AUT Journal of Electrical Engineering

AUT J. Elec. Eng., 50(1)(2018)43-50
DOI: 10.22060/eej.2017.12528.5094

Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks: An Analytical Model for Evaluation and Mitigation of Performance Degradation

A. A. Sharifi*, M. Mofarreh-Bonab

Department of Electrical Engineering, University of Bonab, Bonab, Iran

ABSTRACT: Cognitive Radio (CR) networks enable dynamic spectrum access and can significantly improve spectral efficiency. Cooperative Spectrum Sensing (CSS) exploits the spatial diversity between CR users to increase sensing accuracy. However, in a realistic scenario, the trustworthy of CSS is vulnerable to Spectrum Sensing Data Falsification (SSDF) attack. In an SSDF attack, some malicious CR users deliberately report falsified local sensing results to a data collector or Fusion Center (FC) and, then, affect the global sensing decision. In the present study, we investigate an analytical model for a hard SSDF attack and propose a robust defense strategy against such an attack. We show that FC can apply learning and estimation methods to obtain the attack parameters and use a better defense strategy. We further assume a log-normal shadow fading wireless environment and discuss the attack parameters that can affect the strength of SSDF attack. Simulation results illustrate the effectiveness of the proposed defense method against SSDF attacks, especially when the malicious users are in the majority.

Review History:
Received: 10 February 2017
Revised: 25 August 2017
Accepted: 29 August 2017
Available Online: 5 October 2017

Keywords:
Cognitive Radio
Cooperative Spectrum Sensing
Spectrum Sensing Data Falsification Attack
Malicious User

1- Introduction

Cognitive Radio (CR) technology has been proposed to improve the spectral efficiency by authorizing unlicensed CR users to opportunistically operate in the vacant areas of the licensed frequency bands in the coexisting of the licensed Primary Users (PUs) [1]. The major task of the CR users is to determine the presence of PU signals, which is referred to as spectrum sensing [2, 3]. There are several different methods for spectrum sensing [4], such as energy detection, matched filter detection, and cyclostationary feature detection, etc. Among them, energy detection scheme is an interesting and useful method due to its simplicity and efficiency. Cooperative Spectrum Sensing (CSS) is an effective approach to prevail over the impacts of multipath fading, shadow fading, and hidden station issue [5, 6]. Unfortunately, CSS is vulnerable to Spectrum Sensing Data Falsification (SSDF) attacks [7]. In an SSDF attack, some malicious CR users deliberately send the falsified local sensing results to a base station or Fusion Center (FC) and considerably reduce the cooperative sensing performance [7, 8].

To alleviate the problem of SSDF attack, many approaches have been proposed. The authors in [9] propose a reputation-based scheme to identify the attackers by counting mismatches between their local sensing results and the FC's global decision. They also determine optimal decision strategies for SSDF attackers and the FC using the minimax game theory approach. The authors in [8] and [10] introduce Weighted Sequential Probability Ratio Test (WSPRT). Their method calculates a reputation weight for each CR user and applies in Sequential Probability Ratio Test (SPRT) to improve cooperative sensing performance. Compared with SPRT, the weight scheme improves a correct sensing probability with the cost of increasing sampling from four to six times for WSPRT. WSPRT is also developed in [11] for a centralized CR network, and a new fusion scheme based on spatial correlation method is suggested. The physical location information is combined with reputational weights to improve the collaborative sensing performance. In [12], a defense against SSDF attacks is investigated for both hard decision and soft decision combining schemes. In the hard decision, the FC calculates a credit factor for each CR sensor using a beta reputation system. The obtained factor is used to assign a dynamic weight for each user based on its sensing reports. In the soft decision combining scheme, the Modified Grubbs (MG) test is used to detect the malicious users. A novel defense scheme against the SSDF attack, called Conjugate Prior-based (CoP) is introduced in [13]. The scheme considers the received sensing reports as samples of a stochastic process and obtains the probability density of the random process. The normality or abnormality of each received sensing report is tested based on a confidence interval. The authors in [14] propose an Adaptive Reputation-based Clustering (ARC) against both independent and collaborative SSDF attack and demonstrate that their work neither requires the number of attackers nor attack strategies. In [15], we estimate the credit value of each user and determine the malicious attackers along with their strategies. An appropriate collaborative weight is innovatively assigned for each CR user to improve the cooperative sensing performance. In [16], we also propose a new method that estimates the percentage of malicious users (attack strength) and applies it in K-out-N rule to obtain the optimal value of K that minimizes the Bays risk. A comprehensive survey on the recent advances in the SSDF attack and defense for CSS in CR networks has been made in [17], [18].

In most of the literature on SSDF attacks, it is assumed that the malicious attackers are in minority and have little effect on the final spectrum sensing decision. Their proposed defense strategies are based on users' reputation. The reputation of each user is obtained by comparing its local sensing report with FC's global decision. But, in massive attacks, where

The corresponding author; Email: sharifi@bonabu.ac.ir

there are a large number of malicious users, an appropriate defense method has seldom been studied. When the malicious SSDF attackers are in the majority, the global decision is quite unreliable and the reputation-based methods have less efficiency. On the contrary, we propose a new approach that does not require any prior information about the FC's final decision. First, at the initial stage of spectrum sensing, the mean value of sensing reports is calculated and two important attack parameters are estimated. These parameters are the probabilities that the received reports of a specific user, in both occupied and unoccupied frequency bands, to be falsified. Then, the obtained attack parameters are used in Likelihood Ratio Test (LRT) method to improve the CSS performance. The proposed method considerably addressed SSDF attacks better than the conventional LRT method and maximizes the global correct sensing probability in severe attacks.

2- System Model

The considered system model is an infrastructure-based CR network consisting of one PU transmitter, located at the distance of D kilometers from the center of the network, one FC, and N cooperative CR users that are randomly deployed in a small circular area (~1 Km^2). It is assumed that among N CR users, there are N_a malicious users and the communication range of the PU transmitter covers the whole network. The network model is shown in Fig. 1.

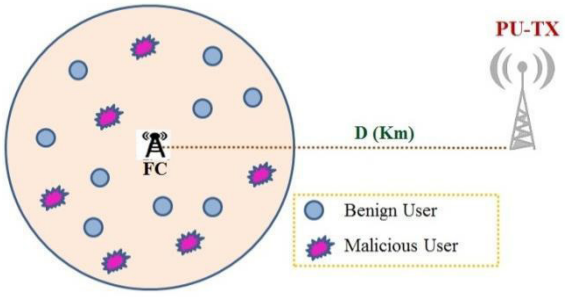

Fig. 1. Network Model

We assume that the energy detection scheme is used for the local spectrum sensing. The local spectrum sensing can be formulated as a binary hypothesis test as follows [3]:

$$X=\begin{cases} n, & H_0 \\ h.s+n, & H_1 \end{cases} \quad (1)$$

The hypothesis H_0 indicates that there is no PU signal and hypothesis H_1 states that PU signal exists. X is the CR user's received signal; s is the PU's transmitted signal; h is the gain of the sensing channel; and n is the Gaussian noise.

The probabilities of detection and false alarm for the j th CR user are p_d^j and p_{fa}^j respectively [19, 20] and can be written as:

$$p_d^j = p\left(X_j > \lambda \middle| H_1\right), \quad p_{fa}^j = p\left(X_j > \lambda \middle| H_0\right). \quad (2)$$

where X_j is the decision statistics and represents the received power of the j th CR user. The parameter λ is the local threshold determined by the Constant False Alarm Rate (CFAR). The probability of miss detection is also defined as

$$p_m^j = p\left(X_j < \lambda \middle| H_1\right) = 1 - p_d^j.$$

The local correct sensing probability of the j th CR user, p_c^j, is also as follows:

$$\begin{aligned} p_c^j &= p\left(X_j < \lambda \middle| H_0\right)\pi_0 + p\left(X_j > \lambda \middle| H_1\right)\pi_1 \\ &= (1 - p_{fa}^j)\pi_0 + p_d^j \pi_1. \end{aligned} \quad (3)$$

where π_0 and π_1 denote the actual idle and busy rate of the channel, respectively.

The transmitted reports of the CR users are binary information obtained from comparing the measured sample power X_j with a predefined threshold λ, and the reports are sent to the FC ("0" denotes an idle channel, and "1" means the presence of PU signal). The communication channels between CR users and the FC are assumed to be error-free in this study.

The received power at the CR user X_j is modeled as a log-normally distributed random variable and is obtained as follows

$$X_j = P_t(dB) - PL(d_j). \quad (4)$$

where $PL(d_j)$ is the log-normal shadowing path loss model which can be represented as

$$PL(d_j) = \overline{PL(d_j)} + X_\sigma. \quad (5)$$

where d_j is the distance from PU to j th CR user, $P_t(dB)$ is the transmitted power of the PU in dB, $\overline{PL(d_j)}$ is the mean of $PL(d_j)$ and X_σ is a zero-mean Gaussian distributed random variable with standard deviation σ_1. The parameter $\overline{PL(d_j)}$ can be found using HATA model [21] which has been proposed by IEEE 802.22 working group as the path loss model for a typical CR network environment. Assume a rural environment. The average path loss for a rural environment is given by [21]:

$$\begin{aligned} \overline{PL(d_j)} &= 27.77 + 46.05 log f_c - 4.78(log f_c)^2 - 13.82 log h_{te} \\ &\quad - (1.1 log f_c - 0.7)h_{re} + (44.9 - 6.55 log h_{te}) log d_j. \end{aligned} \quad (6)$$

where f_c is the carrier frequency, h_{te} and h_{re} are the effective transmitter and receiver antenna height, respectively.

Thus, when hypothesis H_1 holds, the received power of the j th user $X_j(dB)$ is a Gaussian distributed random variable with the mean $\mu_1 = P_t(dB) - \overline{PL(d_j)}$ and standard deviation σ_1. We assume that the CR users are deployed in a small area and the PU transmitter is relatively located far away from the CR network, therefore, the differences due to the path loss are negligible and the average received power μ_1 is the same for all CR users. The mean and variance of the noise are also the same among all CR users.

When hypothesis H_0 holds, the received power of each user is a Gaussian noise power with mean μ_0 and standard deviation σ_0. Therefore, $X_j(dB)$ is expressed as a Gaussian distributed as follows:

$$X_j(dB) \sim \begin{cases} N(\mu_0, \sigma_0^2) H_0 \\ N(\mu_1{}^j, \sigma_1^2) H_1 \end{cases}$$

The conditional Probability Density Functions (PDFs) of the received power X_j, under two hypotheses H_0 and H_1, are shown in Figure 2. The false alarm and miss detection probabilities are depicted in the figure.

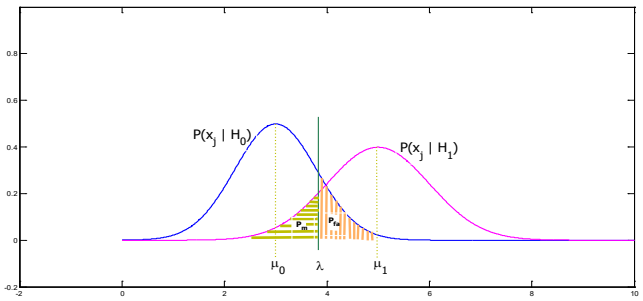

Fig. 2. Conditional PDFs of the local received power

It is assumed that the distance and transmission power of the PU are known for the FC. Hence, the mean value of the received power is known. The values of p_d^j and p_{fa}^j from equation (2) can be written as:

$$p_d^j = p(X_j > \lambda | H_1) = Q(\frac{\lambda - \mu_1}{\sigma_1}),$$

$$p_{fa}^j = p(X_j > \lambda | H_0) = Q(\frac{\lambda - \mu_0}{\sigma_0}). \quad (7)$$

where $Q(.)$ is the Q-function for standard normal distribution. There are several different methods for the hard decision combining which can be found in: Bayesian, Neyman-Pearson (N-P) detection, SPRT [22], WSPRT techniques [10], and K-out-N rule. Two Bayesian and N-P detection schemes are both LRT methods, but each of them has its own threshold selection method.

The LRT hypothesis testing can be expressed as:

$$\Lambda_N = \prod_{j=1}^{N} \frac{p(u_j | H_1)}{p(u_j | H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta \quad (8)$$

where u_j is the binary sensing report of the j th user and η is the global threshold and specified by the acceptable false alarm or miss detection probability.

When the received sample power of j th user is greater than the local threshold λ, channel status' decision is occupied and the binary sensing report, u_j, is equal to 1; otherwise, the frequency band is determined to be idle and u_j is set to be 0. Thus, the values of detection and false alarm probabilities can be written as:

$$p_d^j = p(X_j > \lambda | H_1) = p(u_j = 1 | H_1),$$

$$p_{fa}^j = p(X_j > \lambda | H_0) = p(u_j = 1 | H_0).$$

With considering the transmitted reports of the users, equation (8) can be written as:

$$\Lambda_N = \prod_{j=1}^{N} \frac{p(u_j | H_1)}{p(u_j | H_0)} = \prod_{j=1}^{N} \left[\frac{p(u_j = 1 | H_1)}{p(u_j = 1 | H_0)}\right]^{u_j} \left[\frac{p(u_j = 0 | H_1)}{p(u_j = 0 | H_0)}\right]^{1-u_j} = \prod_{j=1}^{N} \left[\frac{p_d}{p_{fa}}\right]^{u_j} \left[\frac{1-p_d}{1-p_{fa}}\right]^{1-u_j}. \quad (9)$$

3- An Analytical Model of SSDF Attack

There are three typical malicious users. The Always Yes (AY) attackers always report the presence of the PU signal. In this case, the probability of false alarm is increased and the spectrum resource is wasted. The Always No (AN) malicious users always send a local decision saying that "the channel is empty"; hence, the FC may be deceived and it allows CR users to access the channel while the PU signal is actually present. The Always False (AF) attackers send opposite values of their sensing results to the FC. Therefore, they always cause the FC to make a wrong sensing decision. Under AF attacks, both spectrum waste and PU interference are possible.

In the presence of SSDF attacks, the local spectrum sensing result of j th CR user is denoted by v_j and the CR user sends its one-bit output u_j to the FC. For benign CR user, the sensing result v_j and report u_j are the same ($v_j = u_j$). However, for the malicious attacker, the sensing result v_j can be different from report u_j, and it depends on its attack strategy.

The SSDF attack model can be defined in general as it follows. First, the malicious attacker makes its local binary decision v_j. Then, it utilizes two attack probabilities P_0 and P_1, under two hypotheses H_0 and H_1, respectively, to decide whether to perform the attack. If it decides to attack, it will change its sensing decision to report with probability P_0 or P_1 depending on the sensing result v_j. Mathematically, the SSDF attack model can be written as:

Local sensing result (v_j) sensing report (u_j)

$$(H_0) \quad 0 \quad \Rightarrow \quad \begin{cases} \xrightarrow{P_0} & u_j = 1 - v_j \\ \xrightarrow{1-P_0} & u_j = v_j \end{cases}$$

$$(H_1) \quad 1 \quad \Rightarrow \quad \begin{cases} \xrightarrow{P_1} & u_j = 1 - v_j \\ \xrightarrow{1-P_1} & u_j = v_j \end{cases}$$

Such an attack model introduces a smart SSDF attack model. Obviously, for j th "AY" attacker two attack probabilities P_0 and P_1 are 0 and 1, respectively. For "AN" attacker we have $P_0 = 0$ and $P_1 = 1$. Finally, for j th "AF" malicious attacker, these values are the same and equal to 1. Table 1 summarizes the attack probabilities of several types of users.

Table 1: The attack probabilities of several different CR users

User Type	P_0	P_1
'Benign User'	0	0
"AY" attacker	1	0
"AN" attacker	0	1
"AF" Attacker	1	1

The distribution of the local binary hypothesis for j th CR user (benign or malicious) can be formulated as:

$$p(v_j = 0) = \sum_{k=0,1} p(v_j = 0 | H_k) p(H_k) = (1 - p_{fa})\pi_0 + p_m \pi_1,$$

$$p(v_j = 1) = \sum_{k=0,1} p(v_j = 1 | H_k) p(H_k) = p_{fa}\pi_0 + (1 - p_m)\pi_1. \quad (10)$$

The probability function of sensing report u_j, can be written

as:

$$\begin{aligned} p(u_j=0) &= p(u_j=0|v_j=0)\,p(v_j=0) \\ &\quad + p(u_j=0|v_j=1)\,p(v_j=1), \\ p(u_j=1) &= p(u_j=1|v_j=0)\,p(v_j=0) \\ &\quad + p(u_j=1|v_j=1)\,p(v_j=1). \end{aligned} \tag{11}$$

Suppose that among N CR users there are N_a malicious users. Two attack parameters α and β are defined as attack probabilities for a given user j and can be written as

$$\begin{aligned} \alpha &= p(u_j=1|v_j=0) \\ &= p(u_j=1|v_j=0,s_j=\mathfrak{M})\,p(s_j=\mathfrak{M}) \\ &\quad + p(u_j=1|v_j=0,s_j=\mathfrak{B})\,p(s_j=\mathfrak{B}) \\ &= p(u_j=1|v_j=0,s_j=\mathfrak{M})\frac{N_a}{N} + 0\times p(s_j=\mathfrak{B}) \\ &= P_0\frac{N_a}{N}, \end{aligned} \tag{12}$$

and

$$\begin{aligned} \beta &= p(u_j=0|v_j=1) \\ &= p(u_j=0|v_j=1,s_j=\mathfrak{M})\,p(s_j=\mathfrak{M}) \\ &\quad + p(u_j=0|v_j=1,s_j=\mathfrak{B})\,p(s_j=\mathfrak{B}) \\ &= p(u_j=0|v_j=1,s_j=\mathfrak{M})\frac{N_a}{N} + 0\times p(s_j=\mathfrak{B}) \\ &= P_1\frac{N_a}{N}. \end{aligned} \tag{13}$$

The parameter s_j indicates the user type, which can be malicious ($\mathfrak{M}$) or benign ($\mathfrak{B}$). As mentioned before, for benign users the sensing result v_j and sensing report u_j are the same. Thus,

$$p(u_j=1|v_j=0,s_j=\mathfrak{B}) = p(u_j=0|v_j=1,s_j=\mathfrak{B}) = 0.$$

Two parameters P_0 and P_1 which are referred to as attack probabilities are defined as

$$p(u_j=1|v_j=0,s_j=\mathfrak{M}) = P_0,$$

$$p(u_j=0|v_j=1,s_j=\mathfrak{M}) = P_1.$$

Assuming that the attack strategy is the same for all malicious attackers, P_0 and P_1 are independent of index j and

$$p(s_j=\mathfrak{M}) = \frac{N_a}{N}$$

Two conditional probabilities $p(u_j=1|v_j=0)=\alpha$ and $p(u_j=0|v_j=1)=\beta$ are the probabilities that a given user j launches an attack. The CSS process, in the presence of malicious SSDF attackers, is illustrated in Fig. 3.

Finally, equation (11) is simplified and it holds that

$$\begin{aligned} p(u_j=0) &= (1-\alpha)\,p(v_j=0) + \beta\,p(v_j=1), \\ p(u_j=1) &= \alpha\,p(v_j=0) + (1-\beta)\,p(v_j=1). \end{aligned} \tag{14}$$

When there is no SSDF attack and all CR users are benign, we have $\alpha=\beta=0$. In the presence of "AY" attackers, $\beta=0$ and for CR network with "AN" attackers, $\alpha=0$. Finally, for "AF" attackers, two parameters α and β are the same.

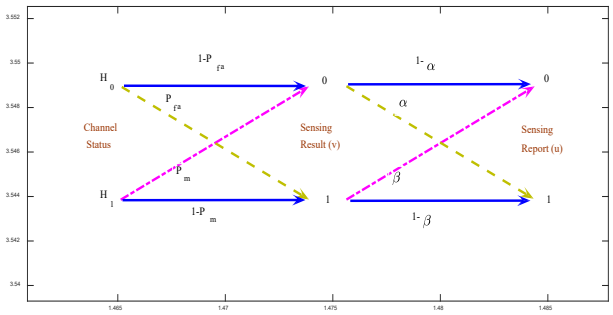

Fig. 3. The process of spectrum sensing in the presence of SSDF attacks

4- Mitigation of SSDF Attack

The proposed scheme consists of two stages: at the first, the attack parameters are estimated and at the second stage, the estimated parameters are applied in the LRT method to alleviate the destructive effect of SSDF attacks. Here, with assuming the attack strategy and without any prior information about the attack population and FC's final decision, two attack parameters α and β are estimated. The estimation of these parameters is based on the received sensing reports from the CR users. The average of the received reports m and its mathematical expectation are obtained as follows,

$$m = \frac{1}{N}\sum_{j=1}^{N} u_j \quad ; \quad \mathrm{E}(m) = \frac{1}{N}\sum_{j=1}^{N}\mathrm{E}(u_j), \tag{15}$$

where

$$\mathrm{E}(u_j) = \sum_{u_j=0}^{1} u_j\,p(u_j) = p(u_j=1), \tag{16}$$

and

$$\begin{aligned} p(u_j=1) &= p(u_j=1|v_j=0)\,p(v_j=0), \\ &\quad + p(u_j=1|v_j=1)\,p(v_j=1). \end{aligned} \tag{17}$$

With regard to equations (12) and (13), equation (17) can be simplified and we have

$$p(u_j=1) = \alpha\,p(v_j=0) + (1-\beta)\,p(v_j=1). \tag{18}$$

Hence, by inserting (10) in (18) and considering equation (15),

$$\begin{aligned} \mathrm{E}(m) = p(u_j=1) &= \alpha\left[(1-p_{fa})\pi_0 + p_m\pi_1\right] \\ &\quad + (1-\beta)\left[p_{fa}\pi_0 + (1-p_m)\pi_1\right]. \end{aligned} \tag{19}$$

Consider equations (12) and (13). Then, we have

$$\beta = \rho\alpha \quad ; \quad (\rho = \frac{P_1}{P_0}).$$

From equation (19), the values of α and β are obtained as follows:

$$\begin{aligned} \hat{\alpha} &= \frac{\mathrm{E}(m)-\psi}{1-(1+\rho)\psi} \quad ; \quad 1 \neq (1+\rho)\psi \\ \hat{\beta} &= \rho\,\hat{\alpha} \end{aligned} \tag{20}$$

where the parameter ψ is defined as follows:

$$\psi = p_{fa}\pi_0 + (1-p_m)\pi_1$$

Two obtained attack parameters α and β are applied in the LRT hypothesis testing. The conditional probability functions of sensing reports, under two hypotheses H_1 and H_0 are expressed as follows

$$\begin{aligned} p(u_j=1|H_1) &= p(u_j=1|H_1, v_j=0)p(v_j=0|H_1) \\ &\quad + p(u_j=1|H_1, v_j=1)p(v_j=1|H_1). \end{aligned} \tag{21}$$

The type of the j th user is independent of the channel statuses H_0 and H_1, thus, the above equation can be expressed as

$$p(u_j=1|H_1) = \alpha(1-p_d) + (1-\beta)p_d. \tag{22}$$

Accordingly,

$$\begin{aligned} p(u_j=1|H_0) &= p(u_j=1|H_0, v_j=0)p(v_j=0|H_0) \\ &\quad + p(u_j=1|H_0, v_j=1)p(v_j=1|H_0) \\ &= \alpha(1-p_{fa}) + (1-\beta)p_{fa}, \end{aligned} \tag{23}$$

and

$$\begin{aligned} p(u_j=0|H_1) &= (1-\alpha)(1-p_d) + \beta p_d, \\ p(u_j=0|H_0) &= (1-\alpha)(1-p_{fa}) + \beta p_{fa}. \end{aligned} \tag{24}$$

Consider equations (22), (23), and (24). Then, the decision statistics of the LRT method, expressed in (9) can be generalized by the following formula,

$$\begin{aligned} \Lambda_N &= \prod_{j=1}^{N} \left[\frac{p(u_j=1|H_1)}{p(u_j=1|H_0)}\right]^{u_j} \left[\frac{p(u_j=0|H_1)}{p(u_j=0|H_0)}\right]^{1-u_j} \\ &= \prod_{j=1}^{N} \left[\frac{\alpha(1-p_d)+(1-\beta)p_d}{\alpha(1-p_{fa})+(1-\beta)p_{fa}}\right]^{u_j} \left[\frac{(1-\alpha)(1-p_d)+\beta p_d}{(1-\alpha)(1-p_{fa})+\beta p_{fa}}\right]^{1-u_j}. \end{aligned} \tag{25}$$

It should be noted that the above equation for $\alpha = \beta = 0$ (no attack scenario) is the same as equation (9).

5- Numerical Results and Discussions

In this section, the performance of the proposed method is evaluated. Results are obtained through Monte-Carlo simulations over 10^4 runs. The PU transmitter with a duty cycle of $P(H_1) = \pi_1 = 0.2$ is located at the distance of $D = 10$ kilometers from the center of the network. The transmitted power of the PU is assumed to be 10 watts. The average noise power μ_0 is assumed to be -106 dBm. The standard deviations of the log-normal shadowing path loss model (σ_1) and noise (σ_0) are considered as 12 and 10, respectively. Each receiver has a typical sensitivity of -94 dBm, which is the minimum power for a signal to be detected [9]. It is also assumed that the transmitter frequency is at UHF band with the value of 617 MHz. The effective heights of the transmitter and receiver antennas are 100m and 1m, respectively. The global threshold η for the LRT method is set as π_0/π_1. We also fix the total number of CR users, say $N = 30$, while varying the number of malicious, say N_a, from 0 to 30. Thus, the corresponding attack's percentage (N_a/N) changes from 0 to 100%.

The convergence of the two attack parameters is shown in Fig. 4. The estimated values for α and β are converged to the constant values after applying almost 100 rounds of spectrum sensing. In the simulation, the initial stage can be set as the first 100 sensing intervals where two attack parameters, namely α and β are estimated and then used in the proposed fusion scheme to improve the cooperative sensing performance.

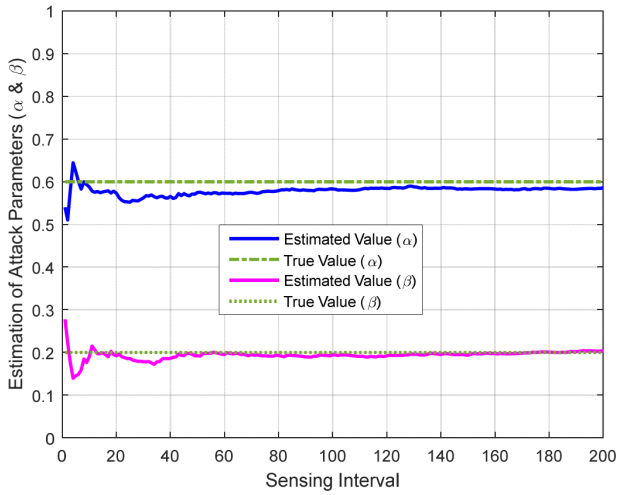

Fig. 4. The convergence of attack parameters (α =0.6, β =0.2)

Fig. 5 shows the global correct sensing probability of the FC with a conventional LRT method versus the percentage of malicious users for several types of attackers, including AY, AN, AF and smart attackers. By increasing the percentage of malicious users, the correct sensing ratio is reduced. As shown in the figure, among these attackers, the correct sensing probability of AY and AN attackers decreased to 0.2 and 0.8 (corresponding to π_0 and π_1), respectively. The AF attackers also experience the greatest magnitude decrease, showing that AF attackers have the most harmful effect on CSS performance.

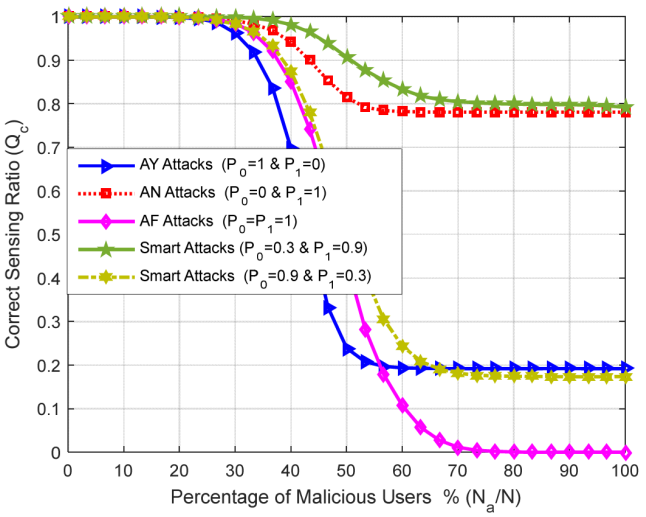

Fig. 5. Correct sensing probability for several types of attackers

Fig. 6 displays the correct sensing probability for the conventional LRT and the proposed methods for AY and AN attackers. As shown in the figure, the proposed method considerably improves the cooperative sensing performance and in the presence of %90 malicious users the obtained gain is almost 0.9.

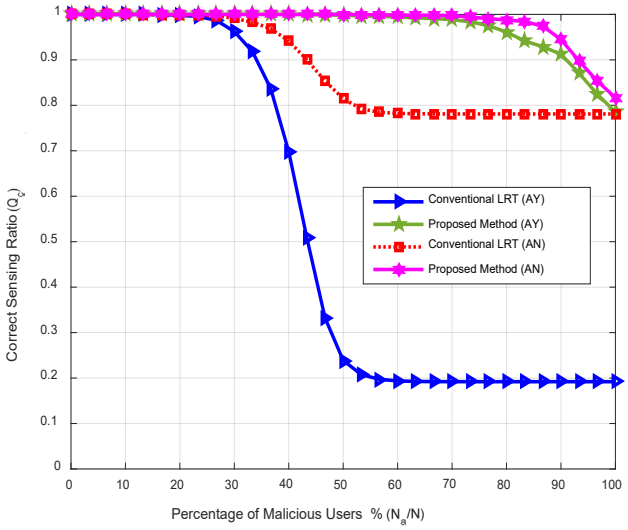

Fig. 6. Correct sensing probability (AY and AN attackers)

Fig. 7 shows the correct sensing probability of the conventional LRT and the proposed method for AF attackers ($P_0 = P_1 = 1$ & $\alpha = \beta = N_a / N$). In the proposed method, the obtained correct sensing probability is descending for $\alpha < 0.5$ and ascending for $\alpha > 0.5$. As equation (25) indicates, changing u_j to $1-u_j$ and α to $1-\alpha$ (β to $1-\beta$) yields no change in the parameter Λ_N. Then the correct sensing probability Q_c for $\alpha > 0.5$ is equal to Q_c for $1-\alpha$. In other words, Q_c is symmetrical around $\alpha = \beta = 0.5$. In the presence of %100 malicious attackers ($\alpha = \beta = 1$), the correct sensing probability is 1.

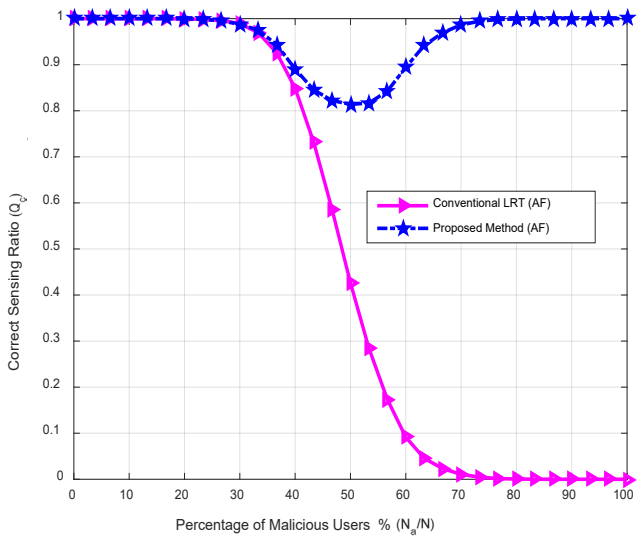

Fig. 7. Correct sensing probability for AF attackers

Fig. 8 depicts the correct sensing probability versus attack parameter α for two values of parameter β (0.3, 0.9) for the conventional LRT and the proposed methods. As shown in the figure, in the conventional LRT method, by increasing both parameters α and β, the correct sensing ratio is remarkably reduced while in the proposed method, increasing α and βcauses a small change in the rate of correct sensing probability. Fig. 9 also depicts the similar results for the correct sensing probability versus attack parameter β for two values of parameter α (0.3, 0.9). As mentioned in the manuscript, the parameter α is defined as the probability of attack for a specific user when its local sensing result is zero ($\alpha = P(u_j = 1 | v_j = 0)$). When $\alpha = 0.9$, 90% of users send falsified spectrum sensing results when their actual sensing decisions are zero and with regard to $p(H_0) = 0.8$ (80% of the channel is vacant) the correct sensing ratio Q_c converges to $p(H_1) = 0.2$ (especially for $\beta < 0.5$).

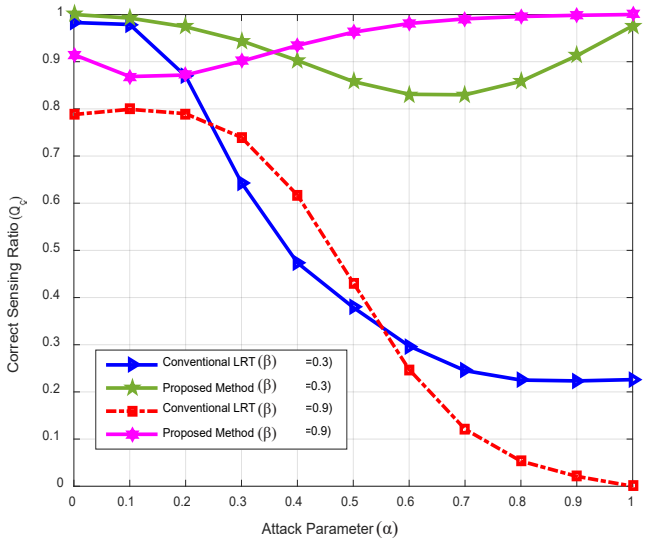

Fig. 8. Correct sensing probability versus attack parameter α

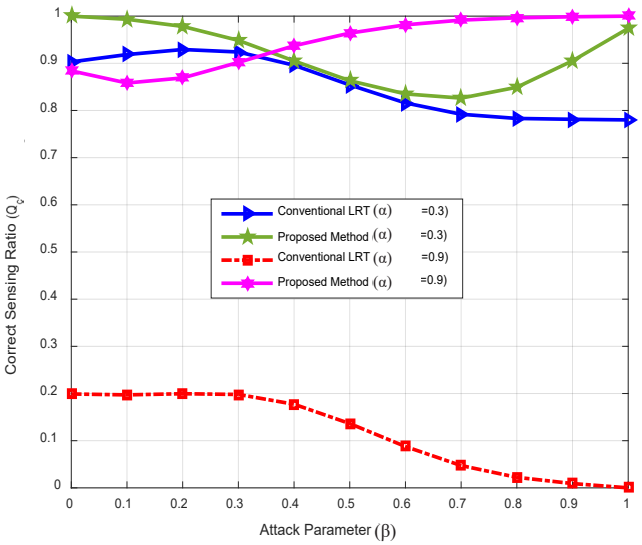

Fig. 9. Correct sensing probability versus attack parameter β

6- Conclusion

In this study, Cooperative Spectrum Sensing (CSS) in the presence of malicious Cognitive Radio (CR) users was investigated and simulated in a centralized CR networks for several types of attackers. An analytical model of Spectrum Sensing Data Falsification (SSDF) attack's behaviors was also developed. With assuming the strategy of malicious users, two attack parameters were estimated. The estimated

values were obtained based on received sensing reports without requiring any prior information of the FC's final decision. The obtained attack parameters were applied in Likelihood Ratio Test (LRT) to mitigate the impact of SSDF attacks. Finally, it was concluded that the proposed approach is a robust defense method against SSDF attacks, especially for CR networks located in the hostile environment.

References

[1] J. Mitola, GQ. Maguire, Cognitive radio: making software radios more personal, IEEE Personal Communication, 6(4) (1999) 13-18.

[2] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE Journal on Selected Areas in Communications, 23(2) (2005) 201-220.

[3] IF. Akyildiz, WY. Lee, MC. Vuran, S. Mohanty, NeXt generation/dynamic spectrum access cognitive radio wireless networks: A survey, Computer Networks, 50(13) (2006) 2127-2159.

[4] T. Yucek, H. Arsalan, A survey of spectrum sensing algorithms for cognitive radio applications, IEEE Communications Surveys & Tutorials, 11(1) (2009) 116-130.

[5] SM. Mishra, A. Sahai, RW. Brodersen, Cooperative sensing among cognitive radios, In Proceedings of the IEEE International Conference on Communications, (2006) 1658-1663.

[6] IF. Akyildiz, Lo BF, R. Balakrishnan, Cooperative spectrum sensing in cognitive radio networks: A survey, Physical Communication, 40(1) (2011) 40-62.

[7] R. Chen, J. m. Park, Y. T. Hou, J. H. Reed, Toward secure distributed spectrum sensing in cognitive radio networks, IEEE Communications Magazine, 46(4) (2008) 50-55.

[8] R. Chen, J. Park, K. Bian, Robust distributed spectrum sensing in cognitive radio networks, In Proceedings of IEEE International Conference on Computer Communications (INFOCOM), (2008) 31-35.

[9] AS. Rawat, P. Anand, H. Chen, PK. Varshney, Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks, IEEE Transactions on Signal Processing, 59(2) (2011) 774-786.

[10] R. Chen, J. Park, K. Bian, Robustness against Byzantine failures in distributed spectrum sensing, Computer Communication, 35(17) (2012) 2115-2124.

[11] CY. Chen, YH. Chou, HC. Chao, Lo. CH, Secure centralized spectrum sensing for cognitive radio networks, Wireless Networks, 18(6) (2012) 667-677.

[12] K. Arshad, K. Moessner, Robust collaborative spectrum sensing in the presence of deleterious users, IET Communications, 7(1) (2013) 49-56.

[13] V. Chen, M. Song, C. Xin, CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks, Wireless Networks, 20(8) (2014) 2521-2528.

[14] C. S. Hyder, B. Grebur, L. Xiao, M. Ellison, ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks, IEEE Transactions on Mobile Computing, 13(8) (2014) 1707-1719.

[15] A. A. Sharifi, M. Sharifi, J. Musevi Niya, Reputation-based likelihood ratio test with anchor nodes assistance, 8th International Symposium on Telecommunications, (2016) 51-56.

[16] A. A. Sharifi, M. J. Musevi Niya, Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach, IEEE Communications Letters, 20(1) (2016) 93-96.

[17] A. G. Fragkiadakis, E. Z. Tragos, I. G. Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks, IEEE Communications Surveys & Tutorials, 15(1) (2013) 428-445.

[18] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, J. Wang, Byzantine attack and defense in cognitive radio networks: A survey, IEEE Communications Surveys & Tutorials, 17(3) (2015) 1342-1363.

[19] H. Urkowitz, Energy detection of unknown deterministic signals, Proceedings of the IEEE, 55(4) (1967) 523-531.

[20] F. F. Digham, M. S. Alouini, M. K. Simon, On the energy detection of unknown signals over fading channels, IEEE Transactions on Communications, 55(1) (2007) 21-24.

[21] T. S. Rappaport, Wireless communications: Principles and Practice, Prentice Hall, (1996).

[22] PK. Varshney, Distributed detection and data fusion, Springer-Verlag, (1997).

Please cite this article using:

A. A. Sharifi and M. Mofarreh-Bonab, Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks: An Analytical Model for Evaluation and Mitigation of Performance Degradation, AUT J. Elec. Eng., 50(1)(2018) 43-50.

DOI: 10.22060/eej.2017.12528.5094