probability $P_{e}$. It can be seen that the two reference systems show a certain degree of change with the change of the reported error probability. That is, as the reported probability $P_{e}$ increases, the probability of the honest node being eliminated is gradually increased, and the probability that the malicious node is identified and rejected gradually decreases. After analysis, it can be concluded that this phenomenon is caused by the fact that the fusion center receives more error information and thus makes a wrong
Abnormal Information Identification and Elimination in Cognitive Networks

Judgment, so that the reputation value of the honest node is lowered and the reputation value of the malicious node is increased. Obviously, in the case of an increased probability of reporting errors, the proposed reference system is more stable than GDaR, that is, the recognition and rejection performance of GDaR is worse under the influence of error information.

Figure 4. Changes of the probability of reporting error $P_e$ between $P_h^\text{iso}$ and $P_h^\text{iso$}$ under the two reference systems

Figure 5 shows the variation of $P_h^\text{iso$}-P_h^\text{iso$}$ with different thresholds $\eta$ under different perceptual time slots $T$. As long as the appropriate threshold $\eta$ is given, $P_h^\text{iso$}-P_h^\text{iso$}$ can get the maximum value. It can be seen that under different values of $T$, the $\eta$ value is different when the maximum value is obtained. In addition, as the perceived time slot $T$ increases, the threshold $\eta$ for obtaining the optimal solution also increases. It can be concluded from the graph that the three curves obtain the highest value at $\eta=T/2$, indicating that the value of the formula (11) is $T/2$, which means that the most efficient abnormal data culling effect is obtained in this case [19-20].

Figure 5. Changes with different thresholds $\eta$ under different perceptual time slots $T$

As shown in Figure 6, the relationship between the reputation value of the user and the time slot $T$ is shown. It can be seen that the reputation value of malicious users and honest users increases with the increase of $T$. The difference is that the growth rate of malicious users is faster than that of honest users. That is, as the time slot $T$ increases, it is easier to distinguish between malicious users and honest users. In other words, when the time slot $T$ is large, the range of the threshold is relatively wider.
6. Conclusion

Cognitive wireless networks are inevitably attacked and tampered with by malicious users. Malicious users capture the sensory nodes through cyber attacks, virus intrusions, etc., tampering with the perceived data and making the electromagnetic cognition biased or even completely reversed. Therefore, based on the defense strategy of SSDF attack in the network, this paper mainly solves the identification and rejection of abnormal information in the electromagnetic spectrum in cooperative sensing, thus ensuring the security and stability of the sensing network and making the spectrum resources more fully and reasonably used. The first step was to construct a robust perceptual user evaluation reference system to effectively identify anomaly information. Then, this paper improved the recognition and elimination algorithm to improve the stability of the reference system, and it finally reduced the impact of abnormal information on the perception performance of cognitive networks.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (61771154), the Fundamental Research Funds for the Central Universities (HEUCFG201830), and the State Key Laboratory of CEMEE (CEMEE2018K0104A).

References