Attack-Aware Cooperative Spectrum Sensing in Cognitive Radio Networks under Byzantine Attack

H. Alizadeh Ghazijahani[1], A. A. Sharifi[2], J. Musevi Niya[1], H. Seyedarabi[1]
1-Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
2-Department of Electrical Engineering, University of Bonab, Bonab, Iran
{hag, a.sharifi, niya, seyedarabi}@tabrizu.ac.ir
Corresponding author: H. Alizadeh Ghazijahani

***Abstract*- Cooperative Spectrum Sensing (CSS) is an effective approach to overcome the impact of multi-path fading and shadowing issues. The reliability of CSS can be severely degraded under Byzantine attack, which may be caused by either malfunctioning sensing terminals or malicious nodes. Almost, the previous studies have not analyzed and considered the attack in their models. The present study introduces a new issue named attack-aware CSS where the objective is to analyze the occurred attack against CR network to ameliorate the performance of data fusion schemes. The novelty includes the modification of Weighted Sequential Probability Ratio Test (WSPRT) algorithm which resulted in Attack-Aware WSPRT (A^2WSPRT). The findings indicated considerable reduction in cooperation overhead and enhancement in correct sensing ratio, especially in severe attacks.**

***Index Terms*-** Attack-Aware, Byzantine attack, Cognitive Radio (CR), Cooperative Spectrum Sensing (CSS), SSDF Attack.

I. INTRODUCTION

The growth of wireless devices and applications results in limited spectrum resource while Federal Communication Commission (FCC) has reported that the licensed users, known as primary users (PU), are available only 15 to 85 percent of time. Cognitive Radio (CR) is one of the enabling technologies to mitigate the spectrum scarcity concern [2]. The policy of CR is to profitable utilization of the available spectrum resources. In this new spectrum access paradigm, CR users, which are named as secondary users (SU), have permission to use the licensed spectrum bands, unless they cause interference in Pus' activities. In CR networks each SU performs spectrum sensing to sense the surrounding area and opportunistically utilizes the white spaces (Unoccupied bands). Detecting the activity of primary users, the CRs leave the spectrum and search for the other vacant spectrums. Therefore, the continuous sensing of the wireless environment is mandatory for the secondary devices. There are some techniques to monitor the channel status, namely *matched filter*,

Manuscript received 11-Jan.-2017 and revised 19-April-2017,
Accepted on 16-June-2017
P- ISSN: 2322-4088
E- ISSN: 2322-3936

cyclostationary and *energy detection*. *Matched filter* correlates the signal with time shifted version and compares between the final output of matched filter and predetermined threshold will determine the PU presence. Hence, if this information is not accurate, then the matched filter operates weakly [3]. *Cyclostationary* feature detection can distinguish PU signal from noise and used at very low Signal to Noise Ratio (SNR) detection by using the information embedded in the PU signal that are not present in the noise. The main drawback of this method is the complexity of calculation. Also, it must deal with all the frequencies in order to generate the spectral correlation function, which makes it a very large calculation. *Energy detection* is another signal detection mechanism using an energy detector (also known as radiometer) to specify the presence or absence of signal in the band. The most often used approaches in the energy detection are based on the Neyman-Pearson (NP) lemma. The NP lemma criterion increases the probability of detection for a given probability of false alarm. It is an essential and a common approach to spectrum sensing since it has moderate computational complexities, and can be implemented in both time domain and frequency domain. With this review, energy detection get as the prevalent method for spectrum sensing which is used in most studies [1, 4].

It is known that the wireless channel is subject to fading and shadowing. When an SU undertakes this kind of condition, it may fail to detect the existence of primary signal. The result is the increase in miss detection probability and may cause interference with PU network [5]. To deal with this phenomenon, Cooperative Spectrum Sensing (CSS) has been introduced. In CSS, CR users report the spectrum sensing results to a fusion center (FC). FC combines the sensing results of multiple SUs to make a final spectrum sensing decision. The decision making techniques are categorized into hard and soft. In hard decision, the users send their local spectrum sensing results to FC with one bit as 0 (idle) or 1 (busy), but in soft decision, the sensed values are sent to FC as raw data.

Performing the Distributed Spectrum Sensing (DSS), the CR network may experience the incidence of Byzantine. The Byzantine failure problem can be caused by malfunctioning sensing terminals or Spectrum Sensing Data Falsification (SSDF) attack [1, 6]. A malfunctioning sensing terminal is unable to perform reliable local spectrum sensing and sends incorrect sensing reports to the FC.

Besides, The sensing phase provides a great opportunity for malicious users to disrupt the network [7]. A malicious user in SSDF attack tries to corrupt the result of the CSS by sending the incorrect local sensing reports to the FC. This attack causes interference between PUs and CRs or non-optimal use of available spectrum and consequently reduces the effective performance of CR network.

There are some works that address the techniques to overcome the Byzantine failure. Recently a comprehensive investigation is published which classifies the existing defense algorithms against typical Byzantine attacks carefully [8]. In the field of prevention of SSDF attack, for example in [9] and [10] the participant nodes in the cooperation are classified into two sets: honest and malicious. Therefore, the authors have tried to assign suspicious level to nodes. They determine the trust value

for each SU based on the past history of its sensing report's accuracy. When the suspicious level of a node goes beyond certain threshold, it will be considered as malicious and its future reports will be aborted [10]. Likewise, in [5], researchers take a similar procedure like [9] and [10]; but their approach does not require any knowledge of attackers. Their idea is to place the report history of each SU in a high-dimensional space and detect possible abnormalities. In [11], users' reputation is used to increase the performance of the cooperative sensing and etiquette reputation is utilized to measure the performance of the SUs in the spectrum sensing process. In [12] a novel reputation based hard decision fusion method is proposed and "AND", "OR" and "*K* out of *N*" fusion rules are used to make final decision. In [1] and [6], weighted sequential probability ratio test (WSPRT) is proposed. A zero-initialized reputation value is considered for each node in the CR network. Whenever the local spectrum sensing report of a node is consistent with the final sensing decision, its reputation value is incremented by one; otherwise it is decremented by one [1]. Using a special function, these values determine the contributions of each node on the final decision procedure. A different manner is introduced in [13] which utilizes cryptographic mechanism to alleviate the possible SSDF attack.

Most of the previous anti-attack methods estimated the validity of nodes to improve the CSS performance under Byzantine attack, but the attack was not analyzed to exploit in the proposed solutions. Undoubtedly, knowing the modality of attack provides us with an authentic view to design a suitable anti-attack method. In this study a new issue named attack-aware CSS is presented where the scope is to analyze the occurred attack against CR network to increase the performance of the contrast data fusion manners. In this regard, there are three head functions that must be done at FC as follows.

1. Attack strategy detection; SSDF attack occurs in different types including always false, always free, and always busy. Detecting the strategy of the attack can be suitable to improve the performance of some manners using attack-aware approach. Also, it can be realized simply by perceiving the behavior of nodes during some cooperation times. Where, the attack strategy is assumed to be known for the FC.
2. Estimation of the attack extension factor; in this approach, knowing the ratio of number of attacker nodes to all nodes in the network, named as attack extension factor, is the most important parameter. This is estimated using the diversity of received sensing results which have been reported by SUs. The analytical expression is stated in section 4.
3. Exploitation of the analysis results; the extracted information of the extension factor and strategy of the attack are used to improve the weighted version of sequential detection scheme, WSPRT. The method is detailed in the following sections.

It is worth mentioning that this study does not introduce a new technique to deal with SSDF. The purpose is to introduce and maneuver on the new concept named attack-aware in the scope of security. This idea can be also applied in other fields of wireless communication security.

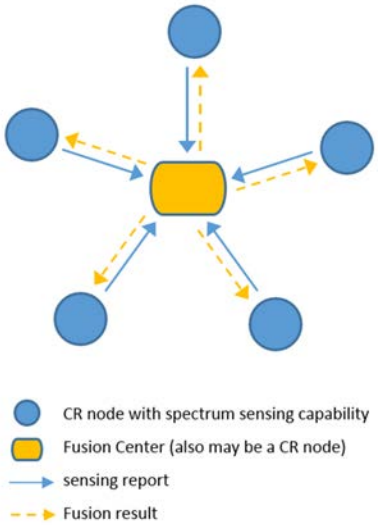

Fig. 1. CSS model.

The rest of the paper is structured as follows. Section 2 presents a brief background on CSS and SSDF attack. The WSPRT algorithm is described in section 3. Section 4 deals with attack-aware notion and its functions. Correspondingly, the WSPRT improvement using attack-aware technique is discussed. Simulation platform, results and discussions are presented in section 5. Finally, conclusion remarks are drawn in section 6.

II. CSS AND SSDF ATTACK

Spectrum sensing is the main function of CR networks. If the spectrum sensing is properly done, it prevents CR network interference from PU transmitter. The PU detection can be formulated as a binary hypothesis testing problem as follows [14, 15]:

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

where $x(t)$ denotes the received signal at the CR user, $S(t)$ is the transmitted PU signal, $h(t)$ is the channel gain of the sensing channel, $n(t)$ is the zero mean Additive White Gaussian Noise (AWGN), H_0 represent the null hypothesis that only noise is present and H_1 represent the alternate hypothesis that both PU signal and noise is present. Choosing the energy detection as spectrum sensing method the decision statistic is:

$$Y = \sum_{n=1}^{2q} |x(n)|^2$$

where q is the time-bandwidth product and γ is the detection threshold determined by the target false-alarm probability [16]. For the evaluation of detection performance, the probabilities of detection P_d and false-alarm P_{Fa} are defined as [17]:

$$P_d = P(Y > \gamma | H_1), \;\; P_{Fa} = P(Y > \gamma | H_0) \quad (2)$$

The probability of miss-detection is defined as:

$P_m = 1 - P_d = P(Y < \gamma | H_1)$

The accuracy of the local sensing detection for each node is characterized by a total correct probability, defined as follows:

$$P_c = P_d P(H_1) + (1 - P_{Fa}) P(H_0) \quad (3)$$

Collaborative spectrum sensing increases the precision of spectrum sensing with spatial diversity. In CSS, each node locally senses the spectrum and sends either its decision or the measured data (e.g. energy level in a given channel) to its neighbors or FC. Fig. 1 shows a simple model of CSS. Two types of data fusion frameworks have been proposed for CSS, hard-decision combining and soft-decision combining schemes [18]. When FC combines the decision, the procedure is called hard combining scheme and if the FC combines the raw data, it is called soft combining.

There are some data fusion techniques which can be found in decision fusion, Bayesian detection and Neyman-Pearson test [5, 11]. In Decision fusion each CR user send decision u_i to a data collector for hard combination through OR, AND and MAJ (majority) rule. The Bayesian detection and NP test require a priori knowledge of the u_i's probabilities under hypothesis zero and one, which can be denoted as $P(u_i|H_0)$ and $P(u_i|H_1)$. The hypothesis test in Bayesian and NP can be shown as:

$$\prod_{i=0}^{m} \frac{P(u_i|H_1)}{P(u_i|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma \quad (4)$$

As in the energy detection based spectrum sensing methods, the performance of collaborative system is highly dependent on the threshold value, so exact determining of γ is very critical [19]. Bayesian and NP test are both a fixed-number Likelihood Ratio Test (LRT); their only difference is the way that the threshold γ is chosen.

In an SSDF attack, a malicious user intentionally sends falsified local spectrum sensing reports to the FC in an attempt to cause the FC to make incorrect spectrum sensing decisions. In either case, Byzantine failures can lead to interference to incumbent and/or under-utilization of fallow licensed spectrum. The attackers that send wrong reports of their sensing results are named as always false attackers. Another one is always free attackers; such that they always report that the channel is free. Third type of attackers are called as always busy attackers, which their purpose is to prevent CR users from accessing the white spaces. But the first one is more prevalent than the others.

III. A REVIEW OF WSPRT DATA FUSION TECHNIQUE

Chen et al. [1, 6] have proposed a weighted sequential probability ratio test (WSPRT) to counter SSDF attack. The authors proposed a more practical method for calculating the priori probabilities and evaluate WSPRT by comparing it with a variety of data fusion techniques such as SPRT, "AND", "OR", MAJ and LRT under various conditions and simulation results indicate that WSPRT is the

most robust against Byzantine Failures among the data fusion techniques that were considered. In this regard, we chose WSPRT as the base data fusion technique and applied our contribution on it.

WSPRT composed of two steps. The first step is a reputation maintenance step, and the second step is the actual hypothesis test. A sensing terminal's reputation ratings are allocated based on the accuracy of its prior sensing results. The reputation value r_i is set to zero at the beginning; whenever its local spectrum sensing report u_i, is consistent with the final sensing decision U, its reputation is incremented by one; otherwise it is decremented by one. The reputation of node i is updated according to the following relation:

$r_i \leftarrow r_i + (-1)^{u_i+u}$

The hypothesis test of WSPRT is based on SPRT. The SPRT technique is a hypothesis test for sequential analysis and supports sampling a variable number of observations [18]. When applying SPRT to data fusion for DSS, one needs to define the following likelihood ratio as the decision variable:

$$S_k = \prod_{i=0}^{k} \frac{P(u_i|H_1)}{P(u_i|H_0)} \quad (5)$$

where *k*, the number of samples, means that *k* CR nodes participate in polling. The *k* is a variable and can be different from m. The fusion decision is based on the following criterion:

$S_k < \mu_0 \Rightarrow \text{accept } H_0$

$S_k > \mu_1 \Rightarrow \text{accept } H_1$

$\mu_0 \leq S_k \leq \mu_1 \Rightarrow \text{take another observation}$

The value of μ_0 and μ_1 are decided by:

$\mu_0 = \frac{\beta}{1-\alpha}, \quad \mu_1 = \frac{1-\beta}{\alpha}$

where α and β are the tolerated false-alarm and miss-detection probabilities, respectively [1, 18]. The procedure is as follows. The FC calculates S_k in (5) using only a node's report. If $S_k < \mu_0$ or $S_k > \mu_1$, correspondingly H_0 or is H_1 is accepted, else another observation is needed to be taken. This process will go on until one of mentioned conditions is reached. Unlike the Bayesian and NP test where the sampling number is a certain definite value, SPRT executes the test sequentially and has a dynamic sampling number for each test. The samples are dealt with one-by-one and the test is terminated when the probability ratio meet either of two bounds. Compared to the other previous schemes, SPRT takes the fewest samples due to its ability to jump out of the test after taking the minimum necessary samples. It can be proved that SPRT minimizes the expected value of k needed to accept either hypothesis H_1 or H_0 [18]. The idea of WSPRT is to modify the likelihood ratio in equation (5). So that, the decision variable S_k, also takes a sensing terminal's reputation into consideration.

$$S_k = \prod_{i=0}^{k} \left(\frac{P(u_i|H_1)}{P(u_i|H_0)}\right)^{w_i} \quad (6)$$

where w_i is defined as the weight of N_i and is a function of r_i: $w_i = f(r_i)$ where $f(.)$ is defined as follows:

$$f(r_i) = \begin{cases} 0 & r_i \leq -g \\ \frac{r_i+g}{\max(r_i)+g} & r_i > -g \end{cases} \quad (7)$$

where, the variable $g(>0)$ is used to meet the requirement of ensuring that enough weight is allocated to a sensing terminal.

All the above schemes need the same knowledge of the priori probabilities i.e., $P(u_i|H_1)$ and $P(u_i|H_0)$. But in practice such data may not be available. Even if such data is available, since priori probabilities change with a sensing terminal's location, empirical data will need to be re-collected every time the sensing terminal moves to a different location. R. Chen *et al* in [1] propose an approach to calculate the probabilities based on the Log-normal shadowing path loss model which can be represented in dB as:

$$\mathrm{PL}(d) = \overline{\mathrm{PL}(d)} + X_\sigma = \overline{\mathrm{PL}(d_0)} + 10\, l \log\left(\frac{d}{d_0}\right) + X_\sigma \quad (8)$$

where d is the distance between the PU transmitter and CR receiver, $\mathrm{PL}(d)$ is the path loss as a function of d, $\overline{\mathrm{PL}(d)}$ is the mean of $\mathrm{PL}(d)$, X_σ is a zero-mean Gaussian distributed random variable with standard deviation σ, d_0 is a close-in reference distance which is determined from measurements close to the transmitter and l is the path loss exponent which indicates the rate at which the path loss increases with distance. The received power $P_r = P_t - \mathrm{PL}(d)$, where P_t is the transmitted power. Assuming the receiver uses an energy detector with a detection threshold γ, the priori probabilities under H_1 can be computed as:

$$P(u_i = 1|H_1) = P(P_r > \gamma|H_1) = P(P_t - \mathrm{PL}(d) > \gamma) = P\left(P_t - \overline{\mathrm{PL}(d)} - X_\sigma > \gamma\right)$$
$$= P\left(X_\sigma < P_t - \overline{\mathrm{PL}(d)} - \gamma\right) = Q\left(\frac{\gamma - P_t + \overline{\mathrm{PL}(d)}}{\sigma}\right) \quad (9)$$

and

$$P(u_i = 0|H_1) = 1 - P(u_i = 1|H_1) = Q\left(\frac{P_t - \sigma - \overline{\mathrm{PL}(d)}}{\sigma}\right) \quad (10)$$

When hypothesis H_0 holds, $P_r = n_0$, where n_0 can be regarded as a Gaussian noise power with mean $\overline{n_0}$ and standard deviation σ_n, similarly the priori probabilities under H_0 can be computed as:

$$P(u_i = 1|H_0) = Q\left(\frac{\gamma - \overline{n_0}}{\sigma_n}\right) \quad (11)$$

$$P(u_i = 0|H_0) = Q\left(\frac{\overline{n_0} - \gamma}{\sigma_n}\right) \quad (12)$$

Algorithm I shows the procedure of WSPR. In the following, the attack-aware idea is implemented on WSPRT.

Algorithm I. WSPRT algorithm [1]

1) $\forall i\ ;\ \ r_i = 0$
2) $for\ each\ spectrum\ sensing\ attempt\ made\ by\ N_0\ \{$
3) $i = 0;\ \ W_n = 1$
4) $get\ a\ spectrum\ sensing\ report\ u_i\ from\ N_i$
5) $W_n \leftarrow W_n . \left(\frac{P(u_i|H_1)}{P(u_i|H_0)}\right)^{f(r_i)}$
6) $if\ \mu_0 < W_n < \mu_1\ then:\ \ i \leftarrow (i+1)\ mod\ (m+1)$ $\quad Go\ to\ step\ 4$
7) $if\ \ W_n \geq \mu_1\ then:\ accept\ H_1 \quad (output\ u = 1)$ $\quad Go\ to\ step\ 12$
8) $if\ \ W_n \leq \mu_0\ then:\ accept\ H_0 \quad (output\ u = 0)$
9) $for\ each\ sampled\ u_i\ , set\ \ r_i \leftarrow r_i + (-1)^{u_i+u}$
10) $\}$

IV. ATTACK-AWARE DATA FUSION TECHNIQUE

To implement an attack-aware FC, first the attack should be analyzed. The analysis has two functions including determining the strategy of SSDF attack and estimating the ratio of attacker nodes number to the entire nodes in the network, which is called attack extension factor and is shown with parameter ψ. The strategy of attack can be realized simply by perceiving the behavior of nodes during some cooperation times. Where, the attack strategy is assumed to be known for the FC. The calculation of the diversity of results which have been reported by SUs is profitable to extract the attack extension factor, presented in detail in the following subsection. The results of analysis are employed in the body of WSPRT, presented in section *B*.

A. Attack Analysis

To the best of our knowledge, the most defense methods against SSDF attack have fixed behavior facing any attack extension factor, and almost there is no strategy to act proportional to the extension factor of the occurred attack.

In the attack-aware technique, the defense manner's parameters are set adaptive to the attack extension factor. This task is a general issue and can be effectively applied to the most defense methods proportional to the corresponding algorithm.

First, the attack extension factor must be estimated. The percentage of attackers in the network can be determined with a variety of innovative methods. Where, the standard deviation (SD) of received sensing reports of SUs is used. By a simple mathematical investigation, it is observed that there is a nonlinear relation between the percentage of attackers and SD of received sensing reports.

Assume that the always false attack occurs against the CR network and the percentage of attackers in the network is ψ. It can be interpreted that considering entire nodes in the network (honest and malicious) each changes its sensing result with probability ψ [20, 21]. The SD value of received reports can be calculated both in the idle and busy states of the channel. When the channel is idle, $(1-\psi)\%$ of participants nodes' reports indicate that the channel is idle (0 mark) and $\psi\%$ of reports indicate that it is busy (1 mark). The idle and busy states are shown with 0 and 1, respectively. The mean and SD values of received reports are as follows:

$$m_I = \frac{1}{N}\sum_{i=1}^{m} u_i = \psi \times 1 + (1-\psi) \times 0 = \psi \tag{13}$$

$$\sigma_I = \left(\frac{1}{N}\sum_{i=1}^{m}(u_i - m_I)^2\right)^{1/2} = \sqrt{\psi - \psi^2} \tag{14}$$

Table I. Mean and standard deviation for different attack strategies in idle and busy states of channel

Attack type	*Always False*	*Always Free*	*Always Busy*
m_I	ψ	0	ψ
m_B	$1-\psi$	$1-\psi$	1
σ_I	$\sqrt{\psi-\psi^2}$	0	$\sqrt{\psi-\psi^2}$
σ_B	$\sqrt{\psi-\psi^2}$	$\sqrt{\psi-\psi^2}$	0

Similarly, when the channel is busy, $(1-\psi)\%$ of nodes send 1 and $\psi\%$ of them send 0 to the FC. Under the above mentioned conditions, the mean and SD values of received reports are as follows:

$$m_B = \frac{1}{N}\sum_{i=1}^{m} u_i = (1-\psi) \times 1 + \psi \times 0 = 1-\psi \tag{15}$$

$$\sigma_B = \left(\frac{1}{N}\sum_{i=1}^{m}(u_i - m_B)^2\right)^{1/2} = \sqrt{\psi - \psi^2} \tag{16}$$

Similarly, the mean and SD values of received reports are calculated for other attack strategies. The results are shown in Table I.

As observed for always false mode, although the mean values of reports in idle and busy states are different, the SD values are the same. To find the attack extension factor, by computing the SD of the reports, $\sigma_{reports}$, the parameter ψ is accessible.

In the always free mode, when the channel state is idle, the mean and SD of reports are zero. This is due to the fact that there is no trace of attack effect in this state. But, in the busy periods, SD is as always false mode and the ψ can be calculated.

Moreover, in always busy mode it can be supposed that there is no attack in busy state and $\sigma_{reports}$ is calculated to estimate the attack extension factor in the idle mode.

B. Attack-Aware WSPRT

The effect of SSDF attack on the CR network can be depicted as a block which its input is spectrum sensing results and the output is reports sent to the FC. The equation (17) represents an interface

matrix describing the channel activity probabilities from the sensing nodes viewpoint under always false, always free and always busy attacks. In this model, $P(H_I)$ and $P(H_B)$ are the channel state probabilities indicating that it is idle or busy, respectively. These probabilities are different in the FC due to the effect of malicious nodes, shown with $P(H_0)$ and $P(H_1)$. For always false attack as an example, $(1-\psi)\%$ of nodes send correct sensing results and $\psi\%$ of them send inverted sensing results to the FC.

$$\begin{bmatrix} P(H_0) \\ P(H_1) \end{bmatrix} = \begin{cases} \begin{bmatrix} 1-\psi & \psi \\ \psi & 1-\psi \end{bmatrix} \begin{bmatrix} P(H_I) \\ P(H_B) \end{bmatrix} & \text{Always false} \\ \begin{bmatrix} 1 & 0 \\ \psi & 1-\psi \end{bmatrix} \begin{bmatrix} P(H_I) \\ P(H_B) \end{bmatrix} & \text{Always Free} \\ \begin{bmatrix} 1-\psi & \psi \\ 0 & 1 \end{bmatrix} \begin{bmatrix} P(H_I) \\ P(H_B) \end{bmatrix} & \text{Always Busy} \end{cases} \tag{17}$$

As mentioned in the previous section, the data fusion problem can be considered as a two-hypothesis detection problem. The optimum decision rule is given by the following likelihood ratio test [22].

$$P[u|H_1]P(H_1) \underset{H_0}{\overset{H_1}{\gtrless}} P[u|H_0]P(H_0)$$

$$\frac{P[u|H_1]}{P[u|H_0]} \underset{<}{>} \frac{P(H_0)}{P(H_1)}$$

As indicated earlier, R. Chen *et al* in [1, 6] considered the simplified form of the likelihood ratio test. However, they did not consider the ratio of channel activity, $P(H_1)/P(H_0)$. Similarly, in some literature, the ratio is eliminated because assumed that it is always constant. We consider the problem of optimization of the data fusion rule by adding the channel activity ratio to the decision variable of WSPRT. The equation (6) is changed to the following form:

$$S_{(a^2)k} = \prod_{i=0}^{k} \left(\frac{P[u_i|H_1]P(H_1)}{P[u_i|H_0]P(H_0)} \right)^{w_i} \tag{18}$$

where $S_{(a^2)}$ is the decision variable for the new WSPRT scheme. The channel activity ratio is shown in equation (19), which is the function of the parameter ψ.

$$\frac{P(H_1)}{P(H_0)} = \begin{cases} \frac{\psi P(H_I)+(1-\psi)P(H_B)}{(1-\psi)P(H_I)+\psi P(H_B)} & \text{Always false} \\ \frac{\psi P(H_I)+(1-\psi)P(H_B)}{P(H_I)} & \text{Always Free} \\ \frac{P(H_B)}{(1-\psi)P(H_I)+\psi P(H_B)} & \text{Always Busy} \end{cases} \tag{19}$$

Knowing the attack strategy, one of the above mentioned three equations is chosen to be applied in equation (18).

Multiplying the channel activity by the decision variable of WSPRT can be interpreted that the decision variable does not change; instead, the decision thresholds μ_0 and μ_1 which are also called tolerated false-alarm and the tolerated miss-detection probabilities respectively, are scrolled according to the attack.

The new WSPRT algorithm is adaptive with the attack extension factor, ψ, and is named as attack-aware WSPRT (A^{2}WSPRT). Algorithm II indicates a pseudo code for A^{2}WSPRT.

Algorithm II. A^{2}WSPRT algorithm

1) $\forall i\ ;\ \ r_i = 0$
2) $for\ each\ spectrum\ sensing\ attempt\ made\ by\ N_0\ \{$
3) $i = 0;\ \ W_n = 1$
4) $get\ a\ spectrum\ sensing\ report\ u_i\ from\ N_i$
5) $W_n \leftarrow W_n \cdot \left(\frac{P(u_i|H_1)P(H_1)}{P(u_i|H_0)P(H_0)}\right)^{f(r_i)}$
6) $if\ \mu_0 < W_n < \mu_1\ \ then:\ \ i \leftarrow (i+1)\ mod\ (m+1)$ $\quad Go\ to\ step\ 4$
7) $if\ \ W_n \geq \mu_1\ then:\ accept\ H_1 \quad (output\ u = 1)$ $\quad Go\ to\ step\ 12$
8) $if\ \ W_n \leq \mu_0\ then:\ accept\ H_0 \quad (output\ u = 0)$
9) $for\ each\ sampled\ u_i\ , set\ \ r_i \leftarrow r_i + (-1)^{u_i+u}$
10) $\}$
11) $m = \frac{1}{N}\sum_{i=1}^{n} u_i\ \ ,\ \ \sigma = \sqrt{\left(\frac{1}{N}\sum_{i=1}^{n}(u_i - m)^2\right)}$

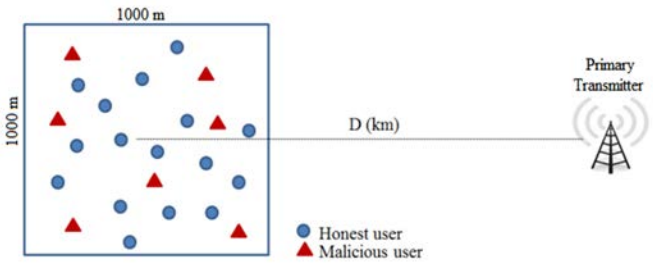

Fig. 2. Network layout.

V. SIMULATION RESULTS AND DISCUSSIONS

A. Simulation Layout

In the simulations, *N* secondary users are supposed to be mobile in the square area with dimensions 1000×1000 m^2. Assuming a 250m transmission range for CR users, a distributed network is created.

Each CR user moves according to the random waypoint mobility model within the range of the network area [23]. The decentralized cooperation scenario is utilized meaning that the SUs operate using optimal transmission parameters [24].

The maximum speed of each node in the network is 10 *m*/*s* and maximum idle time is supposed to be 120*s*. We consider the scenario that there is only one primary user with the activity ratio of 0.2 is considered *D* meter away from the center of the network area. The network model is shown in Fig. 2. All the secondary users within the coverage area of the primary user can sense the signal emitted by the primary user, and make spectrum decision by sensing data interaction with neighbor nodes [25].

The $\overline{\mathrm{PL}}(d)$ function at the equation (8) uses the HATA model which has been proposed by the IEEE802.22 standard team as a path loss for a typical CR network environment [26]. HATA model have different versions for urban and rural environments [27]. Because licensed frequency bands are rarely used in rural areas, CR networks can be implemented in a rural setting. Thus, in the simulations, a path loss model for a rural is utilized. This model is as follows:

$$\overline{\mathrm{PL}(d)} = 27.77 + 46.05\log f_c - 4.78\,(\log f_c)^2 - 13.82\log h_{te} - (1.1\log f_c - 0.7)h_{re} + (44.9 - 6.55\log h_{te})\log d \quad (20)$$

where f_c is the transmitter's signal frequency in MHz, h_{te} and h_{re} are the effective height for transmitter and receiver antennas in meters, respectively. The *d* parameter is the transmitter-receiver distance in kilometers. All items in (20) are in dB.

At the used band, the average noise power, $\overline{n_0}$, is assumed to be -106 dBm and the standard deviation of path loss model and noise is as $\sigma = \sigma_n = 11.8$. α and β for determining the threshold values (μ_0 and μ_1) are 10^{-5} and 10^{-6} respectively. The related parameter for weighting function is $g = 5$. Each node in the network acts as a spectrum sensing unit and an FC in a joint state. Distributed spectrum sensing function is done with 30*s* intervals and the whole simulation time is two hours.

It is assumed that the transmitter frequency is at UHF band with value of 617MHz. Besides, the effective heights of transmitter (ambient) and receiver (nodes) antennas are 100*m* and 1*m*, respectively. At the transmission side, the Effective Isotropic Radiated Power (EIRP) is 200mW. An energy detector with reception sensitivity of -94 dBm is assumed. This sensitivity is the least energy level which is detectable by an energy detector.

Regarding always false, always busy and always free as attack strategies, we set N = 200 and D = 3.5 Km and N_a varies from 0 to 80 at an interval of 4. We are interested to extract two metrics: correct sensing ratio and number of samples (overhead). The first metric is the number of correct final sensing decision derived by the number of total sensing decisions, the number of samples refers to the average number of samples that FC needs to collect from each CR to make a final decision, and it measures the overhead of a particular data fusion technique.

B. Simulation Results

As we mentioned earlier the always free and always busy attackers can be easily identified by FC, then we hereby implement the SD technique to estimate the attack extension factor for always false attackers. Fig. 3 depicts the five CR users' attack extension factor estimation results under always false mode, in which $\psi = 0.2$ (solid lines) and $\psi = 0.5$ (dash lines). These two sets of curves have been resulted of independent simulations. Any node in the network, calculates the ψ, solely. In this figure, it is observed that the curves of ψ converge after about 20 minutes (40 rounds). Moreover, the curves related to the set with $\psi = 0.2$, almost converge around 0.2, whereas an error is seen in the other set. This is because that in addition to the malicious nodes, factors such as AWGN noise, shadowing and path loss disrupt the spectrum sensing procedure of either honest and attacker nodes.

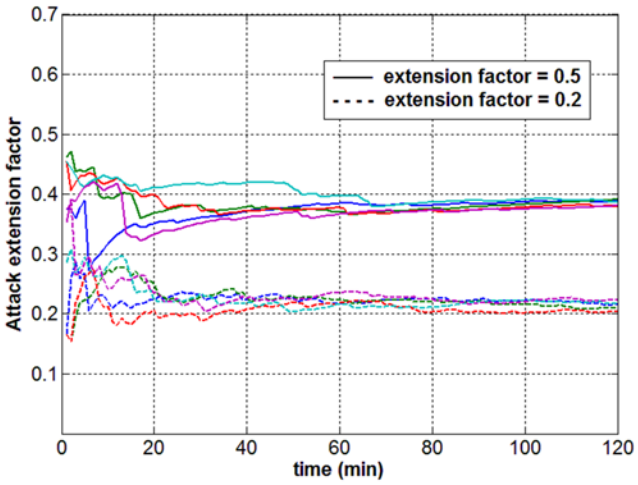

Fig. 3. Attack extension factor estimation of 5 CR users (as samples from $\mathcal{N}$); solid lines for $\psi = 0.5$ and dash lines for $\psi = 0.2$.

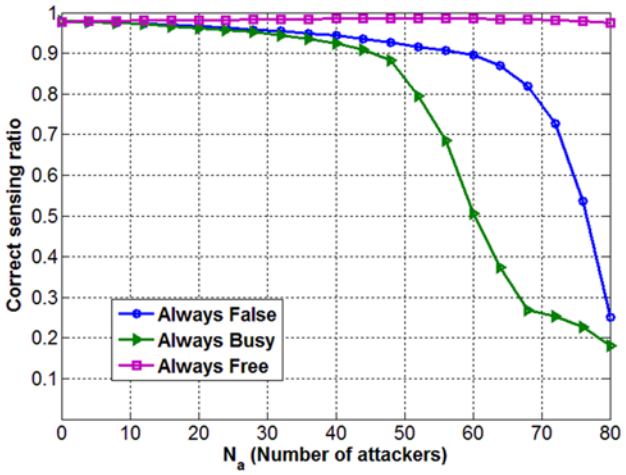

Fig. 4. Correct sensing ratio under all strategies (WSPRT).

Fig. 4 shows the correct sensing ratio versus number of attackers for WSPRT algorithm under the all three SSDF attack strategies. According these results, the WSPRT almost has resulted the smooth curve under always free mode. So, it is not needed to implement the A^{2}WSPRT under always free attack. But in always busy and always false, correct sensing curve is descending and has fallen after about $N_a = 40$ and $N_a = 60$, respectively.

In Fig. 5 the correct sensing ratio for A^{2}WSPRT and WSPRT algorithms are illustrated under always false mode. Fig. 6 shows the number of samples for A^{2}WSPRT and WSPRT under always false mode. Also, Fig. 7 and Fig. 8 compare the results of WSPRT and A^{2}WSPRT algorithms from the correct sensing ratio and number of samples perspectives under always busy mode, respectively.

As seen, the A^{2}WSPRT possesses extremely encouraging performance compared with WSPRT. According to the fact that the less the number of samples is, the overhead of the algorithm is less; the A^{2}WSPRT needs fewer number of samples than WSPRT.

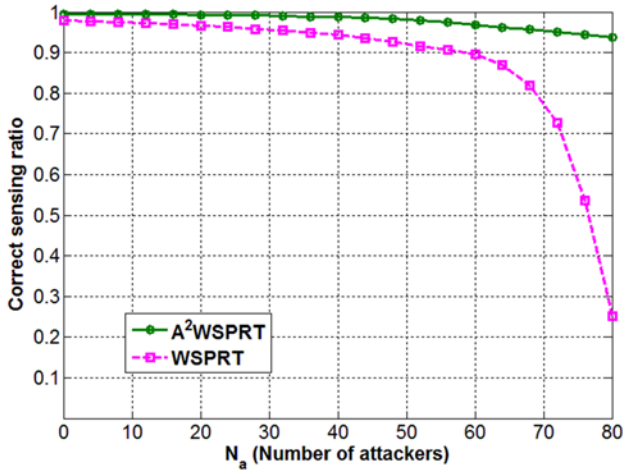

Fig. 5. Correct sensing ratio under always false mode (A^2WSPRT and WSPRT).

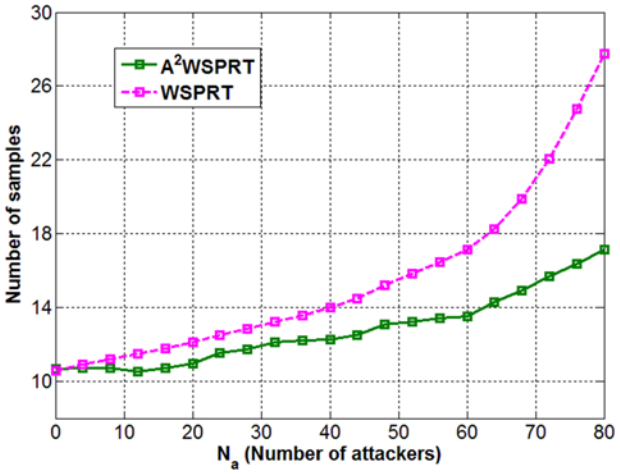

Fig. 6. Number of samples under always false mode (A^2WSPRT and WSPRT).

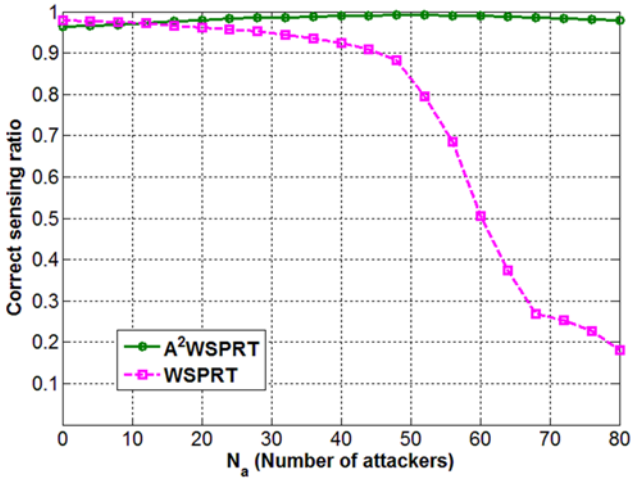

Fig. 7. Correct sensing ratio under always busy mode (A^2WSPRT and WSPRT).

In general, the A^2WSPRT has appropriate performance compared with WSPRT both in correct sensing ratio and the number of samples. This is because that in WSPRT, there is no feedback from

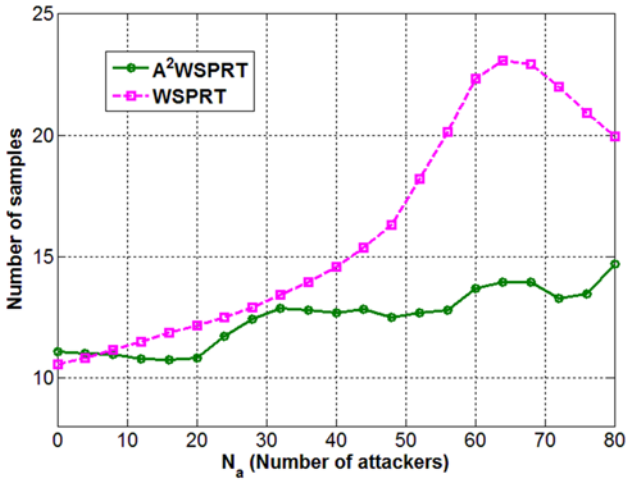

Fig. 8. Number of samples under always busy mode (A^{2}WSPRT and WSPRT).

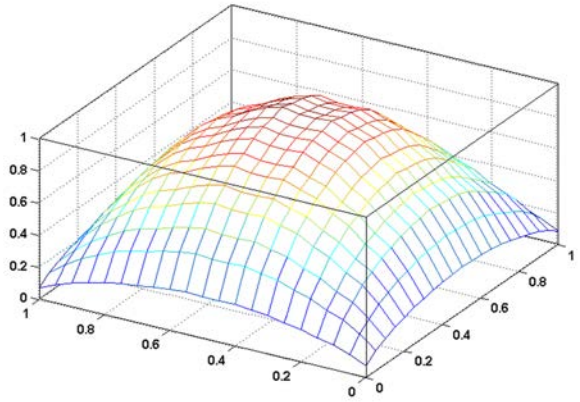

Fig. 9. Mobile nodes' normalized presence density in the square area.

the attack extension factor while in A^{2}WSPRT, the attack extension factor is extracted and usefully employed in the algorithm. Using the attack extension factor in the decision variable in A^{2}WSPRT provides a system which is adaptive to environment conditions.

To investigate the impact of velocity of nodes on the performance of system, we have estimated the nodes' presence density in our model. Fig. 9 shows the normalized presence density of mobile nodes. This graph is independent of nodes' velocity, accordingly, the speed of nodes has no impact on sensing or data fusion performance.

C. Algorithm Complexity

As mentioned, Algorithm I and Algorithm II are pseudo codes for WSPRT and A^{2}WSPRT, respectively. Both Algorithm complexities is of $O(n^2)$. But, the simulation results indicate that the mean number of samples (n) needed for A^{2}WSPRT are 1.5~2 times less than WSPRT one. Accordingly, the algorithm II takes less time than Algorithm I to run, as our simulation times validate.

VI. CONCLUSIONS

In this study, the cooperative CR networks, the SSDF attack, and WSPRT were investigated. Then, the attack-aware technique was presented. To estimate the attack extension factor in a network, a method based on the standard deviation of received sensing reports was proposed and mathematically expression was provided. To illustrate the benefits of the method, it was implemented on the WSPRT and resulted in attack-aware WSPRT (A^2WSPRT) algorithm. The simulation results are provided to indicate the high performance of attack-aware technique in detecting the attack extension factor with high accuracy and improvement of WSPRT algorithm.

REFERENCES

[1] R. Chen, J.-M. J. Park, and K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," *Computer Communications*, vol. 35, pp. 2115-2124, 2012.

[2] S. S. Moghaddam and R. J. Danaloo, "Cooperative compressed sensing for joint terminal localization and spectrum sensing," in *Signal Processing and Information Technology (ISSPIT), 2015 IEEE International Symposium on*, 2015, pp. 203-208.

[3] M. A. Abdulsattar and Z. A. Hussein, "Energy detection technique for spectrum sensing in cognitive radio: a survey," *International Journal of Computer Networks & Communications*, vol. 4, p. 223, 2012.

[4] S. Kumar, J. Sahay, G. K. Mishra, and S. Kumar, "Cognitive radio concept and challenges in dynamic spectrum access for the future generation wireless communication systems," *Wireless Personal Communications*, vol. 59, pp. 525-535, 2011.

[5] W. Wang, H. Li, Y. L. Sun, and Z. Han, "Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, p. 695750, 2009.

[6] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1876-1884.

[7] S. Maric, S. Reisenfeld, and L. Goratti, "A simple and highly effective SSDF attacks mitigation method," in *Signal Processing and Communication Systems (ICSPCS), 2016 10th International Conference on*, 2016, pp. 1-7.

[8] 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, pp. 1342-1363, 2015.

[9] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 3554-3565, 2010.

[10] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, 2009, pp. 130-134.

[11] Q. Pei, B. Yuan, L. Li, and H. Li, "A sensing and etiquette reputation-based trust management for centralized cognitive radio networks," *Neurocomputing*, vol. 101, pp. 129-138, 2013.

[12] D. Chaitanya and K. M. Chari, "Defense against PUEA and SSDF attacks in cognitive radio networks," in *Green Engineering and Technologies (IC-GET), 2016 Online International Conference on*, 2016, pp. 1-5.

[13] L. Cao, H. Zhao, J. Zhang, and Y. Liu, "Secure cooperative spectrum sensing based on energy efficiency under SSDF attack," in *Wireless Symposium (IWS), 2015 IEEE International*, 2015, pp. 1-4.

[14] 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, pp. 2127-2159, 2006.

[15] H. Chen, M. Zhou, L. Xie, and J. Li, "Cooperative Spectrum Sensing with M-ary Quantized Data in Cognitive Radio Networks under SSDF Attacks," *IEEE Transactions on Wireless Communications*, 2017.

[16] F. Zeng, J. Li, J. Xu, and J. Zhong, "A Trust-Based Cooperative Spectrum Sensing Scheme against SSDF Attack in CRNs," in *Trustcom/BigDataSE/I SPA, 2016 IEEE*, 2016, pp. 1167-1173.

[17] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, pp. 523-531, 1967.

[18] P. K. Varshney, *Distributed detection and data fusion*: Springer Science & Business Media, 2012.

[19] A. Habibzadeh and S. S. Moghaddam, "Noise calibrated GLRT-based spectrum sensing algorithm for cognitive radio applications," in *Signal Processing and Information Technology (ISSPIT), 2015 IEEE International Symposium on*, 2015, pp. 174-179.

[20] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Transactions on mobile computing*, vol. 13, pp. 1707-1719, 2014.

[21] L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang, "Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, p. 81, 2014.

[22] Z. Chair and P. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Transactions on Aerospace and Electronic Systems*, pp. 98-101, 1986.

[23] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Transactions on mobile computing*, vol. 2, pp. 257-269, 2003.

[24] L. Gavrilovska and V. Atanasovski, "Spectrum sensing framework for cognitive radio networks," *Wireless Personal Communications*, vol. 59, pp. 447-469, 2011.

[25] Q. Pei, H. Li, and X. Liu, "Neighbor Detection-Based Spectrum Sensing Algorithm in Distributed Cognitive Radio Networks," *Chinese Journal of Electronics*, vol. 26, pp. 399-406, 2017.

[26] G. Chouinard. (2005). *IEEE P802.22 Wireless RANs: Mminutes of Channel Model Subgroup Teleconference*. Available: http://www.ieee802.org/22/

[27] T. S. Rappaport, *Wireless communications: principles and practice* vol. 2: Prentice Hall PTR New Jersey, 1996.