Supporting Trusted Soft Decision Scheme Using Volatility Decay in Cooperative Spectrum Sensing

Feng Zhao[1] and Jingyu Feng[1, 2]

[1] Department of Communication Engineering, Xi'an University of Posts & Telecommunications
Xi'an 710121, China
[e-mail: fjyu1984@163.com]
[2] State Key Laboratory of Information Security (Institute of Information Engineering), Chinese Academy of Sciences, Beijing 100093, China
*Corresponding author: Jingyu Feng

Received November 17, 2015; revised March 7, 2016; accepted April 3, 2016; published May 31, 2016

Abstract

Cooperative spectrum sensing (CSS) for vacant licensed bands is one of the key techniques in cognitive radio networks. Currently, sequential probability ratio test scheme (SPRT) is considered as a powerful soft decision approach to improve the sensing result for CSS. However, SPRT assumes all secondary users (SU) are honest, and thus offering opportunities for malicious SUs to launch the spectrum sensing data falsification attack (SSDF attack). To combat such misbehaved behaviors, recent efforts have been made to trust mechanism. In this paper, we argue that powering SPRT with traditional trust mechanism is not enough. Dynamic SSDF attackers can maintain high trust in an alternant process of submitting honest or false sensing data, resulting in difficultly detecting them. Noting that the trust value of dymamic SSDF attackers behave highly volatile, a novel trusted SPRT scheme (VSPRT) based on volatility decay analysis is proposed in this paper to mitigate the harmful effect of dynamic SSDF attackers in the process of the soft-decision data fusion, and thus improving the accuracy of the final sensing result. Simulation results show that the VSPRT scheme outperforms the conventional SPRT schemes.

Keywords: Cognitive radio, cooperative spectrum sensing, soft decision, security.

This research was supported in part by the National Science Foundation of China (61301091), the National Science Foundation of Shaanxi Province (2014JQ8321), the Open Foundation of State Key Laboratory of Information Security(2015-MS-14), the New Star Team of Xi'an University of Posts & Telecommunications.

http://dx.doi.org/10.3837/tiis.2016.05.007 **ISSN : 1976-7277**

1. Introduction

With the rapid development of wireless communication technologies and the huge demand of the capacity for wireless applications, the wireless spectrum has become more and more scarce. On the other hand, a large portion of the licensed spectrum bands are not utilized efficiently. According to the Federal Communications Commission (FCC), temporal and geographical variations in the utilization of the licensed spectrum range from 15% to 85% [1]. To solve the contradiction between the spectrum scarcity and low spectrum utilization, cognitive radio has been considered as a useful technology, which allows the licensed users (LU) to share their vacant bands with secondary users (SU) who are not assigned bands, thereby increasing the efficiency of the spectrum utilization [2].

Cooperative spectrum sensing (CSS) is the key to the opportunistic use of assigned spectrum bands in cognitive radio networks, since it enables SUs to find the vacant bands in the case of deep shadowing and multipath fading. The main idea of CSS is to enhance the sensing performance by exploiting spatial diversity via the observations of spatially located SUs [3]. By cooperation, SUs can share their sensing data to make a combined decision with increased accuracy as comparing with the individual decisions [4].

However, little research has been done regarding security in cognitive radio, while much more research has been done on spectrum sensing and allocation problems [5]. It is well known that the cognitive radio paradigm imposes human-like characteristics (e.g., learning, adaptation and cooperation) in wireless networks [6]. Meanwhile, CSS is often established randomly among SUs that are unrelated and unknown to each other [7]. This offers opportunities for malicious SUs to launch the spectrum sensing data falsification attack (SSDF attack [8]) to degrade the profits of honest SUs. Therefore, how to efficiently and effectively defend against SSDF attack has become a very challenging issue to achieve better performance of CSS.

To encourage honest sensing data sharing among SUs, recent efforts have been made to indentify malicious SUs in CSS using trust mechanism. In [9], the authors proposed a novel trust-aware hybrid spectrum sensing scheme, in which the Beta Reputation System is used to construct trust scheme. Zeng et al [10] proposed a reputation-based cooperative spectrum sensing scheme, and categorize the trust of each SU into three states. In [11], the authors considered trust as a competitive factor to punish malicious SUs to access any vacant LU spectrum. In [12], the authors measured the trustworthiness of SUs in CSS during the cognition cycle, and incorporate it into the sensing data fusion to reduce the effect of malicious SUs on final spectrum decision making. They estimate whether an SU is trusted or not by his historical behaviors and give low weights to the sensing data from less trusted SUs when generating a final sensing result. But, their successful foundation is built on the fact that malicious SUs always submit false sensing data. To avoid the detection of trust mechanism, malicious SUs can exhibit dynamic behaviors that allow them to partially hide through providing honest sensing data sometimes while launching SSDF attack. Or rather, they can maintain high trust in an alternant process by submitting honest or false sensing data.

In this paper, we propose a novel trust mechanism to counter dynamical SSDF attack, and embed it into a powerful approach-SPRT to enhance its performance for reliable sensing decision. The main contributions of this paper are as following:

- Noting that the individual sensing data of each SU is a binary variable, we evaluate the trust value of each SU with beta function, resulting in less mathematical analysis and computation.
- By analyzing the volatil characteristic of dynamic SSDF attack, the volatility decay index is introduced to conduct the dynamic evaluation of trust, which can mitigate the harmful effect of dynamic SSDF attackers.
- Incorporating such trust mechanism into SPRT [13], we present a novel trusted sequential probability ratio test scheme (VSPRT) based on volatility decay analysis. Compared with SPRT schemes, VSPRT can improve the accuracy of the final sensing result better. We also describe the implementation strategies of VSPRT in detail.

The remainder of this paper is organized as follows. In section 2, preliminaries related on CSS and dynamic SSDF attack. In section 3, we design VSPRT based on our proposed trust mechanism using volatility decay analysis to suppress dynamic SSDF attack. Simulation analysis of VSTRT is given in section 4. Finally, we conclude the paper in section 5.

2. Preliminaries

The CSS process can be viewed as a parallel fusion network [14]. As shown in **Fig. 1**, a central authority called fusion center (FC) controls the process of CSS: individual sensing, data reporting and data fusion [3].

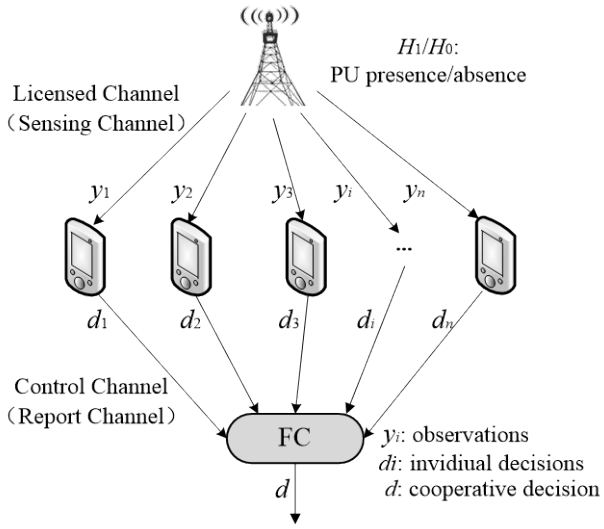

Fig. 1. Modeling CSS as a parallel fusion network.

- **Individual sensing:** Each SU senses the vacant spectrum of a LU via the sensing channel individually.
- **Data reporting:** All SUs submit their sensing data to the FC via the report channel.
- **Data fusion:** The FC combines the received sensing data and determines the presence of LU with a fusion scheme.

In the CSS process, a sensing channel is the selected licensed frequency band where a physical point-to-point link between the LU transmitter and each SU for observing the licensed spectrum, and a reporting channel is a control channel where a physical point-to-point link between each SU and the FC for sending individual sensing information [3]. It can be seen that the two types of channels are given by the network. Thus, the CSS process between SUs

seems will not waste any more spectrums.

Generally, the fusion schemes are generally classified as hard decision and soft decision scheme. In the hard decision scheme [15], SUs abstract their sensing data as "1" or "0" which denotes the hypothesis of the absence (H_1) and the presence (H_0) of the LU spectrum respectively. Although the hard decision consumes much less control channel bandwidth than the soft scheme, it may degrade the detection performance due to the loss of information from quantization. Currently, the FC with using the soft decision scheme can achieve the best performance since it collects the original observations from each SU in the data fusion.

As a typical soft decision scheme, SPRT [13] utilizes the likelihood ratio as the decision variable by sampling the priori probability $P(d_i|H_1)$ and $P(d_i|H_0)$.

$$S_n = \prod_{i=0}^{n} \frac{P(d_i \mid H_1)}{P(d_i \mid H_0)}, \; n=1,2,3... \tag{1}$$

Under the constraint of the false alarm probability (P_{01}) and the miss detection probability (P_{10}), the final sensing result is taken based on the criteria:

$$\begin{cases} S_n \geq \sigma_1 \Rightarrow \text{accept } H_1 \\ S_n \leq \sigma_0 \Rightarrow \text{accept } H_0 \\ \sigma_0 < S_n < \sigma_1 \Rightarrow \text{continue observation} \end{cases}$$

It has been proved that the values of η_0 and $\eta_1$are decided by $\sigma_1 = \frac{1-P_{01}}{P_{10}}$ and $\sigma_0 = \frac{P_{01}}{1-P_{10}}$.

Compared to other soft decision schemes based on a fixed number of observation samples, such as Neyman-Pearson Test [16], Composite Hypothesis Test [17] and D-S Evidence Combination [18], SPRT can maximize the reduction of the detection time in the same test condition since it takes variable number of observation samples as inputs based on need.

However, SPRT assumes all SUs are honest, and thus offering opportunities for malicious SUs to take advantage of CSS and launch SSDF attack by faking data, resulting in a wrong final sensing result.

3. Design of VSPRT

Considering the binary feature of sensing data, we first describe a basic trust evaluation (BTE) mechanism with beta function in this section. Based on this, we design a dynamic trust evaluation (VTE) mechanism using volatility decay analysis to suppress dynamic SSDF attack. Finally, the implementation strategies of VSTRT are described.

3.1 Basic Trust Evaluation

As we know, an SU may play two types of sensing behaviors in CSS: honest or false. Such binary behaviors can affect the evaluation of trust. His trust value can be enhanced if the SU submitted honest sensing data in the past, or be reduced by false sensing data.

Recently, one of the most popular designs using binary input (i.e., positive or negative) to evaluate trust is based on beta function. It first counts the number of positive and negative behaviors that a user has conducted, and then calculates the trust value with beta probability density functions (PDF) denoted by $Beta(\alpha, \beta)$ [19].

$$Beta(\theta \mid \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{2}$$

where θ is the probability of sensing behaviors, $0 \le \theta \le 1$, $\alpha > 0$, $\beta > 0$.

Take example for the i-th SU (SU_i), hon_i and fal_i denote the number of honest sensing (positive) and false sensing (negative) performed by SU_i. His trust value (T_i) can be caculated with beta function as: $T_i = Beta(hon_i + 1, fal_i + 1)$.

Consider the case $\Gamma(n) = (n-1)!$ when n is an integer [20]. It can be deduced that the expectation value of the beta function is given by: $E[Beta(\alpha, \beta)] = \alpha/(\alpha+\beta)$. Thus, T_i can be further described as follows:

$$T_i = \frac{1 + hon_i}{2 + hon_i + fal_i} \tag{3}$$

In the BTE scheme, T_i is a real number ranging from 0 (complete distrust) to 1 (complete trust). The more SU_i often submits honest sensing data, the higher trust value he will get, and vice verse.

3.2 Volatility Deacy to Trust Value

In general, the basic goal of SSDF attackers is to illegally occupy or disturb the LU spectrum. Such attackers can be classified according to their attack intention [21].

- **Always-busy**: The attackers declare that the licensed user is active, although there are no LU singals. In this case the FC makes a wrong decision that LUs are present and will not use the spectrum. The intention of such attackers is to gain exclusive access to the target spectrum.
- **Always-free**: The attackers submit an absent licensed signal, although there are LUs using their spectrums. In this case the FC makes a wrong decision that the LU spectrums are free and will use them. The intention of such attackers is to give interference to LUs.

These two types of SSDF attackers are dangerous. Fortunately, they can be easily detected by current trust mechansim if malicious SUs always send false sensing data to the FC. This is because they will obtain a lower trust value when they always submit false sensing data.

To avoid the detection of trust mechanism, malicious SUs have to change their attack strategies and launch SSDF in a dynamic way (hereinafter "DSSDF"). They can exhibit dynamic behavior that allows them to maintain high trust in an alternant process of submitting honest or false sensing data.

Unlike SSDF attackers, DSSDF attackers are extremely sensitive to their trust value. Assuming SU_i is a DSSDF attacker, he launches DSSDF attack under the constraint

$$\delta \le T_i \le \delta + \omega$$

δ is the threshold of trust value. As each $T_i \in [0,1]$, δ is usually set to a moderate value, such as 0.5. For $T_i \ge \delta$, SU_i will be not identified by trust mechanism since he is marked as honest. This inspires DSSDF attackers to find an attack procedure to maintain their trust value. That is, SU_i should maintain his trust value between $[\delta, \delta+\omega]$, in which ω ($\delta \le \omega \le 1-\delta$) is the trust warning line for DSSDF attackers. Under the constraint $\delta \le T_i \le \delta+\omega$, the DSSDF attack procedure can be conducted in a round mode including "Attack" → "Self-check" → "Boost" phases, as shown in **Fig. 2**.

- **Attack:** SU_i submits false sensing data when $\delta \le T_i \le \delta+\omega$.
- **Self-check:** SU_i self-checks whether $T_i<\delta$ after each attack. Yes, continue the "Attack" phase. No, go to the "Boost" phase.
- **Boost:** Malicious SUs submit honest sensing data to boost their trust value until $T_i \ge \delta+\omega$.

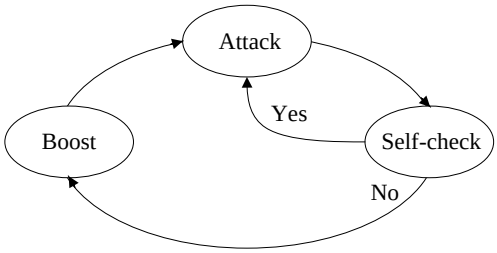

Fig. 2. A round of DSSDF attack procedure.

It can be seen that the core of DSSDF attack is the trust value. To further analyze the variation of SU_i's trust value, we perform a simple simulation scenario, as shown in **Fig. 3**.

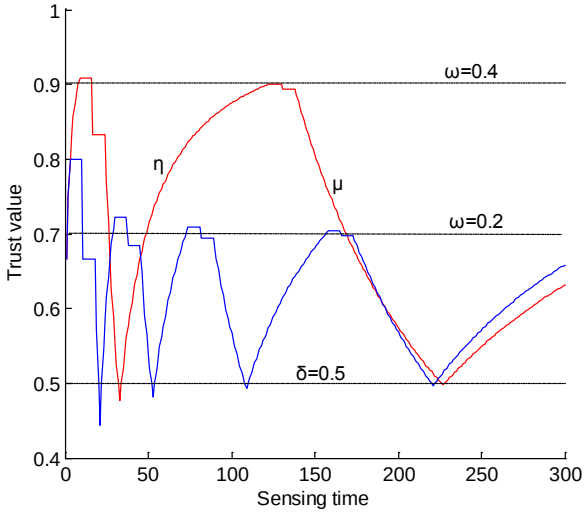

Fig. 3. Volatility variation of SU_i's trust value.

From **Fig. 3**, we can find that SU_i's trust value fluctuates from $\delta+\omega$ to δ. With a higher value in ω such as 0.4, SU_i can get more number of attacks. We can also find η denotes the numbers of boosting trust that SU_i need consume and μ denotes the number of attacks that SU_i can obtain. Both η and μ can be updated with sensing time k adaptively by the following procedure.

Procedure Updating (η, μ)
Input: T_i, k
Output: η, μ
1: At k=0, initialize $\eta=\eta_1=\eta_2=0$, $\mu=\mu_1=\mu_2=0$, *attack*=0;
2: **for** $k \ge 1$ **do**
3: **for** each SU_i **do**
4: **if** (*attack*==0) **then**

```
        It means SU_i should boost his trust;
        if (T_i ≤δ) then
            η_1=k;
        end if
        if (T_i ≤δ||δ≤T_i≤δ+ω) then
            SU_i submits honest sensing data;
            η_2=k;
        end if
        η=η_2-η_1;
        if (T_i ≥δ+ω) then
            attack=1;
        end if
      else if
        It means SU_i can launch SSDF attack;
        if (T_i ≥δ+ω) then
            μ_1=k;
        end if
        if (T_i ≥δ+ω||δ≤T_i≤δ+ω) then
            SU_i submits false sensing data;
            μ_2=k;
        end if
        μ=μ_2-μ_1;
        if (T_i ≤δ) then
            attack=0;
        end if
      end if
    end for
    k++;
end for
```

To counter DSSDF attack, the best measure is to suppress the increase of DSSDF attackers' trust value. Noting that the trust value of DSSDF attackers behave highly volatile, we can find the wavelength (λ) of their trust value is $\eta+\mu$. Obvious, η shoud be encouraged and μ should be suppressed. The larger μ value an SU makes, the more decay to trust value he will be gotten.

Here, the time is divided into m time windows (*TW*), where m is a large positive integer. The length of each time window is allocated adaptively to λ. So, the volatility decay index to trust value at *h-th TW* can be described as:

$$\varphi(h)=\frac{\sum_{k=1}^{h}\eta_k-\sum_{k=1}^{h}\mu_k}{\sum_{k=1}^{h}\eta_k+\sum_{k=1}^{h}\mu_k} \tag{4}$$

Fot SU_i his trust value at *h-th TW* can be further calculated as:

$$T_i^h = \begin{cases} \dfrac{1+hon_i}{2+hon_i+fal_i}, & h=0 \\ \varphi(h-1)T_i^{h-1}, & h>0 \end{cases} \tag{5}$$

3.3 Implementation Strategies

The effectiveness of supporting a trust mechanism depends not only on the parameters and metrics for evaluating trust, but also on the implementation of the trust mechanism in a soft decision scheme for CSS. In the VSPRT scheme, the trust value of each SU should be considered dynamically and can be used as the weight of the soft decision. Such method can improve the detection probability of SPRT in the face of DSSDF attack.

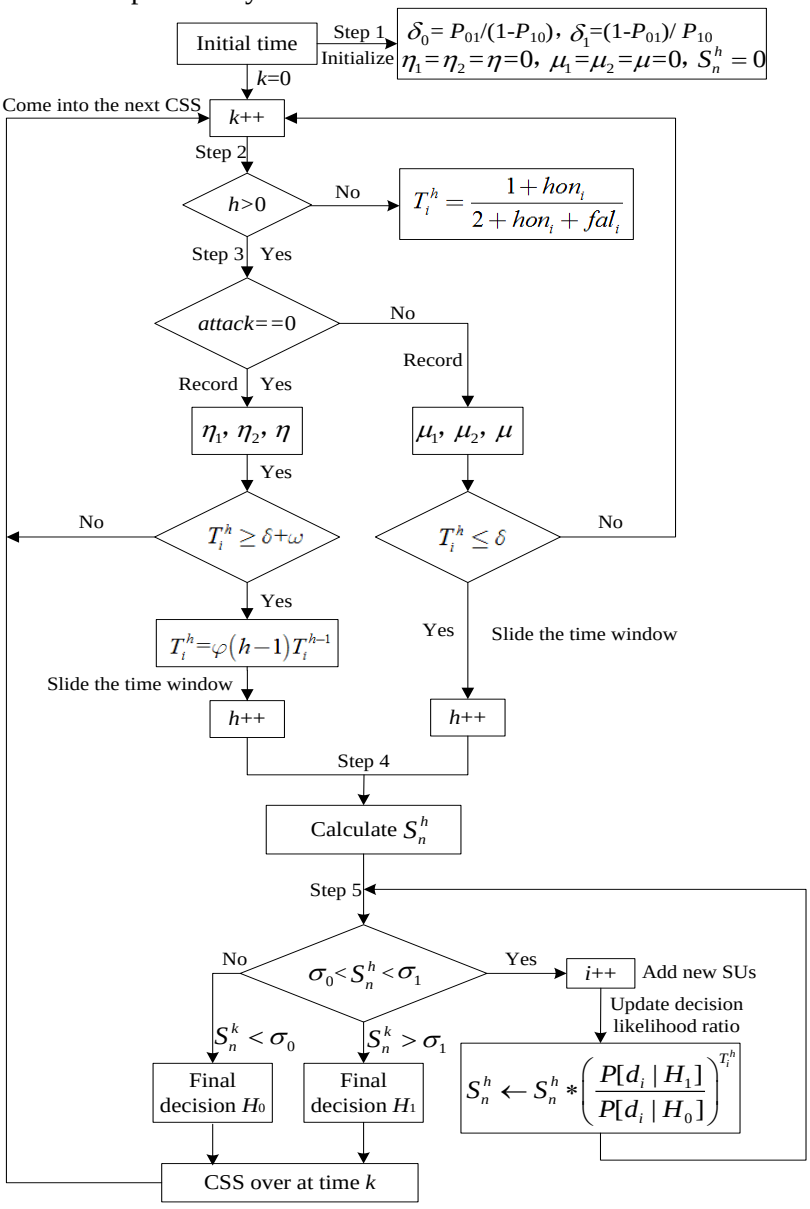

Fig. 4. Implementation strategies of VSPRT.

By incorporating the dynamic trust weight into SPRT, the decision likelihood ratio at *h-th TW* can be calculated as:

$$S_n^h = \prod_{i=0}^{n} \left(\frac{P[d_i \mid H_1]}{P[d_i \mid H_0]} \right)^{T_i^h}, n=1,2,3... \quad (6)$$

It can be seen that $T_i^h \to 1$ on condition that SU_i always submits honest sensing data. No exponential decay happens in S_n^h. When DSSDF attackers are engaged in honest or false sensing alternately, $T_i^h \to 0$, and it has no negative impact on S_n^h. Based on this, compared S_n^h with (σ_0, σ_1), the FC can make a reliable sensing result in the face of DSSDF attack. **Fig. 4** shows the implementation process of VSPRT.

Step 1. At initial time (k=0), initialize $\sigma_0=P_{01}/(1-P_{10})$, $\sigma_1=(1-P_{01})/P_{10}$, $\eta_1=\eta_2=\eta=0$, $\mu_1=\mu_2=\mu=0$, and $S_n^h=0$.
Step 2. Check $h>0$? If yes, continue Step 3. If not, initialize T_i^h at h=0.
Step 3. Perform Procedure Updating (η, μ) and calcuate T_i^h with Eq.(5).
Step 4. Based on the variable samples testing [12], extract the local sensing data of some SUs into CSS fusion, and use their trust value as the exponential weight to calculate S_n^h.
Step 5. Perform the dual-threshold decision related on (σ_0, σ_1). For $\sigma_0 < S_n^h < \sigma_1$, add new SUs to CSS fusion, and update with Eq.(6). For $S_n^h < \sigma_0$, make the final decision H_0. For $S_n^h > \sigma_1$, make the final decision H_1.

4. Simulation Analysis

We would perform four simulations to validate the VSPRT scheme and show its effectiveness.

4.1 Simulation Setup

The simulations are performed based on the energy detection, in which the licensed signal is a baseband QPSK modulated signal under the AWGN (additive white Gaussian noise) environment. The general simulation setup is shown in **Table 1**.

Table 1. Description of simulation elements

Parameters	Description	Default
N	Number of SUs	60
L	Number of LUs	5
cycle	Number of cycle simulation	300
mt	Number of Monte Carlo simulation	5000
mp	Percentage of malicious SUs	0~40%
δ	Threshold of trust value	0.5
ω	Trust warning line	0.3

In the simulation, the SUs are split into two types: malicious SUs and normal SUs. The behavior pattern for malicious SUs is to carry out honest or false sensing by launching DSSDF attack in the light of (δ, $\delta+\omega$). Considering the case of deep shadowing and multipath fading, the behavior pattern for normal SUs is modeled to submit honest sensing data at the probability of 0.8.

4.2 Simulation Results

The simulations are executed by cycle-based fashion. At each cycle, all SUs are selected to perform CSS with each other randomly. After a few cycles, a trusted network topology is gradually formed by trust mechanism. The FC then uses trust mechanism to perform CSS actions at each cycle, and update the trust value on the corresponding SUs. Firstly, we performed two simulations to validate VSPRT in terms of suppressing DSSDF attack.

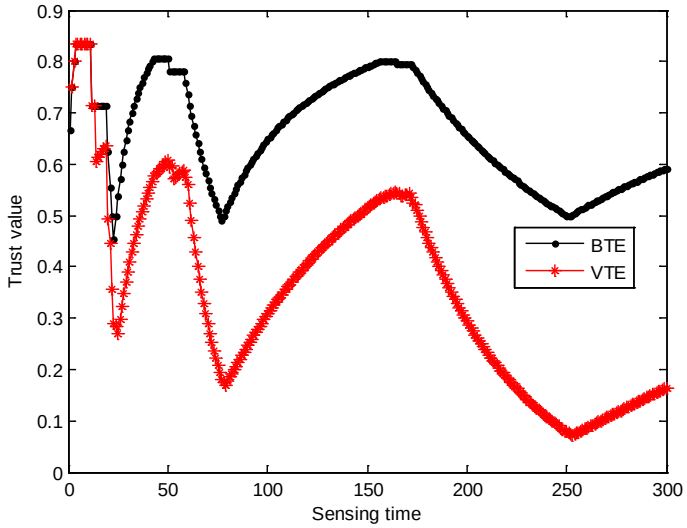

Fig. 5. Variation of a malicious SU's trust value.

Simulation 1. We choose a malicious SU randomly to observe the variation of his trust value in the BTE and VTE mechanism. As shown in **Fig. 5**, DSSDF makes the malicious SU's trust value fluctuate with the increase of sensing time. Meanwhile, his trust value generally outweighs δ in BTE. Fortunately, his trust value is rarely larger than δ in VTE. This is because the volatility decay index can suppress the boost of trust value which is promoted by launching DSSDF attack.

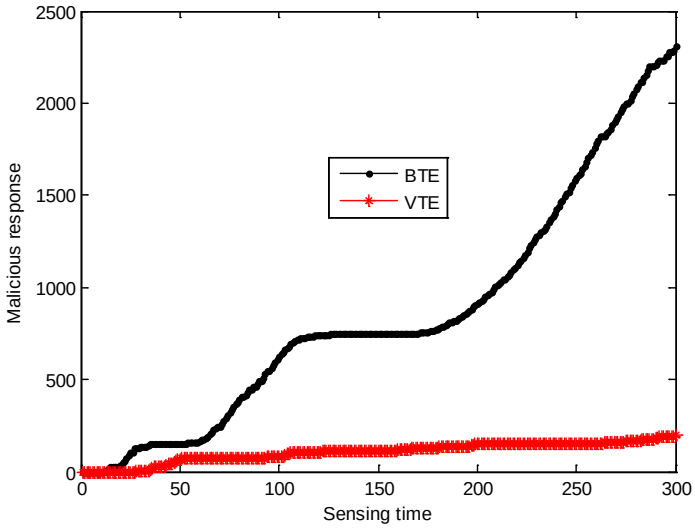

Fig. 6. Suppressing malicious responses.

Simulation 2. Malicious SUs submit false sensing data in CSS, which generates a large amount of malicious responses in each sensing time. So, the best measure to suppress malicious SUs is to reduce malicious responses. **Fig. 6** shows the effectiveness of reducing malicious responses. In BTE, malicious SUs' trust value decreases slowly, so they can have more time to submit false sensing data, resulting in more malicious responses. However, in VTE, malicious SUs' trust value declines rapidly, and lies in [δ, $\delta+\omega$] for a very short time, and thus suppressing malicious responses effectively.

From the above two simulations, we can see that the DTE scheme can suppress DSSDF attack effectively. Therefore, this mechanism is embedded into VSPRT to validate its improving the sensing performance compared with SPRT [12] and TNA [7] in the Always-busy and the Always-free attack pattern respectively. In the following simulations, we use P_{01}=1e-05 and P_{10}=1e-06 for the three types of soft decision schemes by using the Monte Carlo simulation.

Simulation 3. In the Always-busy attack pattern, the performance of soft decision schemes relies on the probability of correct sensing (The sum of the probability of sensing H_1 and H_0 correctly) for the LU spectrums. As shown in **Fig. 7**, VSPRT significantly outperforms SPRT with the percentage of malicious SUs. Although both VSPRT and TNA employ the exponential weight to eliminate the effect of malicious SUs in the same simulation environment, VSPRT is also better than TNA in the probability of correct sensing since TNA lacks the consideration of evaluating trust dynamically.

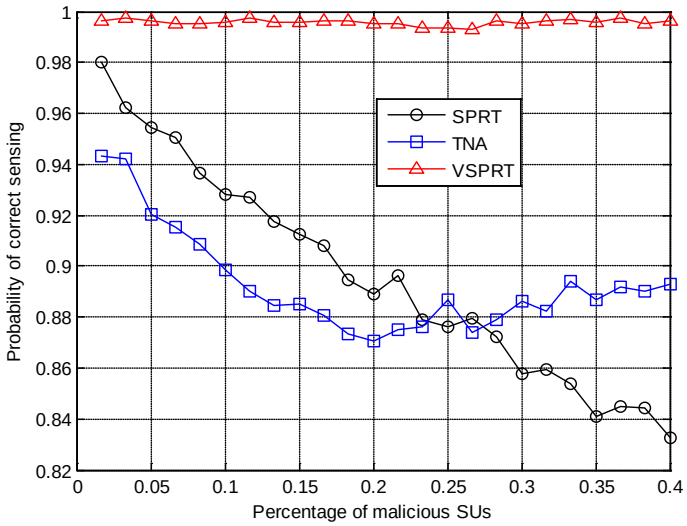

Fig. 7. Probability of correct sensing at Always-busy.

Simulation 4. In the Always-free attack pattern, a lower probability of miss detection (The miss probability of misleading H_1 as H_0) also indicates the better performance for soft decision schemes. As shown in **Fig. 8**, VSPRT can identify malicious SUs dynamically by introducing the volatility decay index, so its performance outperforms SPRT with the percentage of malicious SUs and is more stable than TNA.

5. Conclusion

In this paper, we have proposed a dynamic trust evaluation mechanism based on volatility decay analysis to defend against DSSDF attack. The the volatility decay index is introduced in the mechanism to evaluate the trust of SUs dynamically, which can mitigate the harmful effect of malicious SUs and thus improving the accuracy of the final sensing result. Meanwhile, such dynamic trust mechanism is embedded into VSPRT to enhance its performance for reliable sensing result. The implementation strategies of VSTRT are described in detail. Simulation results show that the VSPRT scheme can suppress DSSDF attackers effectively, and outperforms the conventional SPRT and TNA scheme.

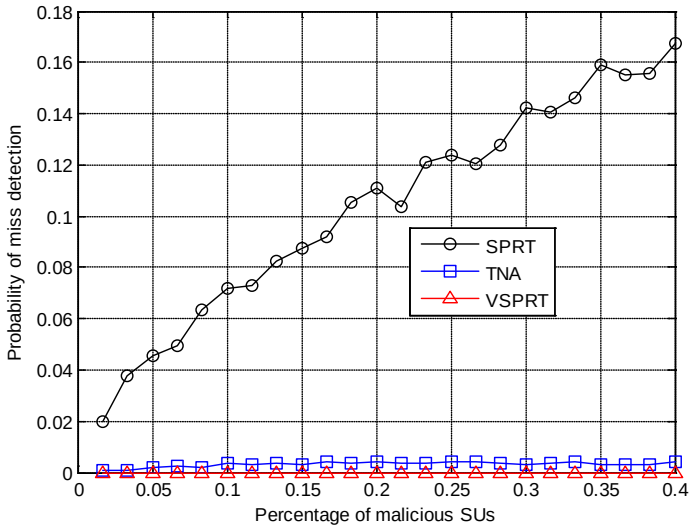

Fig. 8. Probability of miss detection at Always-free.

References

[1] Federal Communications Commission, "Spectrum Policy Task Force," *Rep. ET Docket*, no. 02-135, Nov. 2002. http://www.fcc.gov/sptf/files/SEWGFinalReport_1.pdf

[2] H. Fang, L. Xu, C. Huang, "Dynamic Opportunistic Spectrum Access of Multi-channel Multi-radio Based on Game Theory in Wireless Cognitive Network," in *Proc. of the IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, pp.127-132, December 11-13, 2013. Article (CrossRef Link)

[3] I. F. Akyildiz, B. F. Lo and R. Balakrishnan, "Cooperative Spectrum Sensing in Cognitive Radio Networks: A survey," *Physical Communication*, vol. 4, no. 1, February, pp. 40-62, 2011. Article (CrossRef Link)

[4] D. Cabric, S. Mishra and R. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios," in *Proc. of Asilomar Conference on Signals, Systems, and Computers*, pp. 772–776, November 7-10, 2004. Article (CrossRef Link)

[5] J. Minho, H.L Han, D. Kim, et al, "Selfish Attacks and Detection in Cognitive Radio Ad-hoc Networks," *IEEE Networks*, vol.27, no.3, pp.46-50, June 2013. Article (CrossRef Link)

[6] F. R Yu, M. Huang and H. Tang, "Biologically Inspired Consensus-based Spectrum Sensing in Mobile Ad hoc Networks with Cognitive Radios," *IEEE Network*, vol. 24, no. 3, pp. 26-30, June, 2010. Article (CrossRef Link)

[7] J.Y Feng, Y.Q Zhang, G.Y Lu, et al, "Securing Cooperative Spectrum Sensing against Rational SSDF Attack in Cognitive Radio Networks," *KSII Transactions on Internet and Information Systems*, vol.8, no.1, pp.1-17, January, 2014. Article (CrossRef Link)
[8] R. L Chen, J. M Park and Y. T Hou, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, April, 2008. Article (CrossRef Link)
[9] T. Qin, H. Yu and C. Leung, "Towards a Trust-aware Cognitive Radio Architecture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 86-95, April, 2009. Article (CrossRef Link)
[10] K. Zeng, P. Pawełczak and D. Cabri, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 26-228, March, 2010. Article (CrossRef Link)
[11] J.Y Feng, G.Y Lu, H Chang, "Behave well: How to Win a Pop Vacant Band via Cooperative Spectrum Sensing," *KSII Transactions on Internet and Information Systems*, vol.9, no.2, pp.1321-1336, April, 2015. Article (CrossRef Link)
[12] Q. Q Pei, B. B Yuan, L. Li and H. N Li, "A Sensing and Etiquette Reputation-based Trust Management for Centralized Cognitive Radio Networks," *Neurocomputing*, vol. 101, no. 4, pp. 129-138, July, 2013. Article (CrossRef Link)
[13] Y. U Liu, X. R Li, "Operating Characteristic and Average Sample Number Functions of Truncated Sequential Probability Ratio Test ," in *Proc. of the 5th IEEE International Conference on Information Fusion*, pp.1776-1783, July 9-12, 2012. Article (CrossRef Link)
[14] R. Chen, J. M. Park and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *Proc. of 27th IEEE INFOCOM Conference*, pp. 1876–1884, April 13-18, 2008. Article (CrossRef Link)
[15] E. Peh, Y. C Liang, Y. L Guan and Y. G Zeng, "Optimization of Cooperative Sensing in Cognitive Radio Networks: A Sensing-Throughput TradeoView," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 5294-5299, November, 2009. Article (CrossRef Link)
[16] Y. Sung, L. Tong and H. Poor, "Neyman-Pearson Detection of Gauss-markov Signals in Noise: Closed-form Error Exponent and Properties," *IEEE Transaction on Information Theory*, vol.52, no.4, pp.1354-1365, Sept., 2006. Article (CrossRef Link)
[17] S. Zarrin, T. J Lim, "Composite Hypothesis Testing for Cooperative Spectrum Sensing in Cognitive Radio," in *Proc. of the 2009 IEEE International Conference on Communications*, pp.1-5, June 14-18, 2012. Article (CrossRef Link)
[18] Q. H Peng, K. Zeng, J.Wang, et al, "A Distributed Spectrum Sensing Scheme Based on Credibility and Evidence Theory in Cognitive Radio Context," in *Proc. of the 17th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp.1-5, Sept.11-14, 2006. Article (CrossRef Link)
[19] A. Jøsang and R. Ismail, "The Beta Reputation System," in Proc. *the 15th Bled Electronic Commence Conference*, pp. 1-14, June 17-19, 2002. Article (CrossRef Link)
[20] Gamma function. http://en.wikipedia.org/wiki/Gamma_function
[21] H. Rif-Pous, M. Blasco and C. Garrigues, "Review of Robust Cooperative Spectrum Sensing Techniques for Cognitive Radio Networks," *Wireless Personal Communications*, vol. 67, no. 2, pp. 175-198, November, 2011. Article (CrossRef Link)

Feng Zhao Feng Zhao received his M.Phil in Computer Science from Xi'an University of Architecture and Technology, China, in 2005. He is currently a senior lecturer in Department of Communication Engineering, Xi'an University of Posts & Telecommunications, China. His main research interests include cooperative spectrum sensing and network security.

Jingyu Feng Jingyu Feng received his B.S. degree in electrical information science and technology from Lanzhou University of Technology, China, in 2006. He received his Ph.D. degree from Xidian University, China, in 2011. He is currently a vice professor in Department of Communication Engineering, Xi'an University of Posts & Telecommunications, China. He is also a postgraduate director of University of Chinese Academy of Sciences, China. His main research interests include wireless security, trust management and cooperative spectrum sensing.