An Effective and Optimal Fusion Rule in the Presence of Probabilistic Spectrum Sensing Data Falsification Attack

Abbas Ali Sharifi
Department of Electrical Engineering, University of Bonab, Bonab, Iran
sharifi@bonabu.ac.ir

***Abstract*- Cognitive radio (CR) network is an excellent solution to the spectrum scarcity problem. Cooperative spectrum sensing (CSS) has been widely used to precisely detect primary user (PU) signals. The trustworthiness of the CSS is vulnerable to spectrum sensing data falsification (SSDF) attack. In an SSDF attack, some malicious users intentionally report wrong sensing results to cheat the fusion center (FC) and disturb the FC's global decision on the PU activity. In this paper, we introduce an effective data fusion rule called attack-aware optimal voting rule (AOVR) to confront the SSDF attack in the CSS procedure. In the beginning stages of the cooperative sensing, two important SSDF attack parameters are estimated and then applied in a conventional voting rule to acquire an optimal number of CR users to minimize the global error probability. Two estimated attack parameters include the probabilities of attack in both occupied and empty frequency bands. Simulation results confirm that the proposed attack-aware approach achieves very good performance over the existing conventional cooperative sensing methods.**

***Index Terms*-** Attack-aware; optimal voting rule; spectrum sensing data falsification attack; cognitive radio.

I. INTRODUCTION

Cognitive radio (CR) technology has been raised as a new technology to allow unlicensed secondary user to attainment the licensed frequency bands [1], [2]. In a CR paradigm, unlicensed secondary users recognize the vacant frequency bands and opportunistically utilize them in a dynamic way while not causing interference to licensed primary users (PUs) [3]. Hence, spectrum sensing plays an important rule for unlicensed users to access the frequency bands assigned to the licensed users in a CR network. Among the available spectrum sensing methods, energy detection (ED) is the simplest method because of not requiring prior knowledge of the received signal. In an ED scheme, each CR user locally senses the spectrum and determines the presence or absence of the PU signal [4].

Manuscript received 17-August-2018 and revised 20-Feb.-2019,
Accepted on 23-April-2019

P- ISSN: 2322-4088
E- ISSN: 2322-3936

The local spectrum sensing result by a single CR user is untrustworthy as the CR users usually encounter with multipath fading, shadow fading, and hidden station problems [3], [5]. Therefore, cooperative spectrum sensing (CSS) has been proposed to employ spatial diversity and fulfill the high accuracy of PU signal detection [6]. In the CSS process, each CR user submits either one binary digit about its sensing decision or the measured energy to the FC. When the FC fuses the binary sensing decisions, it is called a hard-decision approach and if it combines the received energies, then it is called soft-decision combining approach [7].

Unfortunately, the accuracy of the CSS process can be reduced affected by the spectrum sensing data falsification (SSDF) attacks [8]. In such an attack, some malicious CR users intentionally report wrong sensing decision to the FC in order to disrupt the global decision on the PU activity and deteriorate reduce the spectrum usage and notably reduce the CSS performance. To overcome this security attack, several studies have been conducted in the previous literature [9-17]. In the work reported by authors in [9], weighted sequential probability ratio test (WSPRT) was proposed that obtain an adaptive cooperative weight for each CR user and uses the sequential probability ratio test (SPRT). The WSPRT was also investigated in [10] where reputational weights were merged by location information to acquire a new dynamic weight for each CR user. An effective approach to separate abnormal local sensing reports from all of the incoming reports was presented in [11]. The received sensing reports were considered as samples of a random variable and the probability density function (pdf) of the random variables was obtained by a conjugate prior (CoP) technique. After calculation of the pdf, each received sensing report was checked for the normality based on confidence interval. If any received sensing result was detected as abnormal, then it was not allowed to cooperate in decision making on the PU activity. The normality test was also employed in [12] by performing a non-normal filtering and Shapiro-Wilk's test. The authors in [12] claimed that their proposed method neither require the malicious users' locations nor the pdf of malicious users' reported data. In [13], we proposed a new fusion scheme that estimates the percentage of attackers and then applies it in K-out-of-N fusion rule to obtain an optimal value of K that minimizes the Bays risk. In [14], we considered a credit factor for each CR user based on its sensing history. The malicious attackers and their strategies were simultaneously determined. Finally, a proper dynamic collaborative weight was allocated for each CR user to improve the cooperative sensing performance. We also proposed a new weighted defense approach against the massive SSDF attack [15]. Some anchor nodes were deployed and the cooperation weight of each CR is calculated based on the fitness of its local sensing report with anchor nodes' global decision. The comprehensive research on the SSDF attack and defense strategies is also reviewed in [16] and [17].

In this study, we have proposed a novel hard-decision combining scheme called attack-aware optimal voting rule (AOVR). More precisely, we developed our contribution that has presented in [13] and generalized to the several various types of malicious attackers. Furthermore, an analytical

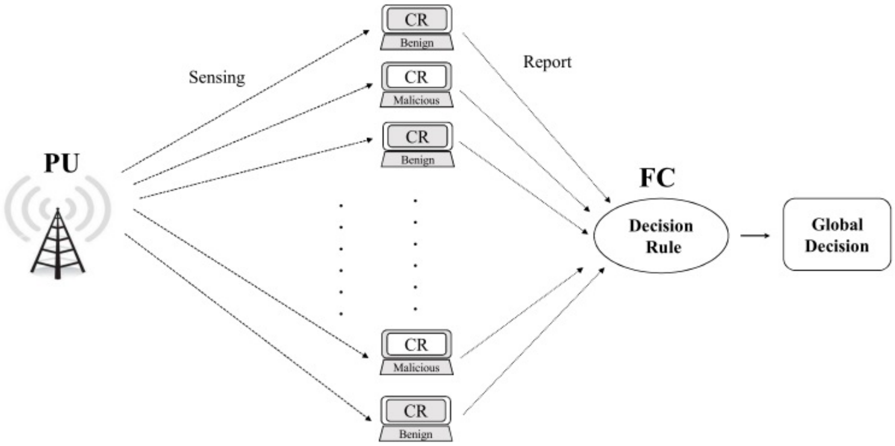

Fig. 1. Network Model

model of the SSDF attacks' behavior is investigated by the mathematical expressions. In the proposed AOVR method, two important SSDF attack parameters are estimated and then innovatively applied in a conventional voting rule to improve the CSS performance. The estimated parameters include probabilities that the received report of a specific user (can be either benign or malicious), in both occupied and unoccupied frequency bands, to be falsified from "0" to "1" and "1" to "0". We compare the performance of the suggested AOVR approach with conventional OVR under a different number of attackers. The proposed approach overcomes the SSDF attacks considerably better than the conventional method.

II. SYSTEM MODEL

The considered system model has one PU transmitter, one FC, and N cooperative CR users. It is assumed that among N CR users, there are N_a malicious users. The proposed system model is shown in Fig. 1.

In order to access available spectrum, energy detection scheme is used for local spectrum sensing. The local spectrum sensing problem can be expressed as a binary hypothesis test in the energy detection as follows [3]:

$$x(t) = \begin{cases} n(t); & H_0 \\ h(t)S(t) + n(t); & H_1 \end{cases} \tag{1}$$

The hypothesis H_0 states that there is no PU signal and hypothesis H_1 indicates that PU signal is present. $x(t)$ is the received signal of the CR users, $S(t)$ is the PU's transmitted signal, $h(t)$ is the sensing channel gain, and $n(t)$ is the additive Gaussian noise.

The false alarm and miss detection probabilities for the *j*'th CR user are P_{fa}^{j} and P_{m}^{j} respectively [4], [18].

$$P_{fa}^{j} = P\left(x_j > T \middle| H_0\right), \quad P_{m}^{j} = P\left(x_j < T \middle| H_1\right) \tag{2}$$

where x_{j} is the decision statistics and indicates the received power of the *j*'th sensor, *T* is the local threshold and predefined by the constant false alarm rate (CFAR). The local error probability P_{e}^{j} of the *j*'th user can be written as:

$$P_{e}^{j} = P\left(x_j > T \middle| H_0\right) p(H_0) + P\left(x_j < T \middle| H_1\right) p(H_1) = P_{fa}^{j} p(H_0) + P_{m}^{j} p(H_1) \tag{3}$$

where $p(H_0)$ and $p(H_1)$ respectively denote the actual idle and busy rate of the channel.

The binary sensing results of the CR users, obtained from comparing the measured sample power x_{j} with a predefined threshold *T*, are sent to the FC ("0" denotes the vacant frequency band and "1" means the presence of PU signal). We assumed that the communication channels between CR users and the FC are error-free. The received power at the CR user x_{j} can be formulated as a log-normally distributed random variable and can be written as follows:

$$x_j = P_t(dB) - PL(d_j) \tag{4}$$

where $PL(d_{\mathrm{j}})$ is the log-normal shadowing path loss model and can be represented as:

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

where d_{j} is the *j*'th user distance to PU transmitter, P_{t}(dB) is the transmitted power level of the PU in dB, $\overline{PL(d_j)}$ is the mean of $PL(d_{\mathrm{j}})$ and X_σ is a zero-mean Gaussian distributed random variable with standard deviation σ_1. The parameter $\overline{PL(d_j)}$ can be expressed by the HATA model which has been suggested by the IEEE 802.22 working group as the path loss model for a typical CR network environment. Assuming a rural environment, the average path loss model for a rural environment is given by [19]:

$$\overline{PL(d_j)} = 27.77 + 46.05 logf_c - 4.78(logf_c)^2 - 13.82 logh_{te} - \left(1.1 logf_c - 0.7\right) h_{re} + (44.9 - 6.55 logh_{te}) logd_j \tag{6}$$

where f_{c} is the carrier frequency, h_{te} and h_{re} are the effective transmitter and receiver antenna height, respectively. When hypothesis H_1 holds, the received power of the *j*'th user x_{j}(dB) is a Gaussian distributed random variable with 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 from the CR network, thus, differences in the averaged received powers due to path loss are negligible and the parameter μ_1 is identical for all CR users. The mean and variance of the Gaussian noise are also the same among all CR users. When hypothesis H_0 holds, the received power of each user is a Gaussian random variable with mean μ_0 and standard deviation σ_0. Therefore, x_j(dB) is expressed as a Gaussian distributed as follows:

$$x_j(dB) \sim \begin{cases} Normal(\mu_0, \sigma_0^2) & H_0 \\ Normal(\mu_1, \sigma_1^2) & H_1 \end{cases} \tag{7}$$

III. Optimal voting rule

As mentioned before, the local measured power of the *j*'th CR user x_j is compared with a predefined threshold *T* and then a binary decision u_j is transmitted to the FC. When the measured power is greater than the local threshold *T*, the decision about channel status is occupied and binary sensing report, u_j, is equal to 1; otherwise, the frequency band is determined to be vacant and u_j is set to be 0. In the *K*-out-of-*N* fusion rule, all of the binary received reports are summed up in the FC and compared with the threshold *K*, obviously, the OR rule corresponds to the case of *K*=1, majority and AND rules correspond to the case of *K*=*N*/2 and *K*=*N*, respectively. The global false alarm and miss detection probabilities of the *K*-out-of-*N* rule are respectively given by [18]

$$\begin{aligned} Q_{fa}(K) &= \sum_{\ell=K}^{N} \binom{N}{\ell} P_{fa}^{\ell} (1 - P_{fa})^{N-\ell} \\ Q_m(K) &= \sum_{\ell=0}^{K-1} \binom{N}{\ell} (1 - P_m)^{\ell} P_m^{N-\ell} \end{aligned} \tag{8}$$

where two parameters P_{fa} and P_m are the local false alarm and miss detection probabilities, respectively. These parameters are computed as:

$$\begin{aligned} P_{fa} &= P(u_j = 1 | H_0) = P\left(x_j > T | H_0\right) = Q(\frac{T - \mu_0}{\sigma_0}) \\ P_m &= P(u_j = 0 | H_1) = P\left(x_j < T | H_1\right) = Q(\frac{\mu_1 - T}{\sigma_1}) \end{aligned} \tag{9}$$

where *Q*(.) is the *Q*-function for standard normal distribution. It is assumed that the location and transmission power level of the PU tower are known for the FC. Therefore, the mean value of the received power is known. The global error probability can also be defined as

$$Q_e(K) = Q_{fa}(K)\, p(H_0) + Q_m(K)\, p(H_1) \tag{10}$$

Assuming that $Q_e(K)$ represents a single minimum, the optimum *K* will be obtained based on the following optimization problem

$$K_{opt} = \arg\min_K (Q_e(K)) \tag{11}$$

By substituting (8) and (9) into (10), the global error probability $Q_e(K)$ is obtained and the equation (10) can be expanded by performing the discrete operation on $Q_e(K)$ as

$$\begin{aligned}\nabla Q_e(K) &= Q_e(K+1) - Q_e(K) = 0 \\ &= \left[Q_{fa}(K+1)p(H_0) + Q_m(K+1)p(H_1)\right] - \left[Q_{fa}(K)p(H_0) + Q_m(K)p(H_1)\right] = 0 \\ &= \left[Q_{fa}(K+1) - Q_{fa}(K)\right]p(H_0) - \left[Q_m(K) - Q_m(K+1)\right]p(H_1) = 0 \\ &= \binom{N}{K}(P_{fa})^K(1-P_{fa})^{N-K}p(H_0) - \binom{N}{K}(1-P_m)^K(P_m)^{N-K}p(H_1) = 0\end{aligned} \tag{12}$$

The integer value for K is obtained as the following equation

$$\left(\frac{1-P_m}{P_{fa}}\right)^K \left(\frac{P_m}{1-P_{fa}}\right)^{N-K} = \frac{p(H_0)}{p(H_1)} \tag{13}$$

Taking logarithm on (13) and rearranging in term of K_{opt} gives:

$$k_{opt} = \frac{N-\varphi_0}{1+\psi_0} \tag{14}$$

where

$$\varphi_0 = \frac{\log(p(H_0)/p(H_1))}{\log(P_m/(1-P_{fa}))} \quad ; \quad \psi_0 = \frac{\log(P_{fa}/(1-P_m))}{\log(P_m/(1-P_{fa}))}$$

IV. THE PROPOSED ATTACK-AWARE OPTIMAL VOTING RULE (AOVR)

There are three different strategies for the attackers: “always yes” (AY), “always no” (AN), and “always false” (AF) strategies. In AY strategy, the malicious attackers, without sensing the spectrum, 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 “AN” attackers, without performing spectrum sensing, always submit a local decision saying that “there is no PU signal”; hence, the FC may be deceived and allow the CR users to access the channel while in fact, the PU signal is present. The “AF” attackers perform spectrum sensing and send the opposite values of their sensing results to the FC. Therefore, they always cause FC to make a wrong sensing decision. In this case, both spectrum waste and PU interference are possible. In the presence of SSDF attacks, the local spectrum sensing result of the *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. However, for the malicious attacker, the sensing result v_j can be different from report u_j, and it depends on the attack strategy. The SSDF attack model can be defined in general as follows: Firstly, the malicious attacker makes its local binary decision v_j. Then, it

Table.1. Attack probabilities of several different CR users

Attack Probabilities	"Benign User"	"AY" Attacker	"AN" Attacker	"AF" Attacker	"Probabilistic" Attacker
P_0	0	1	0	1	$0< P_0<1$
P_1	0	0	1	1	$0< P_1<1$

utilizes two attack probabilities P_0 and P_1, under two hypotheses H_0 and H_1, respectively, to decide whether to perform an 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. Such an attack model introduces a smart SSDF attack model. Obviously, for "AY" attacker two attack probabilities P_0 and P_1 are always 1 and 0, respectively. For "AN" attacker we have always P_0=0 and P_1=1. Finally, for "AF" malicious attacker, these values are the same and equal to 1. Two possible values of P_0 and P_1 for different types of attackers are listed in Table. 1 for convenience.

The probability functions of sensing report and sensing result for the j'th CR user (benign or malicious) can respectively be formulated as:

$$\begin{aligned} P\left(v_j=0\right) &= \sum_{k=0,1} P\left(v_j=0 \middle| H_k\right) p(H_k) = (1-P_{fa})p(H_0)+P_m p(H_1) \\ P\left(v_j=1\right) &= \sum_{k=0,1} P\left(v_j=1 \middle| H_k\right) p(H_k) = P_{fa} p(H_0)+(1-P_m)p(H_1) \end{aligned} \tag{15}$$

and

$$\begin{aligned} P\left(u_j=0\right) &= P\left(u_j=0 \middle| v_j=0\right)P(v_j=0)+P\left(u_j=0 \middle| v_j=1\right)P(v_j=1) \\ P\left(u_j=1\right) &= P\left(u_j=1 \middle| v_j=0\right)P(v_j=0)+P\left(u_j=1 \middle| v_j=1\right)P(v_j=1) \end{aligned} \tag{16}$$

Assuming 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 follows:

$$\begin{aligned} \alpha &= P\left(u_j=1 \middle| v_j=0\right) = P\left(u_j=1 \middle| v_j=0, s_j=\mathfrak{M}\right)P(s_j=\mathfrak{M}) + P\left(u_j=1 \middle| v_j=0, s_j=\mathfrak{B}\right)P(s_j=\mathfrak{B}) \\ &= P\left(u_j=1 \middle| v_j=0, s_j=\mathfrak{M}\right)\frac{N_a}{N}+0\times P(s_j=\mathfrak{B}) = P_0\frac{N_a}{N} \end{aligned} \tag{17}$$

and

$$\begin{aligned} \beta &= P\left(u_j=0 \middle| v_j=1\right) = P\left(u_j=0 \middle| v_j=1, s_j=\mathfrak{M}\right)P(s_j=\mathfrak{M}) + P\left(u_j=0 \middle| v_j=1, s_j=\mathfrak{B}\right)P(s_j=\mathfrak{B}) \\ &= P\left(u_j=0 \middle| v_j=1, s_j=\mathfrak{M}\right)\frac{N_a}{N}+0\times P(s_j=\mathfrak{B}) = P_1\frac{N_a}{N} \end{aligned} \tag{18}$$

The parameter s_j indicates the user type, which can be malicious ($\mathfrak{M}$) or benign ($\mathfrak{B}$). As mentioned before,

$$P\left(u_j=1\middle|v_j=0,s_j=\mathfrak{M}\right)=P_0$$
$$P\left(u_j=0\middle|v_j=1,s_j=\mathfrak{M}\right)=P_1$$
$$P\left(u_j=1\middle|v_j=0,s_j=\mathfrak{B}\right)=0$$
$$P\left(u_j=0\middle|v_j=1,s_j=\mathfrak{B}\right)=0$$

Assuming that the attack strategy is the same for all malicious attackers, thus, P_0 and P_1 are independent from index *j*.

When the number of cooperative CR users, *N*, is large enough, we have

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

Two attack parameters *α* and *β* are the probabilities that a given user *j* to launch an attack. When there is no SSDF attack and all CR users are benign, we have *α*=*β*=0. In the presence of “AY” attackers, *β*=0 and for CR network with “AN” attackers, *α*=0. Finally, for “AF” attackers, two parameters *α* and *β* are the same. Considering the attack parameters, the equation (16) is simplified to:

$$\begin{aligned}P\left(u_j=0\right)&=(1-\alpha)P\left(v_j=0\right)+\beta P\left(v_j=1\right)\\P\left(u_j=1\right)&=\alpha P\left(v_j=0\right)+(1-\beta)P\left(v_j=1\right)\end{aligned}\tag{19}$$

Applying the *K*-out-of-*N* rule, the global false alarm and miss detection probabilities are respectively given by

$$\begin{aligned}Q_{fa}\left(K\right)&=\sum_{\ell=K}^{N}\binom{N}{\ell}\left[P_{fa}^{new}\right]^{\ell}\left[1-P_{fa}^{new}\right]^{N-\ell}\\Q_{m}\left(K\right)&=\sum_{\ell=0}^{K-1}\binom{N}{\ell}\left[1-P_{m}^{new}\right]^{\ell}\left[P_{m}^{new}\right]^{N-\ell}\end{aligned}\tag{20}$$

where

$$\begin{aligned}P_{fa}^{new}&=P(u_j=1|H_0)=P(u_j=1|H_0,v_j=0)P(v_j=0|H_0)+P(u_j=1|H_0,v_j=1)P(v_j=1|H_0)\\&=\alpha(1-P_{fa})+(1-\beta)P_{fa}\end{aligned}$$

$$\begin{aligned}P_{m}^{new}&=P(u_j=0|H_1)=P(u_j=0|H_1,v_j=0)P(v_j=0|H_1)+P(u_j=0|H_1,v_j=1)P(v_j=1|H_1)\\&=(1-\alpha)P_m+\beta(1-P_m)\end{aligned}$$

similarly,

$$\begin{aligned}1-P_{fa}^{new}&=P(u_j=0|H_0)=P(u_j=0|H_0,v_j=0)P(v_j=0|H_0)+P(u_j=0|H_0,v_j=1)P(v_j=1|H_0)\\&=(1-\alpha)(1-P_{fa})+\beta P_{fa}\end{aligned}$$

$$\begin{aligned}1-P_{m}^{new}&=P(u_j=1|H_1)=P(u_j=1|H_1,v_j=0)P(v_j=0|H_1)+P(u_j=1|H_1,v_j=1)P(v_j=1|H_1)\\&=\alpha P_m+(1-\beta)(1-P_m)\end{aligned}$$

Like the equation (12), we have

$$K_{opt} = \frac{N-\varphi_1}{1+\psi_1} \tag{21}$$

where

$$\varphi_1 = \frac{\log(p(H_0)/p(H_1))}{\log\left(P_m^{new}/(1-P_{fa}^{new})\right)} = \frac{\log(p(H_0)/p(H_1))}{\log\left(((1-\alpha)P_m+\beta(1-P_m))/((1-\alpha)(1-P_{fa})+\beta P_{fa})\right)}$$

$$\psi_1 = \frac{\log\left(P_{fa}^{new}/(1-P_m^{new})\right)}{\log\left(P_m^{new}/(1-P_{fa}^{new})\right)} = \frac{\log\left((\alpha(1-P_{fa})+(1-\beta)P_{fa})/(\alpha P_m+(1-\beta)(1-P_m))\right)}{\log\left(((1-\alpha)P_m+\beta(1-P_m))/((1-\alpha)(1-P_{fa})+\beta P_{fa})\right)}$$

V. Practical Consideration and Limitation

Here, 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 E(m) are obtained as [20]

$$m = \frac{1}{N}\sum_{j=1}^{N} u_j \quad ; \quad \mathrm{E}(m) = \frac{1}{N}\sum_{j=1}^{N}\mathrm{E}(u_j) \tag{22}$$

where

$$\mathrm{E}(u_j) = \sum_{u_j=0}^{1} u_j P(u_j) = P(u_j=1) \tag{23}$$

With regard to equation (19),

$$\mathrm{E}(m) = P(u_j=1) = \alpha\left[(1-P_{fa})p(H_0)+P_m p(H_1)\right] + (1-\beta)\left[P_{fa}p(H_0)+(1-P_m)p(H_1)\right] \tag{24}$$

Regarding the equations (17) and (18),

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

from the equation (24), the values of α and β are obtained as follows:

$$\overset{\wedge}{\alpha} = \frac{\mathrm{E}(m)-\psi}{1-(1+\rho)\psi} \quad ; \quad 1 \neq (1+\rho)\psi$$

$$\overset{\wedge}{\beta} = \rho\overset{\wedge}{\alpha}$$

where the parameter ψ is defined as follows:

$$\psi = P_{fa}p(H_0) + (1-P_m)p(H_1)$$

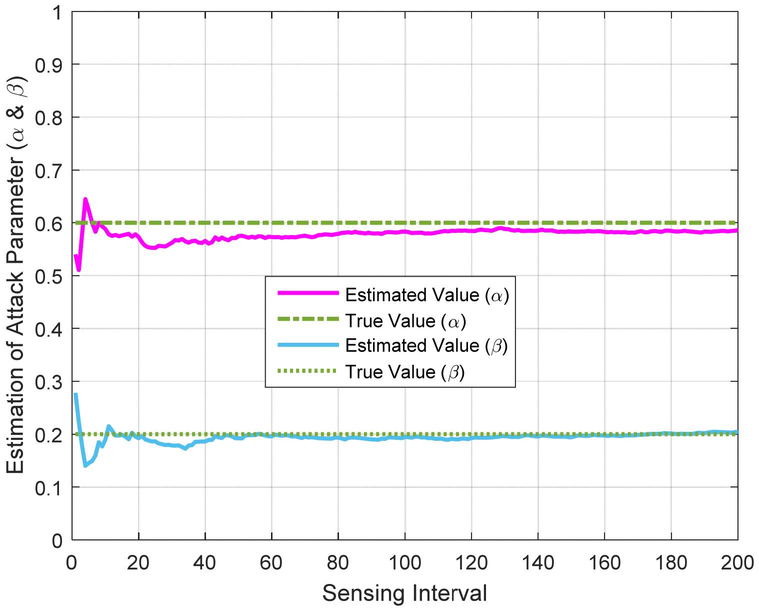

Fig. 2. The convergence of attack parameters (α=0.6, β=0.2)

VI. NUMERICAL RESULTS AND DISCUSSIONS

To evaluate the performance of the proposed AOVR approach, computer simulation results are obtained over 10^4 runs in MATLAB software. The PU transmitter with $p(H_1)$=0.2 is set to a distance of D=3km from the center of the CR network. The transmitted power of the PU is supposed to be 200 mW and the 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 carrier frequency of the PU signal is 617 MHz and the effective heights of the transmitter and receiver antennas are 100m and 1m, respectively. We also fix the total number of CR sensors, N=30 while varying the number of malicious, from 0 to 18, corresponding attack's percentage (N_a/N) changes from 0 to 60%.

Fig. 2 shows the convergence of two attack parameters α and β. The estimated values are converged to the constant values after applying almost 100 rounds of spectrum sensing. At the beginning of the simulation, almost 100 sensing intervals are performed to estimate of two attack parameters α and β and then the obtained parameters are applied in the proposed method to improve the cooperative sensing performance.

Fig. 3 displays the total error probability versus parameter K for benign users and multiple attackers. As shown in the figure, for a given attack strategy there is an optimal value for K that

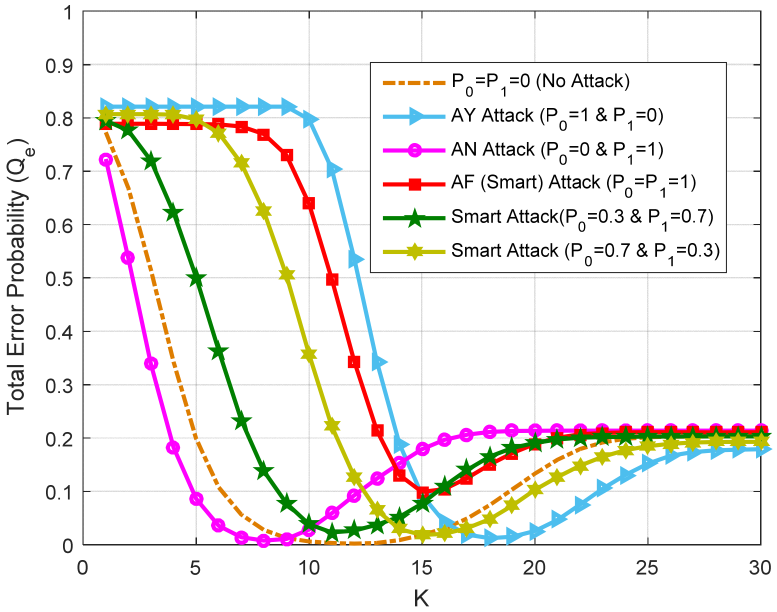

Fig. 3. The total error probability versus *K* for benign and malicious users

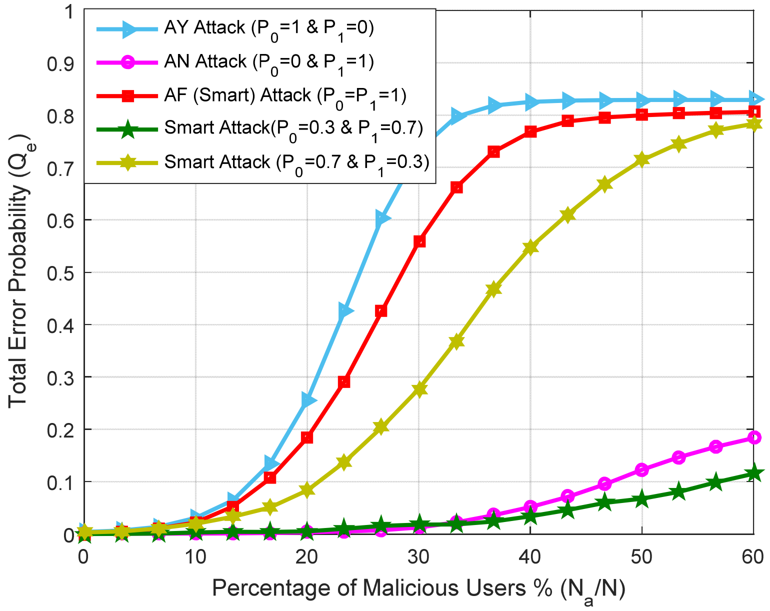

Fig. 4. The total error probability versus attack population for several different types of attackers

minimizes the total error probability. Therefore, we plan to obtain the optimal value for *K* so as to minimize the global error probability.

The total error probability versus the attack population is shown in Fig. 4. In this case, AY, AN, AF and probabilistic (smart) attackers are considered. Obviously, the error probability is increased with increasing the percentage of malicious attackers. Among these attackers, the error probability of AY

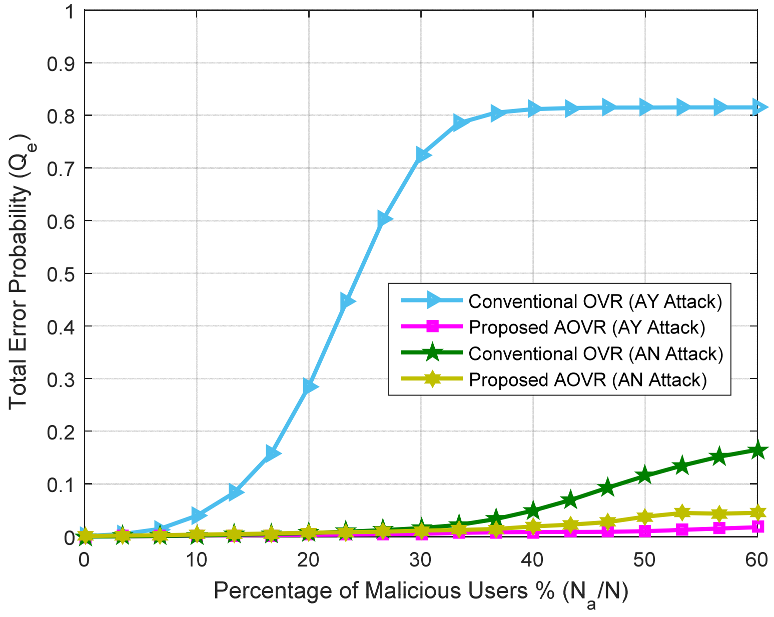

Fig. 5. The total error probability versus attack population

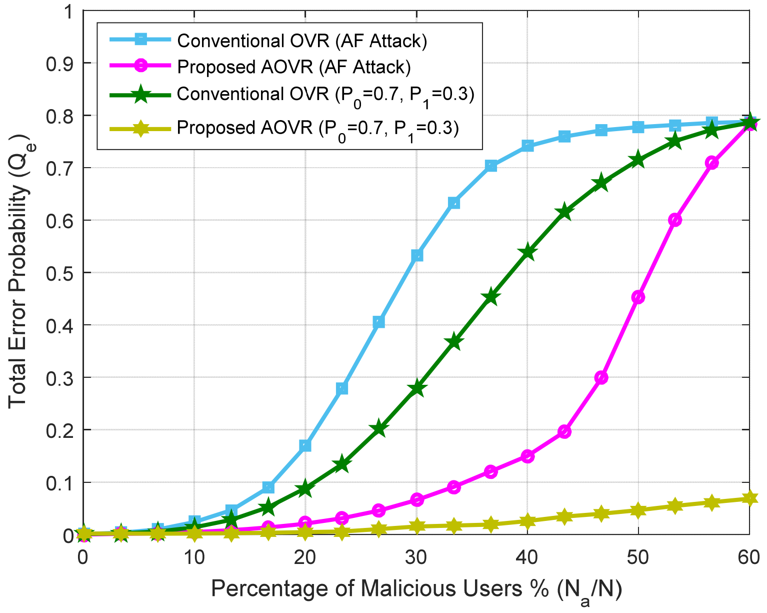

Fig. 6. The total error probability versus attack population

and AN attackers increased to 0.8 and 0.2 (corresponds to $p(H_0)$ and $p(H_1)$) respectively.

Figs. 5 and 6 display the total error probability versus attack population. As shown in these figures, in conventional OVR (the case that there is SSDF attack and the FC is not aware), increasing the attack population dramatically increases the error probability. On the contrary, in the proposed AOVR, increasing attack population causes a small change in the rate of total error probability.

Fig. 7 depicts the total error probability versus attack parameter P_0 in P_1=0.3 and P_1=0.7 for conventional OVR and proposed AOVR methods. As shown, the proposed AOVR method

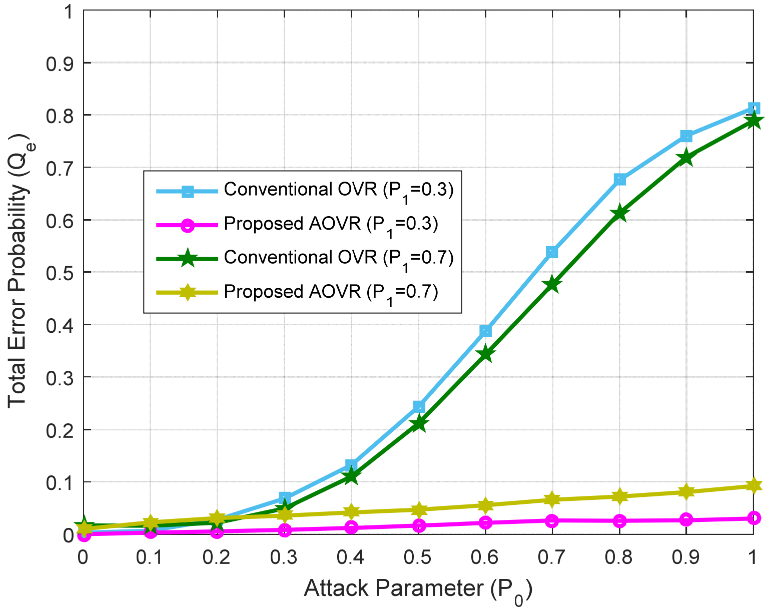

Fig. 7. The total error probability versus attack parameter

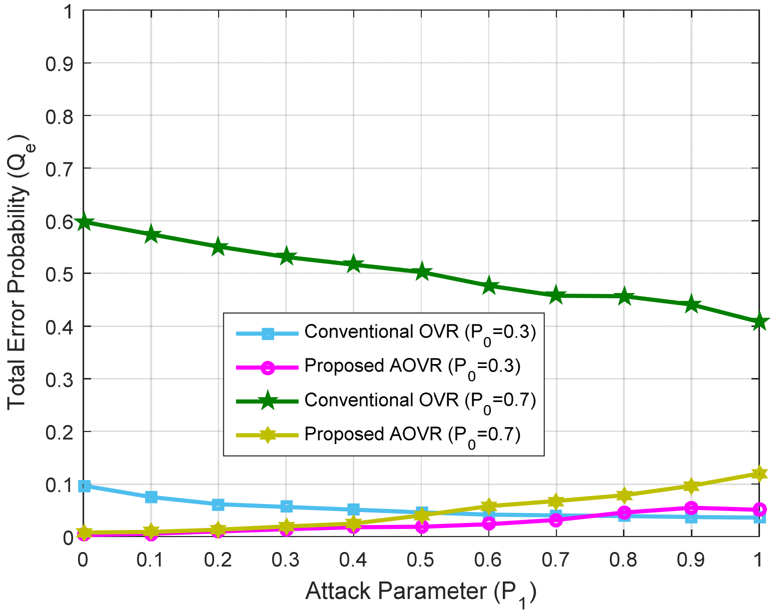

Fig. 8. The total error probability versus attack parameter

remarkably improves the performance of CSS under smart SSDF attacks. Fig. 8 also shows similar results versus attack parameter P_1 when the parameter P_0 is set to 0.3 and 0.7.

VII. Conclusion

In this study, to mitigate the destructive impact of spectrum sensing data falsification (SSDF) attacks, a novel secure cooperative spectrum sensing (CSS) scheme called attack-aware optimal voting rule (AOVR) was proposed. An analytical model of the SSDF attack was also investigated. In the initial stages of simulation, two important attack parameters were estimated and then applied in conventional OVR to improve the CSS performance. Two estimated attack parameters include the probabilities of SSDF attack in both occupied and unoccupied frequency bands. It was concluded that the proposed AOVR is a robust defense strategy against SSDF attacks, especially, for CR networks located in hostile environments.

REFERENCES

[1] J. Mitola and G.Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communication*, vol. 6, no. 4, pp. 13-18, August 1999.

[2] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[3] I.F. Akyildiz, W.Y. Lee, M.C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, Sept. 2006.

[4] F.F. Digham, M.-S. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," *Proceedings of the IEEE International Conference on Communications*, vol. 5, pp. 3575-9, May 2003.

[5] S.M. Mishra, A. Sahai, and R.W. Brodersen, "Cooperative sensing among cognitive radios," *Proceedings of the IEEE International Conference on Communications*, pp. 1658-1663, June 2006.

[6] I.F. Akyildiz, B.F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 40, no. 1, pp. 40-62, March 2011.

[7] J. Ma, G. Zhao, and Y. Li, "Soft combining and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Transaction on Wireless Communications*, vol. 7, no. 11, pp. 4502-4507, Nov. 2008.

[8] R. Chen, J. M. Park, Y. T. Hou and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, April 2008.

[9] R. Chen, J. Park, and K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," *Computer Communication*, vol. 35, no. 17, pp. 2115-2124, Oct. 2012.

[10] C.Y. Chen, Y.H. Chou, H.C. Chao, and C.H. Lo, "Secure centralized spectrum sensing for cognitive radio networks," *Wireless Networks*, vol. 18, no. 6, pp. 667-677, March 2012.

[11] V. Chen, M. Song, and C. Xin, "CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks," *Wireless Networks*, vol. 20, no. 8, pp. 2521-2528, Nov. 2014.

[12] J. C. Clement, "Jettison the defectives: a robust cooperative spectrum sensing scheme in a cognitive radio networks," *Circuits Syst Signal Process*, DOI 10.1007/s00034-017-0672-9, Sept. 2017.

[13] A.A. Sharifi and M. J. Musevi Niya, "Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach," *IEEE Communications Letters*, vol. 20, no. 1, pp. 93-96, Jan. 2016.

[14] A.A. Sharifi and J. Musevi Niya, "Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks," *Wireless Personal Communications*, vol. 90, no. 1, pp. 75-91, Sept. 2016.

[15] A.A. Sharifi, M. Sharifi, and J. Musevi Niya, "Reputation-based likelihood ratio test with anchor nodes assistance," *8th Internationa Symposium on Telecommunications*, Tehran, Sept. 2016.

[16] A.G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428-445, First Quarter 2013.

[17] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342-1363, Third Quarter 2015.

[18] P.K. Varshney, Distributed detection and data fusion, *Springer-Verlag*, 1997.

[19] T.S. Rappaport, Wireless communications: Principles and Practice, *Prentice Hall*, 1996.

[20] 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 Journal of Electrical Engineering*, vol. 50, no. 1, pp. 43-50, Winter & Spring 2018.