symmetry

Article

Comprehensive Reputation-Based Security Mechanism against Dynamic SSDF Attack in Cognitive Radio Networks

Fang Ye, Xun Zhang and Yibing Li *

College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China; yefang0923@126.com (F.Y.); zhangxun0611@gmail.com (X.Z.)

* Correspondence: liyibing0920@126.com; Tel.: +86-133-0460-5678

Academic Editor: Angel Garrido
Received: 8 November 2016; Accepted: 30 November 2016; Published: 3 December 2016

Abstract: Collaborative spectrum sensing (CSS) was envisioned to improve the reliability of spectrum sensing in centralized cognitive radio networks (CRNs). However, secondary users (SUs)' changeable environment and ease of compromise make CSS vulnerable to security threats, which further mislead the global decision making and degrade the overall performance. A popular attack in CSS is the called spectrum sensing data falsification (SSDF) attack. In the SSDF attack, malicious cognitive users (MUs) send false sensing results to the fusion center, which significantly degrades detection accuracy. In this paper, a comprehensive reputation-based security mechanism against dynamic SSDF attack for CRNs is proposed. In the mechanism, the reliability of SUs in collaborative sensing is measured with comprehensive reputation values in accordance with the SUs' current and historical sensing behaviors. Meanwhile a punishment strategy is presented to revise the reputation, in which a reward factor and a penalty factor are introduced to encourage SUs to engage in positive and honest sensing activities. The whole mechanism focuses on ensuring the correctness of the global decision continuously. Specifically, the proposed security scheme can effectively alleviate the effect of users' malicious behaviors on network decision making, which contributes greatly to enhancing the fairness and robustness of CRNs. Considering that the attack strategy adopted by MUs has been gradually transforming from simplicity, fixedness and singleness into complexity, dynamic and crypticity, we introduce two dynamic behavior patterns (true to false and then to true (TFT) and false to true and then to false (FTF)) to further validate the effectiveness of our proposed defense mechanism. Abundant simulation results verify the rationality and validity of our proposed mechanism.

Keywords: cognitive radio networks; collaborative spectrum sensing; dynamic spectrum sensing data falsification attack; comprehensive reputation

1. Introduction

With the rapid development of wireless services and applications, the conventional static spectrum management policy inevitably causes scarcity in specific spectrum bands. Moreover, a large portion of the allocated spectrum is unused occasionally, leading to underutilization and wastage of valuable spectrum resources [1]. As the most promising solution to the spectrum scarcity problem, cognitive radio networks (CRNs) have attracted widespread attention recently. With this new communication paradigm, unlicensed users (also referred to as secondary users, SUs) can opportunistically utilize the spectrum for licensed users (also referred to as primary or incumbent users, PUs). When the primary user is detected back to the band, SUs in the band must forsake the spectrum immediately. Therefore, as an initial step, SUs must accurately sense the spectrum occupancy conditions for available opportunities to avoid any interference with the licensed users [2].

However, due to SUs' changeable environment and ease of compromise, the open characteristic of CRNs produces various security threats in the reliability of sensing data in CRNs [3]. For example, channel impairment, such as shadowing and multipath fading, lead to the fact that local spectrum sensing conducted by the individual user is often incorrect. Although the participation of multiple SUs in collaborative spectrum sensing (CSS) contributes to the improvement of detection accuracy, the global decision making may be misguided when SUs intentionally or unintentionally send falsified sensing information to the fusion center (FC) during coopesration. This sort of attack in CSS, called the spectrum sensing data falsification (SSDF) attack (also referred to as Byzantine attacks), significantly degrades collaborative detection correctness [4].

To address the above issues, various secure CSS schemes have been proposed [5–13]. When simple attack patterns are adopted by only a few malicious users (MUs) in CRNs, the schemes presented in [5–7] can work well enough. The concept of applying the trust and reputation model in CRNs has also attracted interest recently [8–12]. A reputation-based secure CSS algorithm with trusted node assistance based on [5–7] was proposed in [8], which started with trusted SUs merely to assure the inerrability of global decision making. In [9], a soft reputation-based sensing scheme was presented by modeling the operative mode of PU as a renewal process. These two schemes can still work availably even in the presence of a large number of malicious users. Qingqi Pei exploited the cognitive cycle to build the trust model, thus ensuring the security of CSS [10]. The authors in [11] considered the number of false sensing as the attenuation factor of trust to punish MUs; however, they ignored the dynamic characteristics of SSDF attack behavior. In [12], the OGKmethod was employed to mitigate the effect of MUs and improve sensing robustness. A novel trust scheme called SensingGuardis proposed in [13] to mitigate the harmful effect of SSDF attackers and enhance the performance of CSS.

Nevertheless, all of the existing methods mentioned above possess respective limitations. The schemes proposed in [5–7] become defective either by the increasing proportion of malicious users or in the face of complex attack strategies. Others in [8–10] have no ability to maintain robustness under the presence of a high proportion of MUs, while the rest of the methods, as in [11–13], cannot cope with complicated attack patterns.

To target the aforementioned problems in the CSS, this paper establishes a comprehensive reputation-based security mechanism against dynamic SSDF attack patterns for CRNs. Specifically, each SU is assigned one comprehensive reputation by the FC, and the reliability of SUs in collaborative sensing is measured with comprehensive reputation in accordance with SUs' historical sensing behaviors. Meanwhile, a punishment strategy is presented to revise the reputation, among which a reward factor and a penalty factor are introduced to encourage SUs to engage in positive and honest sensing activities. The whole mechanism focuses on mitigating the threat of dynamic malicious behaviors on network decisions and ensuring the correctness of the global decision continuously. Simulation results verify the robustness and effectiveness of the proposed security mechanism. Our scheme maintains a satisfactory sensing performance even under the circumstance that a large portion of malicious cognitive users exists in the network and employs complex attack behavior patterns. The improvements and novelties of our proposed scheme are presented clearly in Table 1, which concerns the main characteristics of the above defense schemes and compares them with the characteristics of our proposed scheme.

The rest of the paper is organized as follows. The system model and dynamic malicious attack behavior patterns are described in detail in Section 2. The proposed comprehensive reputation-based security mechanism and data fusion solution are respectively discussed in Sections 3 and 4. The simulation results are presented in Section 5. Finally, Section 6 concludes this paper.

Table 1. Performance enhancements achieved by the advanced SSDF defense mechanisms in CRNs.

Performance Enhancement Compared with Existing Approaches	Counter a Small Number of Attackers	Counter a High Proportion of Attackers	Counter Simple Attack Patterns	Counter Complex Attack Patterns
Chen et al. [5]	×		×	
Zhao and Zhao [6]	×		×	
Kaligineedi et al. [7]	×		×	
Zeng et al. [8]	×		×	×
Du [9]	×		×	×
Pei et al. [10]	×		×	×
Feng et al. [11]	×	×	×	
Lu et al. [12]	×	×	×	
FENG et al. [13]	×	×	×	
Our's	×	×	×	×

2. Application Scenario

In this section, we give a brief introduction of the cognitive radio network model adopted in this paper and establish the security problems against Byzantine attacks.

2.1. Network Architecture

The problem of spectrum sensing is to decide whether a particular slice of the spectrum is available or not. Consider a cognitive radio network where K secondary users are collaborating in the spectrum sensing process in the presence of one primary user, as shown in Figure 1. Without loss of generality, the energy detection [14–16] method is applied by each SU for individual spectrum sensing. Based on its observations, each SU solves a hypothesis testing problem and discriminates between the two hypotheses during the t-th sensing slot.

$$\begin{aligned} \mathcal{H}_0: &\quad x_i(t) = v_i(t) \\ \mathcal{H}_1: &\quad x_i(t) = h_i s_i(t) + v_i(t) \end{aligned} \tag{1}$$

where $x_i(t)$ represents the received signal at the i-th SU, h_i is the complex channel gain between the PU and SU$_i$, and the sensing channel is assumed to be time-invariant during the sensing process. The PU's transmitted signal, $s_i(t)$, is assumed to be a BPSK modulated signal. The noise $v_i(t)$ is additive white Gaussian noise (AWGN) with zero mean and variance σ_v^2. $s_i(t)$ and $v_i(t)$ are mutually independent. The hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ represent the absence and presence of the PU, respectively.

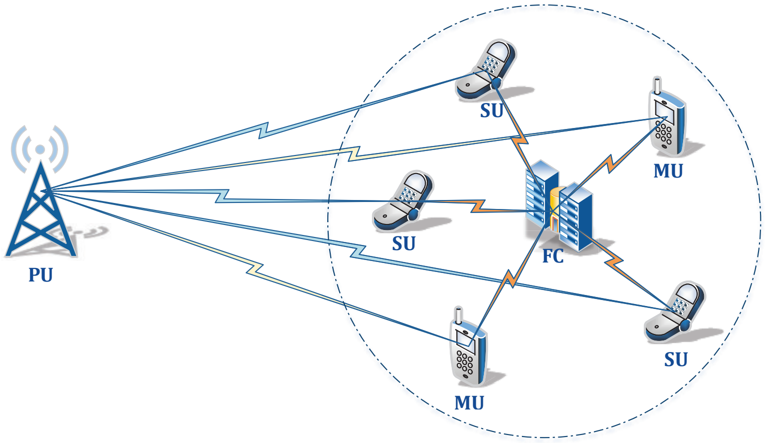

Figure 1. The sketch map of the network scene model.

In our system model, the test statistics for the energy detector for the i-th cognitive user is computed as the sum of the received signal energy over an interval of N samples and is given by:

$$Y_i \sim \begin{cases} \chi^2_{2m}, & \mathcal{H}_0 \\ \chi^2_{2m}(2\gamma_i), & \mathcal{H}_1 \end{cases} \tag{2}$$

Under hypothesis $\mathcal{H}_0$, the test statistic Y_i is a random variable whose probability density function is a chi-square distribution χ^2_{2m} with $N = 2m$ degrees of freedom, and $m = TW$ is the time-bandwidth product; otherwise, Y_i follows a non-central chi-square distribution $\chi^2_{2m}(2\gamma_i)$ with N degrees of freedom and non-central parameter $2\gamma_i$. The instantaneous signal-to-noise ratio (SNR) at the i-th SU is γ_i.

We consider the case in which each individual SU makes a one-bit hard decision, $d_i(t)$, on the absence or presence of the PU based on the sensing information, such that:

$$d_i(t) = \begin{cases} 0, & decision\,\mathcal{H}_0 \quad if\, Y_i < \lambda_i \\ 1, & decision\,\mathcal{H}_1 \quad if\, Y_i \geq \lambda_i \end{cases} \tag{3}$$

where λ_i is the decision threshold of SU$_i$. Then, the detection probability and false alarm probability of SU$_i$ can be respectively expressed as:

$$\begin{aligned} P_d^{(i)} &= P\{d_i(t) = 1 \mid \mathcal{H}_1\} \\ P_f^{(i)} &= P\{d_i(t) = 1 \mid \mathcal{H}_0\} \end{aligned} \tag{4}$$

In this model, each SU in the network forwards its processed binary local decision $u_i(t)$ to the central entity, then the fusion center makes the final decision $u_0(t)$ about the state of the spectrum based on all of the information received from the participating SUs. The communication channels between SUs and the FC are assumed to be error-free in this paper.

In collaborative spectrum sensing, the global probabilities of false alarm, detection and misdetection for evaluating the performance of final joint decisions are expressed as Q_f, Q_d and Q_m, respectively, which can be written as follows [1]:

$$Q_f = \sum_{l=n}^{K} \binom{K}{l} \prod_{j=1}^{l} P_f^{(j)} \prod_{i=l+1}^{K} (1 - P_f^{(i)}) \tag{5}$$

$$Q_d = \sum_{l=n}^{K} \binom{K}{l} \prod_{j=1}^{l} P_d^{(j)} \prod_{i=l+1}^{K} (1 - P_d^{(i)}) \tag{6}$$

$$Q_m = 1 - Q_d \tag{7}$$

where $P_d^{(i)}$ and $P_f^{(i)}$ respectively denote the local detection probability and false alarm probability of the i-th SU. It can be seen that the OR fusion rule corresponds to the case of $n = 1$; the AND fusion rule corresponds to the case of $n = K$; and the majority fusion rule corresponds to the case of $n \geq K/2$.

2.2. Dynamic Attack Behavior Patterns

As the input data of the cognition cycle's follow-up processes, sensing information sent by SUs is essential to network decision. Therefore, at the sensing information reporting stage, the system's expectation is that SUs can actively report true sensing data to the FC. However, the FC may receive wrong or dishonest sensing data due to channel shading, shadowing and SSDF attack [17,18]. In particular, the SSDF attack is caused by two reasons: (1) SUs with cognition ability are compromised, and their reports are falsified; (2) the malfunction or fault of SUs leads to sensing reports contrary to the fact.

Although dishonest manners appear in different patterns, their common goal is to mislead the FC to make wrong decisions on current channel states. To be specific, the common attack models include [19,20]:

- Always present (AP): the attacker asserts the channel is busy in any case, i.e., $u_i(t) = 1$;
- Always absent (AA): the attacker asserts the channel is idle in any case, i.e., $u_i(t) = 0$;
- Always opposite (AO): the attacker with strong sensing ability always sends sensing reports contrary to its local spectrum sensing results, i.e., $u_i(t) = 1 - d_i(t)$.

With the booming growth of artificial intelligence, the attack patterns adopted by malicious users become increasingly complicated, which should be carefully taken into consideration. The attack strategy adopted by malicious cognitive users has been gradually transforming from simplicity, fixedness and singleness into complexity, dynamic and crypticity. They are inclined to achieve the goal of gaining additional spectrum access opportunities by cheating, undermining the licensed user and cognitive systems or other purposes to a larger extent. Besides, in an actual network, an individual SU can change between the true and false state back and forth due to both objective and artificial causes. Particularly, in a hostile environment, an honest SU may be manipulated by its adversary, thus suffering severe performance degradation (even turning into a malicious user) during a certain period. However, the adversary may evacuate from the battlefield after a while, and the behavior of the SU will transform again. Still another condition is, when the block that shelters an SU no longer exists, or the SU leaves the shadow zone, a better performance may be achieved.

Based on the above argumentation, we introduce two dynamic behavior patterns in this paper, which are the behavior of changing from true to false and then to true (TFT) and the behavior of changing from false to true and then to false (FTF); the details of the patterns are as follows.

2.2.1. TFT Behavior Pattern

Specifically, in the TFT behavior pattern, cognitive users with a virtuous nature report correct and true sensing results to the fusion center according to its normal working condition in the first period of time; due to some uncontrollable factors, such as being controlled by the enemy or sheltered from the shadow block, the SU reports false decisions for the next period; when it gets rid of the enemy or leaves the shadow zone, the user resubmits normal sensing data. The "true" and "false" respectively denote the normal working status (NWS) and temporary working status (TWS) of cognitive users. This kind of malicious dynamic behavior occurs under the unconsciousness and passiveness of cognitive users.

In the TFT behavior pattern, the detection probability and false alarm probability of SU$_i$ in NWS are denoted by $P_{d1}^{(i)}(\text{TFT})$, $P_{d3}^{(i)}(\text{TFT})$ and $P_{f1}^{(i)}(\text{TFT})$, $P_{f3}^{(i)}(\text{TFT})$, respectively.

$$P_{d1}^{(i)}(\text{TFT}) = P_{d3}^{(i)}(\text{TFT}) = P\{u_i(t) = 1 \mid \mathcal{H}_1\} = P\{d_i(t) = 1 \mid \mathcal{H}_1\} = P_d^{(i)} \tag{8}$$

$$P_{f1}^{(i)}(\text{TFT}) = P_{f3}^{(i)}(\text{TFT}) = P\{u_i(t) = 1 \mid \mathcal{H}_0\} = P\{d_i(t) = 1 \mid \mathcal{H}_0\} = P_f^{(i)} \tag{9}$$

We use $P_{d2}^{(i)}(\text{TFT})$ and $P_{f2}^{(i)}(\text{TFT})$ to indicate the detection and false alarm probability of SU$_i$ in TWS:

$$P_{d2}^{(i)}(\text{TFT}) = P\{u_i(t) = 1 \mid \mathcal{H}_1\} = P\{d_i(t) = 0 \mid \mathcal{H}_1\} = 1 - P_d^{(i)} \tag{10}$$

$$P_{f2}^{(i)}(\text{TFT}) = P\{u_i(t) = 1 \mid \mathcal{H}_0\} = P\{d_i(t) = 0 \mid \mathcal{H}_0\} = 1 - P_f^{(i)} \tag{11}$$

2.2.2. FTF Behavior Pattern

In the FTF behavior pattern, cognitive users with a vicious nature report incorrect and false sensing results to the fusion center according to its normal attacking condition in the first period of time; in order to avoid exposing their own malicious identity, malicious users will temporarily disguise themselves as normal SUs and submit true local decision results within the next period of time; after successfully achieving the purpose of deception, malicious users immediately expose their harsh nature and resubmit the reversed local decision results. "False" and "true" denote the NWS and TWS of SUs, respectively. This kind of malicious dynamic behavior arises when cognitive users possess deliberate and proactive motivation.

In the FTF behavior pattern, the detection and false alarm probability of SU$_i$ in NWS are denoted by $P_{d1}^{(i)}$(FTF), $P_{d3}^{(i)}$(FTF) and $P_{f1}^{(i)}$(FTF), $P_{f3}^{(i)}$(FTF), respectively.

$$P_{d1}^{(i)}(\mathrm{FTF}) = P_{d3}^{(i)}(\mathrm{FTF}) = P\{u_i(t) = 1 \mid \mathcal{H}_1\} = P\{d_i(t) = 0 \mid \mathcal{H}_1\} = 1 - P_d^{(i)} \tag{12}$$

$$P_{f1}^{(i)}(\mathrm{FTF}) = P_{f3}^{(i)}(\mathrm{FTF}) = P\{u_i(t) = 1 \mid \mathcal{H}_0\} = P\{d_i(t) = 0 \mid \mathcal{H}_0\} = 1 - P_f^{(i)} \tag{13}$$

$P_{d2}^{(i)}$(FTF) and $P_{f2}^{(i)}$(FTF) are employed to indicate the detection and false alarm probability of SU$_i$ in TWS.

$$P_{d2}^{(i)}(\mathrm{FTF}) = P\{u_i(t) = 1 \mid \mathcal{H}_1\} = P\{d_i(t) = 1 \mid \mathcal{H}_1\} = P_d^{(i)} \tag{14}$$

$$P_{f2}^{(i)}(\mathrm{FTF}) = P\{u_i(t) = 1 \mid \mathcal{H}_0\} = P\{d_i(t) = 1 \mid \mathcal{H}_0\} = P_f^{(i)} \tag{15}$$

Precisely speaking, both behavior patterns possess a sensing performance similar to normal SUs within a certain period and the performance similar to AO attackers in the other period. It can be seen from the difference of their respective detection and false alarm probability that these two generalized behavior patterns exert distinct effects on CSS, which will be shown later. For the convenience of expression, the cognitive users described by both of these behavior patterns are referred to as malicious secondary users in this paper.

3. Comprehensive Reputation-Based Security Mechanism

In order to identify and defend against the complicated attack behavior of malicious users more effectively and rapidly, this paper proposes a novel reputation-based security mechanism. In the mechanism, each SU is allocated a continuously updated comprehensive reputation (CR) value by the FC in accordance with its reported sensing data. The CR value evaluates the reliability and correctness of the individual user's sensing data sent to the FC. Higher reputation means that the user's sensing data in the past are more beneficial for the FC to make the right global decisions. The CR value is an important reference in the next sensing round.

The comprehensive reputation integrally considers four influencing factors of user reliability, including current reliability, historical reputation, reward factor and punishment factor. A malicious user obtains low reputation and fusion weight due to submitting falsified sensing data, and the FC weakens its harmful effect in the process of data fusion or directly ignores its sensing results. The comprehensive reputation adequately measures and reflects the reliability of individual sensing results for cognitive users in an appropriate time scale and is constantly changed and updated.

3.1. Current and Historical Reputation

3.1.1. Current Reliability

In CSS, the global decision is usually more reliable than local decisions [21,22]. Therefore, the global decision can be treated as a reference to determine whether the sensing result of a single user is errorless or not at one certain slot.

The current reliability is the consistency check between the local decision of SUs and the final decision of the FC. The setting principle is to slow down the ascending rate and speed up the descending rate to improve the reliability of reputation; SSDF attackers can be availably restrained in this way. Considering that the comprehensive reputation will be updated at the end of each sensing round with higher calculation frequency, thus this requires the reputation quantization algorithm to be simple and efficient. In view of the above analysis, the current reliability value of the i-th SU at the t-th sensing slot is as follows:

$$CurR_i(t) = (-1)^{u_i(t)+u_0(t)} \times \tau^{\theta}, \quad t = 1, 2, \cdots \tag{16}$$

where $u_i(t)$ and $u_0(t)$ respectively represent the local report and global decision made by the i-th SU and FC. The current reputation will be incremented by one if $u_i(t)$ is consistent with $u_0(t)$; otherwise, it will be decremented by τ^{θ}. The constant τ acts on accelerating descent velocity and decelerating increased velocity, $\tau > 1$. The specific size of τ can be adjusted according to the actual situation to achieve the compromise of weighted efficiency and correctness. When $\tau = 2$, the cumulative rate of consistency accuracy is only half of the decay rate. The calculation method of θ is as follows:

$$\theta = \begin{cases} 1, & u_i(t) \neq u_0(t) \\ 0, & u_i(t) = u_0(t) \end{cases} \tag{17}$$

3.1.2. Historical Reputation

The reputation is the subjective probability prediction of the subject concerning whether the object can complete a certain collaborative activity correctly and non-devastatingly, and historical sensing behavior reflects the reliability variation of cognitive users. In order to highlight the historical behavior of SUs in the role of reputation evaluation, we introduce the historical reputation variable denoted as $HisR_i(t)$ to describe and evaluate the reliability of the i-th SU at the t-th slot.

If all of the historical reputation of cognitive users is taken into account, that would require much storage space occupation and high computing complexity. Hence, we consider employing an observing window to assess the detection stability of SUs in the most recent period. The observation window calculates the weighted sum of the corresponding CR value in up-to-date L sensing events and moves forward along with the occurrence of a new sensing event.

Historical sensing information has a near-far effect on the update process of reputation; in reality, recent sensing events in historical sensing behaviors play a more significant role than long-term sensing events in real-time reputation calculation. Therefore, the reputation of different slots should be endowed with distinct time weights, called the time attenuation factor (TAF) in this paper. The TAF of the comprehensive reputation for the i-th SU at the $(t-k)$-th time slot is represented as $\alpha_{i,k}$.

$$\alpha_{i,k} = \frac{L-k}{\frac{L(L+1)}{2}} = \frac{2(L-k)}{L(L+1)} \tag{18}$$

With sensing time increasing, even if a misbehaving user wins high trust in a certain slot, during the period of its opportunistic attack, the reputation of the attacker will gradually decay over time. Time attenuation factor contributes greatly to supervising and urging cognitive users to submit genuine sensing results continuously.

The historical reputation $HisR_i(t)$ of the i-th SU at the t-th sensing slot is evaluated as the following rule:

$$HisR_i(t) = \sum_{k=1}^{L} \alpha_{i,k} ComUpR_i(t-k), \quad k = 1, 2, \cdots, L \quad t = 1, 2, \cdots \tag{19}$$

where $ComUpR_i(t-k)$ denotes the CR value of SU$_i$ at the $(t-k)$-th slot; L is the length of the observation window.

In the calculation of historical reputation, the observation window length should not be set too small; otherwise, the decay rate of the reputation value is too fast to fully assess the reliability of the cognitive users, and the historical behavior information cannot be brought into sufficient usage; on the other hand, remaining sensitive to the potential behavior change of SUs requires that L should not be set too large, either. In actual spectrum sensing, the length of the observation window can be reasonably selected according to the computation time length of the reputation value and the change of the sensing performance of the cognitive users.

Instead of only considering the influence of SUs afterone sensing round is exerted on the current CR value, the design regulation of historical reputation conducts distributed processing for the instantaneous growth or decline of the reputation value via choosing appropriate observation lengths of the window according to specific demand; thus, the adverse effects of the burst fluctuation of the reputation value on the reliability of the cognitive users can be avoided.

3.2. Punishment Strategy

Since security has played a major role in CRNs, numerous research works have mainly focused on attack detection based on detection probability, but few of them took the penalty of attacks into consideration and neglected how to implement effective punitive strategies against attackers. In addition, in the dynamic SSDF attacks; behavior pattern, malicious users alternately submit authentic and spurious sensing data; general reputation mechanisms cannot effectively identify this sort of attack, and MUs may always be in a believable state, while a well-built reputation update mechanism should be sensitive to changes in users' behaviors and able to punish their villainy.

Aiming at this issue, this paper introduces a reward and punishment strategy to modify the CR value in line with the behavior characteristics of cognitive users, in which a reward factor and a penalty factor are introduced to encourage SUs to engage in positive and honest sensing activities. On the one hand, the reputation of users who continuously report false sensing results ought to be attenuated in a timely manner, making them unable to participate in cooperative sensing; on the other, users who conduct persistent honest sensing are supposed to be rewarded appropriately, thus encouraging them to continue to submit real detection outcomes.

3.2.1. Reward Factor

Assuming the i-th SU performed true sensing at the $(t-k)$-th round and continuous honest sensing behaviors occur in the next $(t-h+1, t-h+2, \cdots, t-1)$-th sensing round, then the reward factor has a positive effect on modifying the CR value of the cognitive user. The calculation of the reward factor is according to the following method:

$$RewF_i(t) = |\frac{1}{h-1}(\sum_{l=t-h}^{t-1} ComUpR_i(l) - \max ComUpR_i(l))| \tag{20}$$

where $ComUpR_i(t)$ is the CR value of SU$_i$ at the t-th sensing round and h denotes the times of continuous honest sensing events.

h sensing reputation values are employed during the computational process of the reward factor. The reward dynamics is constantly adjusted with the cumulative reputation. However, MUs may accumulate relatively high reputation through continuously providing honest decision results inside a shorter time; in view of this kind of speculation, the calculation of the reward factor removes the maximum reputation value $\max ComUpR_i(l)$ of SU$_i$ in h successive true sensing slots, thus reducing the reward intensity for honest sensing efforts. Only by ceaselessly submitting real local results can SUs establish a favorable credit status for themselves; thus the reward factor can motivate cognitive users to make a positive contribution to collaborative sensing.

3.2.2. Penalty Factor

Supposing SU$_i$ conducted false sensing at the $(t-g)$-th slot and continuous false sensing behaviors emerge in the following $(t-g+1, t-g+2, \cdots, t-1)$ sensing round, then the penalty factor has influence on inhibiting malicious attack behavior. The calculation method of penalty factor is as follows:

$$PenF_i(t) = |\frac{1}{g-1}(\sum_{l=t-g}^{t-1} ComUpR_i(l) - \min ComUpR_i(l))| \tag{21}$$

where $ComUpR_i(t)$ is the CR value of SU_i at the t-th sensing round and g denotes the times of continuous false sensing events.

The punishment scheme follows a habit of human society, that is the initial criminal punishment is light, and the cumulative crime will be punished heavily. Therefore, the greater the threat is, the more serious of a punishment should be imposed. The penalty factor removes the minimum value in g; CR values are removed in the penalty factor computing; in this way, the influence of accidental behavior on reputation in spectrum sensing is weakened; moreover, cognitive users will pay a great price for short-term opportunistic behavior caused by their unlikely mind, so as to achieve the purpose of restraining malicious attacks.

3.3. Calculation of the CR Value

In the proposed security mechanism, four influential elements for evaluating sensing reliability are generally considered, including current reliability, historical reputation, reward factor and punishment factor. We utilize $ComUpR_i(t)$ to represent the comprehensive reputation value of the i-th SU at the t-th sensing slot:

$$ComUpR_i(t) = \rho_0 \cdot HisR_i(t) + \rho_1 \cdot CurR_i(t) + \beta \cdot RewF_i(t) + \gamma \cdot PenF_i(t) \tag{22}$$

where ρ_0 and ρ_1 respectively are the proportion coefficients of historical reputation and current reliability, $0 < \rho_0, \rho_1 < 1$ and $\rho_0 + \rho_1 = 1$. Their values can be appropriately adjusted according to the demand of network security. When demand for the sensitivity of the security mechanism is higher, increase ρ_1, which means raising the weight of current trust evidence; then, it can be detected immediately once any untrustworthy behavior appears; when the long-term influence of reputation plays an important role, increase ρ_0, which signifies raising the weight of historical reputation to encourage the SUs to be legitimate in the long run. In fact, ρ_1 is a kind of response speed; a high speed of response means that cognitive users can make more effective and rapid response to changes in their CR value. The determination method of β and γ is as follows:

$$\beta = \begin{cases} 1, & continuous\ honest\ sensing\ events\ exist \\ 0, & else \end{cases} \tag{23}$$

$$\gamma = \begin{cases} -1, & continuous\ false\ sensing\ events\ exist \\ 0, & else \end{cases} \tag{24}$$

The literature [23] has pointed out that data fusion schemes become completely incapable, and no reputation-based fusion scheme can achieve any performance gain when the number of attackers exceeds a certain fraction in the CRN. If the number of independent attackers is greater than half of the total users, the FC will be rendered “blind”. To tackle this problem and ensure the correctness of the global decision, we assume only some reliable nodes (RN), instead of all SUs, are trustworthy initially. In reality, the RNs can be a base station, access point, cluster head, etc. Since they share the generality as foundations of the cognitive system, it is reasonable to grant the position of these RNs exceeding that of the remaining SUs.

In the first instance, only RNs participate in the deciding procedure, meaning the global decision is made merely based on their sensing results. Though the remaining SUs are not contained in the step of cooperative sensing, their CRs are accumulated continuously. A SU can be considered as a reliable one only when its CR value exceeds the predetermined reputation threshold η_r.

Employ C to describe the set of RNs, and $A(t)$ represents the set of cognitive users that can participate in the fusion decision, which are given by:

$$C = \{i|\mathrm{SU}_i \text{ is a CN}\} \tag{25}$$

$$A(t) = \{j|ComUpR_i(t) \geq \eta_r, \quad j \in \{1, 2, \cdots, N\}\}, \quad t = 1, 2, \cdots \tag{26}$$

where C is determined on the basis of the specific circumstance, while $A(t)$ varies with the results of identifying procedure each sensing round.

The initial CR values are $ComUpR_{i\in C}(0) = \eta_r + \Delta$ and $ComUpR_{i\notin C}(0) = \eta_r - \Delta$ for RNs and remaining nodes, respectively. The setting of margin Δ is to distinguish RNs from other SUs, namely the degree of tolerance for potentially sensing errors. Consequently, only SUs belonging to C make contributions to the global decision making for the first round, then the range enlarges to $A(t)$.

Unlike the existing mechanisms, the proposed security mechanism does not abandon any user, and their identification is conducted all the way. This is more equitable and reasonable particularly when the complicated behavior patterns are taken into account, noticing that one FTF user that behaves poorly at the intermediate stage may obtain a better performance eventually.

3.4. Reliable Nodes' Credibility Verification

This step is conducted within the RNs by inspecting the variances of their CR values. After the identifying step completed at each round, we compare the real-time CR value of each RN $ComUpR_i(t),\ i \in C$ with its highest CR value in previous sensing slots, which is denoted by $ComUpR_{i\max}(t-1)$. Initially, $ComUpR_{i\max}(0) = \eta_r + \Delta,\ i \in C$. If the real-time CR value $ComUpR_i(t)$ is higher than $ComUpR_{i\max}(t-1)$, then the new highest CR value is updated as the current one, otherwise $ComUpR_{i\max}(t)$ remains unchanged. Accordingly, the highest CR value update mode can be presented as:

$$ComUpR_{i\max}(t) = \begin{cases} ComUpR_i(t), & ComUpR_i(t) > ComUpR_{i\max}(t-1) \\ ComUpR_{i\max}(t-1), & ComUpR_i(t) < ComUpR_{i\max}(t-1) \end{cases} \quad i \in C,\ t = 1, 2, \cdots \tag{27}$$

Then, the following inequality set is verified immediately:

$$ComUpR_{i\max}(t) - ComUpR_i(t) < \Delta \quad i \in C,\ t = 1, 2, \cdots \tag{28}$$

where Δ denotes the degree of tolerance for potentially sensing errors as discussed earlier. If all RNs satisfy the above inequalities, the deciding procedure can be performed directly; otherwise, it means that the local results sent by the corresponding RN have been inconsistent with the global decision many times. Under such a circumstance, we conclude that the global decision is incorrect (which may be caused by various reasons), considering that these RNs are trusted all of the time. This verification process is called sustained credible node assistance (SCNA). In order to ensure the correctness of the final decision in the future, resetting is performed before center fusion, which is to clear all of the accumulated CR and weight values via setting them to the initial state. The accumulation restarts hereafter. In this step, the inequality set Equation (25) serves as a trigger and decides whether the resetting is required.

4. Comprehensive Reputation-Based Data Fusion Solution

4.1. Weight Allocation

The center data fusion is ultimately implemented after the above steps are accomplished, in which all of the elected trusted users will participate. Distinct fusion weights are allocated to SUs corresponding to their comprehensive reputation values. Users with greater reputation have stronger impact on the final decision making; hence, the sensing accuracy of CSS can be improved.

The fusion weight value for the i-th SU at the t-th sensing slot can be calculated as:

$$w_i(t) = \begin{cases} 0, & i \notin A(t) \\ \frac{ComUpR_i(t-1)}{\overline{ComUpR_i(t-1)}}, & i \in A(t) \end{cases} \quad t = 1, 2, \cdots \tag{29}$$

where:

$$\overline{ComUpR_i(t-1)} = \frac{ComUpR_i(t-1)}{\sum_{i \in A(t)} ComUpR_i(t-1)}, \quad t = 1, 2, \cdots \tag{30}$$

denotes the average CR value of reliable nodes. The initial weight is $w_{i \in C}(0) = 1$, $w_{i \notin C}(0) = 0$.

4.2. Measurement Combining Stage

Evidently, the idea of comprehensive reputation updating and sustained credible node assistance are not restricted to specific designated fusion techniques and can be widely applied. For simplicity, we employ the majority fusion rule as an example in this paper, which is proven to be relatively ideal in both detection accuracy and energy efficiency [23].

Majority rule implies that the final decision is in accord with the decision of the majority of the received local decisions. Assuming M SUs are qualified to participate in the collaboration, mathematically, the final decision is made according to the majority rule as follows:

$$Final\ Decision \begin{cases} 1 \equiv occupied, & if \sum_{i=1}^{M} w_i u_i \geq \frac{M}{2} \\ 0 \equiv unoccupied, & else \end{cases} \tag{31}$$

Similar to the local decision, the accuracy and reliability of the final decision is measured and evaluated by two acknowledged metrics, the global false alarm probability (Q_f) and the global misdetection probability (Q_m). Both depend on the final decision rather than the local decision.

4.3. The Mechanism Flow

Based on the above discussions, the operation process of the comprehensive reputation-based security mechanism is shown in Figure 2. The CSS system starts working with the step of reputation initialization; all SUs conduct individual sensing to obtain the one-bit decision result. If the CR value $ComUpR_i(t)$ of SU$_i$ exceeds reputation threshold η_r, then FC would allow this user to join the cooperation. Different fusion weights are assigned to qualified cognitive users for center decision fusion. After obtaining the global decision $u_0(t)$, credibility verification is performed for reliable users to ensure that the whole CSS system has not been held hostage by malicious users. If all RNs pass the verification, then the CR values can be updated in accordance with users' sensing behaviors, which comprises the current reliability, historical reputation, reward factor and penalty factor. Consequently, the proposed security mechanism gives a system-wide view of the satisfaction of a cognitive user.

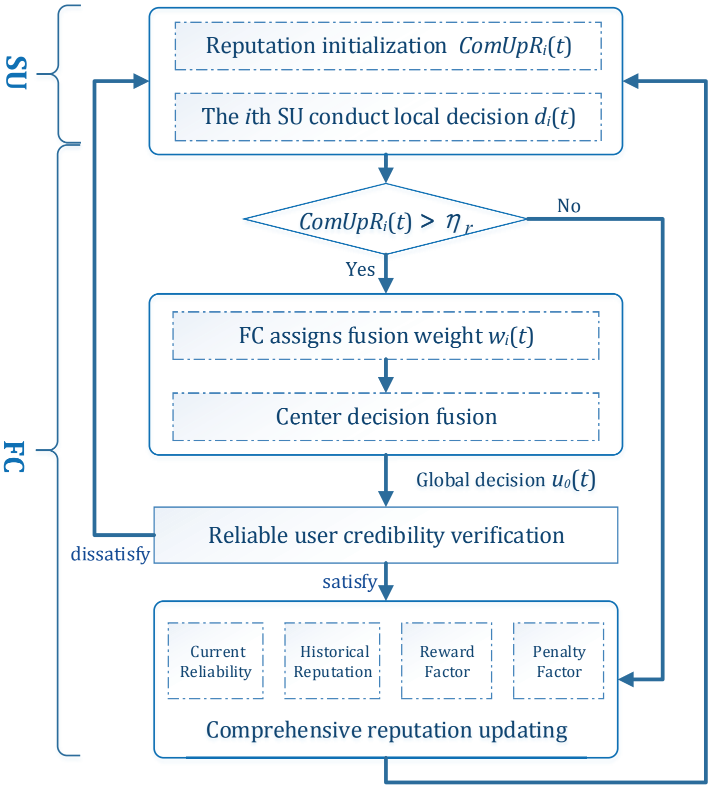
SU
FC
Reputation initialization $ComUpR_i(t)$
The ith SU conduct local decision $d_i(t)$
$ComUpR_i(t) > \eta_r$
No
Yes
FC assigns fusion weight $w_i(t)$
Center decision fusion
Global decision $u_0(t)$
Reliable user credibility verification
dissatisfy
satisfy
Current Reliability
Historical Reputation
Reward Factor
Penalty Factor
Comprehensive reputation updating

Figure 2. The flow chart of the proposed security mechanism.

5. Numerical and Simulation Results

In this section, we present the numerical results for the proposed reputation mechanism. The simulations are conducted with $K = 50$ cognitive users in a centralized CRN, among which $N_1 = 10$ reliable nodes exist. In the numerical simulation, the sensing performance is given as the reference curve when malicious users employ the AO attack strategy. We investigate the impact of malicious users exerted on the collaborative sensing when the two dynamic behavior patterns introduced in Section 2.2 are used. The number of MUs is expressed as N_0, and the proportion of MUs is set to [0, 0.8]. That is, from no malicious users exist in the network (the proportion is 0%), till 40 cognitive nodes, all are misbehaving users except the 10 reliable nodes (the proportion is 80%).

Without loss of generality, the primary signal is assumed to be the BPSK signal with $P(H_1) = 0.3$, and all SUs experience independently and identically distributed (i.i.d.) fading or shadowing with the same average SNR $\gamma = -10$dB to simplify the implementation. The time-band product m is five, and the same energy detection threshold $\lambda = 12$ is utilized. The entire simulation runs 100,000 rounds, and we assume that the moment of behavior changes respectively occurs at the 40,000 and 70,000 round in both the TFT and FTF patterns. For the sake of taking advantage of the user's historical sensing results, the observation window length L is set to three. The margin $\Delta = 50$ is set to evidently distinguish RNs from other SUs in the initial sensing stage, namely the degree of tolerance for potentially sensing errors. To avoid mistaking normal SUs as MUs, h and g should not be too small, meanwhile the proposed punishment strategy should be sensitive enough to punish misbehaving users or reward honest users; thus, h and g should not be too large. Hence, we set the times of continuous/false sensing events $h = g = 3$. The reputation threshold $\eta_r = 100$ is set to effectively identify MUs and prevent them from participating in the collaboration in each sensing slot. We set the variable τ to two to ensure that the cumulative consistency accuracy rate of current reliability in the comprehensive reputation value is only half of the decay rate, which is also a compromise of weighted efficiency and correctness. The proportion coefficients of historical reputation and current reliability in the CR value calculation ρ_0 and ρ_1 are set to 0.5 to balance current trust evidence and the long-term influence of reputation. All simulations are conducted in the MATLAB R2015a environment.

The following six scenarios are carefully considered in this section:

- Scenario 1 there are N_1 RNs in the CRN, performing CSS with no reputation mechanism;
- Scenario 2 there are K RNs in the CRN, performing CSS with no reputation mechanism;
- Scenario 3 there are N_0 misbehaving SUs and $K - N_0$ RNs in the CRN, performing CSS with the proposed scheme in this paper;
- Scenario 4 there are N_0 MUs in the CRN, performing CSS with the security scheme in [13];
- Scenario 5 there are N_0 MUs in the CRN, performing CSS with the security scheme in [12];
- Scenario 6 there are N_0 MUs and N_1 RNs in the CRN, performing CSS with the proposed security scheme in this paper to counter diverse SSDF attacks.

The purpose of considering Scenarios 1–3 is to provide the simulation experiments with clear contrast reference curves. Specifically, we consider Scenario 1 to explore when all SUs are reliable cognitive nodes; what the performance of the non-reputation-based sensing scheme is like under diverse SSDF attacks. Scenario 2 is set to experiment on the performance of the non-reputation-based method in the presence of partial reliable users. In Scenario 3, there are only two kinds of cognitive users, i.e., RNs and MUs, and we test the detection performance under this circumstance when suffering different types of SSDF attack. Scenarios 4 and 5 are two contrast algorithms to further verify and evaluate the effectiveness of the proposed mechanism in this paper.

5.1. The Sensing Performance under AO Attack

As mentioned above, the always opposite attack strategy refers to the attack mode that MUs report after reversing the local decision result. Figures 3 and 4 present the cooperative sensing performance under AO attack. The horizontal axis accounts for the proportion of malicious users. The vertical axis in Figure 3 represents the global false alarm probability Q_f, and the vertical axis in Figure 4 represents the global misdetection probability Q_m.

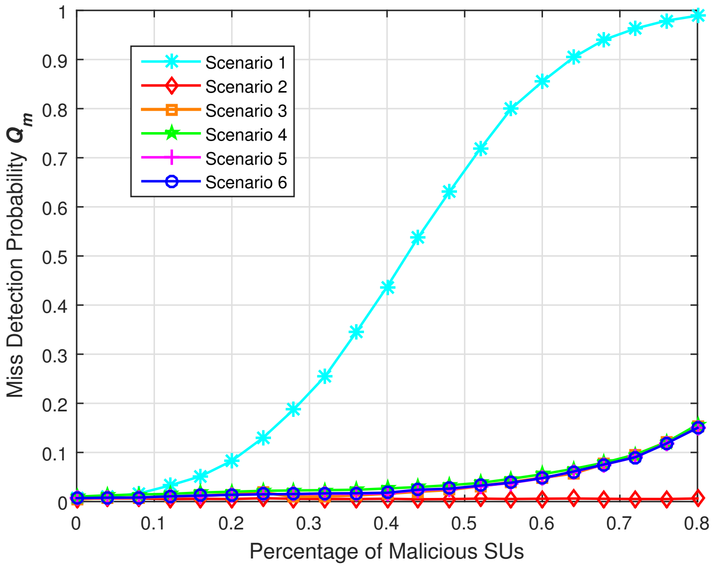

Figure 3. The misdetection probability under the always opposite (AO) attack.

It can be seen from the Figures 3 and 4, when there is no malicious users in the network (Scenario 2), the optimal sensing performance can be achieved if K cognitive users are reliable nodes. Additionally, the detection performance under Scenario 3, in which $K - N_0$ RNs participate in the collaboration, is inferior to that in Scenario 2. The detection performance of the scheme with no reputation mechanism in Scenario 1 dropped dramatically under the AO attack pattern, which means it is indispensable for CRNs to adopt a necessary and effective security mechanism to defend against various types of spiteful attack behaviors. When the number of MUs exceeds half of all cognitive users, the sensing performance is even worse than that of random guessing. Besides the proposed reputation mechanism (Scenario 6), the scheme in [12] (Scenario 5) and [13] (Scenario 4) can achieve the equivalent performance of $K - N_0$ reliable nodes, meaning that they can availably identify the malicious SUs and eliminate their harmful effects via only using reliable reported results for fusion decision making.

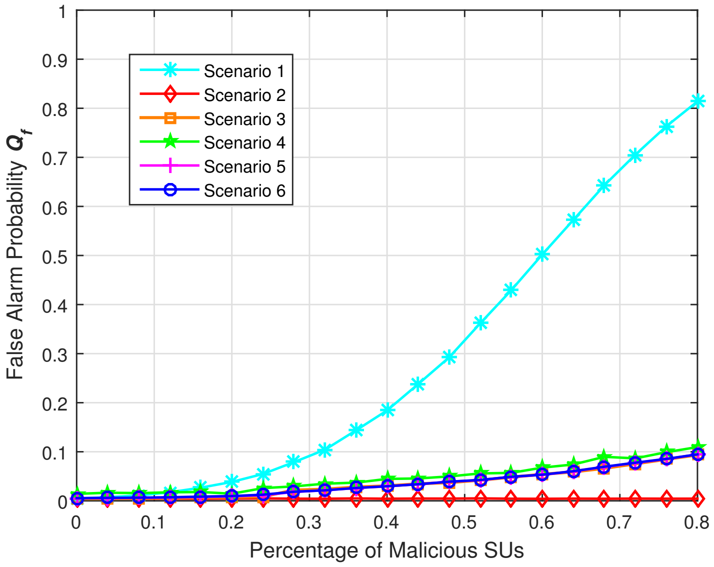

Figure 4. The false alarm probability under AO attack.

5.2. The Sensing Performance under TFT Attack

As introduced in Section 2.2, in the TFT behavior pattern, cognitive users report true sensing results in the first period of time; the SU reports false decisions for the next period; the user finally resubmits the normal sensing data. Figures 5 and 6 show the collaborative sensing performance of the above several scenarios under the TFT attack.

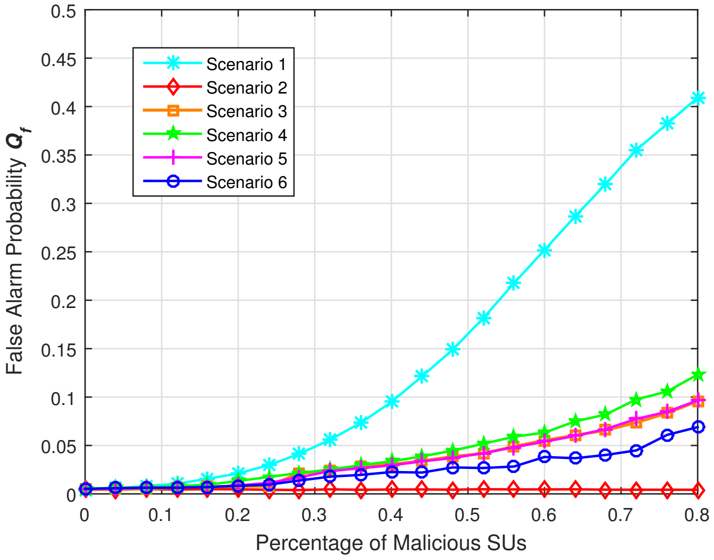

Figure 5. The false alarm probability under the true to false and then to true (TFT) attack.

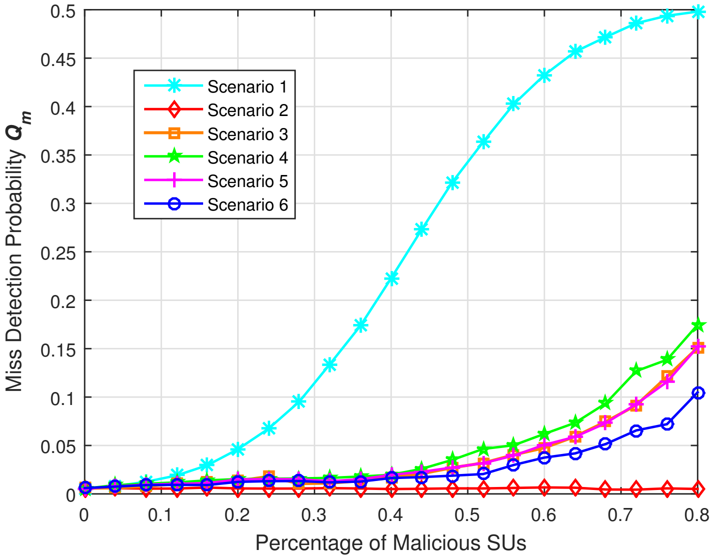

Figure 6. The misdetection probability under the TFT attack.

Through the observation, we can learn that the sensing performance of Scenarios 1 and 2 are identical to that in Section 5.1, which is attributed to the non-participation of misbehaving cognitive users. Scenario 5 still can achieve the sensing performance when $K - N_0$ reliable nodes are collaborating; the performance in Scenario 4. It is worth noting that the proposed mechanism in this paper can achieve better performance than the schemes in [12,13]. When MUs occupy 80% of all of the SUs, specifically, the false alarm probability of the proposed mechanism in this paper, [12,13] respectively, is 0.0690, 0.0965 and 0.1233, and the misdetection probability, respectively, is 0.1020, 0.1506 and 0.1748. The proposed mechanism in this paper possesses an obvious performance advantage both in false alarm probability and misdetection probability compared to the contrasted algorithms.

The reason for the performance advantage is that the cognitive users with poor performance at the initial stage will be permanently abandoned in the literature [12,13], which does not consider that the SUs' behavior may be dynamically changed, and a better individual user's sensing performance may be obtained after a period of time. In this paper, the mechanism is proposed to continuously evaluate the reliability of each cognitive user through the calculation of the comprehensive reputation. Our scheme forgives the repentance behavior (change from poor performance to good performance) of cognitive users, that is continually mitigating the effect of the correctness of reported results in earlier time slots exerted on assessing the reliable degree of cognitive users. SUs are allowed to continue to participate in the fusion decision of cooperative spectrum sensing when the comprehensive reputation value exceeds the reputation threshold. This way is equivalent to increasing the user number of participation cooperative sensing, thus obtaining an obvious gain of the sensing performance.

5.3. The Sensing Performance under FTF Attack

As presented in Section 2.2, in the FTF behavior pattern, SUs report false sensing results to the FC in the first period of time and then report true decisions for the next period; the user finally resubmits reversed local decision results. Figures 7 and 8 show the collaborative sensing performance of the above several scenarios under the FTF attack.

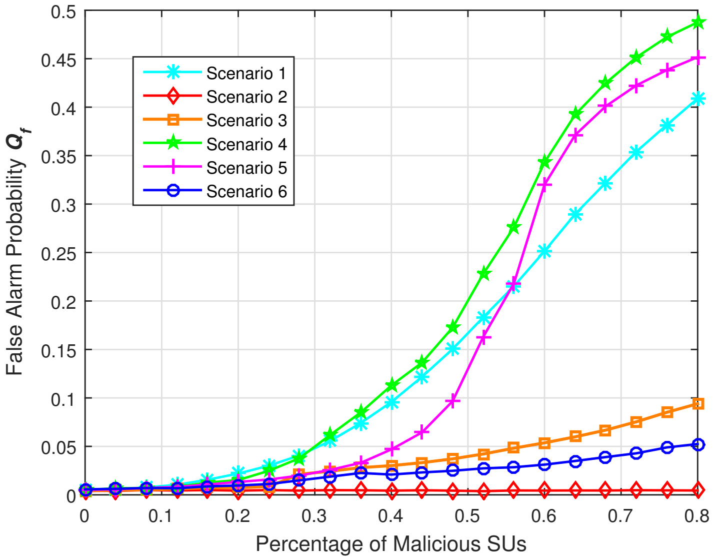

Figure 7. The false alarm probability under the false to true and then to false (FTF) attack.

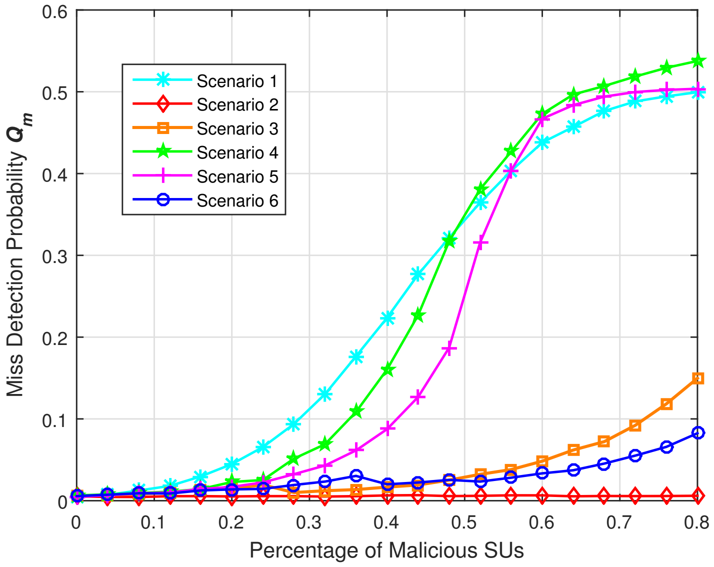

Figure 8. The misdetection probability under the FTF attack.

Similarly, the sensing performances of Scenarios 1 and 2 are identical to that in Section 5.1. However, the performance of Scenarios 4 and 5 deteriorated significantly when malicious SUs adopt the FTF attack mode. In Figure 7, when the proportion of MUs is greater than 40%, the performance of the algorithms in Scenarios 4 and 5 sharply declines. The false alarm probability of the proposed mechanism in this paper, [12,13] respectively, is 0.0524, 0.4516 and 0.4876 when the percentage of MUs is 80%, meaning that while the ratio of MUs continues to increase (account for the majority), the algorithms in [12,13] become completely ineffective.

This phenomenon can be explained as follows: in the stage of temporary working status in FTF attack, malicious cognitive users, together with normal SUs, obtain a higher level of reputation through accumulation and are identified as cognitive users that can participate in the fusion decision. When the working state of MU changes from TWS to NWS and it resubmits reversed local decision results, it affects the fusion decision process, which makes the false alarm probability and detection probability of the global decision increase simultaneously because of its higher reputation level. Especially when they occupy a higher proportion, these malicious users are enough to control the global decision making process of the fusion center; at this moment, the entire collaborative sensing system is hijacked by malicious users.

In Figure 8, the misdetection probability of the proposed mechanism in this paper, [12,13] respectively, is 0.0138, 0.1693 and 0.2291 when MUs occupy 80% of all SUs, which means that the proposed method can effectively reduce the misdetection probability of CSS, meanwhile protecting the system from complex SSDF attacks. In other words, even if the malicious cognitive user accounts for a high proportion, as 80%, the CSS algorithm based on the reputation mechanism in this paper still possesses higher robustness. The obvious performance advantage profits from reliable nodes' credibility verification. If the declining range of some reliable user's CR value is greater than Δ, the global decision fusion of the FC is identified as occurring persistent errors and triggers the resetting mechanism to clean the comprehensive reputation value for each cognitive user. This method avoids the global decision of the FC being controlled by MUs and reduces the adverse effects of MUs on the global decision results, ultimately achieving better performance than $K - N_0$ users cooperating.

6. Conclusions

In order to effectively resist malicious cognitive users' attack behaviors in cognitive radio networks, the security mechanism for CSS is studied in this paper. We first introduce two new cognitive user dynamic behavior patterns to describe the changing behavior strategies of SUs. On this basis, a comprehensive reputation-based security mechanism against dynamic SSDF attack is proposed. In the mechanism, current and historical sensing behaviors of cognitive users are utilized to integrally evaluate sensing reliability; moreover, a punishment strategy is presented to encourage SUs to engage in positive and honest sensing activities. In addition, the sustained verification of reliable nodes ensures the correctness of the global decision of the fusion center and prevents collaborative sensing from being hijacked by misbehaving cognitive users. Simulation results verify that the proposed security mechanism can effectively alleviate the effect of SUs' malicious behaviors, which guarantees the effectiveness and robustness of CRNs.

Acknowledgments: This paper is funded by the National Natural Science Foundation of China (Grant No. 51509049), the Natural Science Foundation of Heilongjiang Province, China (Grant No. F201345), the Fundamental Research Funds for the Central Universities of China (Grant No. GK2080260140) and the National key research and development program (2016YFF0102806).

Author Contributions: Fang Ye conceived of the concept and performed the research. Xun Zhang conducted the experiments to evaluate the performance of the proposed security mechanism and wrote the manuscript. Yibing Li reviewed the manuscript. All authors have read and approved the final manuscript.

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

References

1. Axell, E.; Leus, G.; Larsson, E.G.; Poor, H.V. Spectrum sensing for cognitive radio: State-of-the-art and recent advances. *IEEE Signal Proc. Mag.* **2012**, *29*, 101–116.
2. Haykin, S. Cognitive radio: Brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 201–220.
3. Althunibat, S.; Denise, B.J.; Granelli, F. Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7308–7321.
4. Zhang, L.Y.; Ding, G.R.; Wu, Q.H.; Zou, Y.L.; Han, Z.; Wang, J.L. Byzantine attack and defense in cognitive radio networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1342–1363.
5. Chen, R.L.; Park, J.M.; Bian, K. Robust distributed spectrum sensing in cognitive radio networks. In Proceedings of the 27th Conference on Computer Communications (INFOCOM 2008), Phoenix, AZ, USA, 13–18 April 2008.
6. Zhao, T.; Zhao, Y. A new cooperative detection technique with malicious user suppression. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009.
7. Kaligineedi, P.; Khabbazian, M.; Bhargava, V. K. Malicious user detection in a cognitive radio cooperative sensing system. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 2488–2497.

8. Kun, Z.; Paweczak, P.; Cabric, D. Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Commun. Lett*. **2010**, *14*, 226–228.
9. Du, D. Soft reputation-based secure cooperative spectrum sensing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 23–25 March 2012.
10. Pei, Q.Q.; Yuan, B.B.; Li, L.; Li, H.N. A sensing and etiquette reputation-based trust management for centralized cognitive radio networks. *Neurocomputing* **2013**, *101*, 129–138.
11. Feng, J.Y.; Lu, G.Y.; Bao, Z.Q. Supporting trustworthy cooperative spectrum sensing in cognitive radio networks. *J. Comput. Inf. Syst*. **2014**, *10*, 1–12.
12. Lu, J.Q.; Wei, P. Improved cooperative spectrum sensing based on the reputation in cognitive radio networks. *Int. J. Electron*. **2015**, *102*, 855–863.
13. Feng, J.Y.; Lu, G.Y.; Bao, Z.Q.; Zhang, L. Securing cooperative spectrum sensing against rational SSDF attack in cognitive radio networks. *KSII Trans. Internet Inf. Syst*. **2014**, *8*, 1–17.
14. Digham, F.F.; Alouini, M.S.; Simon, M.K. On the energy detection of unknown signals over fading channels. *IEEE Trans. Commun*. **2007**, *55*, 21–24.
15. Zhang, R.; Zhang, J.; Zhang, Y.; Zhang, C. Secure crowdsourcing-based cooperative pectrum sensing. In Proceedings of the 2013 Proceedings of IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2526–2534.
16. Qin, Z.; Li, Q.; Hsieh, G. Defending against cooperative attacks in cooperative spectrum sensing. *IEEE Trans. Wirel. Commun*. **2013**, *12*, 2680–2687.
17. Bhattacharjee, S.; Debroy, S.; Chatterjee, M.; Kwiat, K. Trust based fusion over noisy channels through anomaly detection in cognitive radio networks. In Proceedings of the 4th International Conference on Security of Information and Networks, Sydney, Australia, 14–19 November 2011; pp. 73–80.
18. Hu, Z.; Ranganathan, R.; Zhang, C.; Qiu, R.C.; Bryant, M.; Wicks, M.C.; Li, L. Robust non-negative matrix factorization for joint spectrum sensing and primary user localization in cognitive radio networks. In Proceedings of the 2012 International Waveform Diversity & Design Conference (WDD), Kauai, HI, USA, 22–27 Janaury 2012; pp. 303–307.
19. 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.
20. Khan, A.A.; Rehmani, M.H.; Reisslein, M. Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. *IEEE Commun. Surv. Tutor*. **2016**, *18*, 860–898.
21. Rawat, A.S.; Anand, P.; Chen, H.; Varshney, P.K. Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks. *IEEE Trans Signal Proc*. **2011**, *59*, 774–786.
22. Zina, C.; Hasna, M.; Hamila, R.; Hamdi, N. Location privacy preservation in secure crowdsourcing-based cooperative spectrum sensing. *EURASIP J. Wirel. Commun. Netw*. **2016**, *85*, 1–11.
23. Althunibat, S.; Sucasas, V.; Marques, H.; Rodriguez, J.; Tafazolli, R.; Granelli, F. On the trade-off eetween security and energy efficiency in cooperative spectrum sensing for cognitive radio. *IEEE Commun. Lett*. **2013**, *17*, 1564–1567.