JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-15, No.-1, January (2020) pp 39-56 ISSN (Print) 0973-8975

Malicious Node Restricted Quantized Data Fusion Scheme for Trustworthy Spectrum Sensing in Cognitive Radio Networks

Arpita Chakraborty[1], Jyoti Sekhar Banerjee[2], Abir Chattopadhyay[3]

[1,2] Dept. of ECE, Bengal Institute of Technology, Kolkata, INDIA-700150
[3]Dept. of ECE, University of Engineering & Management, Kolkata, INDIA-700156

[1]chakraborty_arpita2006@yahoo.com, [2]tojyoti2001@yahoo.co.in, [3]abir_chattopadhyay@yahoo.co.in

Corresponding Author: Arpita Chakraborty

https://doi.org/10.26782/jmcms.2020.01.00004

Abstract

Accuracy in spectrum sensing is very much required in cognitive radio network, which is a revolutionary paradigm to drift the spectrum underutilization problem. To enhance the detection performance in presence of shadowing or fading multiple SUs cooperate among themselves. But the collaboration and so the detection process is severely affected by the presence of some harmful secondary users known as Malicious users. As a result of this false sensing, spectrum wastage or interference with primary users may happen which are not at all desired for the system. The proposed approach in this paper has intelligently excluded these malicious users from the decision making process and thus improves the efficiency of the system.

Keywords : Cognitive radio, fusion rules, cooperative spectrum sensing, quantized fusion rule

I. Introduction

With the exponential growth of modern wireless applications the demand for available radio spectrum is increasing simultaneously, putting a significant pressure on the network. Consequently the static frequency distribution mechanism finds its inability to meet up the emerging need. Here came the most efficient and competent technology Cognitive Radio (CR) [VIII, XIII, XXXI], which exploits dynamic and opportunistic spectrum access strategy to resolve the problem of radio resource under utilization as well as miss utilization. In CR network, the unlicensed users or Secondary Users (SUs) may utilize the vacant licensed spectrum together with the Primary Users (PUs) maintaining a pre defined threshold value, i.e., interference temperature [XII, XXV, XXVI, XVIII-XX]. The most challenging part of SUs is to detect the presence of PU in order to acquire the unused spectrum. But in case of multi path fading or shadowed environment, it becomes difficult for SUs to properly detect the existence of the signal transmitted by PU and interference takes place. To confront this problem, the concept of “Collaborative Spectrum sensing” [I-III, IX, X, XVI, XXIV, XXXVII] has been introduced, where the decisions from multiple SUs have been considered to take a unanimous decision about the presence of primary signal. This situation demands from all the neighboring SUs to be very authentic, which may not be possible in real time always. Few SUs, who try to emulate the behavior of PU and transmit fake signals to the fusion center, are termed as Malicious Users (MUs). These MUs mislead the genuine SUs and hamper the system performance to a great extent. MUs can be identified through the process of evaluation of location information and monitoring strength of received signal as done in [XXIX]. Primary and secondary signals may be segregated using an algorithm for signal classification and is presented in [XXXV]. A natural defense mechanism [VII, XXII] to combat the intrusion of MUs has been shown in [XXXII]. The hazards created by MUs in distributed spectrum sensing have been discussed in [XXX]. Further different type of attacks in cognitive radio environment, their corresponding shielding mechanisms and other security [XXI] issues have been discussed in [XXXVI].

In this correspondence the authors have tried to eliminate the MUs from taking decision about the presence of PUs and thus the detection process and as well as the total performance of the entire system get improved. Each SU is evaluated on the basis of its quality of transmission, i.e., how reliably it can forward data to the destination, and accordingly, its suspicious level is measured. If the suspicious level of a specific SU becomes higher than a pre decided threshold level, it is treated as a MU and it is banned from taking part in the detection process. Thus, the secondary nodes are classified into honest users (HU) and malicious users (MU). After each transmission process, the suspicious level is being updated. Simulations without any defense mechanism as in [XXXII] and the proposed method with various specifications have been conducted in MATLAB platform. In absence of any defense mechanism the system performance gets deteriorated even in presence of a single MU and obviously it gets worse when multiple MUs are there. The proposed method significantly improves the performance of the detection process through segregating HUs from MUs and finally rejecting their reports from the final decision making process. If a node behaves genuinely and suddenly starts behaving bad, its suspicious level gets increased and when the value exceeds a pre-defined threshold it is treated as a MU and is banned. Finally, using Fuzzy logic the most eligible HUs are selected from various parameters and their respective decisions are considered for the detection of PU.

The rests have been arranged as follows. In section II, authors have described the system model comprising collaborative spectrum sensing process, Malicious Attack models and a table containing list of notations used throughout. Section III explicitly describes the claimed approach of trustworthy collaborative spectrum sensing using Fuzzy logic based Data Fusion Scheme. In section IV experimental simulations, used parameters and obtained various graphs have been produced to prove the supremacy of the proposed approach over the existing mechanisms. Section V concludes the paper and puts few glimpses on future scope of it too.

II. System Model

Under this section we'll be describing the concept of cooperative spectrum sensing [V, VI] and the disturbances caused by the malicious users.

A. Collaborative Spectrum Sensing

Here in this section cooperative spectrum sensing scheme and the malicious users (MU) created probable disturbances have been described. As a channel experiences shadowing or fading, the spectrum sensing performance also degrades significantly. To overcome these problems collaborative sensing has been proposed that combines several secondary users' (SU) results of detection for achieving better performance. This process is popularly known as collaborative spectrum sensing (CSS).

In this correspondence we have considered a centralized cooperative spectrum sensing network model that consists of a number of Cognitive Radio (CR) [XIV-XVII] users or Secondary User (SU) and an Access point or Fusion Center (FC). We have chosen the most popular and dominating approach of cooperation among CR users for spectrum sensing -'Parallel Fusion Scheme'- [X] (see fig. 1) as it emphasizes the sensing process comely.

Without loss of generality let there are V (such that $V = \{ i = 1,2, \ \ldots.., \ V \}$) number of SUs in a geographical area and among them only N number of SUs can take part in cooperation due to availability of free channels. We use a variable ch_i^b to denote the channel availability:

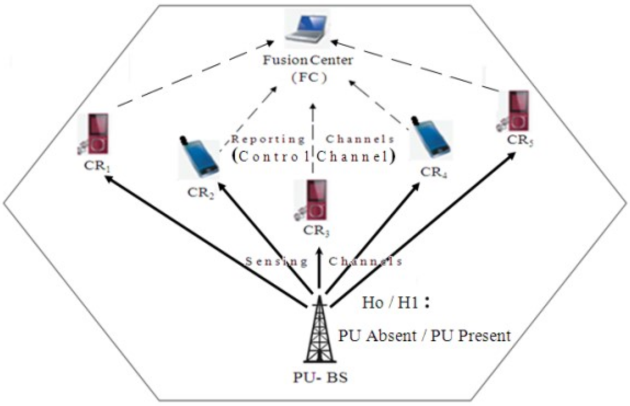


Fig. 1 Parallel Fusion Scheme of CSS in Cognitive radio System

$$ch_i^b = \begin{cases} 1, \ ch \ \ b \in B \ \text{of} \ \ i\,\text{th} \ \ \text{SU} \ \ \text{is available} \\ 0, \ ch \ \ b \in B \ \text{of} \ \ i\,\text{th} \ \ \text{SU} \ \ \text{is un - available} \end{cases}$$

(1)

Here B is the set of equal-bandwidth channels available in that geographical area for both PUs and SUs. Again $N(\in V)$ may be represented as:

$$N = \sum_{i \in V} v_i \Big| ch_i^b = 1 \tag{2}$$

Suppose each SU utilizes K (such that $K = \{k = 1,2, \ldots\ldots, K\}$) number of samples from the signal received for the purpose of energy detection [XVII] during the process of spectrum sensing. Hence sensing of spectrum can be basically reduced to an identification problem and modeled as binary hypothesis test consisting of two hypotheses H_0 (Absence of PU) and H_1(Presence of PU). The signals under hypothesis are of the following form:

$$H_0 : \quad Y(k) = n_i(k) \tag{3}$$

$$H_1 : Y(k) = h_i . S(k) + n_i(k) \tag{4}$$

Where $Y(k)$ is the signal received by SUs, $S(k)$ are samples of the signal transmitted by (PU), $n_i(k)$ is the noise of the receiver for the ith CR user, that is considered to be an i.i.d. random process with zero mean, unit variance and independent of the primary signal under H_1. To study the impact of the detection ability of ith SU, 'Detection probability' (Pd_i) and 'false alarm probability' (Pf_i) are defined as follows:

$$Pd_i = \Pr\left\{\Psi_i = 1 \middle| H_1\right\} \tag{5}$$

$$Pf_i = \Pr\left\{\Psi_i = 1 \middle| H_0\right\} \tag{6}$$

All the FC synchronized CR users, sense the presence of Primary User (PU) individually and their sensed local data are forwarded to the FC through the bandwidth limited common control channels. By combining the sensing data [XI] from different cooperating SUs FC takes the central cooperative decision regarding the presence or absence of the PU. There are various methods for combining these data like Hard decision fusion, Soft decision fusion, Quantized data fusion, and Non uniform Quantized data fusion schemes. For better understanding the notations have been put in tabular manner (Table 1) as below:

B. Malicious Intrusion

To combat multipath fading, receiver uncertainty problem in order to detect the presence of PU, SUs cooperate among themselves, which is popularly known as Cooperative Spectrum Sensing and from studies it is seen that this process improves the primary user detection significantly. But at the same time, this process suffers from the attack of malicious users also.

Table 1: Notations used in this paper

Notations	**Definitions**
V	Number of SUs in a geographical area
N	Number of SUs can take part in cooperation

ch_i^b	channel availability
$\Pr(A)$	Attack Probability
φ	Attack strength
ξ	Attack threshold
$\omega_n(t)$	Sensed energy of n^{th} node
$R_n(t)$	Report forwarded to FC by n^{th} node
E_t	All observations from time slot 1 to 't'
$\gamma_n(t)$	Suspicious Level of n^{th} node
λ_n	Type of a node, $\lambda_n \in \{HU, MU\}$
η	Suspicious threshold
α	Malicious User (MU) set
β	Honest User (HU) set
R_β	Reporting set of HUs
$\Pi_n(t)$	Trust Factor
$Q_i\left(Ch_{Sensing}, Ch_{Reporting}\right)$	Quality of sensing and reporting channel

Malicious Users (MU)

All the cooperating SUs are not cooperative actually; few of them are malicious also who reduce the throughput of the CR network by reporting high energy values when the PU signal is not present even. The malicious users then transfer its own message over the vacant channel selfishly. Thus in two ways MUs attack the CSS scheme: i) they either transmit high energy signal indicating presence of PU, when PU is not actually present there and hence probability of false alarm (Pf_i) gets increased and available bandwidth for CR system decreases. ii) MUs can also transmit low energy valued signal indicating the absence of PU, when PU is actually there and thus probability of detection (Pd_i) gets decreased causing interference with the PU or licensed system.

Malicious Attack Models

Malicious attacks are modeled in terms of the following three parameters, i) Attack Threshold ξ, ii) Attack Strength φ , and iii) Attack Probability $\Pr(A)$. Let the nth node's observation about the presence of PU and its report forwarded to the FC at time slot 't' be denoted by $\omega_n(t)$ and $R_n(t)$ respectively. Thus the two attack models are described as follows:

False Alarm (FA) Attack: It is not obvious that the attacker will attack in all the rounds, rather it randomly decides to attack or not in a round with probability $\Pr(A)$. In a particular time slot 't', if the sensed energy $\omega_n(t)$ is observed to be greater than the attack threshold (ξ), the attacker does not attack and reports only $\omega_n(t)$; otherwise, the attacker will attack with probability $\Pr(A)$ and it will report $\omega_n(t)+\varphi$. This process is summarized as follows:

$$R_n(t) = \begin{cases} \omega_n(t) & \text{if } [\omega_n(t) > \xi] \;\; ; \Rightarrow \text{No Attack} \\ \omega_n(t)+\varphi & \text{if } [\omega_n(t) < \xi] \;\; ; \Rightarrow \text{Attack with probability (Pr(A))} \end{cases} \tag{7}$$

False Alarm and Miss Detection (FAMD) Attack: In every time slot the attacker chooses to attack or not with probability $\Pr(A)$. In case it does not attack, the attacker reports only $\omega_n(t)$ exactly what it has sensed. Otherwise, i.e. when the MU decides to attack with probability $\Pr(A)$, it reports the following:

$$R_n(t) = \begin{cases} (\omega_n(t)-\varphi) & \text{if } [\omega_n(t) > \xi] \;\; ; \Rightarrow \text{Attack with probability (Pr(A))} \\ (\omega_n(t)+\varphi) & \text{if } [\omega_n(t) < \xi] \;\; ; \Rightarrow \text{Attack with probability (Pr(A))} \\ \omega_n(t) & \Rightarrow \text{No Attack} \end{cases} \tag{8}$$

Detection and Elimination of Ideal Malicious Nodes

In this correspondence we have adopted a heuristic "onion peeling" approach to detect the ideal malicious user set in a batch by batch way. According to the reports Type of a Node or User (λ_n) can be Malicious (MU) or Honest (HU) and (E_t) is assumed to be all observations from time slot 1 to 't'. The possibility of a secondary node to be MU gets decided from its 'Suspicious Level' $\gamma_n(t)$, which is again calculated in the following way from the report $R_n(t)$ conveyed to the FC:

$$\begin{aligned} \gamma_n(t) &= \Pr(\lambda_n = MU | E_t) \\ &= \frac{\Pr(E_t|\lambda_n = MU)\Pr(\lambda_n = MU)}{\Pr(E_t|\lambda_n = MU)\Pr(\lambda_n = MU) + \Pr(E_t|\lambda_n = HU)\Pr(\lambda_n = HU)} \end{aligned} \tag{9}$$

If the Suspicious Level $(\gamma_n(t))$, which shows the possibility of a node to be MU, crosses a certain threshold (η), the node is treated as a malicious node. Mathematically it can be formulated as below:

$$SU_n \leftarrow MU\big|(\gamma_n(t) \geq \eta)$$

or, $$SU_n \leftarrow MU\Big|_{Pr(\lambda_n = MU|E_t)} \geq \eta \tag{10}$$

Here the value of η is chosen to be 0.99 and can be modified as per requirement. Next the report forwarded by this nth MU node will be rejected by FC from PU detection process and will be added to the MU set (α) such that $\alpha \subset \{1, ..., N\}$ and α can even be an empty set that indicates not a single MU is present.

$$\therefore \quad SU_n \leftarrow MU\big|_{(\gamma_n(t) \geq \eta)} \in \alpha \quad ; \forall n \in N \tag{11}$$

Thus the MUs and their reports $R_n(t)$ are screened out by the FC in the first phase and hence a trustworthy CSS can be achieved. The rest SUs whose 'Suspicious Level' $\gamma_i(t)$ is below the threshold η are not malicious (MU) and are referred to as Honest users (HU) as follows:

$$SU_i \leftarrow HU\big|_{(\gamma_i(t) < \eta)}$$

or, $$SU_i \leftarrow HU\Big|_{Pr(\lambda_i = HU|E_t) < \eta} \tag{12}$$

These non malicious users belong to the HU set (β) and it is defined as below:

$$SU_i \leftarrow HU\big|_{(\gamma_i(t) < \eta)} \in \beta \quad ; \forall i \in N$$

$$\therefore \quad \beta = \left\{HU_i\big|_{i \notin \alpha}\right\} ; \forall i \in N \text{ and } (\alpha \cap \beta) = \phi \tag{13}$$

The individual reports of the HUs are stored to FC under the set Honest User's reporting set (R_β) and can be formulated as: $R_\beta = \left\{R_i\Big|_{\substack{i \in \beta \\ \& i \notin \alpha}} \quad ; \forall i \in N\right\}$ and the reports from MUs $\left(R_j\big|_{j \in \alpha}\right)$ are rejected by FC.

III. Proposed Trustworthy Collaborative Spectrum Sensing using Fuzzy Logic Based Data Fusion Scheme

We have studied different CSS mechanisms where all the SUs with available channels use to take part in spectrum sensing process with the aim to detect the presence of PU. But participation of MUs actually hampers this process as they cause both high False alarm and Miss Detection. To achieve trustworthy spectrum sensing MUs are first detected on the basis of their Suspicious Level $(\gamma_n(t))$ and are excluded in the first phase of CSS. Even in the next phase all the Honest (HU) or non malicious SUs will not take part in the detection process of PU. Rather they will be evaluated further on the basis of some important parameters like SNR, Trust Factor, Quality of sensing and reporting channel and accordingly their fitness values will be calculated using Fuzzy Logic, the multi valued decision making engine.

Fitness Measuring Parameters

1. **SNR:** It is a very popular metric for cooperative SU selection and is calculated at the FC in the following way,

$$\mathrm{SNR}_{\mathrm{FC}}\left(\mathrm{SU}_{\mathrm{i}}\right)\Big|_{\mathrm{i}\in\beta} = \frac{\mathrm{E}_{\mathrm{S}}\left|\mathrm{h}_{\mathrm{SU}_{\mathrm{i}},\mathrm{FC}}\right|^{2}}{\mathrm{N}_{0}\mathrm{B}} \tag{14}$$

Here, $\mathrm{E_S}$ is the transmitted signal energy during each detection interval, $\mathrm{N_0}$ is the band noise, and B is the total band width.

2. **Trust Factor:** The trust factor $(\Pi_n(t))$ gives a measure of reliability of a particular user. Basically this

parameter calculates the possibility of a SU to be reliable or authentic. Again this factor gets calculated from the reports $(\mathrm{R_n}(t))$ they have conveyed to the FC as shown in the equation 15.

$$\begin{aligned} &\Pi_n(t) = \Pr\left(\lambda_{\mathrm{n}} = \mathrm{HU}\,|\mathrm{E}_{\mathrm{t}}\right) \\ \therefore\quad &\Pi_n(t) = 1 - \gamma_n(t) \end{aligned} \tag{15}$$

3. **Quality of Sensing and Reporting Channel:** It describes the SU node's sensing as well as reporting channel quality. The SUs who have vacant channels can take part in cooperative detection of PU. FC decides which channel to be scanned in order to determine the presence of PU and the cooperating SU scans that very channel using its sensing channel and reports back to FC using its reporting channel. In other words sensing channel is the link persisting between the selected secondary node $\mathrm{SU_i}$ and the channel to be scanned. Reporting channel is the link between $\mathrm{SU_i}$ and FC. Instantaneous gains of the sensing channel $\mathrm{H_{i,\,PU}}(\mathrm{Ch_{Sensing}})$ and reporting channel $\mathrm{H_{i,\,PU}}(\mathrm{Ch_{Reporting}})$ are formulated as,

$$\mathrm{H}_{\mathrm{i,\,PU}}\left(\mathrm{Ch}_{\mathrm{Sensing}}\right) = \left|\mathrm{h}_{\mathrm{i,PU}}\right|^{2} = \left\{\mathrm{d}_{\mathrm{i,\,PU}}^{-\alpha} \times \left|\mathrm{g}_{\mathrm{i,PU}}\right|^{2}\right\}\ ;\ \mathrm{i}\in\beta \tag{16}$$

$$\mathrm{H}_{\mathrm{i,\,FC}}\left(\mathrm{Ch}_{\mathrm{Reporting}}\right) = \left|\mathrm{h}_{\mathrm{i,FC}}\right|^{2} = \left\{\mathrm{d}_{\mathrm{i,\,FC}}^{-\alpha} \times \left|\mathrm{g}_{\mathrm{i,FC}}\right|^{2}\right\}\ ;\ \mathrm{i}\in\beta \tag{17}$$

Here, the concept of aggregate channel model has been employed that considers both path loss and slow Rayleigh fading (i.e., channel coefficients are stationary during one time slot) [XV] in order to simulate the wireless environment. Here α is the path loss coefficient, $\mathrm{d_{i,j}}$ is the distance between nodes i and j and $\mathrm{g_{i,j}}$ is the fading coefficient modeled as a zero-mean, complex Gaussian random variable with unit variance ($\sigma^2_{\mathrm{i,j}} = 1$). All the channels are considered to be slow fading and their information may be obtained through RTS/CTS of IEEE802.11. The overall quality of sensing and reporting channel $\mathrm{Q_i}\left(\mathrm{Ch_{Sensing}}, \mathrm{Ch_{Reporting}}\right)$ of a particular $\mathrm{SU_i}$ is formulated as the linear weighted combination of Instantaneous reporting and sensing channel gains as below,

$$\mathrm{Q_i}\left(\mathrm{Ch_{Sensing}}, \mathrm{Ch_{Reporting}}\right) = \mathrm{W_1} * \mathrm{H_{i,PU}}\left(\mathrm{Ch_{Sensing}}\right) + \mathrm{W_2} * \mathrm{H_{i,FC}}\left(\mathrm{Ch_{Reporting}}\right);\ \mathrm{i}\in\beta \tag{18}$$

Here the value of W_1 and W_2 are chosen arbitrarily in such a way that their sum results unity, i.e., $(W_1 + W_2 = 1)$ and $(W_2 = 1 - W_1)$. In this correspondence, both the Sensing and Reporting channels are assumed to be equally important and hence their corresponding weights are set equal, i.e., $W_1 = W_2 = 0.5$. Otherwise, the weights of the corresponding channels may be set according to its importance and as per user's choice.

More Reliable Honest User (HU) selection from Fitness value measured by Fuzzy Rule base

Introduction to Fuzzy Logic

In this section we have discussed fuzzy logic briefly [IV, XIV-XV, XXIII, XXVII-XXVIII, XXXIII-XXXIV]. Usually the steps followed in fuzzy logic are described as follows:

1. Receive input parameters to analyze.
2. Formation of Rule base using if-then fuzzy rule base.
3. Derive a single output by doing average and weighting the results of every individual rule.
4. Apply defuzzification of the output.

Application of fuzzy logic helps in averaging the sharp segregation between normality and abnormality.

Proposed Scheme

The SUs from HU set (β) are again evaluated and their fitness values are calculated with respect to the above mentioned three parameters SNR, Trust Factor and Quality of Sensing and Reporting channel. Next on the basis of fitness value of individual SU, a few will be selected from the lot and More Reliable HU (MRHU) is formed whose reports will actually be considered for the detection of PU (shown in Fig. 2). Here we are using Fuzzy Logic based fitness calculation. Let the inputs to the Fuzzy controller for an individual SU be SNR, Trust Factor and Quality of Sensing and Reporting channel and their corresponding output be Fuzzy Fitness value of that SU, where X, Y, Z are input variables and the corresponding output variable W are described as follows:

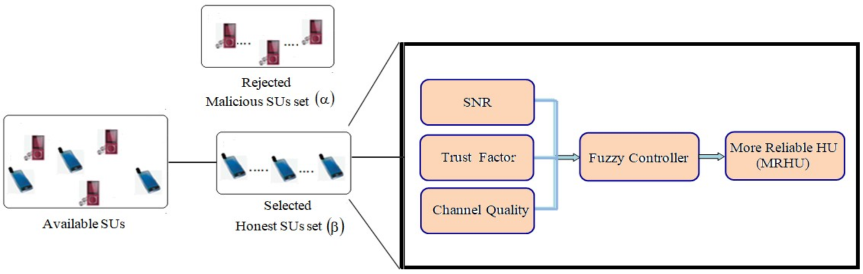


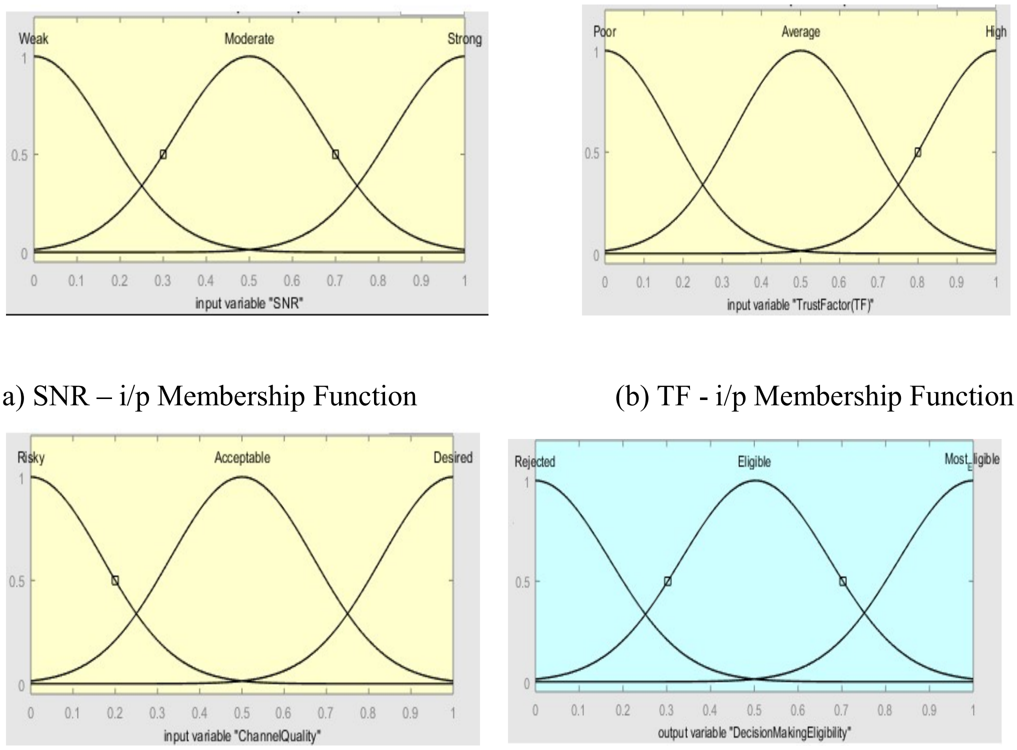
Fig. 2. Fuzzy Controller for More Reliable HU selection rejecting MU

$$\mu_{D_q}(W_{SUi}) = f\left\{T\left(\mu_{A_m}(X_{SUi}), \mu_{B_n}(Y_{SUi}), \mu_{C_p}(Z_{SUi})\right)\right\}$$

$$= \arg\ \text{Max}\left[\text{Min}\left\{\mu_{A_m}(X_{SUi})\, t\, \mu_{B_n}(Y_{SUi})\, t\, \mu_{C_p}(Z_{SUi})\right\}\right], \quad m, n, p, q \in (1,2,3) \tag{19}$$

$$\begin{aligned} &X = SNR_{FC} \in \{A_1, A_2, A_3\} \in \{\text{Weak, Moderate, Strong}\}, \\ &Y = \text{Trust factor (TF)} \in \{B_1, B_2, B_3\} \in \{\text{Poor, Average, High}\}, \\ &Z = Q\left(Ch_{Sensing}, Ch_{Reporting}\right) \in \{C_1, C_2, C_3\} \in \{\text{Risky, Acceptable, Desired}\}, \\ &W = \text{Eligibility} \in \{D_1, D_2, D_3\} \in \{\text{Rejected, Eligible, Most Eligible}\} \end{aligned}$$

The fuzzy membership functions for the three inputs and one output criteria are shown in the Fig. 3;



a) SNR – i/p Membership Function

(b) TF - i/p Membership Function

(c) Channel Quality –i/p Membership Function

(d) Decision making eligibility – o/p Membership

Fig. 3. Membership functions of different input and output fuzzy sets

Applying inputs to the Fuzzy Inference System (FIS) (shown in the Fig. 4.), which is considered to be Mamdani here, the output fuzzy set (Most Eligible HU) is obtained as shown in the Fig. 3. In order to get the system output, according to the inputs applied, we have designed 27 fuzzy rules. The output membership function of the Eligibility of the HU gets selected employing the 27 rules and thus the More Reliable HU is selected.

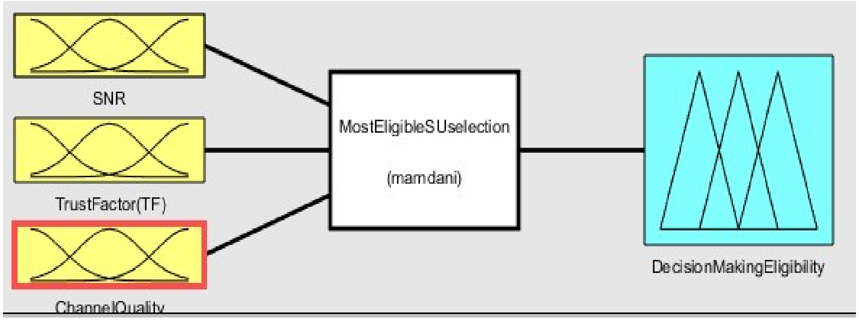
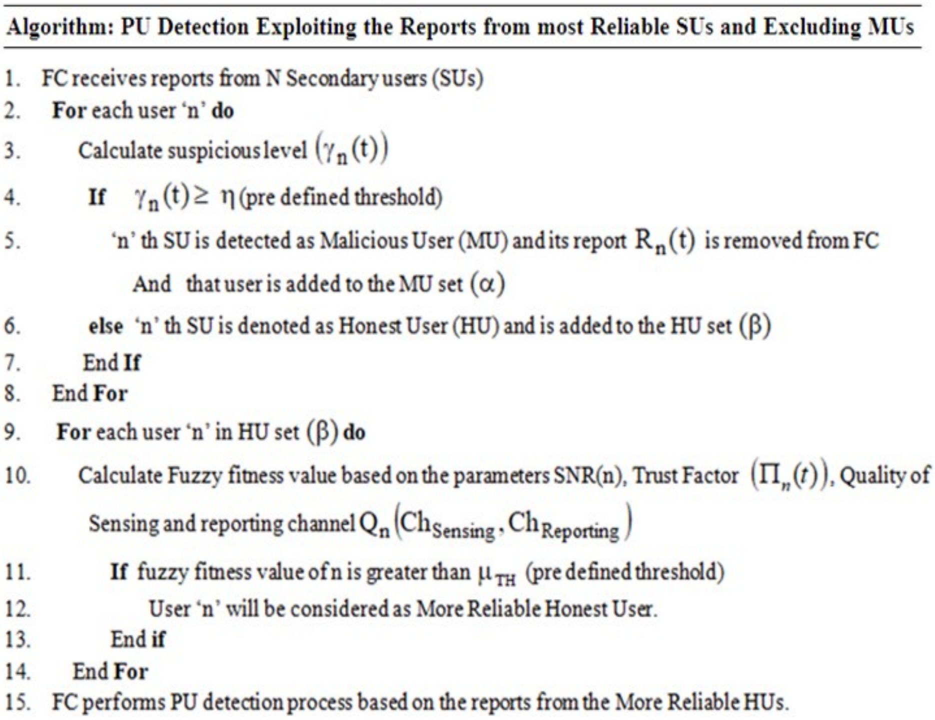


Fig. 4. Model of the proposed Most Eligible HU selection System (Mamdani Type)

If the fuzzy membership value of a particular HU is greater than μ_{TH}, which is a pre defined threshold (here it is assumed to be 0.5), it is treated as the most eligible HU and its report is considered for the detection of PU. Finally, the decision $(\Psi(t))$ regarding the presence or absence of PU is taken by the FC in the following way

$$\Psi(t) = T\left(R_{\beta 1}, R_{\beta 2}, ..., R_{\beta i}\right) \ \forall i \in \beta \ \& \left(\mu_{D_q}\left(W_{SUi}\right) \geq \mu_{TH}\right) \qquad (20)$$

T is a data fusion operator processing the reports conveyed by the most eligible SUs. The algorithm for detection of the PU exploiting the reports from most reliable SUs and excluding the reports of MUs, is presented below;

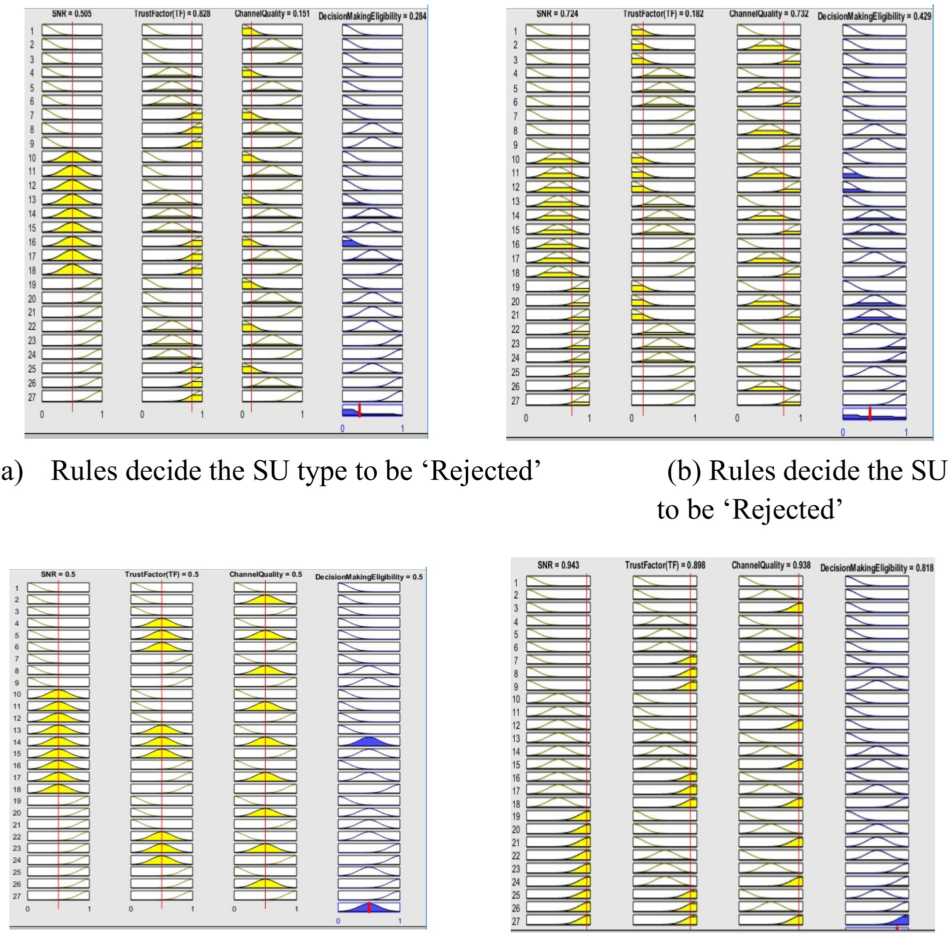


Algorithm: PU Detection Exploiting the Reports from most Reliable SUs and Excluding MUs

```
FC receives reports from N Secondary users (SUs)
 For each user 'n' do
     Calculate suspicious level $(\gamma_n(t))$
       If   $\gamma_n(t) \geq \eta$ (pre defined threshold)
           'n' th SU is detected as Malicious User (MU) and its report $R_n(t)$ is removed from FC
              And  that user is added to the MU set $(\alpha)$
       else 'n' th SU is denoted as Honest User (HU) and is added to the HU set $(\beta)$
       End If
 End For
 For each user 'n' in HU set $(\beta)$ do
     Calculate Fuzzy fitness value based on the parameters SNR(n), Trust Factor $(\Pi_n(t))$, Quality of
       Sensing and reporting channel $Q_n(Ch_{Sensing}, Ch_{Reporting})$
         If fuzzy fitness value of n is greater than $\mu_{TH}$ (pre defined threshold)
              User 'n' will be considered as More Reliable Honest User.
         End if
     End For
 FC performs PU detection process based on the reports from the More Reliable HUs.
```

IV. Results and Discussion

Here simulation results have been presented for the sake of establishing results analytically. Authors have chosen Fuzzy logic for simulation as it considers logic of multiple values and multiple inputs to drive the final decision. The results of simulation have been depicted in Fig. 5 and 6. Figure. 5 explains the decision making eligibility of a SU based upon different i/p conditions. Figure. 5(a) and (b) depict that the selected SU is of group 'Rejected' as either Channel quality or Trust Factor is Low in spite of other input parameters to be considerable. Figure. 5(c) demonstrates that the selected SU is of group 'Eligible' as all the three input parameters are of average value and figure. 5(d) decides the user to be 'Most Eligible' as all the three inputs are having high values.



(a) Rules decide the SU type to be 'Rejected' (b) Rules decide the SU to be 'Rejected'

(c) Rules decide the SU to be 'Eligible' (d) Rules decide the SU type to be 'Most Eligible'

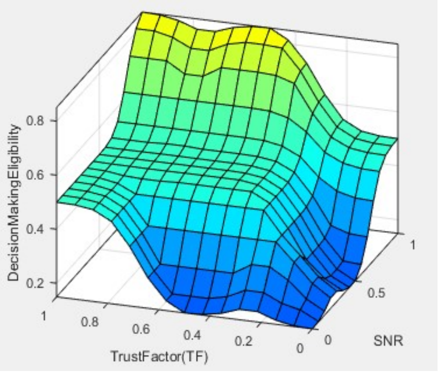
Fig. 5. The fuzzy inference rules based on the Mamdani fuzzy Inference system (FIS)

Membership value calculation of the SUs are executed varying different selection parameters like SNR, Trust factor and Channel Quality and are documented in the following Table 2.

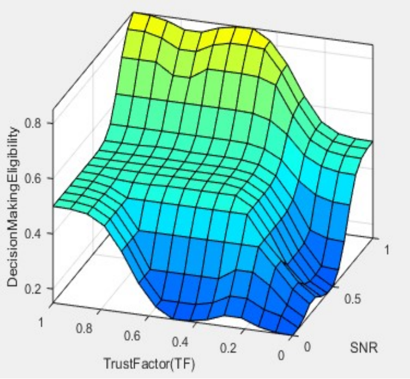
Table 2: Membership values of SUs obtained from Mamdani-type FIS

SNR	Trust Factor	Channel Quality	Decision making Eligibility	Comment
0.724	0.182	0.732	0.429	Rejected
0.505	0.828	0.151	0.284	Rejected
0.141	0.714	0.776	0.396	Rejected
0.807	0.849	0.859	0.703	Eligible
0.5	0.5	0.5	0.5	Eligible
0.516	0.807	0.568	0.502	Eligible
0.937	0.947	0.926	0.819	Most Eligible

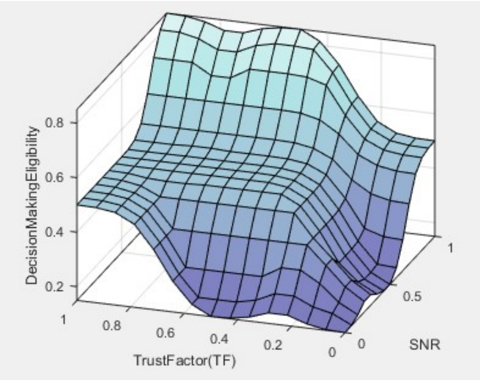
Figure.6 (a), (b) and (c) describe the surface view of the system which show the chances of the decision making ability of the SU to be 'Most Eligible' as both Channel Quality and Trust Factor are 'Desired' and 'High' (shown in Figure.6 (a)) Figure 6(b) shows the decision making eligibility of SU to be 'Rejected' as Trust Factor is 'Poor', though SNR is 'Strong'. Decision making capability of SU is 'Eligible' as both Trust Factor and SNR are 'Average' or 'moderate' (shown in figure 6(c)).



(a)



(b)



(c)

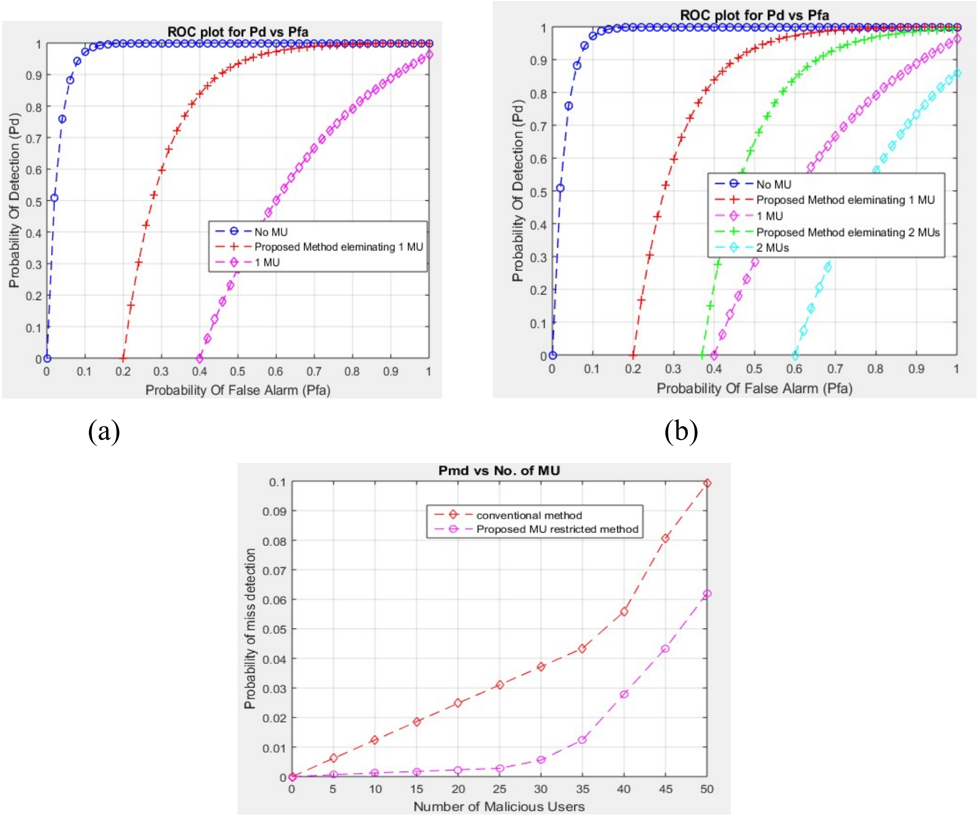
Fig. 6. (a), (b), (c) Surface view of Mamdani-type FIS

In Fig. 6 authors have plotted ROC for Pd versus Pfa in different environments like in presence or absence of MUs considering the parameters given in table3 to simulate in MATLAB software. Probability of detection (Pd) gets improved as the MUs have been detected and rejected from the decision making process.

Table 3: Parameters for Simulation in MATLAB platform

Simulation parameters	
Primary Data Rate	0.4 bits/s/Hz
Secondary Data Rate	0.2 bits/s/Hz
$\sigma^{2}_{PT,\mathrm{PD}} = \sigma^{2}_{ST,\mathrm{SD}} = \sigma^{2}_{ST,\mathrm{SRi}} = \sigma^{2}_{\mathrm{SRi},SD}$	1
$\sigma^{2}_{PT,\mathrm{SD}} = \sigma^{2}_{ST,\mathrm{PD}}$	0.1
$\sigma^{2}_{PT,\mathrm{SRi}} = \sigma^{2}_{\mathrm{SRi},PD}$	0.2
Transmit SNR	25dB
Number of Cooperating Relays	4

In figure.7(c) we have plotted variation of probability of miss detection (Pmd) in presence of number of MUs in the one hop neighbor. It is proved from the simulation results that the proposed method outperforms the conventional methods in terms of detection probability eliminating MUs. Even, probability of miss detection gets reduced as MUs are rejected from decision making in the proposed scheme of this correspondence.



(a)

(b)

(c)

Fig. 7. (a) Pd vs Pfa behavior in proposed method rejecting 1MU, (b) comparison of Pd vs Pfa behavior in proposed method rejecting 1&2 MUs, (c) Pmd vs Number of MUs

V. Conclusion

Malicious SUs may hamper the collaborative spectrum sensing performance massively. Hence these harmful MUs are to be detected wisely and consequently their decisions are to be rejected while taking decision regarding the presence or absence of SUs. In this correspondence, the most important selection technique for most eligible SUs based on fuzzy logic is proposed in multi-user cooperative cognitive radio systems. This proposed technique has considered three input parameters for eligible SU selection jointly viz, SNR, Channel Quality and Trust Factor, to combat against the untrustworthy SUs with the aim to improve system performance. This fuzzy logic–based practicable solution for eligible secondary user selection is not complex rather less time consuming. So, it can be comfortably evolved into application programs and further can be utilized in real-time scenario.

References

I. A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05), pp. 131– 136, November 2005

II. A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, vol. 2, no. 2, pp. 71–82, 2007

III. A. Ghasemi, & E. S. Sousa, "Spectrum sensing in cognitive radio networks: the cooperation-processing tradeoff", Wireless Communications and Mobile Computing, 7(9), 1049-1060, 2007

IV. A. Chakraborty, and J.S. Banerjee, "An Advance Q Learning (AQL) Approach for Path Planning and Obstacle Avoidance of a Mobile Robot". International Journal of Intelligent Mechatronics and Robotics, 3(1), pp 53-73 2013

V. A. Chakraborty, J. S. Banerjee, and A. Chattopadhyay, "Non-Uniform Quantized Data Fusion Rule Alleviating Control Channel Overhead for Cooperative Spectrum Sensing in Cognitive Radio Networks". In: Proc. IACC, pp 210-215 2017

VI. A. Chakraborty, J. S. Banerjee, and A. Chattopadhyay, "Non-uniform quantized data fusion rule for data rate saving and reducing control channel overhead for cooperative spectrum sensing in cognitive radio networks", Wireless Personal Communications, Springer, 104(2), 837-851, 2019

VII. D. Das, et. al., "Analysis of Implementation Factors of 3D Printer: The Key Enabling Technology for making Prototypes of the Engineering Design and Manufacturing", International Journal of Computer Applications, pp.8-14, 2017

VIII. E. Hossain, D. Niyato, and Z. Han, "Dynamic Spectrum Access in Cognitive Radio Networks", Cambridge University Press, Cambridge, UK, 2008

IX. E. Visotsky, S. Ku ffher, and R. Peterson, "On collaborative detection of TV transmissions in support of dynamic spectrum sharing", in Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05), pp. 338–345, Baltimore, USA, November 2005

X. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Physical Communication (Elsevier) Journal, vol. 4, no. 1, pp. 40-62, March. 2011

XI. I. Pandey, et. al., "WBAN: A Smart Approach to Next Generation e-healthcare System", In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 344-349, IEEE, 2019

XII. J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal", IEEE Personal Communications, vol. 6, no. 4, pp. 13–18, 1999

XIII. J. Mitola III, "Cognitive Radio--- An Integrated Agent Architecture for Software Defined Radio".Royal Institute of Technology, 2000

XIV. J. S. Banerjee, A. Chakraborty, and A. Chattopadhyay, "Relay node selection using analytical hierarchy process (AHP) for secondary transmission in multi-user cooperative cognitive radio systems", in Proc. ETAEERE 2016, LNEE-Springer, Dec. 2016

XV. J. S. Banerjee, A. Chakraborty, and A. Chattopadhyay, "Fuzzy based relay selection for secondary transmission in cooperative cognitive radio networks", in Proc. OPTRONIX 2016, Springer, India, Aug. 2016

XVI. J. S. Banerjee, et. al., "A Comparative Study on Cognitive Radio Implementation Issues", International Journal of Computer Applications, vol.45, no.15, pp. 44-51, May.2012

XVII. J. S. Banerjee, A. Chakraborty, and A. Chattopadhyay, "Reliable best-relay selection for secondary transmission in co-operation based cognitive radio systems: A multi-criteria approach", Journal of Mechanics of Continua and Mathematical Sciences, 13(2), 24-42, 2018

XVIII. J. S. Banerjee, and A. Chakraborty, "Fundamentals of Software Defined Radio and Cooperative Spectrum Sensing: A Step Ahead of Cognitive Radio Networks". In Handbook of Research on Software-Defined and Cognitive Radio Technologies for Dynamic Spectrum Management, IGI Global, pp 499-543 2015

XIX. J. S. Banerjee, A. Chakraborty, and K. Karmakar, "Architecture of Cognitive Radio Networks". In N. Meghanathan & Y.B.Reddy (Ed.), Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks, IGI Global, pp 125-152 2013

XX. J. S. Banerjee, and A. Chakraborty, "Modeling of Software Defined Radio Architecture & Cognitive Radio, the Next Generation Dynamic and Smart Spectrum Access Technology". In M.H. Rehmani & Y. Faheem (Ed.), Cognitive Radio Sensor Networks: Applications, Architectures, and Challenges, IGI Global, pp. 127-158 2014

XXI. J. Banerjee, et. al., "Impact of machine learning in various network security applications", In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 276-281, IEEE, 2019

XXII. J. S. Banerjee, et. al., "A Survey on Agri-Crisis in India Based on Engineering Aspects", Int. J. of Data Modeling and Knowledge Management, 3(1–2), pp.71-76, 2013

XXIII. J. S. Banerjee, A. Chakraborty, and A. Chattopadhyay, "A novel best relay selection protocol for cooperative cognitive radio systems using fuzzy AHP", Journal of Mechanics of Continua and Mathematical Sciences, 13(2), 72-87, 2018

XXIV. K. B. Letaief and W. Zhang, "Cooperative spectrum sensing", in Cognitive Wireless Communication Networks, Springer, New York, NY, USA, 2007

XXV. Laneman, J. N., et al. "Cooperative diversity in wireless networks: Efficient protocols and outage behavior", IEEE Trans. Inform. Theory, 50(12), pp.3062-3080, 2004

XXVI. M. K. Simon, & M. S. Alouini, [Digital communication over fading channels]. John Wiley & Sons, Hoboken, NJ, Vol. 95, 2005

XXVII. O. Saha; A. Chakraborty, and J. S. Banerjee, "A Decision Framework of IT-Based Stream Selection Using Analytical Hierarchy Process (AHP) for Admission in Technical Institutions", In: Proc. OPTRONIX 2017, IEEE, pp. 1-6, Nov. 2017

XXVIII. O. Saha; A. Chakraborty, and J. S. Banerjee, "A Fuzzy AHP Approach to IT-Based Stream Selection for Admission in Technical Institutions in India", In: Proc. IEMIS, AISC-Springer, pp. 847-858, 2019

XXIX. R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks", IEEE Journalon Selected Areas in Communications,vol.26,no.1,pp. 25–37, 2008

XXX. R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks", in Proceedings of IEEE International Conference on Computer Communications (INFOCOM '08), pp. 31–35, Phoenix, Ariz, USA, April 2008

XXXI. S. Haykin, "Cognitive radio: brain-empowered wireless communications", IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201–220, 2005

XXXII. S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios", in Proceedings of the IEEE International Conference on Communications (ICC '06), vol. 4, pp. 1658–1663, Istanbul, Turkey, June 2006

XXXIII. S. Paul, A. Chakraborty, and J. S. Banerjee, "A Fuzzy AHP-Based Relay Node Selection Protocol for Wireless Body Area Networks (WBAN)", In: Proc. OPTRONIX 2017, IEEE, pp. 1-6, Nov. 2017

XXXIV. S. Paul, A. Chakraborty, and J. S. Banerjee, "The Extent Analysis Based Fuzzy AHP Approach for Relay Selection in WBAN", In: Proc. CISC, (pp. 331-341). Springer, Singapore, 2019

XXXV. T. Newman and T. Clancy, "Security threats to cognitive radio signal classifiers", in Proceedings of the Virginia Tech Wireless Personal Communications Symposium, Blacksburg, USA, June 2009

XXXVI. T. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation", in Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks
and Communications (Crown Com '08), Singapore, May 2008

XXXVII. Z. Han and K. J. R. Liu, "Resource Allocation for Wireless Networks: Basics, Techniques, and pplications", Cambridge University Press, Cambridge, UK, 2008