Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Fuzzy-based reliable and secure cooperative spectrum sensing for the smart grid

Laila Nassef*, Reemah Alhebshi

Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

ARTICLE INFO

Article history:
Received 27 July 2020
Received in revised form
8 October 2020
Accepted 13 October 2020

Keywords:
Spectrum sensing data falsification attack
Fuzzy fusion
Reliability
Sensing reputation

ABSTRACT

Cognitive radio is a promising technology to solve the spectrum scarcity problem caused by inefficient utilization of radio spectrum bands. It allows secondary users to opportunistically access the underutilized spectrum bands assigned to licensed primary users. The local individual spectrum detection is inefficient, and cooperative spectrum sensing is employed to enhance spectrum detection accuracy. However, cooperative spectrum sensing opens up opportunities for new types of security attacks related to the cognitive cycle. One of these attacks is the spectrum sensing data falsification attack, where malicious secondary users send falsified sensing reports about spectrum availability to mislead the fusion center. This internal attack cannot be prevented using traditional cryptography mechanisms. To the best of our knowledge, none of the previous work has considered both unreliable communication environments and the spectrum sensing data falsification attack for cognitive radio based smart grid applications. This paper proposes a fuzzy inference system based on four conflicting descriptors. An attack model is formulated to determine the probability of detection for both honest and malicious secondary users. It considers four independent malicious secondary users' attacking strategies of always yes, always no, random, and opposite attacks. The performance of the proposed fuzzy fusion system is simulated and compared with the conventional fusion rules of AND, OR, Majority, and the reliable fuzzy fusion that does not consider the secondary user's sensing reputation. The results indicate that incorporating sensing reputation in the fusion center has enhanced the accuracy of spectrum detection and have prevented malicious secondary users from participating in the spectrum detection fusion.

1. Introduction

A smart grid is evolving towards a more modernized smarter grid to provide two-way communications of information and electricity to support the diverse applications (Fadel et al., 2015). Bidirectional communications are essential for monitoring and control of power generating stations, transmission lines, distribution centers, and smart homes, where Wireless Sensor Networks are impeded in every part of the smart grid (Yigit et al., 2016). Home Area Networks (HANs) consists of devices and appliances that communicate with their home controller and/or smart meter to exchange data with the utility control center. A group of smart meters in each Neighborhood Area Networks (NANs) is connected to a data collector to aggregate data to the utility for further analysis through the Wide Area Networks (WANs). These communication networks use different communication technologies in various spectrum bands, one of which is the radio frequency band. Smart grid applications require stringent demand for the spectrum to satisfy the Quality of Service (QoS) requirements of diverse applications. However, radiofrequency bands are overloaded and suffer from interference from multiple coexisting technologies. Cognitive Radio (CR) solutions provide a highly attractive communication technology to access the underutilized frequency bands. This enabling technology opens up the licensed spectrum bands to the unlicensed Secondary Users (SUs) (Toma et al., 2020). SUs are allowed to sense, observe, and learn from the environment to opportunistically access underutilized frequency

* Corresponding Author.

Email Address: lmohamed@kau.edu.sa (L. Nassef)

https://doi.org/10.21833/ijaas.2021.02.013

Corresponding author's ORCID profile:
https://orcid.org/0000-0001-9707-1259

2313-626X/© 2020 The Authors. Published by IASE.

bands of licensed Primary Users (PUs) (Akyildiz and Brandon, 2011).

The Dynamic Spectrum Access (DSA) allows reliable communication, avoids the license costs, and allows sharing of the spectrum among multiple communication networks (Akyildiz et al., 2006). In addition, SUs can also be aware of their wireless environment to reconfigure their transmission parameters to communicate over the most reliable available spectrum. These reliable communications are vital for the successful deployments of the smart grid, where failure to transmit some events to the utility or back to actuators to perform certain prescribed actions results in major operational problems (Fadel et al., 2017). CR technology can be integrated with traditional networks due to their software-based nature (Huang et al., 2020). CR enabled networks can provide substantial benefits to both the utility and service provider to deploy WSNs to perform usual functions in addition to spectrum sensing. Furthermore, the utility can deploy CR-based smart meters that communicate over the advanced metering infrastructure (Khan et al., 2017). Currently, Wireless Regional Area Network (WRAN) is proposed to allow wireless broadband services in wide rural areas to access TV bands opportunistically (Dehalwar et al., 2016).

The most common technique to detect PUs signal or channel occupancy is by using energy detection (Bae et al., 2017). However, local sensing is inefficient due to propagation impairments (Mustapha et al., 2015). Therefore, the Cooperative Spectrum Sensing (CSS) is used to combine the spectrum sensing reports from multiple SUs. Report fusion can be distributed or centralized (Akyildiz and Brandon, 2011). In distributed CSS, local sensing reports are exchanged with neighbors SUs, while in centralized CSS, SUs send their local sensing reports to a centralized Fusion Center (FC) (Hernandes and Abrao, 2020). However, a cluster-based CSS is more suitable for the smart grid where each cluster is controlled by a CR-based Cluster Head (CH) to collect sensing reports and forward these reports to the FC (Nassef et al., 2018). Hard fusion or soft fusion can be used (Fu et al., 2018). However, the accuracy of the decision depends highly on the received spectrum sensing reports, the reliability of the wireless channels, and the trustworthiness of the cooperating SUs. These critical and conflicting parameters result in inaccurate spectrum decision reports and consequently waste the opportunities to access the available spectrum or cause interference to the PUs.

On the other hand, the smart grid inherits most of the security vulnerabilities commonly found on wireless communication networks, sensor networks, and the Internet as a whole (Ansere et al., 2019). A smart grid is vulnerable to security threats that target traditional networks, plus new security threats related to the cognitive features of the software-based air interface. The current spectrum sensing techniques do not provide a security mechanism to defend against these newly introduced attacks (Nassef and Alhebshi, 2016). The current cryptography security solutions cannot deal with this internal type of attack that initiates from malicious SUs within the network (Fragkiadakis et al., 2014). One of the cognitive-related attacks is the Spectrum Sensing Data Falsification (SSDF) attack (Chen et al., 2017), where malicious SUs send falsified sensing decisions to mislead the FC and to disrupt the network operation. This attack may waste the opportunity for other SUs to access the spectrum and also cause interference to PU. Furthermore, malicious SUs can work independently or collaborate and can use different attacking strategies (Wan et al., 2019). Security solutions proposed for both Cognitive Radio Ad Hoc Networks (CRAHNs) and Cognitive Radio Networks (CRNs) are not applicable for the resource-constrained CR-based WSNs (Joshi et al., 2013).

Among the possible solutions to prevent the SSDF attack is to evaluate the trustworthiness of cooperative SUs (Wang et al., 2018). A reputation-based detection scheme to detect SSDF attacks was considered in Wang et al. (2017). An attack aware cooperative spectrum sensing to defend against SSDF is proposed in Sharifi (2019) to estimate node behavior based on the estimated attack strength. The SUs' reputation values are developed in (Ye et al., 2016) based on their current and historical sensing behaviors. They used a punishment strategy to recompute the reputation to ensure correct global decisions. A multinomial Bayesian trust model is proposed in Bhattacharjee et al. (2015) to defend against SSDF attacks by classifying nodes into honest or malicious. A double adaptive threshold technique is proposed in Khan et al. (2019) to differentiate the honest and malicious nodes by assigning weights to nodes using a Maximal Ratio Combining (MRC) scheme. Dempster-Shafer evidence theory is used at the FC to combine the decision of all the honest nodes. A sequential CSS in the presence of dynamic byzantine attack for mobile networks to defend against dynamic SDFF attacks is designed in Wu et al. (2018), where consistency of individual sensing report is checked. Reputation management combined with subcarrier modulation-based CSS scheme is presented in Zheng et al. (2016) to achieve robustness against unreliable subcarriers due to harsh industrial environments. Both trust and reputation are used in Bennaceur et al. (2018) to secure the network against SSDF. A cooperative multiband detection scheme to optimize the detection performance and maximize the throughput in the existence of malicious users is presented in Saber and Sadough (2016). Moreover, a trust management scheme based on sensing reputation is developed in Kar et al. (2017) to defend against SSDF attacks. They used sensing reputation based on history and consistency factor to isolate malicious nodes from spectrum sensing decision making.

Fuzzy logic was used to develop communication protocols for clustered based networks to select CHs. Both energy efficiency and enhance network lifetime were considered based on three factors of the node's remaining energy, the distribution of neighboring nodes or node degree, and the closest node to the base station. The aim was to decrease energy consumption and increase network lifetime (Rasheed et al., 2018). Finally, a fuzzy-based CSS to improve the probability of spectrum detection in a harsh smart grid environment was developed in Nassef and Alhebshi (2016). However, combining the reliability of communication channels with node behavior was not considered. The objective of this paper is to propose a Fuzzy Inference System (FIS) to improve spectrum detection performance in the presence of malicious SUs. The aim is to evaluate the impact of SSDF attack on fusion decisions, to propose an attack detection to classify SU's behavior, and be able to prevent malicious SU's from cooperating in the fusion process. The proposed FIS allows intermediate values to have a degree of membership function defined in the interval [0, 1]. The FIS inputs apply different functions to determine output using some formulated rules. The FIS takes crisp inputs and produces fuzzy output, which needs defuzzification to extract the crisp output that represents the fuzzy set. It is based on four descriptors of sensing reputation, channel condition, energy, and the probability of detection in the smart grid environment. To the best of our knowledge, there is no previous work that has proposed a secure and reliable cluster-based CSS that is designed especially for a smart grid environment. Therefore, this paper proposes a cluster-based CSS to detect and prevent SSDF malicious activities in a CR-based smart grid. The sensing reputation of SU is computed to classify SUs as honest, malicious, and suspected. A FIS based on sensing reputation of SUs behaviors, channel condition, energy, and the local probability of detection is proposed to enhance the accuracy of spectrum sensing detection.

The rest of the paper is organized as follows. Section II develops the threat model and evaluate performance indicators in both benign network and under SSDF attack with different attacking strategies and attacking probabilities. Section III develops the sensing reputation algorithm to detect SSDF attacks and to classify network nodes as trusted, malicious, and suspicious. Section IV proposes the fuzzy-based trust and reliable fusion to mitigate the impact of SSDF attacks based on four fuzzy descriptors to enhance the accuracy of spectrum decisions. Section V presents the simulation environment, performance metrics, simulation scenarios, and results analysis, where the proposed model is compared with the benign and attacked scenarios. Finally, Section VI provides the conclusion and future work.

2. Threat model

The network consists of N number of SUs that are uniformly distributed in a square area A of LxL sides and k number of PUs. Nodes are clustered into q clusters, and each cluster is assumed to occupy an area of $\frac{L^2}{q}$ square meters. Each cluster has one Cluster Head (CH) to communicate with member nodes $n_c = \frac{N}{q}$, where n_c is the number of SUs in each cluster. The network architecture includes at the higher level a network controller (FC) in which different applications are implemented. The FC selects the frequency bands to be sensed and instructs all network nodes to perform individual sensing. Correspondingly, it receives the sensing reports from all cluster heads. The cluster-based CSS is used to reduce the overhead associated with sensing reports transmission at the WAN level and with limiting effects of malicious SUs within the cluster to enhance attack detection accuracy. ALL SUs continuously scans k channels to construct their local occupancy vector and transmits their sensing reports to FC through their corresponding CH^j. The honest SU_i transmits the same actual vector while malicious SU_i transmits a modified report to falsify the occupancy of some channels. Based on the received vectors, CHs submit their reports to FC, which employs fusion rules to make a cluster decision about the spectrum occupancy of all of k_c channels. For the hard fusion, the binary decision of SU_i about all channels are constructed as a binary vector u_i^{act} and submitted to FC through the corresponding CH^j over the error-free channel. For soft fusion, the actual energy and channel conditions are constructed. The occupancy vector u_i^{act} is constructed as:

$$\{u_i^{act} = \{u_1, \dots, u_k\} \tag{1}$$

where

$$u_k \begin{cases} = 0 & if\ channel\ is\ vacant \\ = 1 & if\ channel\ is\ occupied \end{cases}$$

In a benign network, two error performance indicators are defined. The probability of false alarm P_{fa} which are the probability of sensing the presence of a PU when the channel is vacant and the probability of miss detection P_{md} which is the probability of not sensing a PU when the channel is occupied. Therefore, for honest SUs, $P_{fa} = P(u_i = 1\,|H_0)$ and $P_{md} = P(u_i = 0\,|H_1)$. These honest SUs do not change their sensing decision u_j results and they advertise v_i to CH such as $P(v_i = 1\,|u_i = 1) = 1$, $P\big(v_i = 0\,\big|u_j = 1\big) = 0$, $P(v_i = 0\,|u_i = 0) = 1$, and $P(v_i = 1\,|u_i = 0) = 0$. Then the probability of detection of individual SUs, P_{detect}^H, is defined as:

$$P_{detect}^H = P\big(v_j = 0\,|H_0\big)\,P\big(H_0\big) + P\big(v_j = 1\,|H_1\big)\,P\big(H_1\big) = (1 - P_{fa})P_{vacant} + (1 - P_{md})P_{occupied} \tag{2}$$

The performance indicators for "$l\ out\ of\ n_c$" fusion in a benign environment is formulated as:

$$P_d{}^{CH^j} = \sum_{i=l}^{n_c} \binom{n_c}{l} \left(P_d{}^H\right)^i (1 - P_d{}^H)^{n_c - i} \tag{3}$$

$$P_{fa}{}^{CH^j} = \sum_{i=l}^{n_c} \binom{n_c}{l} \left(P_{fa}{}^H\right)^i (1 - P_{fa}{}^H)^{n_c - i} \tag{4}$$

where

$$\binom{n_c}{l} = \frac{n_c!}{l!\,.\,(n_c - l)!}.$$

When malicious SUs decide to launch the attack with a probability of P_{mal}, they modify sensing reports sent to the CH to influence the decision about the channel status. Different attacking strategies can be used based on the attack's objectives. The first strategy can be "Always YES" in which malicious nodes always report that the channel is occupied with increasing the probability of false alarm and with causing channel underutilization. The second strategy can be "Always NO" in which malicious nodes always report that the channel is vacant to lower the detection probability and increase interference to the PU. The third attack can be "Always Opposite" in which the opposite decision is reported to increase false alarm probability and decrease detection probability. The fourth attack can be a "random attack" in which a random decision is reported. Always yes and always no strategies are easily identified after several rounds of CSS due to constant sensing reports. However, always opposite and random strategies are the most harmful attacks.

The clustered based CSS consists of a number of SUs that are defined as $n_c = n_a + n_h$, where n_a nodes are the number of malicious nodes; n_h are a number of honest nodes and n_c is the total number of cluster members. In each cluster, there is a percentage of $\theta_{mal} = \frac{n_a}{n_c}$ malicious SUs that defines the attack strength. When SU_i decides to attack with a probability P_{mal}, the advertised vector $\{u_i^{adv}\}$ of SU_i may be different from the actual vector u_i^{act} where honest nodes would have the same $(u_i = v_i)$, and malicious nodes would have submitted the report v_i that will depend on its attack strategy. The advertises vector v_i^{adv} will be,

$$u_i^{adv} \begin{cases} = u_i^{act} & if\ \ node\ i \in\ H\ (honest\ SUs) \\ \neq u_i^{act} & if\ \ node\ i \in\ M\ (melicious\ SUs) \end{cases} \tag{5}$$

Since all the honest SUs n_h are sensing the same channels, their sensing reports should be similar. The dissimilar reports are received from the n_a malicious SUs. It is assumed that $n_a \ll n_c$Where the number of sensing reports from honest SUs is greater than the number of sensing reports from the malicious SUs for the proper operation of the majority fusion, which considers only the maximum number of similar sensing reports to reach a decision. Without loss of generalities, the following is the detection probability of an individual malicious SU_i and defined as P_{detect}^a,

$$P_{detect}^a = P(v_i^a = 0\ |H_0)\ P(H_0) +\ P(v_i^a = 1\ |H_1)\ P(H_1) = \Big((1 -\ P_{mal}\ )\big(1 - P_{fa}\ )\big) + P_{mal}P_{fa}\ \Big)\ P_{vacant} + \big((1 -\ P_{mal}\ )(1 - P_{md}\ ) + P_{mal}P_{md}\ \big)\ P_{occupied} \tag{6}$$

For $l\ out\ of\ n_c$ fusion where $l = \frac{n_a + n_h}{2}$, the P_{detect}^H follows a binomial distribution with parameter n_h and P_{detect}^a also follows a binomial distribution with parameter n_a. Therefore, the overall detection probability P_{detect} is calculated using the joint distribution of detection probability of independent, honest SUs and independent malicious nodes as follows:

$$P_{detect} =\ \ P(n_a +\ n_h) > l = \sum_{y=1}^{n_h} \psi(n_h\,, y, P_{detect}^H)\ \sum_{x=l-y}^{n_a} \psi(n_a\,, x, 1 - P_{detect}^a) \tag{7}$$

where

$$\psi(n_a, y, P_{detect}^H) = \binom{n_a}{y}\ \left(P_{detect}^H\right)^y\ (1 - P_{detect}^H)^{n_a - y},$$

and

$$\psi(n_a, x, 1 - P_{detect}^a) = \binom{n_a}{x}\ \left(1 - P_{detect}^H\right)^x\ (P_{detect}^H)^{n_a - x}$$

3. Computation of sensing reputation

To secure the network against the SSDF attack, the sensing reports are collected from all clusters. In each cluster, reports are highly correlated, and malicious reports can be detected based on their similarity (or difference) with reports from honest SUs. The SU's behavior is classified into honest and malicious based on their sensing reputation, which is computed based on direct and indirect trust. Trust is an expectation of a SU's behavior, and for simplicity, trust is formulated for one cluster. In this case, an indirect trust level is not required as all communications are performed between CH^j and it's immediate cluster members. Trust is dependent on time, and SUs can gain or lose trust with time. A single observation is not sufficient to estimate the behavior of the nodes. The trust value should be dynamically updated due to its dependence on the percentage of malicious SUs. However, updating the trust value frequently often results in the rapid consumption of energy, and it may not reflect trust value efficiently if the interval for the trusted update is too long. SUs usually observe the spectrum over a time window that may be adjusted depending on the user requirement and computational resource availability. A larger time window of observation allows a more accurate estimation of SU's behavior but consumes more resources. Trust is computed based on previous and current sensing reports. Over the sliding time window T, the history of the last spectrum sensing periods is used to classify nodes as Trusted, malicious, and suspicious using trust level. The trust value is modeled as a random variable in the range of [0, 1] (Bai et al., 2017), where the probability of expectation to effectively evaluate the trustworthiness of a SU is computed using the Beta distribution. Beta probability distribution function is computed using two parameters of the number of positive behavior of honest SUs (u_i^h)) and the number of negative behavior of malicious nodes (u_i^m) (Kar et al., 2017). The probabilistic estimation of the future trust and uncertainty about the behavior of a SU is captured from a history table that is created for each channel to record sensing reports from each SU during the T_{cs} sensing periods. The accumulated number of times the sensing reports that were similar to the final decision is computed as positive observations "u_j^h," and the accumulated number of times the number the sensing report was different from the final decision computed as the negative observations "u_i^m ." These accumulated evidences formulate the trust relationship between CH and SU. The direct trust level is defined as the expectation $E[Beta(u_j^h, u_j^m)]$ and is computed as $TL'[u_j^t] = \frac{|u_i^h|}{u_i^h + u_i^m}$. The average trust level is computed as $TL[u_i] = \frac{1}{n_c}\sum_0^n TL'[u_i^t]$. The same way for the malicious level that is computed as $SL'[u_j^t] = \frac{|u_i^m|}{u_i^h + u_i^m}$

The Sensing Reputation $SR[u_i]$ is computed using the sliding time window that moves to remove the recorded history based on three factors. The first factor is the historical trust level with an attenuation factor $\mu(t)$ to weight the historical experience based on timestamp t, where the newer sensing period is weighted more than, the older one. The second factor is the incentive factor to reward honest SUs for their honest behavior and also punish malicious SUs by decreasing their trust level. The third factor is the consistency factor that maintains an honest trust level. These factors are weighted with different weights to compute the $SR\left[u_j\right]$ for each SU_j as follows:

$$SR[u_i] = w_1 * \frac{\sum_{x=1}^{t} TL[u_i^x] * \mu(t)}{T} + w_2 * \left(1 - \frac{1}{n}\sum_0^n SL'[u_i^t]\right) + w_3 * \left(1 - \sqrt{\sum_{x=1}^{t} \frac{\left(TL[u_i^x] - \frac{TL[u_i^1] + TL[u_i^2] + \cdots, TL[u_i^t]}{T}\right)^2}{T-1}}\right) \quad (8)$$

where weights $w \in [0,1]$ and $\sum_{e=1}^{t} w_e = 1$. These weights are adjusted according to the demand of the network. w_1 is specified to give more weight to current sensing reports for immediate detection of node behavior, w_2 is used to inhibit malicious behavior, and w_3 is used to encourage the SUs to be honest for a long time. The trust value is computed over all sensed channels as follows:

$$[u_i^x] = \frac{(TL[u_i^1] + TL[u_i^2] + \cdots, TL[u_i^t]) * \mu(t)}{T} \quad (9)$$

A predefined threshold δ is used to classify a node's behavior-based node's sensing reputation. Initially the $SR\left[u_j\right]$ of all SUs are assigned a value $\delta = 0.5$ which is used to initialize the network when no historical trust file is found. With time, the $SR\left[u_j\right]$ will be modified, and SUs are classified as honest, malicious, or suspicious based on the following predefined threshold for the three categories as follows:

$$u_i = \begin{cases} Honest & if\ SR[u_i] \geq 0.9 \\ Malicious & if\ SR[u_i] < \delta \\ Suspicious & Otherwise \end{cases} \quad (10)$$

4. Proposed fuzzy inference system

Fuzzy fusion to enhance spectrum detection accuracy in unreliable harsh smart grid environments was developed in Nassef and Alhebshi (2016). The proposed FIS considers both reliability and the presence of malicious by incorporating four fuzzy descriptors to detect spectrum: Sensing reputation, channel condition, energy difference, and the local probability of detection. The four input descriptors have three levels of linguistic values to reflect the different degree of membership of the input linguistic variable and specified as follows:

Descriptor 1: The sensing reputation SR has 3 input linguistic variables of malicious, suspicious, and honest.
Descriptor 2: The channel condition has 3 input linguistic variables of poor, good, excellent.
Descriptor 3: The difference of the energy difference of sensed energy of SU to the average of all SUs in the cluster. It has 3 input linguistic variables of high, medium, and low.
Descriptor 4: The local probability of detection has an input linguistic variable of low, medium, and high.

The output linguistic variable $P_{d\,i}^{c}$ has seven linguistic values of very high, high, med-high, med, med-low, low, very low. All of the seven membership functions are represented by triangular functions, as shown in Fig. 1. The four input parameters with three different levels give a total of 81 fuzzy IF-THEN rules. The two extreme rules are located between these two cases:

Case (1): If SR is malicious, SNR is poor, DIFF is high and local P_d is low, then the fuzzy cluster decision is very low.
Case (2): If SR is honest, SNR is excellent, DIFF is low, and P_d is high, then the fuzzy cluster decision is very high.

5. Simulation environment

Simulations are performed to create the same environment found in HAN to investigate the newly introduced SSDF attack and validate the effectiveness of the proposed FIS. The network consists of 100 nodes, and a percentage of these nodes are selected to be malicious. It is also assumed that initially, all nodes are authorized by the FC, which knows the node's location and sensing parameters of all clusters. The performance of the hard fusion rules is simulated and compared with the performance of the proposed FIS. Simulation is carried first in a benign environment, then independent SSDF attack with various strategies are introduced. The traffic and propagation models are based on the requirements of the smart grid environment. The simulation parameters are summarized in Table 1.

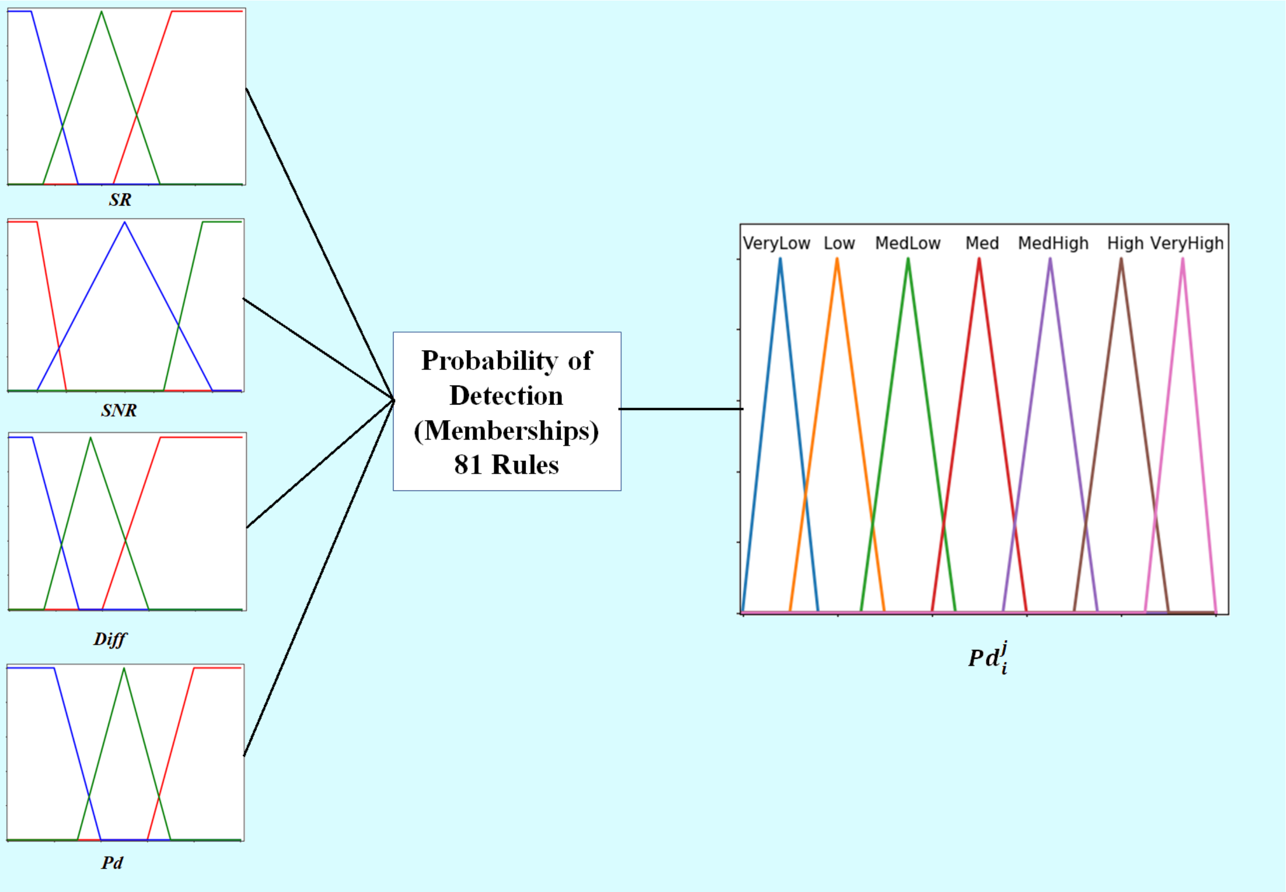

Fig. 1: Membership functions of proposed FIS

Table 1: Common simulation parameters

Parameter	Values	Parameter	Values
Network diameter	100 m	Traffic type	CBR
Frequency band	2.4G Hz	Data rate	250 kbps
Number of SUs	100	Packet size	512B
SU coverage radius	35 m	Sensing duration	1msec
Number of PUs	5	Number of samples	500
Receiver sensitivity	-85 dBm	Sampling duration	0.1msec
PU coverage radius	50 m	Super frame duration	10msec
Path loss exponent	4.2	Shadowing Variance	4.0

5.1. Simulation results and analysis

Two scenarios to evaluate the performance of proposed fusion schemes are considered. The first scenario evaluates the probability of detection against the probability of false alarm for the majority fusion under the impact of different independent SSDF attack strategies with 10% malicious nodes. Results indicate that the performance of majority fusion degraded quickly when the percentage of malicious nodes is 10 % as compared with the case of no malicious attacks (0%). The highest degradation is achieved with the opposite attack strategy as compared to always yes and always no attack strategies. The majority of fusion cannot distinguish between honest SUs from malicious SUs, which greatly impacts the fusion process due to inaccurate sensing reports. The figure also presents the impact of random attack strategy and 10% percentage of malicious SUs on the fuzzy reliable fusion where sensing reputation is disabled to consider the impact of reliability with no measure of sensing reputation on detection of SSDF attacks. The improvement is attributed to reliability considerations. As indicated in Fig. 2, the proposed fuzzy scheme shows better results with the introduction of 10 % of malicious SUs and provided the best performance due to its effectiveness in detecting malicious SUs and isolating them from participating in the fusion process, which enhanced detection accuracy.

The second scenario shows the effect of increasing the percentage of malicious nodes on detection performance. When there are no malicious SUs, the difference between proposed fusion and reliable fusion is due to the impact of taking channel condition into consideration.

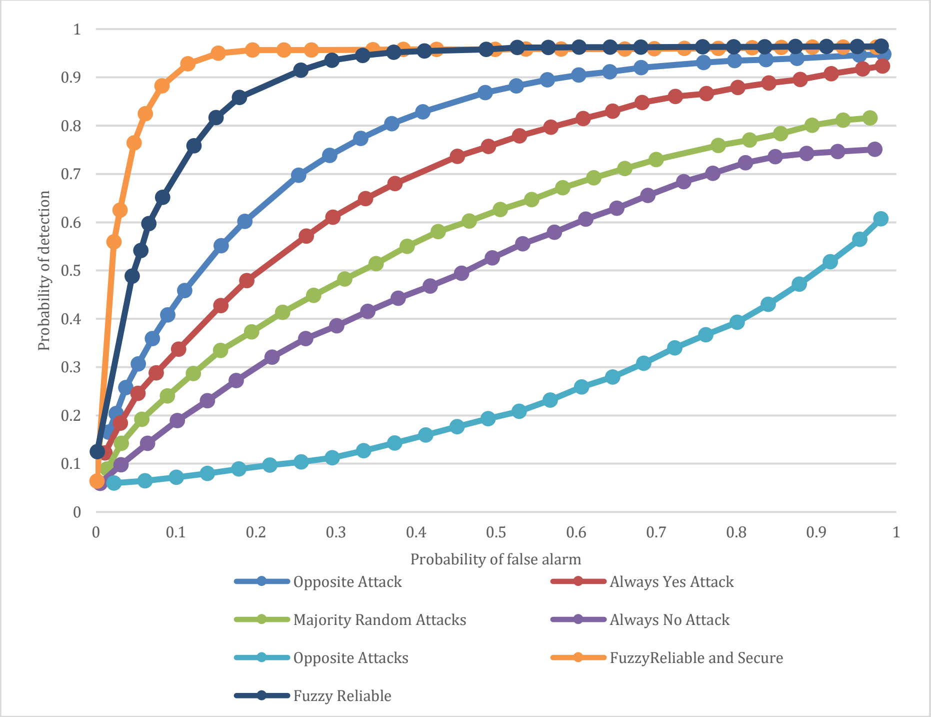

Fig. 2: The probability of detection against the probability of false alarm for majority fusion under 10% of SSDF attack

The detection performance of proposed fuzzy fusion has no measures for sensing reputation, and performance dropped quickly when the percentage of malicious SUs increases due to incorrect sensing reports, which impacted the spectrum decision. On the other hand, the proposed fuzzy fusion exhibits more robustness and maintains a relatively good performance as the percentage of malicious nodes increases. As indicated in Fig. 3, the proposed fuzzy fusion has the advantage of integrating the sensing reputation to provide more accurate results, which contributed to the performance improvement. The proposed fuzzy-based secure fusion has prevented malicious SUs from participating in detection probability, which enhanced detection accuracy. Using the proposed FIS, malicious SUs are not allowed to participate in fusion once they are detected. However, suspected nodes are continuously monitored to evaluate their behavior.

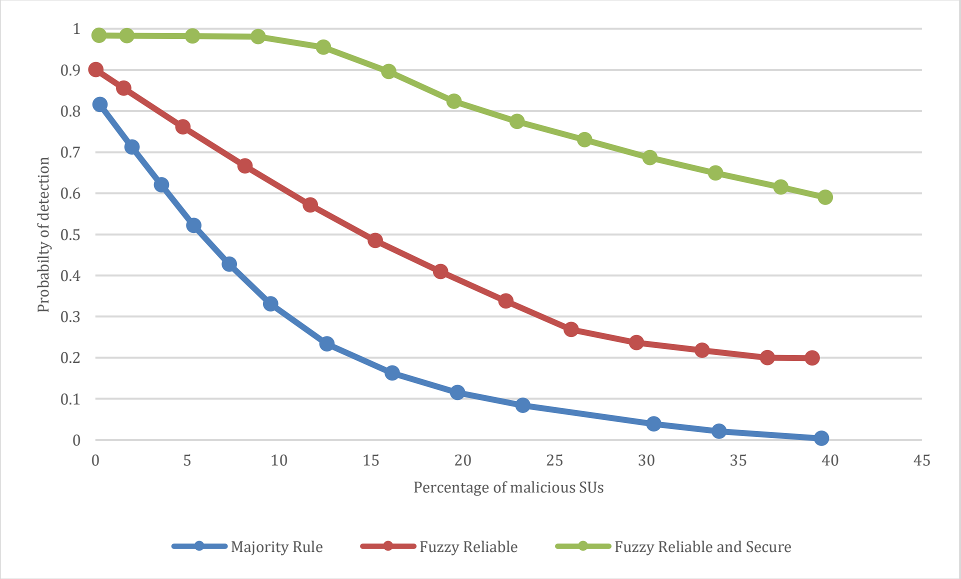

Fig. 3: The probability of detection against the percentage of malicious SUs

6. Conclusion and future works

The exponential growth of wireless applications and the spectrum scarcity problem, along with the traditional static spectrum allocation, have caused unreliable communications in the harsh smart grid environment. The unlicensed spectrum band suffers from a spectrum inefficiency problem while the licensed spectrum band is underutilized. Cognitive radio is proposed to allow opportunistic access to these underutilized spectrum bands. The local spectrum detection is inefficient, and a cooperative spectrum sensing is employed to enhance detection accuracy. However, cooperative spectrum sensing is vulnerable to SSDF attacks in which malicious SUs modify their sensing reports to force the fusion center to make the wrong spectrum decision. Sensing reputation is developed to classify SUs as honest, malicious, and suspicious. A fuzzy inference system is proposed to maintain a good detection performance in the presence of malicious SUs. It is based on four conflicting fuzzy descriptors of node's sensing reputation, channel condition, difference of local sensing to the average of cluster cooperative sensing, and the local probability of detection. The proposed FIS has prevented malicious SUs from participating in the fusion process and also allowed to keep track of suspicious SU's behavior. The proposed FIS was evaluated through simulation, and the results demonstrated that the proposed scheme was effective in enhancing detection probability as compared to fuzzy reliable and majority fusion under independent SSDF attacks. However, the effect of launching collaborative malicious SSDF attacks needs to be considered along with other attacks that target the spectrum sensing phase as well as other phases of the cognitive cycle. A deep learning approach is now considered to enhance attack detection and prevention for multiple types of spectrum sensing attacks under a wide range of scenarios, propagation environment, topology, and/or attack strategies that will be based on the dataset obtained from the current simulation work.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Akyildiz IF, Lee WY, Vuran MC, and Mohanty S (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Computer Networks, 50(13): 2127-2159. https://doi.org/10.1016/j.comnet.2006.05.001

Akyildiz IF, Lo BF, and Balakrishnan R (2011). Cooperative spectrum sensing in cognitive radio networks: A survey. Physical Communication, 4(1): 40-62. https://doi.org/10.1016/j.phycom.2010.12.003

Ansere JA, Han G, Wang H, Choi C, and Wu C (2019). A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks. IEEE Internet of Things Journal, 6(4): 6748-6759. https://doi.org/10.1109/JIOT.2019.2911109

Bae S, So J, and Kim H (2017). On optimal cooperative sensing with energy detection in cognitive radio. Sensors, 17(9): 2111. https://doi.org/10.3390/s17092111 **PMid:28914753 PMCid:PMC5621099**

Bai P, Zhang X, and Ye F (2017). Reputation-based Beta reputation system against SSDF attack in cognitive radio networks. In the Progress in Electromagnetics Research Symposium-Fall, IEEE, Singapore, Singapore: 792-799. https://doi.org/10.1109/PIERS-FALL.2017.8293243

Bennaceur J, Idoudi H, and Azouz Saidane L (2018). Trust management in cognitive radio networks: A survey. International Journal of Network Management, 28(1): e1999. https://doi.org/10.1002/nem.1999

Bhattacharjee S, Chatterjee M, Kwiat K, and Kamhoua C (2015). Multinomial trust in presence of uncertainty and adversaries in DSA networks. In the MILCOM 2015-2015 IEEE Military Communications Conference, IEEE, Tampa, USA: 611-616. https://doi.org/10.1109/MILCOM.2015.7357511

Chen H, Zhou M, Xie L, and Li J (2017). Cooperative spectrum sensing with M-ary quantized data in cognitive radio networks under SSDF attacks. IEEE Transactions on Wireless Communications, 16(8): 5244-5257. https://doi.org/10.1109/TWC.2017.2707407

Dehalwar V, Kalam A, Kolhe ML, and Zayegh A (2016). Compliance of IEEE 802.22 WRAN for field area network in smart grid. In the IEEE International Conference on Power System Technology, IEEE, Wollongong, Australia: 1-6. https://doi.org/10.1109/POWERCON.2016.7754046

Fadel E, Faheem M, Gungor VC, Nassef L, Akkari N, Malik MGA, and Akyildiz IF (2017). Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. Computer Communications, 101: 106-120. https://doi.org/10.1016/j.comcom.2016.12.020

Fadel E, Gungor VC, Nassef L, Akkari N, Malik MA, Almasri S, and Akyildiz IF (2015). A survey on wireless sensor networks for smart grid. Computer Communications, 71: 22-33. https://doi.org/10.1016/j.comcom.2015.09.006

Fragkiadakis A, Angelakis V, and Tragos EZ (2014). Securing cognitive wireless sensor networks: A survey. International Journal of Distributed Sensor Networks, 10(3): 393248. https://doi.org/10.1155/2014/393248

Fu Y, Yang F, and He Z (2018). A quantization-based multibit data fusion scheme for cooperative spectrum sensing in cognitive radio networks. Sensors, 18(2): 473. https://doi.org/10.3390/s18020473 **PMid:29415448 PMCid:PMC5856117**

Hernandes AG and Abrao T (2020). Distributed average consensus optimization for cooperative spectrum sensing in cognitive radio ad hoc networks. Emerging Telecommunications Technologies, 31(7): e3965. https://doi.org/10.1002/ett.3965

Huang XL, Tang XW, and Hu F (2020). Dynamic spectrum access for multimedia transmission over multi-user, multi-channel cognitive radio networks. IEEE Transactions on Multimedia, 22(1): 201-214. https://doi.org/10.1109/TMM.2019.2925960

Joshi GP, Nam SY, and Kim SW (2013). Cognitive radio wireless sensor networks: Applications, challenges and research trends. Sensors, 13(9): 11196-11228. https://doi.org/10.3390/s130911196 **PMid:23974152 PMCid:PMC3821336**

Kar S, Sethi S, and Sahoo RK (2017). A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks. Wireless Personal Communications, 97(2): 2523-2540. https://doi.org/10.1007/s11277-017-4621-5

Khan AA, Rehmani MH, and Rachedi A (2017). Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. IEEE Wireless Communications, 24(3): 17-25. https://doi.org/10.1109/MWC.2017.1600404

Khan MS, Jibran M, Koo I, Kim SM, and Kim J (2019). A double adaptive approach to tackle malicious users in cognitive radio networks. Wireless Communications and Mobile Computing, 2019: 2350694. https://doi.org/10.1155/2019/2350694

Mustapha I, Ali BM, Rasid MFA, Sali A, and Mohamad H (2015). An energy-efficient spectrum-aware reinforcement learning-based clustering algorithm for cognitive radio sensor networks. Sensors, 15(8): 19783-19818. https://doi.org/10.3390/s150819783 **PMid:26287191 PMCid:PMC4570397**

Nassef L and Alhebshi R (2016). Secure spectrum sensing in cognitive radio sensor networks: A survey. International Journal of Computational Engineering Research, 6(3): 1-7.

Nassef L, El-Habshi R, and Jose L (2018). Clustering-based routing for wireless sensor networks in smart grid environment. International Journal of Advanced Smart Sensor Network Systems, 8(1/2/3): 1-14. https://doi.org/10.5121/ijassn.2018.8301

Rasheed T, Rashdi A, and Akhtar AN (2018). Cooperative spectrum sensing using fuzzy logic for cognitive radio network. In the Advances in Science and Engineering Technology International Conferences, IEEE, Abu Dhabi, UAE: 1-6. https://doi.org/10.1109/ICASET.2018.8376914 **PMCid:PMC5870312**

Saber MJ and Sadough SMS (2016). Multiband cooperative spectrum sensing for cognitive radio in the presence of malicious users. IEEE Communications Letters, 20(2): 404-407. https://doi.org/10.1109/LCOMM.2015.2505299

Sharifi AA (2019). Attack-aware defense strategy: A robust cooperative spectrum sensing in cognitive radio sensor networks. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 43(1): 133-140. https://doi.org/10.1007/s40998-018-0133-x

Toma OH, López-Benítez M, Patel DK, and Umebayashi K (2020). Estimation of primary channel activity statistics in cognitive radio based on imperfect spectrum sensing. IEEE Transactions on Communications, 68(4): 2016-2031. https://doi.org/10.1109/TCOMM.2020.2965944

Wan R, Ding L, Xiong N, and Zhou X (2019). Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks. International Journal of Distributed Sensor Networks, 15(9): 1550147719870645. https://doi.org/10.1177/1550147719870645

Wang J, Chen R, Tsai JJ, and Wang DC (2018). Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks. Computer Communications, 116: 90-100. https://doi.org/10.1016/j.comcom.2017.11.010

Wang P, Chen C, Zhu S, Lyu L, Zhang W, and Guan X (2017). An optimal reputation-based detection against SSDF attacks in industrial cognitive radio network. In the 13th IEEE International Conference on Control and Automation, IEEE, Ohrid, Macedonia: 729-734. https://doi.org/10.1109/ICCA.2017.8003150

Wu J, Song T, Yu Y, Wang C, and Hu J (2018). Sequential cooperative spectrum sensing in the presence of dynamic Byzantine attack for mobile networks. PloS One, 13(7): e0199546. https://doi.org/10.1371/journal.pone.0199546 **PMid:29975727 PMCid:PMC6033420**

Ye F, Zhang X, and Li Y (2016). Comprehensive reputation-based security mechanism against dynamic SSDF attack in cognitive radio networks. Symmetry, 8(12): 147. https://doi.org/10.3390/sym8120147

Yigit M, Gungor VC, Fadel E, Nassef L, Akkari N, and Akyildiz IF (2016). Channel-aware routing and priority-aware multi-channel scheduling for WSN-based smart grid applications. Journal of Network and Computer Applications, 71: 50-58. https://doi.org/10.1016/j.jnca.2016.05.015

Zheng M, Liang W, Yu H, and Song M (2016). SMCSS: A quick and reliable cooperative spectrum sensing scheme for cognitive industrial wireless networks. IEEE Access, 4: 9308-9319. https://doi.org/10.1109/ACCESS.2016.2641471