Indian Journal of Science and Technology, *Vol 8(28), DOI: 10.17485/ijst/2015/v8i28/71246, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Efficient Spectrum Sensing Framework and Attack Detection in Cognitive Radio Networks using Hybrid ANFIS

B. Senthil kumar[1]* and S. K. Srivatsa[2]

[1]St. Peter's University, Chennai - 600054, Tamil Nadu, India; senb2003@gmail.com
[2]Anna University, Chennai - 600025, Tamil Nadu, India

Abstract

Background: Cognitive radio is being recognized as an intelligent technology due to its ability to rapidly and autonomously adapt operating parameters to changing environments and conditions. In order to reliably and swiftly detect spectrum holes in cognitive radios, spectrum sensing must be used. Accurate spectrum sensing is important in improving the efficiency of cognitive radio networks. False sensing results in either waste of spectrum or harmful interference to primary users who may remotely or physically capture the sensors and manipulate the sensing reports. **Methods:** A novel framework and an innovative approach have been introduced to eliminate the malicious behaviors of secondary users. It is found that spectrum sensing alone cannot prevent the malicious behavior without any information on users' reputation. Based on the evaluation of malicious behavior resistance methods, joint spectrum sensing and malicious nodes detection approach for optimal prevention from sensing falsification is being proposed. **Findings:** The proposed approach minimizes Linear Minimum Mean-Square Errors (LMMSEs) when it is compared with the existing algorithms such spectrum sensing based on HSMM and FNN based spectrum sensing are plotted versus detection probability, false alarm probability. With more malicious nodes proposed schemes are more effective to restrain the false alarms. **Improvement/Application:** The proposed spectrum sensesframework with attack detection which is very effective to determine the malicious users in spectrum holes.

Keywords: Fuzzy Neural Network, Linear Minimum Mean Square Error, Primary User, Secondary User, Spectrum Sensing

1. Introduction

Radio spectrum is one among the most rare and significant resource for wireless communications. This fact, with new perceptions into the use of spectrum has imposed new challenges to the conventional approaches to spectrum management. It is shown by the current measurements that most of the allocated spectrum is largely under-utilized and the Spectrum- Policy Task Force appointed by Federal Communications Commission (FCC) has confirmed the same views[1]. Spectrum efficiency can be enhanced substantially by giving expedient access of these frequency bands to a group of unlicensed potential users. Cognitive Radio (CR)[2] has been put forward as a solution to increase spectrum efficiency by making good use of the unused spectrum in evolving environments. Hence the CR design is a path-breaking radio design philosophy involving intelligent sensing of the bands of spectrum and determination of the transmission characteristics (e.g., symbol rate, power, bandwidth, latency) of a group of potential users based on the primary user's behavior.

Lately, Cognitive Radio (CR) has been suggested as a promising technology to enhance spectrum utilization by providing secondary access to unused licensed bands. For this secondary access, the pre-condition is non-interference to the primary system. This necessity demands spectrum sensing to act as a key function in Cognitive Radio systems. One of the chief components of

*Author for correspondence

the Cognitive Radio concept is the measurement, sensing, learning and being knowledgeable of the parameters related to the radio channel characteristics, availability of spectrum and power, radio's operating environment, user requirements and applications, available networks (infrastructures) and nodes, local policies and other operating restrictions. In terms of Cognitive Radio technology, the users with topmost priority or legacy rights on the usage of a particular part of the spectrum are defined as primary users. Having said this, secondary users, with lower priority, make use of this spectrum without causing any interference to primary users. Hence, it is necessary to the secondary users to have Cognitive Radio capabilities, such as detection of the spectrum with accuracy to check if it is being used by a primary user and to make changes in the radio parameters to use the unexploited part of the spectrum.

Spectrum sensing schemes need a large communication resource which includes sensing time delay, control channel overhead and consumption energy for reporting sensing data to the FC, with large sized networks. This issue has been taken into consideration in some of the analysis done previously[3]. In[4], the authors put forward making use of a censored truncated sequential spectrum sensing technique for conserving energy. Then again, cluster-based Cooperative Spectrum Sensing CSS schemes are looked at for reduction of the energy of CSS[5] and minimization of the bandwidth requirements by reducing the number of terminals reporting to the fusion center[6]. In[7], Chen et al. advised a cluster-based CSS scheme for optimization of the cooperation overhead along with sensing reliability. Truly, these suggested cluster schemes can decrease the amount of direct cooperation with the FC but cannot decrease the communication overhead between CUs and the cluster header. A same kind of problem can be observed in the cluster scheme in[8], though the identification of optimal cluster size to increase the throughput used for negotiation is done. Another fact to be considered of the cluster scheme is improving the sensing performance when the reporting channel is affected from a severe fading environment[9,10].

The load on signal processing techniques can be mitigated to a large extent by using cooperative diversity between Cognitive Radio spectrum sensors. Few Cognitive Radio spectrum sensors under independent fades can help in reduction of individual sensitivity requirements and substantially help in defeating the hidden terminal problem by opposing the shadowing and multi-path effects. Several cooperative sensing schemes have been proposed in the literature[11–13]. Despite this, it was shown in[13] that presence of few malfunctioning sensing devices could negatively impact the performance of cooperative sensing system.

A Malicious User's (MU) presence worsens the detection performance of cooperative spectrum sensing. An MU is an uninvited and unlicensed user, camouflaged in the role of a legal user and transmits false information about the status of the primary signal. In general, known types of MUs include Always Busy (AB), Always Free (AF), Always Opposite (AO) and an MU that transmits high signal with probability α and low signal with probability, 1 – α and we name it α MU. The AB and AF types of MU always produce either a high (H_1) or a low (H_0) signal, respectively, irrespective of the original status of the primary signal. Whereas an AO type of MU, always produces a signal in opposition/contrary to the one observed from its local observation about the status of the PU. The AO MU is observed to be the most harmful type, particularly, when the decision is taken opposite to the real status of PU (if global decision or actual status of the PU is available).

In this research work, we have improvised schemes to recognize and avoid the effect of malicious nodes for the case where adaptive fuzzy inference system is used by the sensing devices in cluster formation. We applied a simple and moderate speedy combination scheme to make the decision process easy at the access point.

Wang et al.[14] examined how to make the security of collaborative sensing better. Especially, the author formulates a malicious user detection algorithm that calculates the suspicious level of secondary users based on their past reports. Then, the author calculates trust values as well as consistency values that are used to reject the influence of malicious users on the primary user detection results. Through modelling, the author showed that even a single malicious user can substantially deteriorate the performance of collaborative sensing. The trust value indicator can tell apart honest and malicious secondary users effectively. The Receiver Operating Characteristic (ROC) curves for the primary user detection exhibit the development in the security of collaborative sensing.

Gao et al.[15] re-examined the already available proposals corresponding to secure collaborative spectrum sensing. Moreover, the author recognized several new location privacy related attacks in collaborative sensing, which are expected to expose secondary users location privacy by tampering their sensing reports and their physical

location. To prevent these attacks, the author introduced a new privacy preserving framework in collaborative spectrum sensing to prevent location privacy leaking. A testbed replicating the actual test system to evaluate the system performance has been conceptualised and modelled by the author.

Althunibat et al.[16] described the effect of multiple malicious users on the energy efficiency of a cognitive radio network is given. A low-overhead security protocol is suggested to deal with SSDF attacks under a compromise between energy efficiency and security. An analysis is given to set the optimal number of security bits required to maximize energy efficiency. Noteworthy improvement on the achievable energy efficiency is shown in the simulation results and the optimal number of bits obviously depends on the selected fusion rule, the number of malicious users and the number of legitimate users.

Wang et al.[17] built a joint spectrum sensing and access framework to nullify the malicious behaviors of both rational and irrational IMUs. Absence of reputation information makes the malicious behavior resistance and deteriorates performance as the honest users may be misjudged as IMUs. The author designed an incentive suitable method to provide a moderate punishment to IMUs, based on the moral hazard principal-agent model. The author's observations show that both spectrum sensing and spectrum access alone cannot prevent malicious behaviors without any information on users' reputation. According to the different properties of malicious behavior resistance by spectrum sensing and spectrum access, the author applies joint spectrum sensing and access for optimal prevention of the IMUs sensing falsification. The suggested malicious behavior resistance mechanism is shown to provide the same significant performance as the ideal case with truthful sensing.

Li et al.[18] took another question in contrary into consideration: could a malicious entity take advantage of space diversity, e.g., an external attacker or an non-trusted Fusion Center (FC), to gain geolocation of a secondary user, without its knowledge, by linking his location-based sensing report to his physical area. The author presented a new location privacy definition to measure the location privacy leaking in collaborative sensing by introducing a Privacy Preserving collaborative Spectrum Sensing (PPSS) scheme, which includes two primitive protocols: Privacy Preserving Sensing Report Aggregation protocol (PPSRA) and Distributed Dummy Report Injection Protocol (DDRI). Especially, PPSRA scheme make use of applied cryptographic techniques to allow the FC to get the consolidated result from various secondary users without learning each individual's values whereas DDRI algorithm can be used to get differential location privacy for secondary users by introducing a novel sensing data randomization technique. We executed and assessed the PPSS scheme in a real-world test system. The assessment results show that PPSS can considerably increase the secondary user's location privacy with a sensible security overhead in collaborative sensing.

Wang et al.[19] implemented a moral hazard principal-agent framework and modelled an incentive suitable method to counter the malicious behaviors of rational and irrational IMUs. The author's observations show that both spectrum sensing and spectrum access alone cannot prevent malicious behaviors without any information on users' reputation. According to the different properties of malicious behavior resistance by spectrum sensing and spectrum access, the author applies joint spectrum sensing and access for optimal prevention of the IMUs sensing falsification. The analysis results show that the mechanism imparts similar performance as the ideal case with perfect sensing.

2. Proposed Methodology

Traditionally deployed sensing techniques in general are associated with sensing spectrum basically in three dimensions which include time, geographic area & frequency. Though, other dimensions do require further exploration to facilitate spectrum opportunity. Consequently, this kind of signals play a major role in the issue related to sensing the spectrum. The following innovative spectrum sensing has been basically suggested so as to counteract issues inherent in current spectrum sensing methods. Suggested spectrum sensing methodology here comprises of specific spectrum segmentation, CRN spectrum sensing cluster formation that can facilitate malicious detection.

2.1 Spectrum Segmentation

Spectrum segmentation serves as a first step to identify the subbands that are in use at a certain time, when a wide portion of the spectrum is observed. The observed band is analyzed to find the boundaries of the different subbands. In this research, improved histogram based on fuzzy is proposed for spectrum segmentation[20]. Before that power spectral density value is calculated for

signal before identifying the boundaries of the band. The proposed FNN model predicts the channel status as "1" for an occupied channel and "0" for unoccupied channel.

Let $[f_0, f_N]$ be the observed frequency range of the radio spectrum. The segmentation process has to estimate $f_0, f_1, f_2 \cdots \ldots f_N$ the boundaries of the N frequency intervals is illustrated in Figure 2.

Step 1: Calculate the power spectral density value for each and every signal using periodogram function.
Step 2: The histogram of the smoothed PSD value (f(i)values) is calculated first. The local maxima of the histogram, whose values exceed a certain threshold m, are searched. Therefore, the threshold on the maxima detection, m, depends on the minimum bandwidth considered for the sub-bands. Let these maxima be called $M_1, \ldots, M_k$. Each interval is the distance between two successive local maxima. Then fuzzifies a newly-generated factor from the multiplication of two factors the interval and he frequency of signals in the interval. The values are proportional to the sub-band widths.
Step 3: Called f_i the PSD level corresponding to the center of the histogram bin, whose occurrence is M_i, the PSD segments whose values lie in a range $[f_i - \delta, f_i + \delta]$ are identified, and a new version of the PSD is generated where these segments are rectified to the value f_i. The tolerance δ depends on the variance of the PSD estimate.
Step 4: The slope of the rectified version of the PSD between two segments is analyzed to detect a boundary. In particular, the boundary is located where a minimum of the PSD between two segments is found. A subband is found only if the corresponding bandwidth is greater than 1. The value of 1 represents the minimum sub-band width. Therefore, it should be chosen starting from the knowledge of the minimum bandwidth of primary users in the observed frequency spectrum.

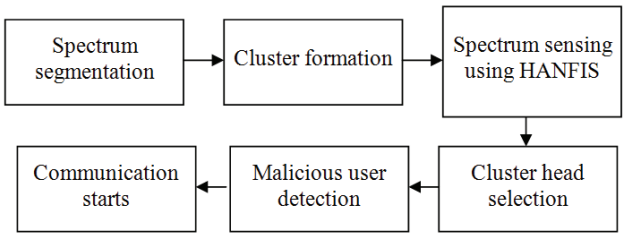

Figure 1. Overall proposed block diagram of secure spectrum sensing.

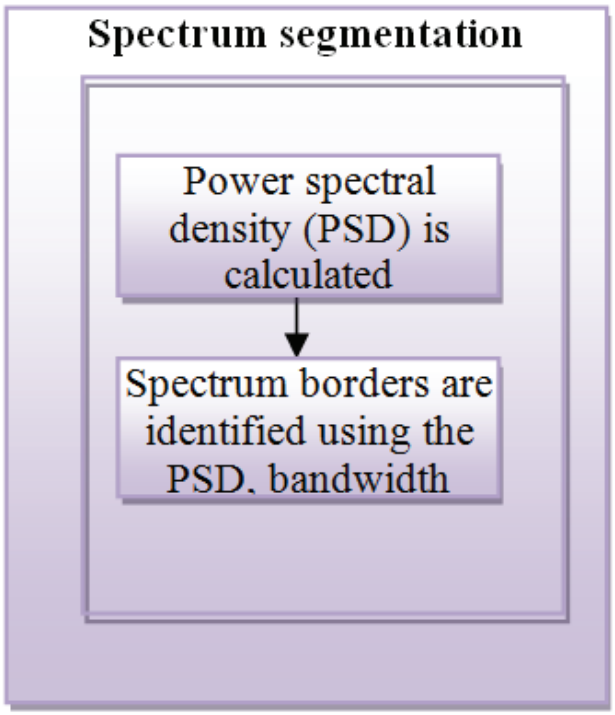

Figure 2. Spectrum segmentation.

2.2 Cluster based Spectrum Sensing

It is imperative for improvisation and development of an efficient CSS or Cooperative Spectrum Sensing scheme in CR or Cognitive Radio. This is often because of potential viewed as a system that enables spectrum utilization enhancement. Cooperative sensing framework comprises of several PUs, cooperating CR users including a FC. Cooperative sensing components have been illustrated in Figure 1. Here every CU is enabled for conducting a spectrum sensing method, referred to as local spectrum sensing in distributed scenario and used for primary user PU signal detection. Prior to the CU sensing process there is grouping of the spectrum value CU's in the form of clusters. SU location found in factual CR networks if found to be distributed in a random manner. Hence as a result a couple of SUs possibly undergo deep fading when others don't. Conversely though, few users adjacent to one other that undergo similar path fading generally have the same SNR. Hence CR network is structured in the form of multiple clusters on the basis of geographical position ase in Figure 3.

SNR for primary signal may be calculated on the basis of the following formula

$$SNR = P_i(d) / N_i B \quad (1)$$

P_i is a primary signal, N_i is band noise and B the bandwidth. Here we propose cluster header selection on

the basis of sensing data reliability. Every SU during the sensing interval deploys samples to execute spectrum sensing through application of the HANFIS detection method. Cluster formation method suggested here has been explained in the Figure 4.

2.2.1 Spectrum Sensing

The hybrid adaptive neuro fuzzy inference system model which is innovative has been introduced for identifying spectrum holes. Suggested technique here potentially predicts channel status if in a state of being occupied or unoccupied and facilitates spectrum sensing. Bandwidth efficiency, power spectral density and capacity over subband are input to hybrid. Subband state prediction is carried out by the adaptive neuro fuzzy inference system. Spectrum sensing here refers to band white spaces detection[21,22].

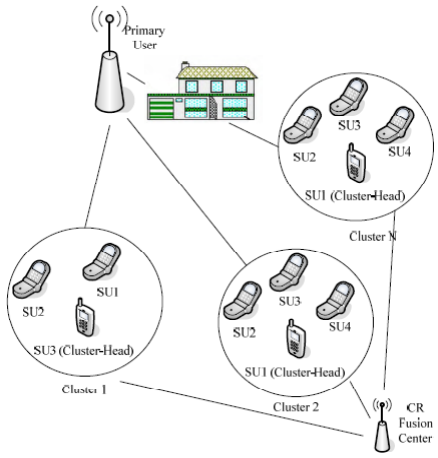

Figure 3. Cluster-based cooperative spectrum sensing.

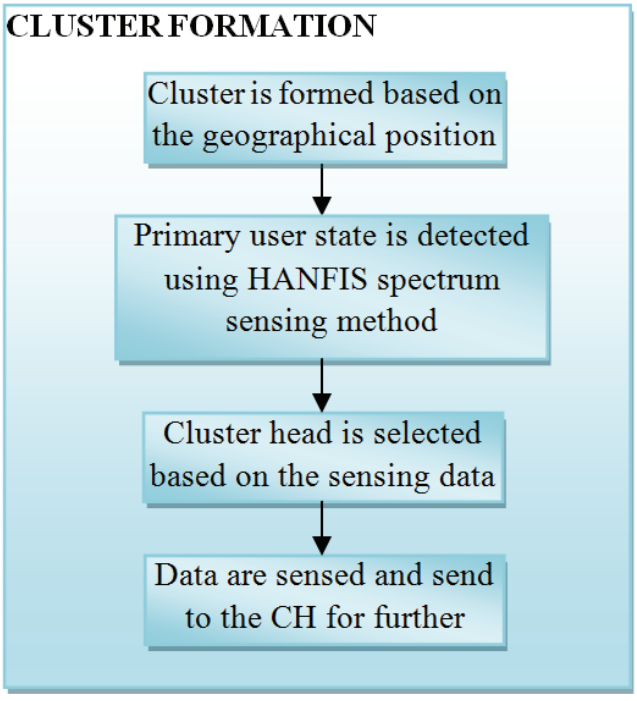

Figure 4. Process cluster formation and cluster head selection.

Local spectrum sensing at the ith CU is essentially a binary hypotheses testing problem:

$$\begin{cases} H_0 : x_i(t) = n_i(t) \\ H_1 : x_i(t) = h_{is}(t) + n_i(t) \end{cases} \quad (2)$$

where H_0 and H_1 correspond, respectively, to hypotheses of absence and presence of the PU signal, $x_i(t)$ represents received data at CU_i hi denotes the gain of the channel between the PU and the CU_i,s(t) is the signal transmitted from the primary user and n(t) is additive white Gaussian noise. Also channels that correspond to various CUs are considered as being independent. Additionally CUs and PUs share a common spectrum allocation.

During practice there is a margin of error in the case of spectrum sensing algorithms. These may be categorized as miss detections & false alarms. Miss detection generally takes place when primary signal is inherent in sensed band & spectrum sensing algorithm chooses the hypothesis H_0 that potentially leads to harmful interference in the case of primary users. Contrarily, false alarm takes place when the state of sensed spectrum band is idle and when spectrum sensing algorithm chooses hypothesis H_1. This leads to missed transmission opportunities and hence lowers spectrum utilization. Physical malicious node takes on multiple identities and behaves as multiple distinct nodes (called Sybil nodes) in the system. Follow a simple interference model wherein the transmissions between neighboring secondary nodes fail if they are within certain distance of each other and use the same frequency band or overlapping frequency bands. On the basis of these parameters, spectrum sensing algorithm performance may be inferred by deploying two probabilities: the probability of miss detection $P_{md} = P(H_0/H_1)$, or its complementary probability of detection $P_d = P(H_0/H_1) = 1 - P_{md}$ and the probability of false alarm $P_{fa} = P(H_1/H_0)$ Large P_d and low P_{fa} values would be desirable. However, a trade-off between P_d and P_{fa} is prevalent which indicated that improving any one of performance metrics would lead to degradation of the other one.

When transmitter received signal, local observation of the i^{th} user is given by

$$S_{LOi} = \sum_{n=1}^{S} \left| x_i (n) \right|^2 \quad (3)$$

where S is the number of samples and is equal to 2TB, and T and B are the sensing time and bandwidth, respectively.

2.2.1.1 Hybrid ANFIS

Jang was the first one to propose the Adaptive Neuro Fuzzy Inference System or ANFIS. Implementation of ANFIS is relatively easy given input/output task and is further applicable in facilitating spectrum sensing that enables identification of spectrum holes. This means that ANFIS model combines ANN and FIS tools as a compound, basically reflecting absence of boundaries that help in distinguishing ANN and FIS features respectively[23,24].

if x_1 is A_1, x_2 is A_2, … , x_n is An Then $y = k_0 + k_1 x_1 + k_2 x_2 + \ldots ,+ k_n x_n$

Where $x_1, x_2, \ldots, x_n$ are considered as input signals $A_1, A_2, \ldots, A_n$ are fuzzy sets and y is the output variable we can find that in such type of fuzzy rule. The output variable is a first order polynomial on input variables.

2.2.1.2 Description of the Method

ANFIS model has six layers; one input, four hidden & one output layer, wherein every layer carries out a specific task of forwarding the signals. Figure 1 shows an ANFIS model.

Input layer is the first layer, where the neurons just transmit received input or crisp signals to the subsequent layer. Namely

$$x_i^1 - y_i^1 \quad (4)$$

Where x_i^1 is the input signal and y_i^1 is the output signal of neuron in the first layer

ANFIS model second layer is the fuzzification layer where the neurons represent antecedent fuzzy sets of fuzzy rules. An input signal is further received by the fuzzification neuron wherein it ascertains channel capacity.This is then deployed for channel transmission rate analysis. Calculating input signal channel capacity is carried out using the following formula

$$C = B \log_2 (1 + SNR) \quad (5)$$

$$y_i^2 = f\left(C\left(x_i^2\right)\right) \quad (6)$$

where f represents the activation function of neuron i, and is set to a certain membership function.

Second hidden layer or the third one is the fuzzy rule layer where every neuron gets signals singularly from fuzzification neurons. These are part of the fuzzy rule antecedents and are representative of the signal spectral efficiency and also help in computation.

$$S_e (x_i) = \frac{B}{\Delta C} \log_2 (1 + SNR) \quad (7)$$

Product operator in the ANFIS, is deployed for evaluation of neuron conjunction overall. Hence we arrive at the following:

$$y_i^3 = \prod_c^m S_e (x_i) c_i \quad (8)$$

$S_e(x_i)c_i$ is the signal from fuzzification neuron c in the second layer to neuron i in the third layer, y_i^2 is the output signal of neuron i in this layer and m is the number of antecedents of the fuzzy rule neuron i represents

Normalization layer is considered here as the fourth layer where every neuron gets signals from the third layer rule neurons. For any given rule it calculates the so-called normalized firing strength. The specific strength value is representative of the channel capacity threshold value as well as spectral efficiency. These are utilized for determination of spectrum subband state.

Defuzzification layer is the fifth one where neurons here are connected to fourth layer normalization neuron respectively. They additionally receive initial input signals $x_1, x_2, \ldots, x_n$. A defuzzification neuron computed the "weighted consequent value" of a given rule as:

$$y_i^5 = x_i^5 \left(k_{i0} + k_{i1} x_1 + k_{i2} x_2 + \cdots + k_{in} x_n\right) \quad (9)$$

x_i^5 is the input and y_i^5 is the output signal of neuron i in the fifth layer; and $k_{i0} + k_{i1} + k_{i2} + \ldots + k_{in}$ is a set of consequent parameters of rule i.

Output or sixth layer is the summation layer. This layer has a single neuron and it computes and summates fifth layer defuzzification neurons and post that it generates overall ANFIS output y as given below:

$$y = \sum_{i=1}^{n} x_i \quad (10)$$

x_i is the signal from defuzzification neuron i in the fifth layer to this summation neuron; and n is the number of defuzzification neurons, specifically the number of fuzzy rules in the ANFIS model.

2.2.1.3 Training ANFIS Model

In majority of the ANFIS models, most frequently used activation function is basically the so-called bell-shaped function, as below:

$$y = \frac{1}{1+\left[\left(x-\frac{s}{r}\right)^2\right]^t} \quad (11)$$

where r, s and t are parameters that respectively control the slope, center and width of the bell-shaped function. During training, specifically parameters may be defined as well as adjusted using the learning algorithm.

Particularly ANFIS employs a hybrid learning or training algorithm which integrates least-squares estimator and the gradient descent technique and then at the end with the Runge Kutta Learning Method (RKLM). At first, initial bell-shaped functionalities are assigned and those that have specific parameters to every fuzzification neuron. Neurons function centre is connected to input x_i, these are such so that division of domain of x_i is uniform. Fnction widths and slopes are formulated to permit adequate function overlapping (s)[25,28]. Training dataset is presented in the training process in a cyclic manner to the ANFIS. In recent work some of the research done under based on the Neural Network (NN) based classification methods[29,30] for various applications. Every cycle in the training examples is referred to as an epoch. Every epoch that constitutes the ANFIS learning algorithm, consists of both forward & backward pass. Forward pass objective is forming and adjusting parameters that follow. Backward pass adjusts activation functionalities parameters.

2.2.2 Cluster Head Selection

Nodes that possess the foremost reliable sensing result assume the cluster header's roles. These roles are making and reporting cluster's decision to FC. For lowering reporting time as well as bandwidth, the foremost reliable cluster head sensing data, is employed to make a cluster decision. This technique method basically implies that decision of a cluster is based on the selective combination technique. FC integrates cluster decisions to take a final decision and then further broadcast final sensing decision to the entire network. Here we propose a cluster header selection on the basis of sensing data reliability. For every sensing interval, most reliable sensing data CU is chosen as the cluster header. Sensing data CR is computed by the probability of detection P_d which is a measure of the interference to the PU and the probability of false alarm P_F which sets the upper bound on spectrum utilization. Detection and false alarm probabilities of the *ith* user are given, respectively, as:

Probability of detection is

$$P_{d,i} = P\left(y_i > \lambda \mid H_1\right) = Q\left(\frac{\lambda_i - N\left(\gamma_i+1\right)\sigma_u^2}{\sigma_u^2\sqrt{2N\left(2\gamma_i+1\right)}}\right) \quad (12)$$

Where λ_i is local channel capacity threshold , γ_i is the Signal to noise ratio and σ_u^2 is the variance. N is the number of sample received signals.

Probability of false alarm

$$P_{f,i} = P\left(y_i < \lambda_i \mid H_0\right) = \left(\frac{\lambda_i - N\sigma_u^2}{\sigma_u^2\sqrt{2N}}\right) \quad (13)$$

Where λ_i is local channel capacity threshold, and σ_u^2 is the variance. N is the number of sample received signals.

On evaluating sensed data results, CRU reliability is computed and this reliability value is employed for cluster head selection. The remaining CRN join as cluster members on the basis of geographical position. Every cluster header usually is not fixed however it is chosen dynamically for every sensing interval on the basis of sensing data quality at every CU.

2.3 Attacks Detection

Malicious secondary users adversely impact spectrum sensing performance. These users are identified on the

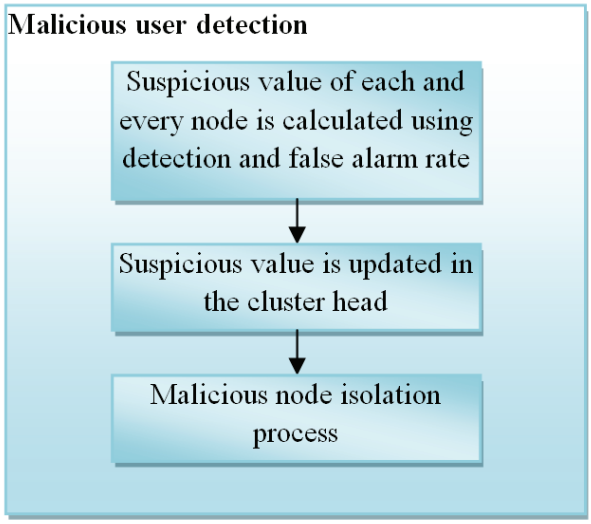

Figure 5. Proposed malicious user detection.

basis of specific network parameters like attack strength and probability. Hence to address this issue arising on account of suspicious level, calculation of nodes is carried out in the cluster. The suspicious value is then retained as a table in the cluster are shown in Figure 5.

2.3.1 Suspicious level calculation

Presence of malicious user in the network is assumed here. We define secondary users as:

$$S_i(t) \square P(T_i = M \mid F_t) \quad (14)$$

as the suspicious level of node i and j at time t, where T_n(= HorM) is the type of node and F_t represents all observations from time slot 1 to time slot t. The suspicious value calculation is described by Wang et al.[14]. The formula used for calculating the suspicious value is:

$$S_i(t) = \frac{\prod_{\tau=1}^{t} \theta_i(\tau)}{\sum_{j=1}^{N} \prod_{\tau=1}^{t} \theta_i(\tau)} \quad (15)$$

Where τ is a time slot, N is number of secondary users present in the cluster and $\theta_i(\tau)$ is a probability of reports at time slot t conditioned that node n is malicious.

$$\theta_i(\tau) = P_{d,i} + P_{f,i} \quad (16)$$

In the cluster users' suspicious values are computed, thereafter these are then updated as in the cluster head. Once spectrum sensing is completed, calculation of node suspicious value is carried out, where the suspicious value that exists below that of the threshold, node is considered as the honest node whereas the particular value that is inherent beyond the threshold, in that scenario that value is considered as malicious. After identification of node as being a malicious node, this information is then passed on to the cluster head. The cluster head in turn forwards the message to other cluster members. This leads to isolation of the suspicious node.

3. Experimental Results

In this section, performance evaluation is done for securespectrum sensing technique in comparison with conventional techniques. The minimum distance between the secondary users and the primary user is 1000m and the maximum distance is about 2000m. For the local spectrum sensing, the bandwidth-time creation[12,26,27] is m = 5. For the primary user transmission power is 200mW. The noise level σ^2 is about –110dBm. The Signal-to-Noise Ratio (SNR) of individual secondary user depends on its position and assumed Rayleigh fading. The parameters employed to measure the performance of the proposed technique are linear MMSE value. It should be noticed that the simulation is not carried out over a physical network model since the proposed work does not depends on any physical layer setting. In a cognitive radio system, each SU has a detection probability $P_{d,i}$ and a false alarm probability $P_{f,i}$ on a primary channel.

In Figure 6, the Linear Minimum Mean-Square Errors (LMMSEs) of the proposed spectrum sensing algorithm is compared with the existing algorithms such spectrum sensing based on HSMM and NN based spectrum sensing are plotted versus the noise variance σ_u^2. The sensing unit is modeled to have a detection probability of $P_d = 0.6$ and a false-alarm probability of $P_f = 0.2$. It is observed that the proposed algorithms achieve the lowest LMMSEs whereas other algorithms had the worst performance, as expected. In addition, as the noise variance increases, the LMMSEs increase and the performance of the estimators of the proposed approach obtained nearer to each other. The Table 1 shows that the values of the comparison

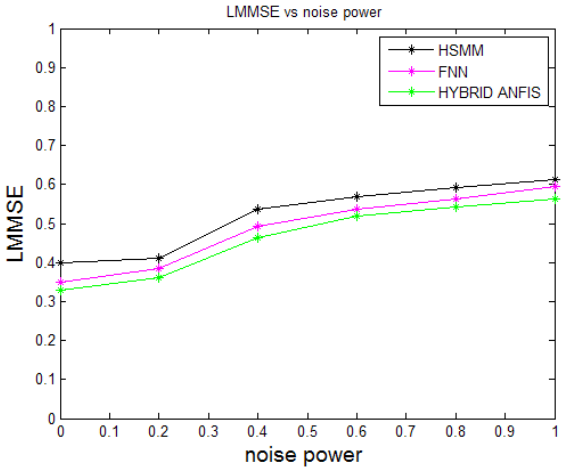

Figure 6. Comparison of LMMSE vs noise power.

Table 1. Comparison of LMMSE vs noise power

Noise power	HSMM based spectrum sensing	FNN based spectrum sensing	Hybrid Secure Spectrum sensing
0.2	0.41	0.385	0.361
0.4	0.536	0.4932	0.4634
0.6	0.568	0.5351	0.5183
0.8	0.593	0.5638	0.5429
1	0.613	0.5943	0.5618

of LMMSE vs. noise power for proposed and existing algorithms.

In Figure 7, the Linear Minimum Mean-Square Errors (LMMSEs) of the proposed spectrum sensing algorithm is compared with the existing algorithms such spectrum sensing based on HSMM and NN based spectrum sensing are plotted versus detection probability. It is observed that the proposed algorithms achieve the lowest LMMSEs whereas other algorithms had the worst performance, as expected. Table 2 shows that the values of the comparison of LMMSE vs detection probability for proposed and existing algorithms.

In Figure 8, the LMMSEs values of the proposed algorithm is compared with the existing algorithm such spectrum sensing based on HSMM and NN based spectrum sensing are plotted versus the false-alarm probability for a detection probability of and $P_d = 0.6$ a noise variance of $\sigma_u^2 = 0.2.$. It is observed that the LMMSEs increase as the false-alarm probability increases. This is mainly because the power of the pilot symbol is reduced (P_{tl} is employed) in the presence of a false alarm; that is, when

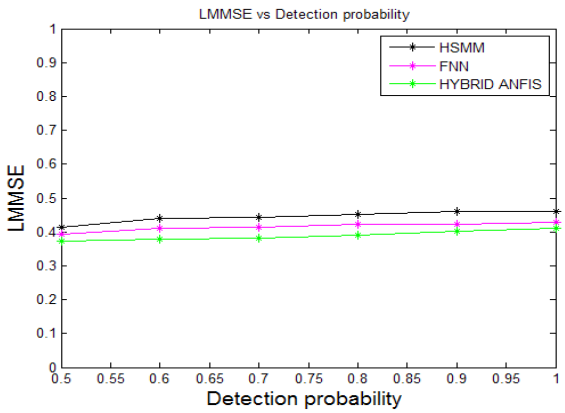

Figure 7. Comparison of LMMSE vs detection probability.

Table 2. Comparison of LMMSE vs detection probability

Detection probability	HSMM based spectrum sensing	FNN based spectrum sensing	Hybrid Secure Spectrum sensing
0.5	0.413	0.3932	0.3735
0.6	0.4386	0.4102	0.3796
0.7	0.4432	0.4138	0.3813
0.8	0.4516	0.4213	0.3918
0.9	0.4594	0.4238	0.4035
1	0.4612	0.4297	0.4106

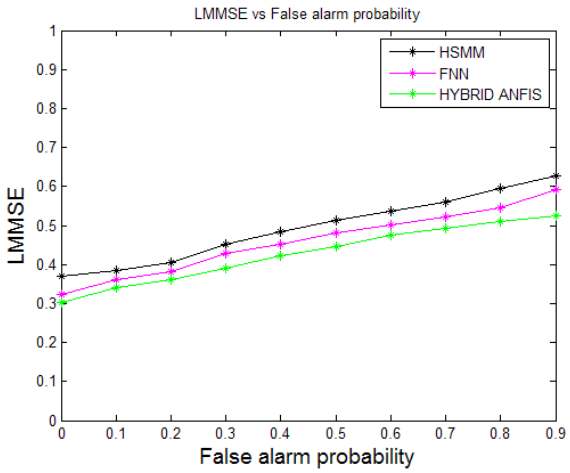

Figure 8. Comparison of LMMSE vs false alarm probability.

Table 3. Comparison of LMMSE vs false alarm probability

False alarm probability	HSMM based spectrum sensing	FNN based spectrum sensing	Hybrid Secure Spectrum sensing
0	0.3689	0.3231	0.3024
0.1	0.3838	0.3618	0.3413
0.2	0.4037	0.3816	0.3618
0.3	0.4514	0.4276	0.3917
0.4	0.4836	0.4518	0.4218
0.5	0.5137	0.4812	0.4467

the channel sensing unit decides that the primary users are present in the system when in fact they are not. Table 3 shows that the experimental values of the proposed algorithm and existing algorithms.

Power Spectral Density (PSD) of the received signal and a simplified function of frequency is minimized. The best fitting simplified function is then used to estimate the subband boundaries. The experimental validation stage has been organized by creating four methods such as optimal scheduling, Hidden Semi Markov Model (HSMM), Fuzzy Neural Network (FNN) and Hybrid Adaptive Neuro Inference System (ANFIS), in which several signals are located on different sub-bands. Two of them represent under various configurations that can be found in certain telecommunication bands.

In particular, the optimal scheduling scenario (Figure 9a) includes with different power density levels and symbol frequencies. The second HSMM (Figure 9b)

represents a frequency band, including signals. In this case, the signals located in the different subbands have different power density levels, but the same symbol period, since the spectrum segmentation is not performed in this schema.

A third Fuzzy Neural Network (FNN) scenario has been added to verify the limits of the methods in critical conditions (Figure 9c). It has been observed, in fact, that the proposed method can fail when signals with high differences in the PSD slopes are present within the observed spectrum. Therefore, in this third scenario, two signals have been provided. The former has a wide band and a high rolloff factor such that the PSD slope is very smooth; the latter is a narrowband signal with a low roll-off factor, thus having a sharp slope. Such a scenario has been repeated several times, by progressively reducing the bandwidth of the narrowband signal thus increasing spectrum sensing results. In Figure 9c, one of the PSDs of such Hybrid Adaptive Neuro Inference System (ANFIS) scenario is reported under malicious node identified results. So in this ANFIS model has been also repeated several times, by progressively reducing the bandwidth of the narrowband signal thus increasing spectrum sensing results and identification of malicious nodes

Figures 10 show the False alarm probability of density of malicious nodes α, the ratio of malicious

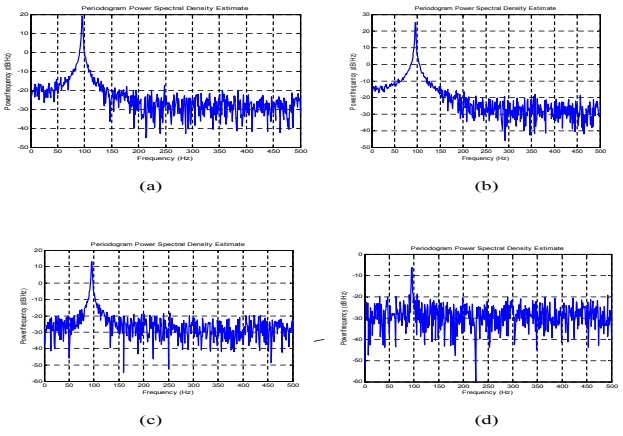

Figure 9. **(a)** PSDs of the Optimal schdeuling considered during the experimental validation phase. **(b)** PSDs of the Hidden Semi Markov Model (HSMM) considered during the experimental validation phase. **(c)** PSDs of the Fuzzy Neural Network (FNN) considered during the experimental validation phase. **(d)** PSDs of the Adaptive Neruo Fuzzy Interfernce System (ANFIS) considered during the experimental validation phase

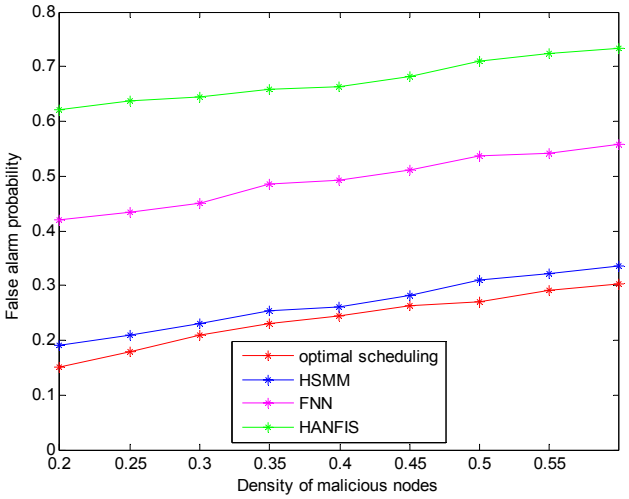

Figure 10. Comparison of the false alarm probability.

Table 4. False alarm probability of α when the population size increases to 1,000, nodes

Density value (α)	False alarm probability			
	optimal scheduling	HSMM	FNN	HANFIS
0.20	0.150	0.190	0.420	0.620
0.25	0.180	0.210	0.435	0.638
0.30	0.210	0.230	0.450	0.645
0.35	0.230	0.254	0.486	0.658
0.40	0.245	0.261	0.492	0.663
0.45	0.262	0.281	0.510	0.681
0.50	0.271	0.310	0.536	0.710
0.55	0.291	0.321	0.541	0.725
0.60	0.302	0.336	0.558	0.734

versus total number of nodes as 1000. The results confirm the behavior discussed earlier; we see a clear separation of the two classes only when the malicious nodes and non malicious nodes. When the density of malicious nodes approaches is 0.7341 for 0.6 density values. It shows that the false alarm detection probability of the proposed schema is high value when compare to other values. The false alarm detection probability of the other schemas such as optimal scheduling, HSMM and FNN are 0.302, 0.3361 and 0.5581 respectively which is very less when compare to proposed schema for the density value of 0.6 ,the values are tabulated in Table 4.

4. Conclusion

A novel spectrum sensing approach is proposed here which is based on artificial intelligence. This proposed work comprises of spectrum segmentation, spectrum sensing and malicious user detection in cognitive radio networks. A spectrum segmentation method is based on the evaluation of improved histogram of the PSD in the observed band is used for identifying the subband boundaries and it is separated by a low computational load. The secondary users are grouped into cluster the cluster head is selected based spectrum sensing. Hybrid ANFIS is proposed for identification of the spectrum hole or free subband in the spectrum that could be chosen to the aspiring SU. The possession is firmed by examining some channel parameters, e.g., SNR, channel capacity, BW efficiency and power spectral density also. The proposed algorithm indicates the channel status occupancy in a quantized index form {0, 1} after right training of the HANFIS.The malicious user is predicted in the cluster in order to avoid the false detection of primary user. The suspicious value is employed for identifying the malicious user. The estimator is used for detecting the false alarm probability and detection probability for proposed algorithms to evaluate the performance. Through by the use of the proposed sensing method, spectrum sensing error can be minimized by satisfying spectrum sensing requirement.

5. Reference

1. Spectrum policy task force report. Technical Report 02-135, Federal Communications Commission; 2002.
2. Mitola J. Software radio architecture. John Wiley & Sons; 2000.
3. Nguyen-Thanh N, Koo I. An efficient ordered sequential cooperative spectrum sensing scheme based on evidence theory in cognitive radio. IEICE Trans Commun. 2010 Dec; E93-B(12):3248–57.
4. Maleki S, Leus G. Censored truncated sequential spectrum sensing for cognitive radio networks. IEEE J Selected Areas Commun. 2013; 31(3):364–78 .
5. De Nardis L, Domenicali D, Di Benedetto MG. Clustered Hybrid Energy-aware cooperative Spectrum Sensing (CHESS). 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM '09), (IEEE Piscataway); Hannover. 2009 Jun 22-24. p. 1–6.
6. Hussain S, Fernando X. Approach for cluster-based spectrum sensing over band-limited reporting channels. IET Commun. 2012 Jul; 6(11):1466–74.
7. Guo C, Peng T, Xu S, Wang H, Wang W. Cooperative spectrum sensing with cluster-based architecture in cognitive radio networks. IEEE 69th Vehicular Technology Conference, IEEE Piscataway; Barcelona. 2009 Apr 26-29. p. 1–5.
8. Karami E, Banihashemi AH. Cluster size optimization in cooperative spectrum sensing. Ninth Annual Communication Networks and Services Research Conference (CNSR), IEEE Piscataway; Ottawa, ON. 2011 May 2-5. p. 13–17.
9. Reisi N, Ahmadian M, Jamali V, Salari S. Cluster-based cooperative spectrum sensing over correlated log-normal channels with noise uncertainty in cognitive radio networks. IET Commun. 2012 Nov; 6(16):2725–33.
10. Sun C, Zhang W, Letaief KB. Cluster-based cooperative spectrum sensing for cognitive radio systems. Proceedings of IEEE International Conference on Communications, IEEE Piscataway; Glasgow. 2007 Jun 24-28. p. 2511–5.
11. Mishra SM, Sahai A, Brodersen RW. Cooperative sensing among cognitive radios. IEEE International Conference on Communications ICC'06; 2006. p. 1658–63.
12. Ghasemi A, Sousa ES. Collaborative spectrum sensing for opportunistic access in fading environments. IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05); Baltimore, MD. 2005 Nov 8-11. p. 131–6.
13. Ganesan G, Li Y. Cooperative spectrum sensing in cognitive radio networks. IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05); Baltimore, MD. 2005 Nov 8-11. p. 137–43.
14. Wang W, Li H, Sun YL, Han Z. Attack-proof collaborative spectrum sensing in cognitive radio networks. 43rd Annual Conference on Information Sciences and Systems (CISS 2009); Baltimore, MD. 2009 Mar 18-20. p. 130–4.
15. Gao Z, Zhu H, Li S, Du S, Li X. Security and privacy of collaborative spectrum sensing in cognitive radio networks. IEEE Wireless Communications. 2012 Dec; 19(6):106–12.
16. Althunibat S, Sucasas V, Marques H, Rodriguez J, Tafazolli R, Granelli F. On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio. IEEE Communications Letters. 2013 Aug; 17(8):1564–7.
17. Wang W, Chen LN, Shin KG, Duan L. Thwarting intelligent malicious behaviors in cooperative spectrum sensing. IEEE Transactions on Mobile Computing. 2015 Nov; 14(11):2392–405.
18. Li S, Zhu H, Gao Z, Guan X, Xing K, Shen X. Location privacy preservation in collaborative spectrum sensing. 2012 IEEE Proceedings INFOCOM; Orlando, FL. 2012 Mar 25-30 p. 729–37.
19. Wang W, Chen L, Shin KG, Duan L. Secure cooperative spectrum sensing and access against intelligent malicious behaviors. 2014 IEEE Proceedings INFOCOM; 2014. p. 1267–75.

20. Oh DC, Lee YH. Energy detection based spectrum sensing for sensing error minimization in cognitive radio networks. International Journal of Communication Networks and Information Security (IJCNIS). 2009; 1(1):1–5.
21. Mitola J. Cognitive radio: An integrated agent architecture for software defined radio [PhD thesis]. Stockholm, Sweden: KTH; 2000.
22. Senthil Kumar B, Srivatsa SK. An efficient channel sensing algorithm based on hidden semi markov model and channel quality predicition. Research Journal of Applied Sciences, Engineering and Technology. 2014 Nov; 8(19):2064–70.
23. Jang JSR. Adaptive network based fuzzy inference system. IEEE Trans On Systems Man and Cybemetics. 1993 May-Jun; 23(3):665–85.
24. Jang JSR, Sun CT, Mizutani E. Neuro-fuzzy and soft computing. PTR Prentice Hall; 1997.
25. Nazzal JM, Elemary IM, Najim SA. Multilayer Perceptron neural network (MLPs) for analyzing the properties of Jordan Oil Shale. World Applied Sciences. 2008; 5(5):546–52.
26. Ghasemi A, Sousa ES. Opporstunistic spectrum access in fading channels through collaborative sensing. Journal of Communications (JCM). 2007; 2(2):71–82.
27. Dana A, Salehi N. Congestion aware routing algorithm for mesh network-on-chip platform. Indian Journal of Science and Technology. 2012 Jun; 5(6):2822–30.
28. Gharghi M, Parvinnia E, Khayami R. Designing a fuzzy rule base system to head cluster election in wireless sensor networks. Indian Journal of Science and Technology. 2013 May; 6(5):4410–5.
29. Gharehchopogh FS, Khaze SR, Maleki I. A new approach in bloggers classification with hybrid of K-nearest neighbor and artificial neural network algorithms. Indian Journal of Science and Technology. 2015 Feb; 8(3):237–46.
30. Abinaya R, Kamakshi S. Improving QOS using artificial neural networks in wireless sensor networks. Indian Journal of Science and Technology. 2015 Jun; 8(12):1–5.