# Secure Collaborative Spectrum Sensing for Distributed Cognitive Radio Networks

Abbas Ali Sharifi[1], Hamed Alizadeh Ghazijahani[2] and Mir Javad Musevi Niya[3]
1-Department of Electrical Engineering, Bonab Branch, Islamic Azad University, Bonab, Iran
2,3-Faculty of Electrical and computer Engineering, University of Tabriz Tabriz, Iran
Email: a.sharifi@tabrizu.ac.ir, hag@tabrizu.ac.ir, niya@tabrizu.ac.ir

Received: Feb. 2013 Revised: Oct. 2014 Accepted: Dec. 2014

**ABSTRACT:**
Spectrum sensing is a key function of Cognitive Radio (CR) networks. An accurate spectrum sensing scheme can improve spectrum utilization. But, in practice, detection performance is often degraded with multipath fading, shadowing and receiver uncertainty issues. To overcome the impact of these issues, Collaborative Spectrum Sensing (CSS) has been shown to be an effective approach to improve the detection performance by exploiting diversity. The reliability of CSS can be severely degraded by Spectrum Sensing Data Falsification (SSDF) attacks. By protecting the CR networks against SSDF attacks, Weighted Sequential Probability Ratio Test (WSPRT) has been proposed. Compared with conventional SPRT, the WSPRT improves correct sensing probability at the cost of increasing sampling overhead. In the present study, weighted majority rule is introduced and combined with the WSPRT to improve trustworthiness of collaborative spectrum sensing in the presence of SSDF attackers. Furthermore, to avoid increasing the sampling overhead, Roulette Wheel Selection (RWS) algorithm is used to collaborative node selection. The proposed method is called Developed WSPRT (DWSPRT). Simulation results show that the DWSPRT is an effective data fusion approach against SSDF attacks, especially for CR networks located in hostile environments.

**KEYWORDS:** Cognitive Radio; Collaborative Spectrum Sensing; SSDF Attack; Data Fusion

## 1. INTRODUCTION

Cognitive Radio (CR) technology has been suggested to improve the frequency spectrum utilization by authorizing unlicensed CR users to operate opportunistically in the free space of the licensed frequency bands in the presence of the licensed Primary Users (PUs) [1]. The main challenge of CR networks is the spectrum sensing with the aim of finding the vacant frequency bands [2].

Collaborative Spectrum Sensing (CSS) has been proposed to prevail over the effect of multipath fading, shadowing, and hidden station problem [3, 4]. Based on how CR users share their local sensing results, the CSS can be performed in two scenarios: centralized or distributed [5]. In centralized collaborative sensing, the CR users send either their decisions or the measured data to a Base Station (BS) or Fusion Center (FC) via Common Control Channel (CCC). In contrast, distributed collaborative sensing does not require any FC for decision-making. Each CR user collects the sensing reports from its neighbors and decides exclusively [6], [7]. When the CR user sends one-bit decision, the procedure is called hard decision combining and when the user sends the measured data, it is called soft decision combining scheme. The performance of hard decision and soft decision is investigated in [8], [9].

Unfortunately, the CSS is vulnerable to Spectrum Sensing Data Falsification (SSDF) attacks [10]. In a SSDF attack, the malicious CR user intentionally sends a falsified local sensing result to the FC in an attempt to cause the FC to make incorrect global decision [10]. To mitigate the problem of SSDF attack, many approaches have been proposed.

A new scheme to countermeasure the SSDF attack in CSS, called Conjugate Prior-based (CoP) is proposed in [11]. The scheme treats the sensing reports as samples of a random variable and reconstructs the probability density of the random variable using a technique known as conjugate prior, and then each sensing report is examined for the normality based on a confidence interval. Once a sensing report is judged as abnormal, this sensing report would be removed from decision-making process at the FC.

The authors in [12] proposed an Adaptive Reputation based Clustering (ARC) against both independent and collaborative SSDF attack. They illustrate that their work requires neither the number of attackers nor attack strategies. They also compare the performance of their algorithm with that of the algorithm proposed in [13] under different attacking strategies.

A hybrid method called Weighted Sequential Probability Ratio Test (WSPRT) is presented in [14], [15]. The WSPRT calculates the node's reputation and

uses Sequential Probability Ratio Test (SPRT) to identify malicious users. Compared with SPRT, the WSPRT improves correct sensing probability at the cost of increasing sampling overhead. In [15] a priori probability that SPRT method requires, is calculated based on the log-normal shadowing path loss model, and the calculation method utilizes the physical location of a sensing terminal. Thus, when a sensing terminal moves to a different location, a priori probability can be immediately calculated without waiting to collect new empirical data. The WSPRT is also developed in [16] for a centralized CR network and a novel fusion scheme based on spatial correlation technique is proposed. The authors utilize geographical information with reputational weights to define a two level FC for secure collaborative sensing.

Although the WSPRT is a useful technique against SSDF attacks but it has two following disadvantages: the first disadvantage of the WSPRT is that when the decision statistic is suspended between two threshold and has not reached to any of the threshold values, the spectrum sensing time is expanded, this condition occurs more and more by increasing the number of attackers. The second disadvantage of the WSPRT is that the sampling overhead is significantly large.

In this study, to mitigate the expansion of sensing time in the WSPRT, weighted majority technique, derived from conventional majority rule, is introduced and used in suspension situations. Also to prevent increasing sampling overhead, Roulette Wheel Selection (RWS) algorithm is used for cooperative node selection. The proposed approach, which is called Developed WSPRT (DWSPRT), can be used to increase the trustworthiness of collaborative spectrum sensing in the presence of SSDF attackers. We compare the performance of our method with the WSPRT [15] under different number of attackers. The proposed method counters SSDF attacks significantly better than the WSPRT and maximizes the correct sensing probability.

The rest of the paper is organized as follows. Section 2 briefly introduces collaborative spectrum sensing and system model. Section 3 presents the main contribution. Simulation results and discussions are presented in section 4. Finally, conclusion remarks are drawn in section 5.

## 2. COLLABORATIVE SPECTRUM SENSING AND SYSTEM MODEL

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 follow [3]:

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

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.

Let us assume that the probability of detection and false alarm rate of the $j^{th}$ CR user are $P_d^j$ and $P_{Fa}^j$ respectively [17, 18].

$$P_d^j = P\{x_j \geq \lambda | H_1\} \quad ; \quad P_{Fa}^j = P\{x_j > \lambda | H_0\} \quad (2)$$

Where $x_j$ is the decision statistics and represents the measured sample power/energy of $x(t)$, $\lambda$ is the local threshold that is determined by the target false-alarm probability. The probability of miss detection for the $j^{th}$ user is defined as:

$$P_m^j = 1 - P_d^j = P\{x_j < \lambda | H_1\} \quad (3)$$

Accordingly, correct sensing probability of the $j^{th}$ CR, $P_c^j$ is as follows:

$$\begin{aligned} P_c^j &= P\{x_j < \lambda | H_0\} P(H_0) + P\{x_j > \lambda | H_1\} P(H_1) \\ &= (1 - P_{Fa}^j) P(H_0) + P_d^j P(H_1) \end{aligned} \quad (4)$$

Where $P(H_0)$ and $P(H_1)$ denote the actual idle and busy rate of the channel, respectively.

The proposed system model is a distributed CR network including a PU transmitter located D kilometers away from the center of CR area, $N$ users are located in a small square area (2Km * 2Km) and move according to the Random Way Point (RWP) mobility model [19] within the range of the network area. It is assumed that among $N$ CR users, there are $N_a$ malicious users and the communication range of PU transmitter covers the whole network. The system model is shown in Fig. 1.

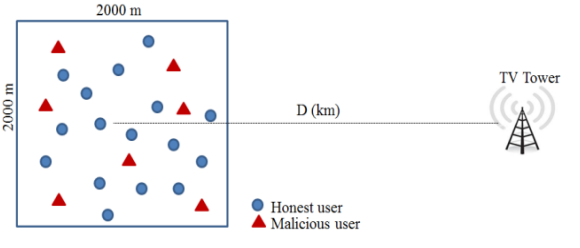


**Fig 1.** Network Layout

The local measured sample powers are compared with a predefined threshold and the comparison results are

sent to FC via CCC. In the current study, the CCC is assumed to be error free.

The received sample power $x_j$ (in dB) is obtained as follows:

$$x_j = P_t(dB) - PL(d_j) \quad (5)$$

Where $PL(d_j)$ is the log-normal shadowing path loss model and can be represented as:

$$PL(d_j) = \overline{PL(d_j)} + X_\sigma \quad (6)$$

Where $d_j$ is the distance from PU to the $j^{th}$ 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 $X_\sigma$ is a zero-mean Gaussian distributed random variable with standard deviation $\sigma_1$.

The $\overline{PL(d_j)}$ in equation (6) employs the HATA model [21], which has been proposed by the 802.22 working group as the path loss model for a typical CR network environment. The HATA model has different versions for urban and rural environments [20]. The current study used the one for rural environments since the real implementation of CR networks is likely to first occur in rural areas where licensed spectrum is less utilized. The model is given by:

$$\begin{aligned}\overline{PL(d_j)} &= 27.77 + 46.05\log f_c - 4.78(\log f_c)^2 \\ &-13.82\log h_{te} - (1.1\log f_c - 0.7)h_{re} \\ &+(44.9 - 6.55\log h_{te})\log d_j\end{aligned} \quad (7)$$

Where $f_c$ is the signal frequency, $h_{te}$ is the effective transmitter antenna height in meters, and $h_{re}$ is the effective receiver antenna height in meters, and $d_j$ is the transmitter-receiver distance in kilometers.

The conditional Probability Density Functions (PDFs) of received power $x_j$, under two hypothesis $H_0$ and $H_1$ are shown in Fig. 2, hence the values of $P_{Fa}$ and $P_m$ are depicted.

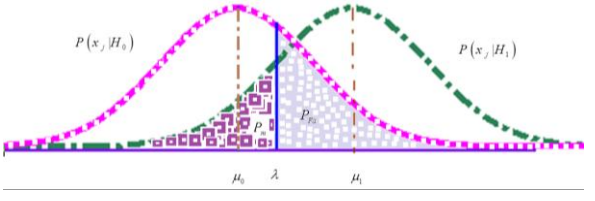


**Fig. 2.** Conditional PDFs of received power

It is assumed that the transmitted power of the PU and the location of CR users are known. Hence, the mean value of received power is known. For simplicity and without loss of generality, the standard deviation of path loss model ($\sigma_1$) and noise ($\sigma_0$) are considered the same ($\sigma_1 = \sigma_0 = \sigma$).

The values of $P_{Fa}^j$ and $P_m^j$ from equation (2) and (3) can be written as:

$$\begin{aligned}P_m^j &= 1 - P\left(x_j \geq \lambda | H_1\right) = 1 - Q\left(\frac{\lambda - \mu_1^j}{\sigma}\right) \\ P_{Fa} &= P\left(x_j > \lambda | H_0\right) = Q\left(\frac{\lambda - \mu_0}{\sigma}\right)\end{aligned} \quad (8)$$

Where $Q(.)$ is the Q-function for standard normal distribution, assuming that the mean and variance of the noise are the same among all CR users, and hence, the index $j$ is omitted from $P_{Fa}^j$.

There are several hard decision methods which can be found in: K-out-N, Bayesian detection, Neyman-Pearson (N-P), SPRT [21] and WSPRT techniques [14, 15]. In K-out-N, all of the sensing reports are summed up and compared with the threshold K, if the sum of reports is greater than K, then the channel status is determined to be occupied and $H_1$ is accepted; otherwise the band is determined to be follow and $H_0$ is accepted. A threshold value 1 is an OR fusion rule, a value N is an AND fusion rule and N/2 is a majority fusion rule. Bayesian and N-P detection are both LRT methods, but each of them has different threshold selection methods.

The LRT hypothesis testing can be expressed as:

$$\Lambda_N = \prod_{j=1}^{N} \frac{P\left(u_j | H_1\right)}{P\left(u_j | H_0\right)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta \quad (9)$$

Where $u_j$ is the binary sensing report of the $j^{th}$ user. $P\left(u_j | H_0\right)$ and $P\left(u_j | H_1\right)$ are the conditional PDFs of $u_j$ under two hypothesis $H_0$ and $H_1$ respectively. $\eta$ is the global threshold that is determined by the target false alarm or miss detection probability.

The hypothesis test step of WSPRT is based on SPRT, which is a hypothesis test for sequential analysis and supports a variable number of observations [21]. The decision variable of SPRT is defined as:

$$\Lambda_n = \prod_{j=1}^{n} \frac{P\left(u_j | H_1\right)}{P\left(u_j | H_0\right)} \quad (10)$$

Note that the number of samples $n$ is a variable and can be different from $N$. For $n \geq N$ every node contribute at least one sample.

The fusion decision is based on the following criterion:

$\Lambda_n \geq \eta_1 \Rightarrow$ accept $H_1$

$\Lambda_n \leq \eta_0 \Rightarrow$ accept $H_0$

$\eta_0 < \Lambda_n < \eta_1 \Rightarrow$ take another observation

The values of $\eta_0$ and $\eta_1$ are defined as:

$$\eta_0 = \frac{B}{1-A} \quad \text{and} \quad \eta_1 = \frac{1-B}{A}$$

Where $A$ and $B$ are the tolerated false alarm probability and the tolerated miss detection probability, respectively [21].

The WSPRT is the modified version of likelihood ratio in (10), so that the decision variable also takes a sensing terminal's reputation into consideration. The decision variable is

$$W_n = \prod_{j=1}^{n} \left( \frac{P\left(u_j \mid H_1\right)}{P\left(u_j \mid H_0\right)} \right)^{w_j} \tag{11}$$

Where $w_j$ is defined as the weight of the $j^{\text{th}}$ user and is a function of node's reputation $r_j$ which is defined as [15]

$$w_j = f\left(r_j\right) = \begin{cases} 0 & r_j \le -g \\ \dfrac{r_j + g}{\max\left(r_j\right) + g} & r_j > -g \end{cases} \tag{12}$$

Where the variable $g\,(>0)$ is used to meet the requirement of ensuring that enough weight is allocated to a sensing terminal. The reputation value of each CR user is set to zero at the beginning; whenever its local spectrum sensing report is consistent with the final sensing decision, its reputation is incremented by one; otherwise it is decremented by one. Assuming the final decision is $U$, then $r_j$ is updated according to the following relation:

$$r_j \leftarrow r_j + (-1)^{u_j + U}$$

The advantage of the WSPRT is that the calculation method utilizes the physical location of a sensing terminal. Thus, when a sensing terminal moves to a different location, a priori probabilities can be immediately calculated without waiting to collect new empirical data.

Despite this capability, the WSPRT has two following disadvantages:

The first disadvantage of the WSPRT is that when the decision statistic $W_n$ is suspended between two threshold and has not reached to any of the threshold values, the spectrum sensing time is expanded, this condition can occurs for the following three reasons:

- First, due to multipath fading, shadowing and hidden station problem, the received power signal is neither weak nor strong that makes $W_n$ placed between two threshold values $\mu_0$ and $\mu_1$.
- Second, the practical environment for distributed networks is mobile and with regarding to the limited transmission range of each CR users; some users have less number of neighbors and with sampling of these neighbors, $W_n$ will not reach the threshold values.
- Third, for some nodes, in many cases, more malicious nodes are neighbors and they make the decision statistic $W_n$ regularly experiences large and small. After polling from all neighbors, $W_n$ is suspended.

Fig. 3 shows nodes distribution in a typical CR mobile Ad-Hoc network with some nodes having enough trustful neighbors and others with less trustful neighbors.

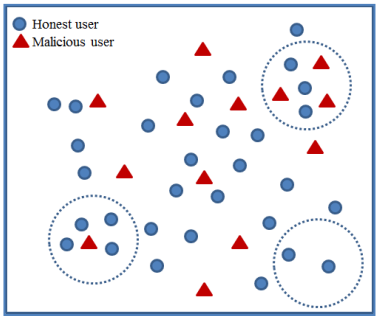


**Fig. 3**. A snapshot of nodes distribution in a typical network with Random Way-Point mobility

The second drawback of the WSPRT is that although this method is a reputation-based mechanism, but the sampling (polling) process is completely uniform random and has no priority in node selection. With the proper policy, the chance of high reputation nodes can be increased for selection and sampling overhead will be decreased, however, in this case, the nodes must be able to identify their neighbors.

## 3. DEVELOPED WSPRT (DWSPRT)

The procedure of the proposed algorithm is described by the following two different algorithms.

### 3.1. Weighted majority rule

In the WSPRT approaches, the decision statistic in some cases remain pending and it doesn't reach none of the threshold values, this situation is more experienced by increasing the number of attackers. It seems, in this case, due to conservative policy, the final report of the channel will be set busy to avoid interference to PU. However, this method increases the amount of false-alarm rate. Thus, weighted majority rule is introduced and is used in suspended situation. In the weighted majority rule, the local decision of each node based on the presence or absence of PU is as follow:

$$S_n^{'} = \sum_{j=0}^{N} w_j (-1)^{1+u_j} \tag{13}$$

The value $S_n^{'}$ is compared with the predefined threshold $c$ and final decision is made as follows:

$$S_n^{'} \underset{H_0}{\overset{H_1}{\gtrless}} c \quad (14)$$

It should be noted that the weighted majority algorithm has no impression on the number of samples, because it is used when the sampling is done from all of the neighbors.

### 3.2. Roulette Wheel Selection (RWS) algorithm

In the WSPRT method, user node selection for gathering the spectrum sensing results is uniform random and has no priority, while the high reputation nodes would have a greater chance for selection. The simplest selection scheme is RWS algorithm; however, each node must identify its neighbors. The RWS is a stochastic algorithm and involves the following technique:

The individuals are mapped to contiguous segments of a line, such that each individual's segment is equal in size to its fitness (weight). A random number is generated and the individual whose segment spans the random number is selected. The process is repeated until the desired number of individuals is obtained (called mating population). This technique is analogous to a roulette wheel with each slice proportional in size to the fitness. For selecting the mating population the appropriate number of uniformly distributed random numbers (uniform distributed between 0 and 1) is independently generated.

In order to explain the proposed method in a clear way, the process flow of the proposed DWSPRT approach is illustrated in Fig 4, where $n_{nbr}$ is the number of CR nodes in the neighborhood of the FC.

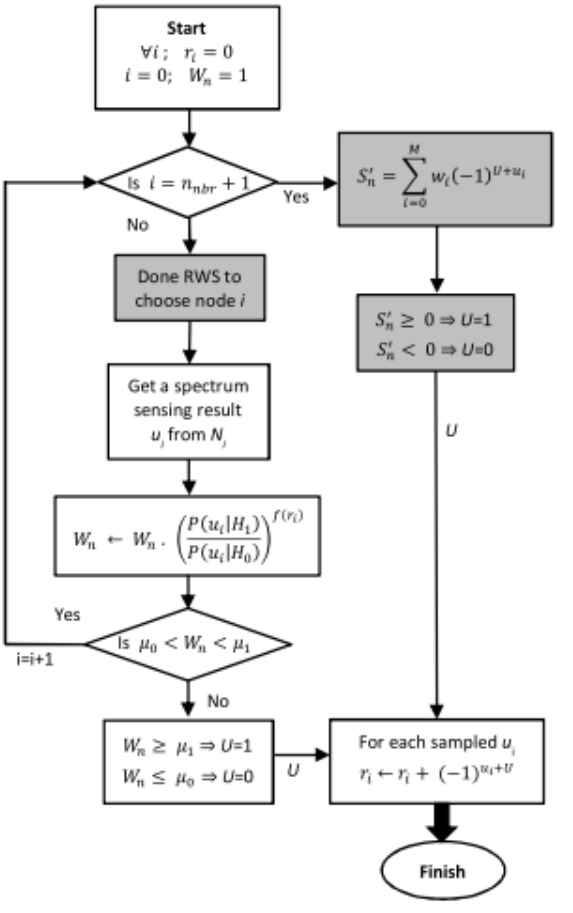


**Fig. 4**. Procedure of the proposed DWSPRT approach

## 4. SIMULATION RESULTS AND DISCUSSIONS

In the simulations, assuming a 250m transmission range for CR users, a distributed network is created. The maximum speed of each node in the network is 10 m/s and maximum idle time is supposed to be 120s. A PU transmitter, TV tower with the activity ratio of 0.2 is considered *D* meter away from the center of the network.

The 3D view of the normalized node distribution density is shown in Fig. 5 which outcomes from the simulation of random waypoint model. This figure shows that the nodes presence probability in the square area of the network has dome outward. In the network, the density of nodes in the center of area is more than that of borders. This phenomenon would provoke the already mentioned problem of suspension situation.

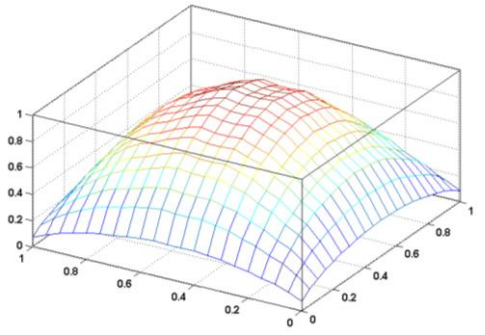

**Fig. 5.** 3D view of nodes distribution density in the network area

In the simulations, the SSDF attackers get two strategies. The attackers that send wrong reports of their sensing results are called as always-false attackers. Another one is always-free attackers; such that they always send the channel is free. We have simulated the DWSPRT approach under both attacks.

The average noise power, $\overline{n_0}$, is assumed to be -106 dBm and the standard deviation of path loss model and noise is considered as the same as $\sigma = \sigma_n = 11.8$. $A$ and B for determining the threshold values ($\mu_0$ and $\mu_1$) are $10^{-5}$ and $10^{-6}$ respectively. The parameter $g$ is also set as 5. Each node in the network, acts both as a spectrum sensing unit and FC. Distributed spectrum sensing function is done with 30s intervals and the whole simulation time is two hours.

It is assumed that the transmitter frequency is at UHF band with value of 617MHz. Also the effective heights of transmitter and receiver antennas are 100m and 1m, respectively. At the transmission side, the Effective Isotropic Radiated Power (EIRP) is 100kW. 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.

We fix $N = 500$ and $D = 60\ Km$, while changing attack types and varying $N_a$ from 0 to 160 at an interval of 20. The distance of 60 Km is well beyond the grade B service counter of TV reception [4]. The threshold value of weighted majority $c$ is selected as zero. We are interested in 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.

In figure 6, the simulation results of WSPRT and the proposed DWSPRT, in the presence of always false attackers, are presented. As shown in the figure, WSPRT experiences a greater magnitude decrease than DWSPRT. In DWSPRT, using the weighted majority rule, in suspension situations, causes the better correct sensing ratio.

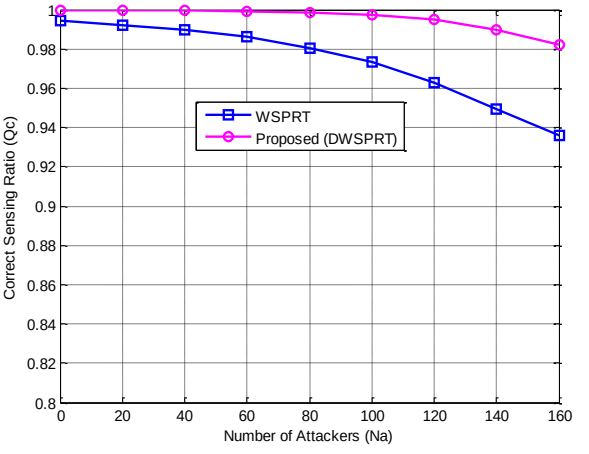


**Fig. 6.** The performance of WSPRT and DWSPRT against always-false SSDF attacks.

Figure 7 shows the number of samples which are needed for decision fusion with WSPRT and the proposed DWSPRT. Always-false malicious attackers are considered in the simulation. As depicted in the figure, the number of samples for DWSPRT is less than that of WSPRT. We obtained it as the fact that in DWSPRT due to using RWS algorithm, high reputation nodes have a greater chance of selection in cooperative spectrum sensing. Thus, the decision statistic quickly reaches the threshold values and consequently the number of samples (overhead) is significantly decreased. Figures 8 and 9 also depict the similar results for always-free SSDF attacks.

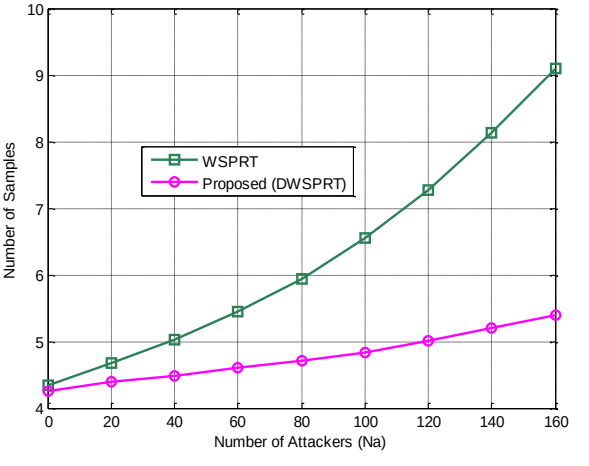


**Fig. 7.** The performance of WSPRT and DWSPRT against always-false SSDF attack

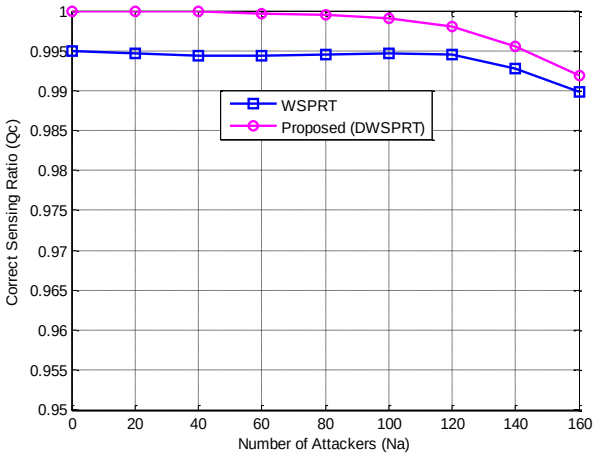


**Fig. 8.** The performance of WSPRT and DWSPRT against always-free SSDF attacks.

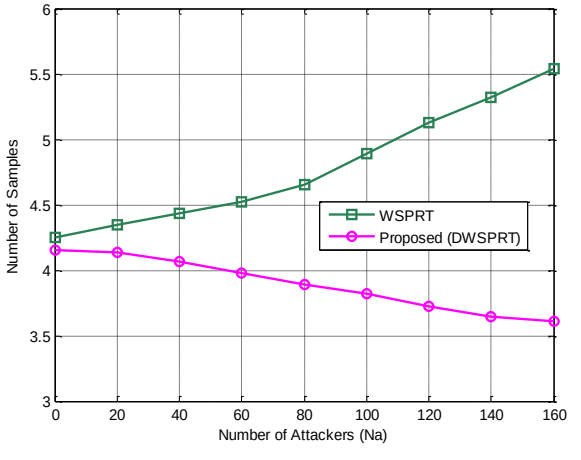


**Fig. 9.** The performance of WSPRT and DWSPRT against always-free SSDF attacks.

## 5. CONCLUSIONS AND FUTURE WORKS

In this study, distributed spectrum sensing in CR networks was investigated, also the reason that most data fusion schemes in collaborative spectrum sensing are vulnerable to Spectrum Sensing Data Falsification (SSDF) attack, was discussed. Weighted Sequential Probability Ratio Test (WSPRT) was developed and demonstrated that the proposed method, Developed WSPRT (DWSPRT), is a robust defense strategy against SSDF attacks. Simulation results supported our expectation and showed that sampling overhead can be reduced and correct sensing ratio can be increased.

As part of our on-going work, we plan to study an analytical model for probability of suspension and weighted majority rule in DWSPRT technique.

## 6. ACKNOWLEDGMENT

The authors would like to acknowledge the Bonab Islamic Azad University (BIAU) for supporting this work by allocating a research grant.

## REFERENCES

[1] J. Mitola III, G. Q. Maguire, "**Cognitive radio: making software radios more personal**," *IEEE Pers. Commun.*, Vol. 6, pp. 13-18, Aug. 1999.

[2] S. Haykin, "**Cognitive radio: brain-empowered wireless communications**," *IEEE J. Selected Areas in Communications*, Vol. 23, pp. 201–220, Feb. 2005.

[3] I. F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty, "**NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey**," *Computer Networks*, pp. 2127–2159, 2006.

[4] S. Mishra, A. Sahai, and R. Brodersen, "**Cooperative sensing among cognitive radios**," *in Proc. IEEE Int. Conf. Commun*, Vol. 2, pp. 1658–1663, May 2006.

[5] I. F. Akyildiz, B. F. Lo, R. Balakrishnan, "**Cooperative spectrum sensing in cognitive radio networks: A survey**," *Physical Communication*, Vol. 4, pp. 40-62, 2011.

[6] G. Ganesan, Y. Li, "**Cooperative spectrum sensing in cognitive radio, part I: two user networks**," *IEEE Transactions on wireless communications*, Vol. 6, pp. 2204-2212, 2007.

[7] G. Ganesan, Y. Li, "**Cooperative spectrum sensing in cognitive radio, part II: multiuser networks**," *IEEE Transactions on wireless communications*, Vol. 6, pp. 2214-2222, 2007.

[8] A. Ghasemi, E. S. Sousa, "**Collaborative spectrum sensing for opportunistic access in fading environments**," In *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks* (DySPAN), Vol. 2, pp. 131-136, 2005.

[9] A. Ghasemi and E. S. Sousa, "**Opportunistic spectrum access in fading channels through collaborative sensing**," *Journal Commun*, Vol. 2, pp. 71-82, 2007.

[10] R. Chen, J. M. Park, Y. T. Hou, J. H. Reed, "**Toward secure distributed spectrum sensing in cognitive radio networks**," *IEEE Communications Magazine*, Vol. 46, pp. 50-55, 2008.

[11] 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*, Vol. 20, pp. 2521-2528, 2014.

[12] C. H. Hyder, B. Grebur, L. Xiao, M. Ellison, "**ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks**," *IEEE Transactions on mobile computing*, Vol. 13, pp. 1707-1719, 2014.

[13] A. S. Rawat, P. Anand, H. Chen, P. K. Varshney, "**Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks**," *IEEE Transactions on Signal Processing*, Vol. 59, pp. 774-786, 2011.

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

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

[16] 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, pp. 667-677, 2012.

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

[18] F. F. Digham, M. S. Alouini, M. K. Simon, "**On the energy detection of unknown signals over fading channels**," *IEEE Transaction on Communications*, Vol. 55, pp. 21-24, 2007.

[19] C. Bettstetter, G. Resta, P. Santi, "**The node distribution of the random waypoint mobility model for wireless ad hoc networks**," *IEEE Trans. Mobile Comput*, Vol. 2, 2003.

[20] T. S. Rappaport, "**Wireless Communications: Principle and Practice**," *Prentice Hall*, 1996.

[21] P. K. Varshney, "**Distributed Detection and Data Fusion**," *Springer-Verlag, New York*, 1997.