An Efficient Collaborative Spectrum Sensing Method in Cognitive Radio Networks: Software-Defined Data Fusion Approach

Hamed Alizadeh Ghazijahani[1] and Abbas Ali Sharifi[2]
1- Department of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran.
Email: hag@tabrizu.ac.ir
2- Department of Electrical Engineering, University of Bonab, Bonab, Iran.
Email: sharifi@bonabu.ac.ir (Corresponding author)

Received: September 2018 Revised: October 2018 Accepted: November 2018

ABSTRACT:
Cognitive Radio (CR) technology has been suggested as a solution to the serious problem of spectrum scarcity in recent years. Cooperative Spectrum Sensing (CSS) is the key function to overcome the destructive effect of hidden station, multipath fading and shadowing problems. As many previous studies have shown, the trustworthiness of the CSS can be strictly degraded under Spectrum Sensing Data Falsification (SSDF) attack. In this paper, we introduce an important dynamic fusion rule called Software-Defined CSS (SD-CSS). The main contribution is to analyze the SSDF attack strategy against the CR network and apply the best fusion rule to increase the cooperative sensing performance. Two important SSDF attack parameters, attack strategy and attack ratio, are estimated and the obtained parameters are then used to choose an appropriate fusion rule to improve the CSS performance. The obtained results confirm considerable improvement in correct sensing ratio in massive attack.

KEYWORDS: Cognitive Radio (CR), Cooperative Spectrum Sensing (CSS), Software-Defined (SD), SSDF Attack.

1. INTRODUCTION

Cognitive Radio (CR) is one of the powerful technologies to improve the spectrum scarcity issue. The main objective of the CR technology is a proper handling of the available spectrum resources [1], [2]. In this technology, each CR user, which is also called as secondary user, performs spectrum sensing to sense its surrounding area and opportunistically utilizes the vacant frequency bands. By the activity of Primary User (PU), the CR user should immediately leave the spectrum and search another vacant spectrum. Therefore, the continuous sensing of the wireless environment is an essential task for the CR users. Several spectrum sensing techniques were explored by researchers, but energy detection is a useful and simple method used in most studies [1], [3].

The CR networks usually suffer from some serious problems, such as: fading, shadowing, and hidden station. When the CR user experiences one or more of these problems, it may fail to detect the presence of licensed PU signal. Thus, miss detection probability may be increased and consequently unwanted interference with the PU signal may be occurred [4]. To overcome this condition, many researchers have been introduced to the idea of Cooperative Spectrum Sensing (CSS). In CSS process, all of CR users report their spectrum sensing results to a base station or Fusion Center (FC) and the FC combines the received sensing reports to make a final sensing decision. The decision-making operation is categorized into hard-decision and soft-decision combining schemes. In hard-decision combining, the CR users send their local spectrum sensing results to the FC with one binary bit as 0 (idle) or 1 (busy), but in soft-decision scheme, the CR users send their measured energy/power from the PU signal.

During the CSS procedure, the CR network may experience the occurrence of Spectrum Sensing Data Falsification (SSDF) attack [1], [3-5]. In a SSDF attack, some malicious CR users intentionally send falsified local sensing results to the FC and attempt to corrupt the global sensing decision [6]. This particular type of attack, causes interference between PU signals and CR users or makes a non-optimal usage of available spectrum resources and consequently the cooperative sensing performance is degraded. There are some works that alleviate the impact of the SSDF attack. For instance, in [7] and [8] the cooperative CR users are divided into two categories: honest and malicious. Then, the authors try to assign a suspicious factor to each user to determine the trust value for each CR based on the

past history of its sensing reports' accuracy. When the suspicious factor of a CR user goes beyond a predefined threshold, it will be considered as a malicious and its future reports will be omitted. In [4], the authors also take a similar procedure like [7] and [8]; but their approach does not require any prior knowledge of the attackers. Their idea is to set the report history of each SU in a high-dimensional vector and detect the possible outliers. In [9], users' reputation is calculated and used to increase the performance of the cooperative sensing. In addition, the obtained reputation is utilized to measure the performance of the CR users in the spectrum sensing process.

In order to improve the correctness of spectrum sensing, we take attack parameters into account while gathering the sensing information. In this study, a novel dynamic data fusion approach called Software-Defined CSS (SD-CSS) is presented where the objective is to analyze the SSDF attack parameters, attack strategy and attack ratio (attack extension factor), to increase the cooperative sensing performance. The main contribution is to utilize an appropriate fusion rule with different attack scenarios under different attack ratios. The proposed SD-CSS method detects the attack strategy and estimates the attack ratio and chooses the best fitting fusion algorithm. Weighted Sequential Probability Ratio Test (WSPRT) is investigated for data fusion task and, according to the attack characteristics, a simple fusion task such as AND rule is also employed and compared with the WSPRT method.

The rest of the paper is organized as follows. Section 2 presents a brief background on the cooperative sensing and SSDF attack. The WSPRT algorithm is described in section 3. Section 4 presents the proposed SD-CSS approach. Simulation results and discussions are provided in section 5. Finally, conclusion remarks are obtained in section 6.

2. COOPERATIVE SPECTRUM SENSING (CSS) AND SSDF ATTACK

Spectrum sensing is a key function of CR networks. If the spectrum sensing process is done carefully, it prevents CR network interference from PU signals. The PU signal detection can be formulated as a binary hypothesis testing problem as follows [10-12]:

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

The null hypothesis H_0 indicates that only noise is present and hypothesis H_1 states that both PU signal and noise are present. The parameter X is the CR user's received signal, S is the PU's transmitted signal, h is the gain of the sensing channel, and n is the Gaussian noise. Two important parameters, probabilities of detection p_d^j and false alarm p_{fa}^j for the j th CR user, are used to evaluate the sensing performance. These parameters can be written as [13]:

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

Where X_j represents the received power of the j th CR user, λ is the local threshold and determined by the Constant False Alarm Rate (CFAR). The accuracy of the local sensing detection for the j th user is characterized by a local correct sensing probability, defined as follows:

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

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

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

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

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

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

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_σ is a zero-mean Gaussian distributed random variable with standard deviation σ_1. The parameter $\overline{PL(d_j)}$ can be found using HATA model [14] which has been proposed 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 for a rural environment is given by [15]:

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

Where f_c is the carrier frequency, h_{te} and h_{re} are the effective transmitter and receiver antenna heights in meters, 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 away from the CR network, thus, differences due to path loss are negligible and the average received power μ_1 is the same for all CR users. The mean and variance of the noise are also the same among all CR users.

When hypothesis H_0 holds, the received power of each user is a Gaussian noise power with mean μ_0 and standard deviation σ_0. Therefore, $X_j(dB)$ is expressed as a Gaussian distributed and the conditional Probability Density Functions (PDFs) of received power X_j, under two hypothesis H_0 and H_1 are shown in figure 1, hence the false alarm and miss detection probabilities are depicted.

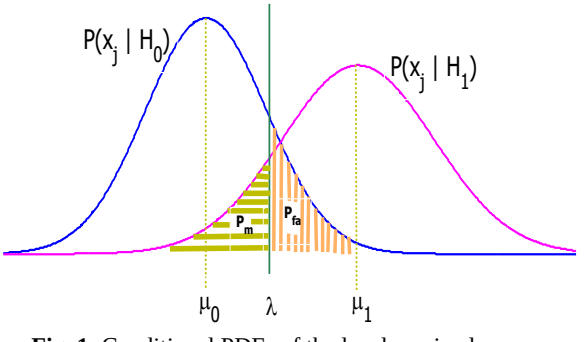

Fig. 1: Conditional PDFs of the local received power.

The values of p_d^j and p_{fa}^j from equation (2) can be written as:

$$p_d^j = p(X_j > \lambda | H_1) = Q(\frac{\lambda - \mu_1}{\sigma_1})$$
$$p_{fa}^j = p(X_j > \lambda | H_0) = Q(\frac{\lambda - \mu_0}{\sigma_0}) \quad (7)$$

Where $Q(.)$ is the Q-function for standard normal distribution.

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

In the presence of the SSDF attack, some malicious users intentionally send falsified local spectrum sensing reports to the FC in an attempt to cause the FC to make incorrect global sensing decisions. There are three typical SSDF attackers. The Always Yes (AY) attackers always report presence of the PU signal. In this case, the probability of false alarm is increased and the spectrum resource is wasted. The Always No (AN) malicious users always send a local decision saying that "the channel is empty"; hence, the FC may be deceived and allow CR users to access the channel while in fact the PU signal is present. The Always False (AF) attackers send opposite values of their sensing results to the FC. Therefore, they always cause that the FC make an incorrect sensing decision. Under AF attacks, both spectrum waste and PU interference are occurred. The proposed network model is shown in figure 2.

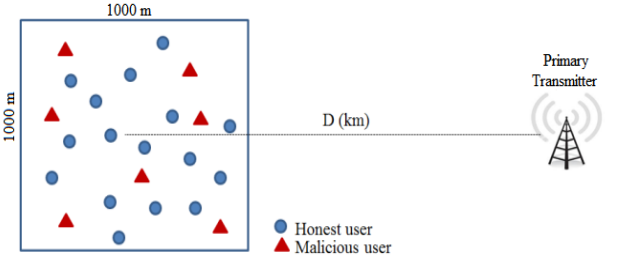

Fig. 2: Network Model.

Please use automatic hyphenation and check your spelling. Additionally, be sure your sentences are complete and that there is continuity within your paragraphs. Check the numbering of your graphics and make sure that all appropriate references are included.

3. WSPRT FUSION TECHNIQUE

The WSPRT approach is an important fusion algorithm which has been introduced by R. Chen et al [1], [16] to reduce the effect of SSDF attacks on CR networks. The WSPRT includes two steps. The first step is a reputation calculation and the second step is the actual hypothesis test. A sensing terminal's reputation rating is allocated based on the accuracy of its prior sensing results. The reputation value of each CR user, r_j, is set to zero at the beginning; whenever its local spectrum sensing report u_j, is consistent with the final sensing decision U, its reputation is incremented by one; otherwise it is decremented by one. The reputation of the j th CR user is updated according to the following relation:

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

The hypothesis test of WSPRT is based on Sequential Probability Ratio Test (SPRT). The SPRT technique is a hypothesis test for sequential analysis and supports sampling a variable number of observations [17]. The decision variable also takes a sensing terminal's reputation into consideration.

$$S_k = \prod_{j=0}^{k} \left(\frac{p(u_j \mid H_1)}{p(u_j \mid H_0)} \right)^{w_j} \tag{8}$$

Where k is the number of samples and w_j is a function of r_j ($w_j = f(r_j)$) as follows:

$$w_j = f(r_i) = \begin{cases} 0 & r_i \le -g \\ \dfrac{r_i + g}{\max(r_i) + g} & r_i > -g \end{cases} \tag{9}$$

Where, the variable g (> 0) is used to ensure that an enough weight is allocated to each user.

All the above-mentioned schemes need the same knowledge of a prior probabilities i.e., $p(u_j \mid H_1)$ and $p(u_j \mid H_0)$. These values can be obtained by the following equations:

$$\begin{aligned} p(u_j = 1 \mid H_1) &= p_d^j = p(X_j > \lambda \mid H_1) = Q\left(\frac{\lambda - \mu_1}{\sigma_1}\right) \\ p(u_j = 1 \mid H_0) &= p_{fa}^j = p(X_j > \lambda \mid H_0) = Q\left(\frac{\lambda - \mu_0}{\sigma_0}\right) \end{aligned} \tag{10}$$

The fusion decision is based on the following criterion:

$$\begin{aligned} &S_k > \mu_1 \Rightarrow \text{accept } H_1 \\ &S_k < \mu_0 \Rightarrow \text{accept } H_0 \\ &\mu_0 \le S_k \le \mu_1 \Rightarrow \text{take another observation} \end{aligned}$$

The values of μ_0 and μ_1 are decided by:

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

Where α and β are the tolerated false alarm and miss detection probabilities, respectively. The WSPRT 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 meets either of two bounds.

4. THE PROPOSED SOFTWARE-DEFINED CSS (SD-CSS)

In the proposed SD-CSS approach, the FC dynamically changes its fusion rule based on the estimated SSDF attack parameters. The suggested scheme continuously monitors the surrounding area to estimate the SSDF attack strategy and its extension factor in the network. Regarding to the performance of the method under different types of SSDF attacks (AY, AN, and AF) and attack ratio (extension factor), alternative data fusion method is temporally utilized. This method should be as simple as possible to start to work promptly without prior experience of the network.

Analysis of the SSDF attack is composed of two stages: detection of attack strategy and estimation of attack ratio. In the cases of AY and AN attackers, by counting the CR users that report a constant value of sensing results, it is convenient to determine the strategy and attack ratio. Obviously, in the case of AF attackers, the percentage of malicious attackers cannot be easily determined. In this case, to estimate the attack extension factor, a solution based on the Standard Deviation (SD) of received sensing reports is innovatively introduced.

It is assumed that the AF attack occurs against the CR network and the percentage of attackers is ψ (attack ratio). It can be interpreted that a specific CR user (can be honest or malicious) changes its sensing result with probability ψ [18], [19]. 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 cooperative nodes report that the channel is idle (0 is reported) and ψ% of reports indicate that the channel is busy (1 is reported). The mean and SD values of received reports in idle state are as follows:

$$m_I = \frac{1}{N}\sum_{i=1}^{m} u_i = \psi \times 1 + (1-\psi) \times 0 = \psi \tag{11}$$

$$\sigma_I = \left(\frac{1}{N}\sum_{i=1}^{m} (u_i - m_I)^2 \right)^{1/2} = \sqrt{\psi - \psi^2} \tag{12}$$

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

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

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

As obtained from the above equations, the mean

values of reports in idle and busy states are different, while the SD values are the same. Thus, the attack extension factor ψ can be obtained by computing the SD value of the received reports.

5. SIMULATION RESULTS AND DISCUSSIONS

In the simulations, N=200 CR users are assumed to be mobile in the square area with dimensions 1000×1000 m^2. Assuming a 250m transmission range for each CR user, a distributed network is created. Each user moves according to the random waypoint mobility model within the range of the network area [20]. The decentralized cooperation scenario is utilized meaning that the SUs operate in an ad-hoc manner using optimal transmission parameters [21]. All the CR users, within the coverage area of the PU, can sense the signal emitted by the PU transmitter and make spectrum decision by sensing data interaction with neighbor nodes [22]. 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, with the activity ratio of $P(H_1)$=0.1, is considered to be D=3500 meters away from the center of the network area. The average noise power, 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. Two parameters 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 both as a spectrum sensing unit and an FC. The CSS function is done with 30s intervals and the whole simulation time is two hours. It is further assumed that the transmitter frequency is at UHF band with value of 617MHz. Besides, the effective heights of transmitter and receiver antennas are 100m and 1m, 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. In AF attack scenario, the number of attackers (N_a) varies from 0 to 100 at an interval of 4.

Fig. 3 depicts the attack factor estimation results under AF mode, in which ψ = 0.2 (solid lines) and ψ = 0.5 (dash lines). These two sets of curves are the results of independent simulations. In this figure, it is observed that the curves of ψ are converged after about 20 minutes (40 rounds of spectrum sensing). Moreover, the curves related to the ψ = 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, some other factors such as Gaussian noise, shadowing and path loss disrupt the spectrum sensing procedure of either honest or attacker nodes. Nevertheless, the result is acceptable for our work, because we need an approximation of attack extension factor.

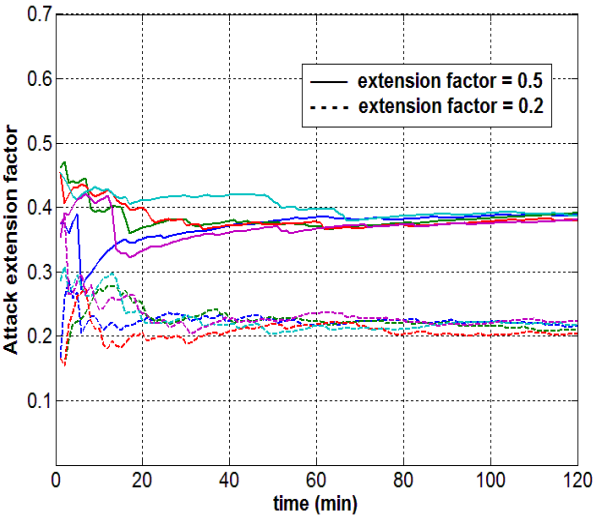

Fig. 3: Estimation of attack extension factor.

Correct sensing ratio versus number of attackers (N_a) for AF, AY, and AN attackers are shown in figures 4, 5 and 6, respectively. In Fig. 4, N_a = 50 (ψ = 0.25) is cross point of two curves and after this point the AND has better correct sensing ratio than WSPRT. The proposed method by estimating the ψ, is able to intelligently switch between WSPRT and AND methods.

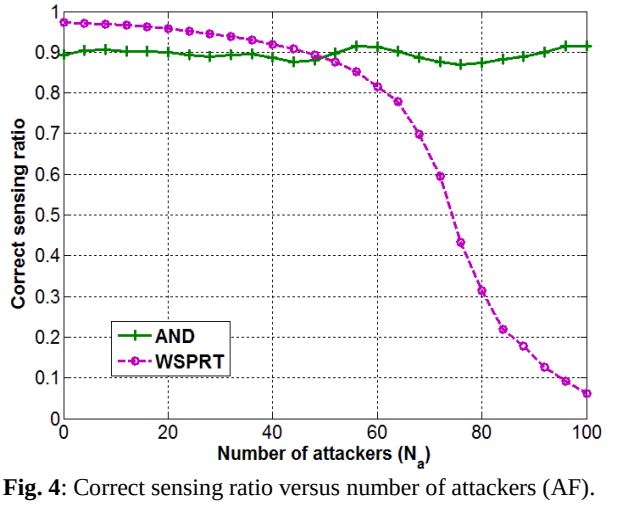

Fig. 4: Correct sensing ratio versus number of attackers (AF).

The correct sensing ratio is also obtained for AY attackers in Fig. 5 but the cross point is around N_a = 40 (ψ = 0.2). In Fig. 6, under AN attackers, the WSPRT fusion algorithm has good performance for all attack extension factors and it is not needed to switch to AND. More precisely, once the proposed method detects the AF and AY attackers, it smartly switches between WSPRT and AND fusion methods based on the estimated value of ψ.

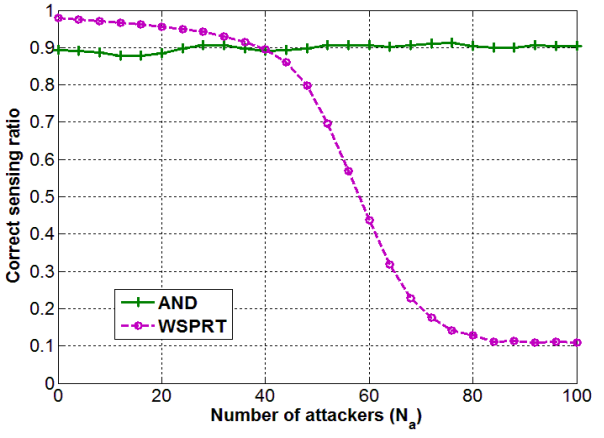

Fig. 5: Correct sensing ratio versus number of attackers (AY).

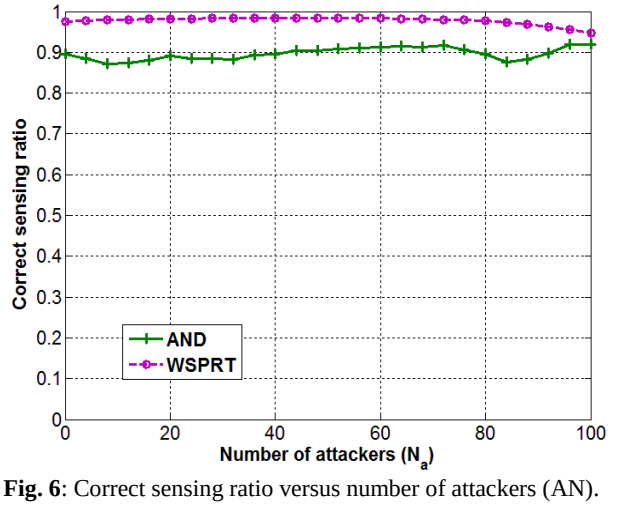

Fig. 6: Correct sensing ratio versus number of attackers (AN).

The results of the SD-CSS and WSPRT fusion methods for AF and AY attackers are shown in figures 7 and 8, respectively. The proposed method is intelligent and aware of attack strategy. Besides, another advantage of the SD-CSS is temporarily stop of CR network activity facing with massive attack to avoid destructive interference with the PU signals.

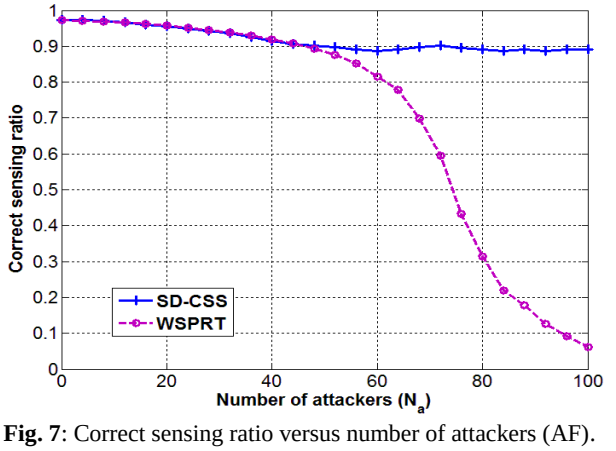

Fig. 7: Correct sensing ratio versus number of attackers (AF).

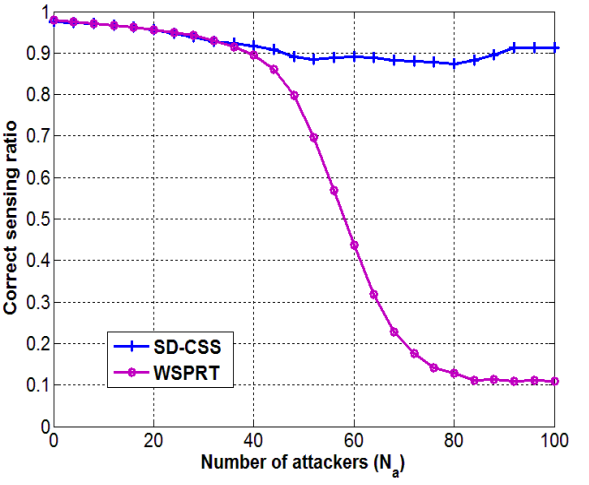

Fig. 8: Correct sensing ratio versus number of attackers (AY).

6. CONCLUSION

In order to secure the information fusion technique for CR network, the CSS, SSDF attack, and WSPRT are investigated and a new adaptive fusion rule called Software-Defined CSS (SD-CSS) technique is introduced. The SSDF attack behavior is thoroughly analyzed and attack extension factor or attack ratio is obtained. To estimate the attack ratio, a method based on the standard deviation of received sensing reports is proposed and mathematical expression is also provided. To illustrate the performance of the proposed method, it is implemented on the WSPRT as the base algorithm and AND fusion scheme as the alternative one. The simulation results are provided to illustrate the effectiveness of the proposed SD-CSS technique in correct sensing ratio. One can utilize other simple methods such as majority rule as alternative algorithm. In the future work, it is aimed to analyze the SSDF with combined attack strategies and design an appropriate SD-CSS framework for such strategies.

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] A. A. Sharifi, J. Musevi Niya, and H. Alizadeh Ghazijahani, "**Secure Collaborative Spectrum Sensing For Distributed Cognitive Radio Networks**," *Majlesi Journal of Electrical Engineering*, Vol. 9, pp. 59-66, 2015.

[3] 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.

[4] 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, pp. 695750- 2009.

[5] 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.

[6] S. Maric, S. Reisenfeld, and L. Goratti, "**A Simple And Highly Effective SSDF Attacks Mitigation Method***," in Signal Processing and Communication Systems (ICSPCS), 10th International Conference on*, pp. 1-7, 2016.

[7] 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.

[8] W. Wang, H. Li, Y. Sun, and Z. Han, "**Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks***," in Information Sciences and Systems, CISS, 43rd Annual Conference on*, pp. 130-134, 2009.

[9] 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.

[10] 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.

[11] H. Alizadeh et al. "**Attack-Aware Cooperative Spectrum Sensing in Cognitive Radio Networks under Byzantine Attack**," *Journal of Communication Engineering*, Vol. 6, pp. 81-98, 2017.

[12] 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*, Vol. 16, No. 8, pp. 5244-5257, 2017.

[13] H. Urkowitz, "**Energy Detection of Unknown Deterministic Signals**," *Proceedings of the IEEE*, Vol. 55, pp. 523-531, 1967.

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

[15] T. S. Rappaport, **"Wireless Communications",** *principles and practice*, Vol. 2: Prentice Hall PTR New Jersey, 1996.

[16] 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*. pp. 1876-1884, 2008.

[17] P. K. Varshney, **"Distributed Detection and Data Fusion"**, *Springer Science & Business Media*, 2012.

[18] 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.

[19] 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.

[20] 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.

[21] L. Gavrilovska and V. Atanasovski, "**Spectrum Sensing Framework for Cognitive Radio Networks**," *Wireless Personal Communications*, Vol. 59, pp. 447-469, 2011.

[22] 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.