A Scheme to Counter SSDF Attacks based on Hard Decision in Cognitive Radio Networks

JIANQI LU, PING WEI
School of Electronic Engineering
University of Electronic Science and Technology of China, Chengdu, Sichuan, China
jianqilu@hotmail.com
ZHE CHEN
Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, Liaoning, China

Abstract: - Cognitive radio is a promising technology to improve the utilization of wireless spectrum resources. A serious threat to cognitive radio networks (CRN) which sense the spectrum in a cooperative manner is the transmission of false spectrum sensing data by malicious secondary nodes, namely spectrum sensing data falsification (SSDF) attacks. SSDF attackers start to attack the network in the case of independent attacks or cooperative attacks and impair the process of data fusion, the performance is deteriorated. In this paper, we propose a scheme that can mitigate the effect of SSDF attacks and improve the robustness of cooperative spectrum sensing (CSS) based on hard decision regardless of independent attacks or cooperative attacks. Simulations verify the effectiveness of the proposed scheme.

Key-Words: - Cognitive radio, Cooperative spectrum sensing, Spectrum sensing data falsification, Hard decision, Robustness

1 Introduction

Cognitive radio (CR) enables much higher spectrum efficiency by dynamic spectrum access, and it is a potential technique for future wireless communications to mitigate the spectrum scarcity issue [1]. The basic idea of CR is to dynamically sense electromagnetic environments, reliably detect the presence of licensed primary radios and opportunistically use the underutilized band for transmissions without causing harmful interference to authorized signals. Spectrum sensing is the key enabling functionality in cognitive radio networks (CRN). Each wireless sensor called secondary user (SU) detects whether the primary user (PU) be present or not periodically.

The existing spectrum sensing techniques can be divided into three categories: energy detection [2], matched filter detection [3] and cyclostationary detection [4]. Due to the advantage of simple implementation, we use the energy detection to sense spectrum in practical situations. Cooperative spectrum sensing (CSS) can alleviate the problem of corrupted detection caused by destructive channel conditions between PU and SU. Each SU forwards its local sensing result to fusion center (FC), then FC decides whether the PU signal is present or not according to a fusion rule. Cooperative SUs would have a better chance of detecting the PU signal by combining the sensing information jointly.

Recently, the security problem in CRN has attracted the attention of many researchers. The CRN is vulnerable to threats from malicious users (MU). In this paper, we consider spectrum sensing data falsification (SSDF) attacks in CRN. To counter SSDF attacks, we propose a scheme to identify the normal users (NU) and remove the MUs from the data fusion process with the help of trusted nodes (TN) such as access point, base station, cluster head, etc. The Gaussian approximation of Binomial distribution is used to decide the threshold for the identification of NUs. After the identifying stage, the remaining SUs are considered as NUs and permitted to send their local sensing results to FC.

The remaining of this paper is organized as follows: In Section 2, system model for the spectrum sensing is presented. The definitions of two categories of SSDF attacks are illustrated in Section 3. The scheme to counter SSDF attacks is illustrated in Section 4. In Section 5, simulations are conducted to show the performance of the scheme proposed in this paper. Finally we make some conclusions in Section 6.

2 System Model

In this section, we assume that the CRN includes N SUs (N_0 MUs, N_1 TNs and others are NUs). According to energy detection, the binary hypothesis test for spectrum sensing can be written as follows:

$$E_i(k)=\begin{cases}\sum_{m=1}^{M}\left|h_i(k)x(m)+n_i(m)\right|^2 & H_1\\ \sum_{m=1}^{M}\left|n_i(m)\right|^2 & H_0\end{cases} \tag{1}$$

where the binary hypothesis H_1 and H_0 represent the PU is present and absent respectively. $E_i(k)$ represents the received energy at the receiver of the ith SU (SU$_\mathrm{i}$) at kth sensing interval. $h_i(k)$ denotes the channel gain of the ith sensing channel at kth sensing interval. M is the number of samples. The sensing channel is block fading, i.e., the channel gain h_i is considered as constant during one sensing interval, $x(m)$ is the PU signal with mean zero and variance δ_x^2, $n_i(m)$ denotes the complex addictive white Gaussian noise (AWGN) with mean zero and variance δ_i^2, where $n_i(m)$ is uncorrelated with $n_j(m)$ ($i\neq j$). Without loss of generality, $x(m)$ and $\{n_i(m)\}$ are assumed to be independent of each other.

According to the central limited theorem (CLT), if M is large enough (e.g., $M\geq 10$), $E_i(k)$ is asymptotically normally distributed as [5]:

$$E_i\left(k\right)\sim\begin{cases}N\left(\left(\gamma_i(k)+M\right)\delta_i^2,2\left(M+2\gamma_i(k)\right)\delta_i^4\right)H_1\\ N\left(M\delta_i^2,2M\delta_i^4\right) \qquad H_0\end{cases} \tag{2}$$

where $\gamma_i(k)$ is the local sensing signal-to-noise ratio (SNR):

$$\gamma_i(k)=\frac{\left|h_i(k)\right|^2\bullet\delta_x^2}{\delta_i^2} \tag{3}$$

To maximize the probability of detection P_d for a given probability of false alarm P_f based on Neyman-Pearson (NP) criterion, the log-likelihood ratio (LLR) can be given by:

$$L_i(k)=\ln\frac{f\left(E_i(k)/H_1\right)}{f\left(E_i(k)/H_0\right)} \tag{4}$$

Hence, the local sensing result is:

$$d_i(k)=\begin{cases}1\ ,\ L_i(k)\geq\lambda_i\\ 0\ ,\ L_i(k)<\lambda_i\end{cases} \tag{5}$$

where $d_i(k)$ is the local sensing result of SU$_\mathrm{i}$ (i=1,2,……,N) at kth sensing interval, and λ_i is the local detection threshold of LLR test for SU$_\mathrm{i}$. In this paper, we assume that CRN is localized in a small scale area, hence the local sensing SNR and λ_i are considered to be identical and the path loss is constant for all sensors. Each SU sends one-bit local sensing result to FC. Therefore, the global sensing result is obtained according to voting rule:

$$D(k)=\begin{cases}1\ ,\ \sum_{i=1}^{N}d_i(k)\geq K\\ 0\ ,\ \sum_{i=1}^{N}d_i(k)<K\end{cases} \tag{6}$$

3 Spectrum Sensing Data Falsification Attacks

Two threats to CRN have been defined as: primary user emulation attacks (PUEA) [6] and spectrum sensing data falsification (SSDF) attacks [7]. In PUEA, a MU forestalls vacant channels by impersonating the PU to prevent other SUs from accessing the idle frequency bands. In SSDF, some MUs introduce false sensing information in the fusion process to disrupt the CSS process. The two names, Malicious users and SSDF attackers, will be used alternatively. MUs attack CRN with a probability by modifying the local sensing results regarding the present state of the PU signal prior to their transmission to FC. The objective of SSDF attackers is to deteriorate the performance of CRN and increase spectrum efficiency or throughput for themselves.

There are two categories of SSDF attacks:

(1)Independent Attacks (IA), each MU starts attacking CRN independently only on its own observation from local energy detection.

(2)Cooperative Attacks (CA), MUs decide the global sensing result cooperatively. Voting rule has been used for cooperation among MUs. Each MU sends the same decision to FC according to P_{mal}, the probability of altering the global decision of all MUs.

4 Scheme to Counter SSDF Attacks

In this section, the spectrum sensing process is divided into two stages: identifying stage and sensing stage. At the first stage i.e., identifying stage, we propose a scheme to identify reliable SUs in

CRN. Then at the sensing stage, FC receives decision reports from all NUs identified in the identifying stage and TNs to make the global decision.

We denote the local sensing result of SU$_i$ at kth time interval as $d_i(k)$, and the sensing result of SU$_i$ at kth time interval received by FC as $D_i(k)$. The reporting channel is perfect.

The relationship between $D_i(k)$ and $d_i(k)$ is given as follows:

(1) for NUs and TNs, $D_i(k)=d_i(k)$;

(2) for MUs, $D_i(k)\neq d_i(k)$.

Each SU in CRN detects PU signal independently, meanwhile all NUs and TNs have the same local probability of detection and local probability of false alarm i.e., $P_{d,i}^{(n)} = P_{d,j}^{(n)} = P_d^{(n)}\ (i \neq j)$, $P_{f,i}^{(n)} = P_{f,j}^{(n)} = P_f^{(n)}\ (i \neq j)$ respectively.

From the viewpoint of FC, the local probability of detection and local probability of false alarm of MU can be denoted as follows:

$$\begin{aligned} P_{d,i}^{(m)} &= P_{mal,i}\left(1-P_{d,i}^{(n)}\right)+\left(1-P_{mal,i}\right)P_{d,i}^{(n)} \\ &= P_{d,i}^{(n)}+\left(1-2P_{d,i}^{(n)}\right)P_{mal,i} \\ P_{f,i}^{(m)} &= P_{mal,i}\left(1-P_{f,i}^{(n)}\right)+\left(1-P_{mal,i}\right)P_{f,i}^{(n)} \\ &= P_{f,i}^{(n)}+\left(1-2P_{f,i}^{(n)}\right)P_{mal,i} \end{aligned} \tag{7}$$

for the simplicity of analysis, we have $P_{mal,i}=P_{mal}$ for all MUs. Therefore we can get that $P_{d,i}^{(m)} = P_d^{(m)}$ and $P_{f,i}^{(m)} = P_f^{(m)}$.

The global sensing result $D(k)$ can be decided only based on the cooperation of TNs at the identifying stage. Majority rule, a special issue of voting rule, is considered as the fusion rule in this paper:

$$D(k)=\begin{cases} 1\ ,\ \sum_{j=1}^{N_1} D_j(k) \geq \left\lceil \dfrac{N_1+1}{2} \right\rceil \\ 0\ ,\ \sum_{j=1}^{N_1} D_j(k) < \left\lceil \dfrac{N_1+1}{2} \right\rceil \end{cases} \tag{8}$$

Assuming T time intervals at the identifying stage, the indicator function of SU$_i$ at kth time interval is given by:

$$I_i(k)=\begin{cases} 1\ ,\ D_i(k)=D(k) \\ 0\ ,\ D_i(k)\neq D(k) \end{cases} \tag{9}$$

When the identifying stage is finished, the total number of $D_i(k)=D(k)$ can be written as $I_i = \sum_{j=1}^{T} I_i(j)$. Once I_i is greater or equal to a predefined threshold μ, SU$_i$ is identified as a NU; otherwise, not. We can get into the sensing stage after we decide whether each SU in CRN is NU or not.

The probability for $I_i(k)$=1 at the identifying stage is obtained as:

$$\begin{aligned} P\left(I_i(k)=1\right) &= P\left(D_i(k)=1,\ D(k)=1\right) \\ &\quad + P\left(D_i(k)=0,\ D(k)=0\right) \\ &= P(H_0)\Big[P\left(D_i(k)=1/H_0\right)\bullet P\left(D(k)=1/H_0\right) \\ &\quad + P\left(D_i(k)=0/H_0\right)\bullet P\left(D(k)=0/H_0\right)\Big] \\ &\quad + P(H_1)\Big[P\left(D_i(k)=1/H_1\right)\bullet P\left(D(k)=1/H_1\right) \\ &\quad + P\left(D_i(k)=0/H_1\right)\bullet P\left(D(k)=0/H_1\right)\Big] \end{aligned} \tag{10}$$

for NUs:

$$\begin{aligned} P^{(n)} &= P\left(I_i(k)=1\right) \\ &= P(H_0)\left[P_f^{(n)}Q_f+\left(1-P_f^{(n)}\right)\left(1-Q_f\right)\right] \\ &\quad + P(H_1)\left[P_d^{(n)}Q_d+\left(1-P_d^{(n)}\right)\left(1-Q_d\right)\right] \end{aligned} \tag{11}$$

for MUs:

$$\begin{aligned} P^{(m)} &= P\left(I_i(k)=1\right) \\ &= P(H_0)\left[P_f^{(m)}Q_f+\left(1-P_f^{(m)}\right)\left(1-Q_f\right)\right] \\ &\quad + P(H_1)\left[P_d^{(m)}Q_d+\left(1-P_d^{(m)}\right)\left(1-Q_d\right)\right] \end{aligned} \tag{12}$$

where Q_d, Q_f are the global probability of detection and the global probability of false alarm only dependent on TNs, respectively:

$$Q_d = \sum_{j=\left\lceil \frac{N_1+1}{2} \right\rceil}^{N_1} \binom{N_1}{j}\left(P_d^{(n)}\right)^j\left(1-P_d^{(n)}\right)^{N_1-j} \tag{13}$$

and

$$Q_f = \sum_{j=\left\lceil \frac{N_1+1}{2} \right\rceil}^{N_1} \binom{N_1}{j}\left(P_f^{(n)}\right)^j\left(1-P_f^{(n)}\right)^{N_1-j} \tag{14}$$

$I_i(k)$ is a independent Bernoulli random variable, therefore the sum of T independent identically distributed Bernoulli random variables follows Binomial distribution i.e., for NUs, I_i~$B(T, P^{(n)})$; for MUs, I_i~$B(T, P^{(m)})$. P_1, P_0 denote the probability of FC identifying a normal user correctly and the probability of FC mistaking a malicious user as normal user, respectively. P_1, P_0 can be written as:

$$P_1 = P(I_i \geq \mu) = \sum_{k=\mu}^{T}\binom{T}{k}\left(P^{(n)}\right)^k\left(1-P^{(n)}\right)^{T-k} \tag{15}$$

And

$$P_0 = P(I_i \ge \mu) = \sum_{k=\mu}^{T} \binom{T}{k} \left(P^{(m)}\right)^k \left(1-P^{(m)}\right)^{T-k} \quad (16)$$

at the identifying stage, we formulate the following optimization problem:

$$\begin{aligned} &\min \ P_0 \\ &s.t. \quad P_1 \ge \theta \end{aligned} \quad (17)$$

where θ is predetermined to be the minimum value of P_1. For large CRN and reasonable time interval size T, we utilize the Gaussian approximation of Binomial distribution.

$$P_1 = Q\left[\frac{\mu - TP^{(n)}}{\sqrt{TP^{(n)}\left(1-P^{(n)}\right)}}\right] \quad (18)$$

and

$$P_0 = Q\left[\frac{\mu - TP^{(m)}}{\sqrt{TP^{(m)}\left(1-P^{(m)}\right)}}\right] \quad (19)$$

where $Q(\cdot)$ denotes the right tail probability of a normalized Gaussian distribution, also referred as Q-function. $Q(\cdot)$ is a monotonic decreasing function, therefore we can mimimize P_0 by setting (18) to θ and substituting (18) into (19):

$$\mu = TP^{(n)} + Q^{-1}(\theta)\sqrt{TP^{(n)}\left(1-P^{(n)}\right)} \quad (20)$$

where the value of θ can be decided according to realistic situations.

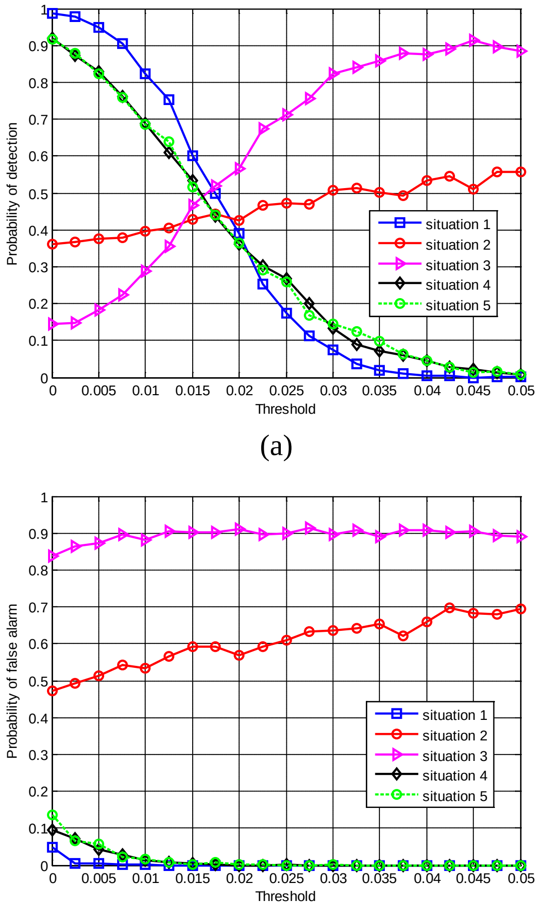
5 Simulations

In this section, we consider five CSS situations as follows:

- *situation 1*: there are no MUs and no TNs in CRN, only N normal SUs;
- *situation 2*: there are N SUs in CRN, including N_0 MUs and N_1 TNs; MUs attack CRN independently (IA);
- *situation 3*: there are N SUs in CRN, including N_0 MUs and N_1 TNs; MUs attack CRN cooperatively (CA);
- *situation 4*: the proposed scheme for situation 2;
- *situation 5*: the proposed scheme for situation 3;

We consider a CRN with 50 SUs, including 30 MUs and 5 TNs. The prior probability of H_1 is 0.2. We set the local probability of detection and local probability of false alarm to 0.7, 0.2 respectively. The number of samples M=50, local sensing SNR $\gamma_i(k)$= -5dB, $\delta_i^2 = 1$. The number of time intervals at the identifying stage T=600. The number of Monte-Carlo simulations is 10000.

Fig.1 depicts the performance of CSS i.e., probability of detection (P_d) and probability of false alarm (P_f) respectively. We can see that the performance of CSS degrades badly as long as there exist SSDF attackers. Comparing the performance for situation 2 with that for situation 3, CA from MUs has a worse impact on the performance of CSS than IA from MUs. The curves for situation 4 and situation 5 approach the curve for situation 1. Hence, it proves that the proposed scheme in this paper improves the robustness of CRN under SSDF attacks regardless of IA or CA. Due to the existence of MUs, the curves for situation 4 and situation 5 deviate from that for situation 1 to some extent.

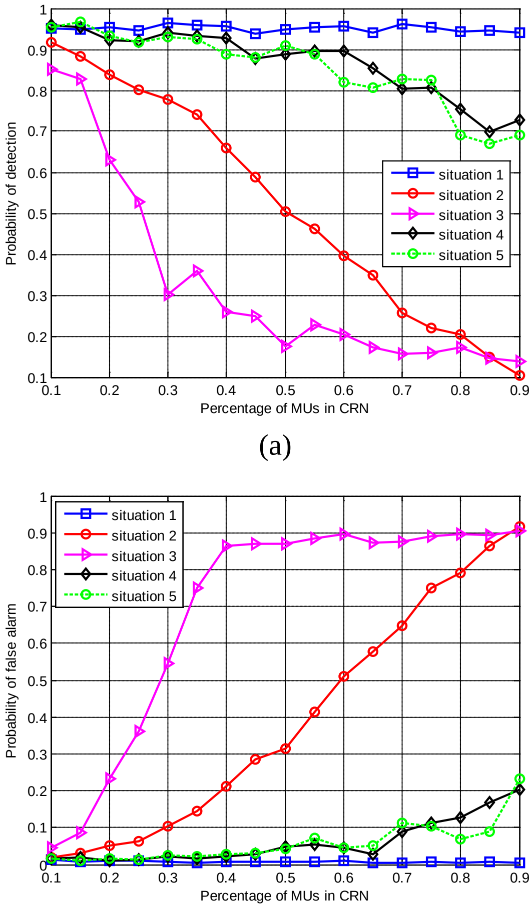


(a)

(b)

Fig. 1. Performance of cooperative spectrum sensing (P_{mal}=0.9, θ=0.9). (a) Probability of detection. (b) Probability of false alarm.

Fig.2 shows the performance of CSS with the increase of percentage of MUs in CRN. According to Neyman-Pearson criterion, the threshold λ in (6) is that makes the P_f in situation 1 be equal to 0.01. It can be seen that CA deteriorates the performance badly. Obviously, the performance for situation 4 and situation 5 outperform those for situation 2 and situation 3. That is to say, the proposed scheme in this paper improves the robustness of CRN under SSDF attacks regardless of percentage of MUs in CRN under IA and CA.

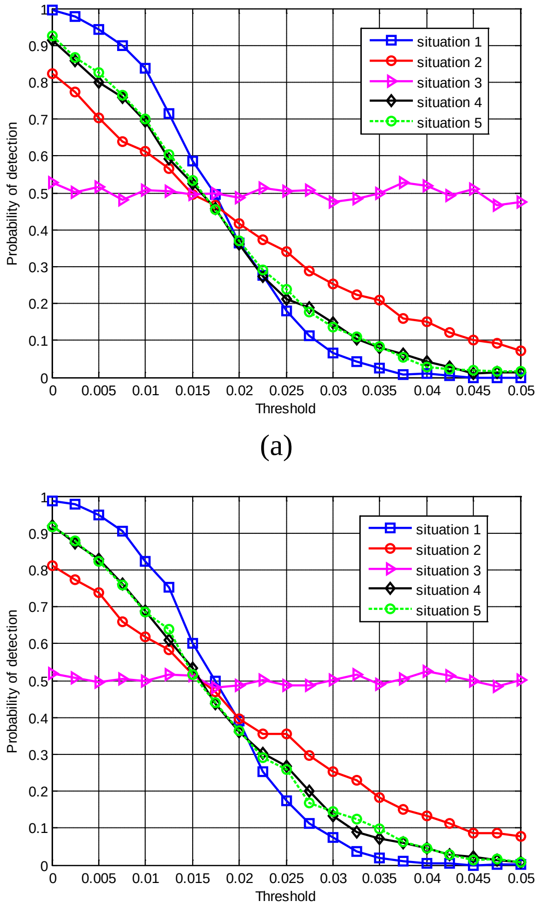


(a)

(b)

Fig. 2. Performance of cooperative spectrum sensing versus the percentage of MUs in CRN. (P_{mal}=0.9, θ=0.9). (a) Probability of detection. (b) Probability of false alarm.

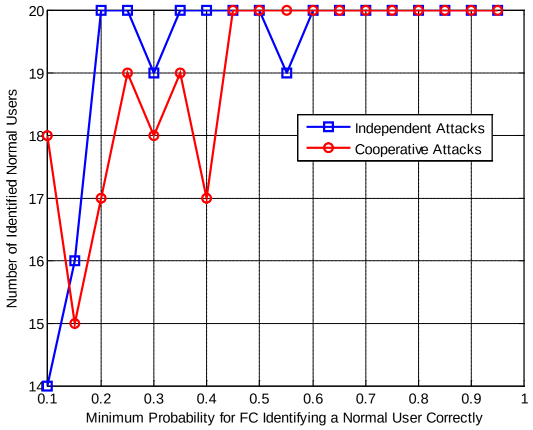
Fig.3(a) and Fig.3(b) depict the probability of detection when P_{mal}=0.5 and θ=0.5, 0.9 respectively. We can see the proposed scheme mitigates the effect of SSDF attacks. However the number of identified NUs is not equal to N-N_0 under the situation that θ is not large enough when P_{mal}=0.5 as shown in Fig.4(a) and Fig.4(c). In order to alleviate the impact of the decrement of P_{mal}, we can improve the requirement of minimum probability for FC identifying a NU correctly i.e., increasing the value of θ. When θ=0.9, the number of identified NUs under both IA and CA in Fig.4 is equal to N-N_0.



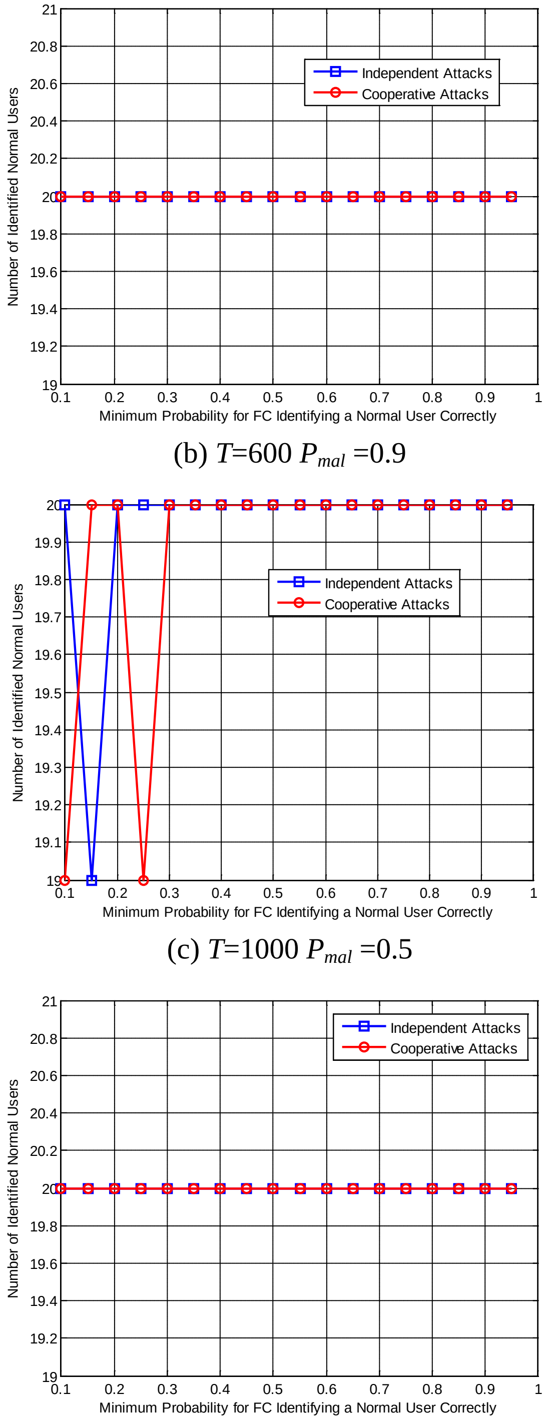
(a)

(b)

Fig. 3. Probability of detection for CSS in CRN (P_{mal}=0.5). (a) θ=0.5. (b) θ=0.9.



(a) T=600 P_{mal}=0.5



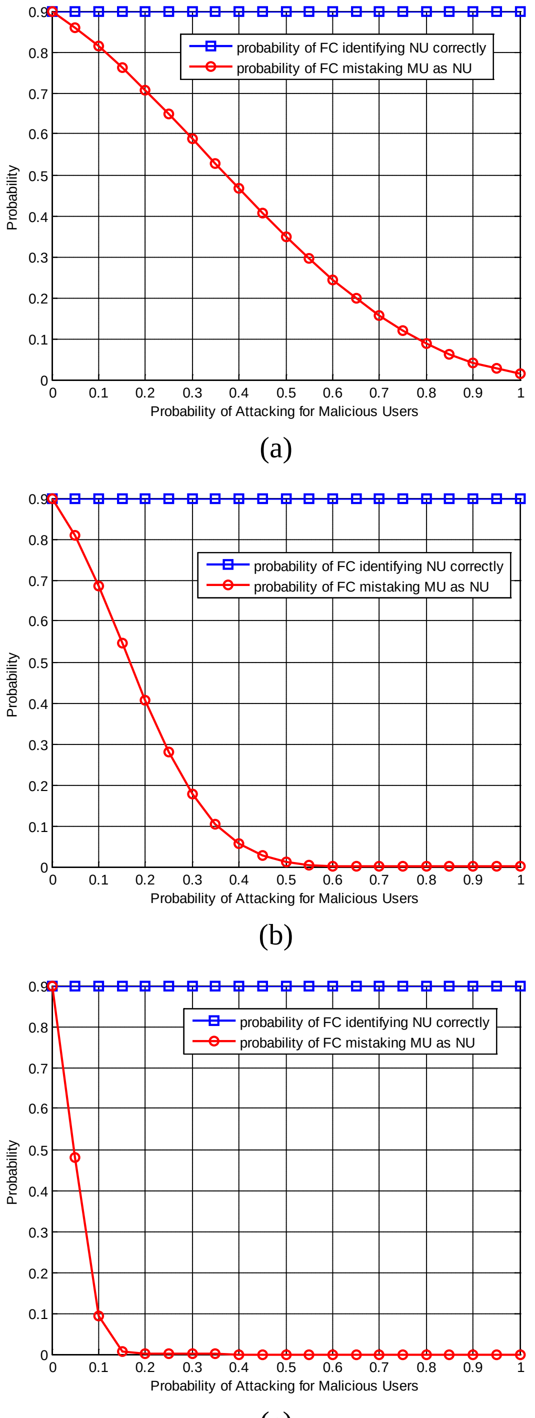
(b) T=600 P_{mal} =0.9

(c) T=1000 P_{mal} =0.5

(d) T=1000 P_{mal} =0.9

Fig. 4. Number of identified NUs versus the maximum probability for FC mistaking a MU as a NU.

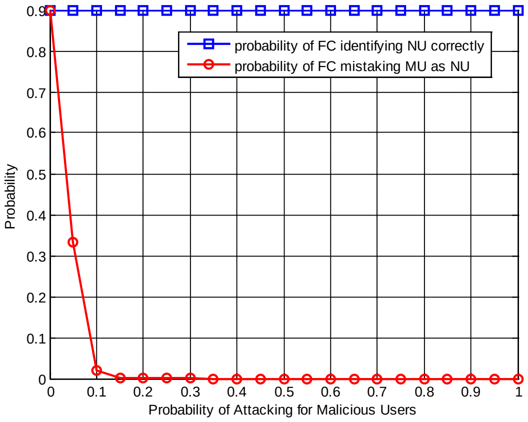
In Fig.5, we set θ to 0.9. We can see the probability of mistaking MU as NU at FC via the probability of attacking for MUs with different values of T. In Fig.5, P_0 decreases as P_{mal} increases. This is because the more greater P_{mal} is, the more easily FC identifies a MU and removes it from the data fusion process. The curve in Fig.5(c) approaches that in Fig.5(d) when T increases from 600 to 1000. However, we set T to a relatively large value T=1000 to counter SSDF when MUs attack CRN with a relatively low probability according to Fig.4(a) and Fig.4(c).



(a)

(b)

(c)



(d)

Fig. 5. Probability of identifying NUs at FC versus the probability of attacking for MUs. (a) *T*=10. (b) *T*=50. (c) *T*=600. (b) *T*=1000.

6 Conclusions

In this paper, we have proposed a scheme to counter SSDF attacks in cognitive radio networks. We have intensively analyzed the impact of parameters at the identifying stage. The proposed scheme is shown to be robust against SSDF attacks. The security issue in large scale cognitive radio networks and more effective ways of identifying normal users will be investigated in the future work.

References:

[1] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE J. Select. Areas Commun, vol.23, 2005.

[2] H. Urkowitz, Energy detection of Unknown Deterministic Signals, Proceedings of IEEE, Vol. 55, 1967, pp. 523-531.

[3] A. Sahai, N. Hoven, R. Tandra, Some Fundamental Limits in Cognitive Radio. Proc. Allerton Conf Commun, 2004

[4] P. D. Sutton, K. E. Nolan, L. E. Doyle, Cyclostationary Signatures in Practical Cognitive Radio Applications, IEEE J. Select. Areas Commun, vol.26, 2005.

[5] Zhi Quan, Shuguang Cui, Ali H. Sayed, Optimal Linear Cooperation for Spectrum Sensing in Cognitive Radio Networks, IEEE J. Select. Topics Signal Processing, vol, 2, 2008.

[6] Ruiliang Chen, Jung-Min Park, Jeffrey H. Reed, Defense against Primary User Emulation Attacks in Cognitive Radio Networks, IEEE J. Select. Areas Commun, vol.26, 2008.

[7] Ruiliang Chen, Jung-Min Park, Kaigui Bian, Robust Distributed Spectrum Sensing in Cognitive Radio Networks, IEEE INFORMCOM, 2008, pp. 31-35.