Resource Allocation and Spectrum Sensing in Cognitive Radio Network with Malicious Users using Soft Computing and Statistical Techniques

By

Noor Gul

Reg. No. 51-FET/PHDEE/S12

Supervised By

Prof. Dr. Ijaz Mansoor Qureshi

A dissertation submitted to I.I.U. in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Department of Electrical Engineering
Faculty of Engineering and Technology
INTERNATIONAL ISLAMIC UNIVERSITYISLAMABAD
2019

DEDICATED TO

My Teachers,

Parents,

Kids, Friends

Sisters and Brothers

CERTIFICATE OF APPROVAL

Title of Thesis: Resource Allocation and Spectrum Sensing in Cognitive Radio Network with Malicious Users using Soft Computing and Statistical Techniques.

Name of Student: Noor Gul

Registration No: 51-FET/PHDEE/S12

Accepted by the Department of Electrical Engineering, Faculty of Engineering and Technology, International Islamic University, Islamabad, in partial fulfillment of the requirements for the Doctor of Philosophy degree in Electronic Engineering.

Viva voce committee:

Prof. Dr. Ijaz Mansoor Qureshi (Supervisor) _____
Professor
Department of Electrical Engineering
Air University, E – 9, Islamabad.

Prof. Dr. Aqdas Naveed Malik (Internal Examiner) _____
Professor / VP (HS&R)
International Islamic University, Islamabad.

Dr. Muhammad Usman (External Examiner-I) _____
Senior Director, NESCOM, Islamabad

Dr. Hafiz Muhammad Faisal Zafar (External Examiner-II) _____
Principle Scientist, PAEC, Islamabad

Dr. Suheel Abdullah Malik (Chairman, DEE) _____
Associate Professor, DEE, FET
International Islamic University, Islamabad.

Prof. Dr. Muhammad Amir (Dean, FET) _____
Professor, DEE, FET
International Islamic University, Islamabad.

February 06, 2019

ABSTRACT

Due to the strict management policy and limited space in wireless spectrum, it is very difficult to overcome the demands of high data rate and bandwidth requirements in the wireless communication. To deal with this problem effectively, random allocation of the spectrum is considered, which resulted in the concept of cognitive radio network (CRN). Resource Allocation and Spectrum sensing in CRN is of high interest, where opportunistic users also called secondary users (SUs), have to detect the licensed primary user (PU) spectrum and make use of the vacant. The effects of multipath fading, shadowing and receiver uncertainty lead to poor spectrum sensing performance of individual users. Cooperative spectrum sensing (CSS) is a solution to acquire accurate information about the PU channel in the fading and shadowing environment. CSS enables each user to share its local sensing information with the neighbors to reach a more precise spectrum sensing decision. The malicious users (MUs) false sensing reports prevent the fusion center (FC) from taking a precise final decision, hence it can reduce effectiveness of CSS system. Many detection and suppression schemes are found in the literature to make the FC decision secure and robust in the presence of these abnormalities.

This dissertation is a contribution to the above mentioned areas. The dissertation is mainly divided into three parts. In the first part, we have proposed two variants of the Kullback Leibler (KL) divergence, including simple KL divergence and weighted KL divergence schemes to prevent the system from always yes, always no, opposite and random opposite categories of MUs without identification. The final decision made by the FC, using simple KL divergence and weighted KL divergences schemes is more precise with high detection, less false alarm and low energy consumption. In the second part, we have proposed heuristic algorithms, including Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) based soft and hard fusion

combination schemes at the FC. In the last part, for efficient detection and mitigation of MUs, we have proposed statistical techniques. In this section, FC is allowed to take its cooperative decision normally about the sensing channel, based on the received local decisions of the cooperative SUs. When enough statistics are collected about the reporting users, Box-whisker's plot (BWP) and Hampel's test (HT) are employed to detect and separate the false sensing data provided by MUs as abnormal data and is able to further shape the hard and soft fusion decisions based on the reported data of the normally reporting users.

The effectiveness and reliability of our proposed techniques are demonstrated in the results and simulations where graphs are plotted for the detection, false alarm, miss-detection and error probabilities against different types of MUs, total number of cooperative users and signal to noise ratios (SNRs).

The spectrum sensing responsibility in the presence of various categories of MUs is a challenging job that is made authentic using KL divergence, GA, PSO and some statistical techniques in the dissertation. The proposed techniques in the dissertation allow the FC to estimate the PU channel status accurately so that the SUs are able to make use of the available spectral holes without any disturbances and interference to the legitimate users. In the industrial environment, sensors and robot in coordination detect the abnormal behavior of any robot, as the malfunctioning in such robots due to any reason reduce overall performance of the system. Therefore, the proposed CSS model can precisely detect faulty sensors and robots in the industrial environment and it has a centralized performance monitoring mechanism.

LIST OF PUBLICATIONS AND SUBMISSIONS

[1] **N. Gul**, I. M. Qureshi, A. Umar, S. Khan, and A. Elahi, "History based forward and feedback mechanism in cooperative spectrum sensing including malicious users in cognitive radio network," PLOS-One, vol. 12, no. 8, p. e0183387, 2017. Doi.org/10.1371/journal.pone.0183387

[2] **N. Gul**, I. M. Qureshi, A. Naveed, A. Elahi, and T. Saleem, "A combination of double sided neighbor distance and genetic algorithm in cooperative spectrum sensing against malicious users," in Proceedings of 2017 14th International Bhurban Conference on Applied Sciences (IBCAST) 2017, Islamabad, Pakistan, pp. 746-753

[3] **N. Gul**, I. M. Qureshi, A. Elahi, and I. Rasool, "Defense Against malicious users in cooperative spectrum sensing using Genetic Algorithm," International Journal of Antenna and Wireless Propagation. vol. 2018, article ID 2346217, p. 1-11, 2018. Doi:10.1155/2018/2346317.

[4] **N. Gul**, I. M. Qureshi, S. Akbar, I. Rasool, and M. Kamran, "One-to-many relation based KL divergence in CSS against malicious users," Wireless Communication and Mobile Computing . vol. 2018, article ID 3153915, p. 1-14, 2018. Doi:10.1155/2018/3153915

[5] **N. Gul**, I. M. Qureshi, A. Naveed, A. Elahi, and Hayatullah, "Cooperative spectrum sensing using optimal hard decision in the presence of abnormalities," Journal of Science, Higher Education Department, KPK, Pakistan 2018. (Accepted for Publication)

[6] **N. Gul**, I. M. Qureshi, A. Naveed, and A. Elahi, "An optimized spectrum sensing decision using Genetic Algorithm," Journal of Science, Higher Education Department, KPK, Pakistan 2018. (Accepted for Publication)

[7] T. Saleem. M. Usman, A. Elahi, and **N. Gul**, "Simulation and performance evaluations of the New GPS L5 and L1 signals," Wireless Communication and Mobile Computing, vol. 2017, article ID 7492703, p. 1-4, 2017 . Doi:10.1155/2017/7492703.

[8] A. Elahi, I. M. Qureshi, **N. Gul**, and T. Saleem, "Application of Differential and cuckoo search algorithm in reduction of sidelobes," 2016 19th international, Multi-topic conference (INMIC), Islamabad, Pakistan, Dec. 2016, pp. 1-4. Doi: 10.1109/INMIC.2016.7840103.

[9] A. Elahi, IM Qureshi,, and **N. Gul**, "Side-lobe reduction in cognitive radio systems using hybrid technique," World Academy of Science, Engineering and Technology, vol. 11, no. 3, p. 213-216, 2017.

[10] A. Elahi, IM Qureshi, SU Khan, F Zaman, and **N Gul**, "Improved algorithms for interference suppression in non-contiguous orthogonal frequency division multiplexing based cognitive radio systems," Neural Computing and Applications (2018), p. 1-13. doi.org/10.1007/s00521-017-3310-3

[11] A. Elahi, I. M. Qureshi, F. Zaman, **N. Gul**, and T. Saleem, "Suppression of Mutual Interference in Noncontiguous Orthogonal Frequency Division Multiplexing Based Cognitive Radio Systems," Wireless Communications and Mobile Computing, vol. 2017, article ID 1860134, p. 1-9, 2017.

[12] A. Elahi, I. M. Qureshi, F. Zaman, and **N. Gul**, "Out-of-Band Radiation Reduction in Cognitive Radio OFDM Systems Hybridizing Firefly Algorithm with Generalized Sidelobe Canceller," Wireless Personal Communications, vol. 100, no. 3, p. 941-956, 2018.

[13] A. Elahi, Z. Khattak, M. Kamran, and **N. Gul**, "Interference Cancellation Technique for OFDM Based Cognitive Radio Systems, " Journal of Science, Higher Education Department, KPK, Pakistan 2018. (Accepted for Publication).

[14] A. Elahi, **N. Gul**, Z. Khattak, and M. Kamran ,"Efficient High Out of Band Reduction for Cognitive Radio Systems, " Journal of Science, Higher Education Department, KPK, Pakistan 2018. (Accepted for Publication)

[15] A. Elahi, I. M. Qureshi, M. Atif, and **N. Gul**, "Interference reduction in Cognitive radio networks using Genetic and Firefly Algorithms," 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), Islamabad, 2017, pp. 96-100.

[16] A. Elahi, A. Waseem, I. M. Qureshi, and **N. Gul**, "Interference Prevention in Cognitive Radio Networks," IEEE 2nd International Conference on Intelligent Systems Engineering, Kuala Lumpur, Malaysia (ICISE 2018), 2018.

SUBMITTED PAPERS:

[1] **N. Gul**, IM. Qureshi, S. Akbar, I. Rasool, and M. Kamran, "Particle swarm optimization based cooperative spectrum sensing in the presence of malicious users," Applied Computational Intelligence and Soft Computing. Article-6321030.

[2] **N. Gul**, IM. Qureshi, A. Elahi, and I. Rasool, "Malicious Users Prevention in a Hard Fusion Scheme using Statistical Features in Cooperative Spectrum Sensing," KS-II Transactions on Internet and Information systems. Article- TIIS-WC-2018-Jan-0118.

[3] **N. Gul**, IM. Qureshi, A. Naveed, and A. Elahi, "Secure Soft combination Schemes against malicious users in cooperative spectrum sensing," Wireless Personal Communication. Article-UCIS-2018-0310.

[4] **N. Gul**, IM. Qureshi, A. Umar, K. Sultan, and A. Elahi, "Malicious Secondary User detection in Cognitive Radio using Statistical Features in Cooperative Spectrum Sensing," Journal Elektronika Ir Elektrotechnika. Article-14450.

[5] **N. Gul**, IM. Qureshi, A. Naveed, and A. Elahi, "Improved sensing against MUs using DSND and GA," Cognitive Computation. Article- COGN-D-18-00103.

ACKNOWLEDGEMENTS

In the name of Allah (Subhanahu Wa Ta'ala), who is the most gracious and the most merciful. I would like to thank Allah for giving me strength and patience to complete this research work. Peace and blessings of Allah be upon His last Prophet Muhammad (Sallulah-o-Alaihihe-Wassalam) and all his Sahaba (Razi-Allah-o-Anhu) who dedicated their lives for Dawah and spread of Knowledge.

I am truly grateful to my supervisor Dr. Ijaz Mansoor Quershi, whose inspiration, ideas and efforts make it possible for me to complete my higher studies. He has been a role model for me and many others in teaching, research and other aspects of life.

I offer my sincere thanks to Dr. Atif Elahi, Dr. M. Sajjad Khan, Dr.Imtiaz Rasool, Dr. Adnan Omar, Dr. Waseem Khan, Dr. Abdul Basit, and Mr. Falak Naz Khalil for their never ending support during last few years. I also thank Muhammad Bilal Khan, Hybat Khan and other PhD scholars for their useful discussions.

I am also thankful to administration at department as well as at university level for their kind support. I am really grateful to my father, mother, sisters and brothers for their love and support throughout my life. I am also very thankful to my wife for her patience, encouragement and prayers during every stage of my PhD degree.

(Noor Gul)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CR	Cognitive radio
CP	Cyclic prefix
AP	Access point
CS	Cyclic suffix
CRN	Cognitive radio network
MANET	Mobile ad-hoc network
DSA	Dynamic spectrum access
DE	Differential evolution
CIWN	Cognitive industrial wireless sensor network
CWSN	Cognitive wireless sensor network
CBS	Cognitive base station
QoS	Quality of service
EP	Evolutionary programming
FCC	Federal communication commission
PDF	Probability distribution function
DDoS	Distributed denial of service attack
FDMA	Frequency division multiple access
GA	Genetic algorithm
HA	Heuristic algorithm
OFDM	Orthogonal frequency division multiplexing
SUs	Secondary users
SDR	Software defined radios

SNR	Signal to noise ratio
ED	Energy detector
MF	Matched filter detector
FD	Feature detector
BS	Base station
PSO	Particle swarm optimization
KLD	Kullback Liebler divergence
PSO-EGC	Particle swarm optimization equal gain combination
ZS	Z Score
CSS	Cooperative spectrum sensing
FC	Fusion center
SS	Spectrum sensing
MU	Malicious user
EGC	Equal gain combination
MGC	Maximum gain combination
SSDF	Spectrum sensing data falsification
GLRT	Generalized likelihood ratio test
OMU	Opposite malicious user
ROMU	Random opposite malicious user
AYMU	Always yes malicious user
ANMU	Always no malicious user
SCSS	Sequential cooperative spectrum sensing
AWGN	Additive white gaussian noise

HFC	Hard fusion combination
AO	Always opposite
RO	Random opposite
AY	Always yes
AN	Always no
MV-HFC	Majority voting hard fusion combination
DSND	Double sided neighbor distance algorithm
MMZ	Minimum mean and Z-score algorithm
PUEA	Primary user emulation attacks
CFAR	Constant false alarm rate
SDF	Soft decision fusion
EGC-SDF	Equal gain combination soft decision fusion
MGC-SDF	Maximum gain combination soft decision fusion
HDF	Hard decision fusion
MV-HDF	Majority voting hard decision fusion
NSU	Normal secondary user
PU	Primary user
GAMV-HDF	Genetic algorithm majority voting hard decision fusion
PSO-MGC	Particle swarm optimization maximum gain combination
OTMSD	One to many sensing distances
WLAN	Wireless Local Area Network
ROC	Receiver operating characteristics
VANET	Vehicular ad-hoc network

CR-MANET	Cognitive radio mobile ad-hoc network
WBAN	Wireless body area network
GPRS	General packet radio service
IoT	Internet of things
CR-VANET	Cognitive radio vehicular ad-hoc network

Chapter 1

Introduction

1.1 Background

The recent increase in the wireless communication applications and high data rate demands in today's environment is the major reason for spectral shrinkages. Spectrum study carried out at various times shows that a large number of frequencies are mostly unoccupied. This leads to the following conclusion: First, it requires a more flexible spectrum management policy of the spectrum and secondly, a more compatible technology.

Different thoughts regarding the flexible spectrum management policy can be found in the literature. Several suggestions include allocation of the spectrum resources to different users dynamically or randomly operating in the same allocated range of frequency. Similarly, to allow the access of the spectral resources to everyone without any constraint, or to use spectrum auctioning that allocate spectrum assets for a limited time to the most demanding user. The literature study recommends that dynamic spectrum allocation is more beneficial as compared to fixed spectrum allocation. This is in accordance with the recent improvements of the spectrum policies. Regulatory bodies have started routing to dynamic spectrum allocation instead of fixed spectrum allocation.

For technology compatibility Gerald Q. Maguire and J. Mitola in 1999 have proposed Cognitive Radio (CR) [1],[2]. CR is an encouraging solution and highly tempting area for the research

community. CR has the capability to dynamically allocate the available spaces in the primary user (PU) channel to the secondary users (SUs) at a certain time and at specific geographic locations. The transmitted signal shape is controlled using different techniques at the transmitter side to allow both the SU and PU to make use of the same spectrum resources with minimum disturbances to transmission [3],[4].

1.2 Research Problem

The individual user spectrum detections have many restrictions. The sensing performance is highly restricted by fading, energy constraints, shadowing and other hidden problems. It is likely that a SU might inaccurately detect the PU activity. In the cooperative spectrum sensing (CSS), SU devices located few wavelengths apart experience unlike fading and attenuation effects. Consequently, the fading is reduced by permitting sensing users to share the detection results and to cooperatively resolve the licensed spectrum tenancy. All cooperative users conduct their local spectrum survey and send data to a common receiver that merge individual SU decisions to yield a final decision of the PU channel [5]-[11].

The involvement of malicious users (MUs) in a CSS reduces the strength of cooperation, therefore their detection and omission is crucial. Significant research is in progress to immune the CSS to the MUs attack. The attacker sends inaccurate sensing information to the fusion center (FC), inducing confusion about the actual spectrum conditions. These attacks are called spectrum sensing data falsification (SSDF), and the fusion schemes needs protection against these attacks.

To improve the sensing performance in presence of MUs, different soft and hard fusion combination schemes are proposed in the literature. These methods can reduce the error

contribution due to opposite, random opposite, always YES and always NO categories of MUs. Therefore, they can efficiently utilize the spectrum holes with minimum disturbance to the licensed PU [12]-[15].

The purpose of this dissertation is to develop an efficient technique for CSS that can minimize the errors contributed by abnormal users. This will enable FC to establish a global decision about the PU channel with high detection, low false alarm and minimum level of interference to the PU.

1.2 Research Methodology

The contributions made by this dissertation are summarized as follows:

1. In the first part, the Kullback Leibler (KL) divergence [16],[17] method for minimizing SSDF attack is considered. In the proposed CSS scheme, each user report to FC about the availability of PU and keep the same evidence in its local database. Based on the KL divergence value, if the FC acknowledges the user as normal, then the user will send unified energy information to the FC based on its current and previous sensed observations. In the second part of this algorithm, another KL divergence algorithm is proposed where the SU local sensing information is utilized with the average sensing information provided by all other users in measuring the KL divergence. In this part, MUs are identified and separated based on the individual SU decisions and the average sensing information received from all other users. This second KL divergence method assigns lower weights to the sensing information of MUs, while the normal SUs information receives higher weights. The proposed scheme is tested in an environment of always YES, always NO, opposite and random opposite categories of MUs. It gives best

detection results as compared to the traditional KL divergence, equal gain combination (EGC) and maximum gain combination (MGC) schemes [18],[19].

2. Next, we focus on the use of double sided neighbor distance (DSND) [20] along-with Genetic Algorithm (GA) for the detection and avoidance of misbehaving users in CSS, so that to make the FC final decision more authentic. GA uses the DSND algorithm for detecting misbehaving user and then utilizes crossover and mutation to select reliable sensing results. The results of the GA are further utilized in the majority voting hard fusion combination schemes [21],[22]. In the second part, GA use one-to-many neighbor distance along-with Z-Score (ZS) as a composite fitness function for the identification of accurate sensing information received from all cooperative users. Simulation results demonstrate that the proposed scheme has surpassed the traditional majority voting hard fusion scheme, the equal gain combination (EGC) and maximum gain combination (MGC) schemes for different numbers of cooperative and MUs. Similarly, the proposed method also outperform the traditional schemes at different levels of the average signal to noise ratios (SNRs) [9],[18],[19],[21],[22].

   In the third proposed scheme, all SUs send soft energy statistics of the PU channel to the FC. The fusion center make use of the particle swarm optimization (PSO) to determine the most suitable energy statistics out of the individual sensing information provided by all cooperative SUs including normal and malicious [23],[24]. An outlier score is determined for all particles using PSO fitness function at the FC. Out of the PSO population, the sensing report with minimum total outlying value is selected as the actual PU channel status on behalf of all cooperating SUs for a global decision. The global decision of the licensed user channel is made with PSO based EGC (PSO-EGC), PSO

based MGC (PSO-MGC) and PSO based Majority voting hard fusion combination schemes (PSO-Hard). Simulation gives high detection, low false alarm and minimum error results for the PSO based soft and hard fusion schemes.

3. Finally, different techniques to reduce the harmful effects of the false sensing data reported by various malicious SUs are investigated. In this part, FC takes a global decision normally based on the local decisions of all cooperative users until the establishment of enough statistics against these cooperative users. FC combines the sensing results of the users and isolates abnormal user as outlier from the normal SUs by taking them out of the hard fusion combination (HFC). Correlation is determined in the local sensing information of individual users and then Box-whiskers plot (BWP) is used to designate an abnormal user as malicious [25]-[30]. A modified HFC scheme is employed in a global decision. Similarly, this part also comprises the investigations for the performance of OTMSD and ZS algorithms for different number of MUs. Both one to many sensing distance (OTMSD) and Z-score (ZS) algorithms are able to detect abnormal user as malicious at the FC and provides more secure detection results in comparison with traditional soft and hard fusion combination schemes. By detecting and omitting MUs a more precise and valid decision is formulated by the soft decision fusion (SDF) schemes at the FC.

1.3 Thesis Organization

The dissertation is organized as follows:

Chapter 1 presents the conceptual design of the whole thesis, stating motivation, problem identification, statement, and definition with general/specific research questions/objectives and

with utility interests. It presents philosophy and hypothesis of the work and a sequential account of how the research proceeds gradually onward. Chapter 2 gives Literature Review of contemporary reported research, which turns out to be critical preparing a ground of why this research is conducted. The relevant theory and issues of concerns are diagrammatically highlighted gearing it into becoming a good reason for the justification of thesis title. Chapter 3 gives the methodological details, and Chapter 4 presents details of the proposed algorithm of forward and feedback mechanism, KL divergence and weighted KL divergence schemes tested in a CSS. Detection, false alarm and error probabilities are calculated for different ratios of cooperative users, malicious users and SNR.

In Chapter 5 is first proposed the use of DSND algorithm for the identification of MUs and then utilized GA to select accurate sensing results out of the sensing information's reported by all cooperative users. In the second part, GA is employed to use OTMSD and ZS as a fitness function to determine accurate sensing data out of the local binary decisions of all cooperative users. Finally, we collect soft energies at the FC and apply the OTMSD and ZS algorithms on these energies using PSO. Performance and reliability of the proposed technique is tested and compared with the traditional schemes in the simulations.

In Chapter 6, we present a new HFC scheme where FC first collect hard binary decisions of the cooperative users and apply hard fusion schemes based on the reports of all cooperative users. After the collection of enough sensing reports from all SUs, correlation is applied on the sensing differences of individual user and the combine sensing reports provided by all other users. SUs with their correlation results dissimilar to the normal users are categorized as malicious using BWP are further isolated from the normal SUs in the history log. In the second part of the chapter, OTMSD and ZS techniques are employed for detection and separation of malicious

users. The OTMSD and ZS results are followed by the HT to separate malicious activity as outlier from the normal users.

Chapter 7 concludes the thesis by stating that the research objectives are achieved and suggestions for further work are given.

1.4 Summary

The spectrum shortage problems indicate that most of the frequency bands are fully or partially occupied by license users. The idea of CR introduces by Gerald Q. Maguire and J. Mitola allows the unlicensed users to utilize the licensed user spectrum when they sense the channel free. Sensing ability of an individual user cannot be fully trusted due to different environmental effects. CSS has the ability to reduce a single user sensing problems but its performance get lowers when any of the users work as MU with forwarding false sensing reports to the FC. Different variations of the soft and hard combination schemes such as MGC, EGC, AND, OR are available in the literature to reduce the impact of including MUs in the combination.

This chapter gives an idea of dividing the thesis into three parts. First, the use of history based KL divergence with feedback mechanism along with the weighted KL divergence at the FC is discussed. Then the use of the GA and PSO heuristic algorithms are discussed that gives optimum PU detection performance as compared to the traditional soft and hard combinations. In the last section, the abnormal users are easily categorized as malicious using BWP and HT based statistical techniques that uses correlations and other sensing stats.

Chapter 2

Literature Review

2.1 Introduction

In this chapter, we present necessary details of the existing CR construction. It starts with the background and motivation to CR technology, then a brief discussion about the CR, its function and network architecture is given. MUs are considered in the non-cognitive radio networks such as cloud computing, internet, wireless sensor network (WSN), mobile ad-hoc network (MANET) and wireless body area network (WBAN). Similarly, cognitive radio network performance is investigated in the presence of selfish users, byzantine users, jammers, eavesdroppers and primary user emulation categories of attacks. A discussion is made about the commonly used spectrum sensing schemes at the SUs. The benefits and strength of using several combination schemes at the FC are shown in comparison with the sensing decisions made by individual users under the fading and shadowing environment along-with MU considerations. Some hard and soft combination schemes such as logical-OR, logical-AND, majority voting, EGC and MGC schemes are discussed and their effectiveness in detecting spectral opportunity is highlighted. The impact of including MUs in the FC global decision is shown and the most commonly used detection schemes are discussed that enable FC to overcome the effects of abnormalities. At last, the applications of different heuristic techniques at the FC are discussed to get to accurate spectrum sensing decisions.

2.2 Background

The user demands for higher data rates and services is increasing rapidly over the last few decades that results in shortage of the spectrum to new services [31]-[33]. In November 2002, spectrum policy task force (SPTF) of the federal communication commission (FCC) has shown in their report that in most of the frequency bands, spectrum access is a serious issue as compared with its physical inadequacy. This is due to the traditional command and control system that restricts the potential spectrum users to obtain such access. Secondly, the spectrum resources are either fully or partially occupied most of the time. To encounter these problems, their recommendations are, to improve the flexibility of spectrum usage, to support and encourage efficient use of the spectrum and to take all dimensions and related issues of the spectrum usage into policy. The aim has been to improve both the technical and economic efficiency of the spectrum management. These recommendations introduce the concept of dynamic spectrum access (DSA), where the un-licensed user also called SU has the right to use the temporarily un-usable spectrum of the licensed user. Therefore, CR has been proposed for efficient use of the spectrum in [34]-[37].

2.3 Cognitive radio

The cognitive word is derived from the Latin word " cognoscere " means "to come to know" or to get awareness of something [38]-[40]. The word CR is introduced by J. Mitola, with the idea of designing a wireless communication system, which is able to provide wireless communication using dynamic spectrum assignment, in order to improve the performance of the wireless transmission, as well as to improve frequency spectrum utilization to solve the underutilization problem of the spectrum [1],[41],[42]. CR is equipped with the features of cognition and re-

configurability, which makes it different from the conventional radio. The ability of cognition allow CR users to sense and collect information about its surrounding environment transmission frequency, allocated power, modulation scheme, and bandwidth etc., enabling them thus to find best available spectrum. In CR, cognitive re-configurability is the ability of the radio to swiftly adapt to the operational parameters according to environmental information to attain best operational performance. The platform of software-defined radio (SDR) provides cognitive re-configurability, which is the basic building block of cognitive radio. The convergence of the digital radio and computer software has made the SDR a practical reality [1],[3],[43]. To make best use of the available spectral resources in an opportunistic manner, cognitive radio empowers opportunistic users to search for the spectrum holes, selecting the most suitable free channel, sharing its spectrum sensing information with other users, and to make the occupied channel free for the transmission of the PU, when it is reclaiming the channel.

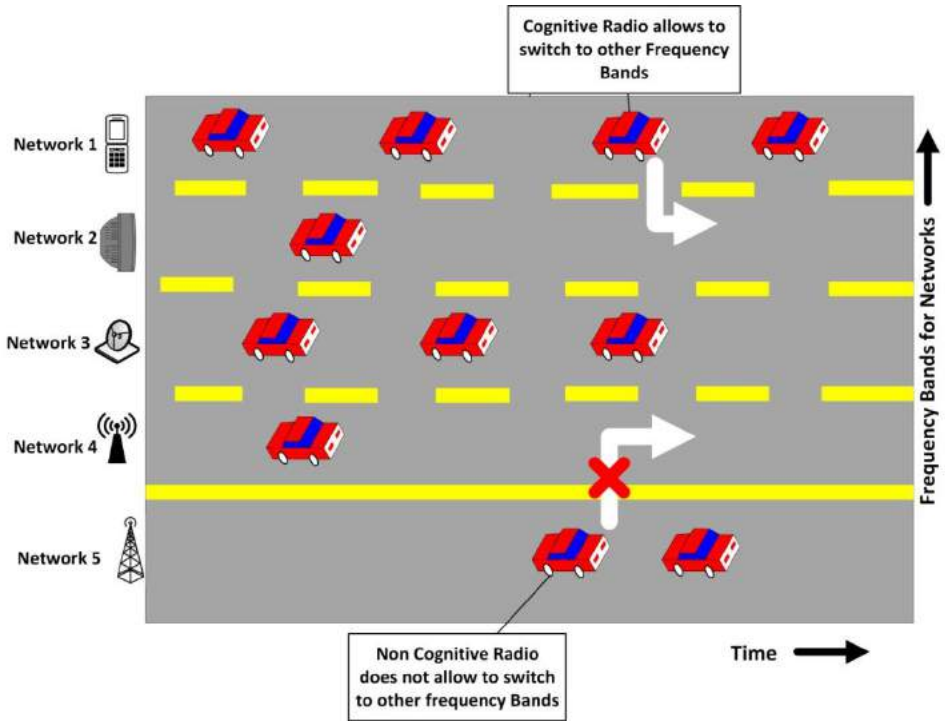

Figure 2. 1 Spectrum hand-off in cognitive radio network

2.4 Functions of Cognitive Radio

The duty cycle of CR is shown in Figure 2. 2, including detection of available spectral holes, selecting the best frequency bands, coordinating their local spectral information with other users and to vacate the spectral resources for the primary user when it appears.

2.4.1 Spectrum sensing and analysis

The first step in the dynamic spectrum utilization is the spectrum sensing and analysis. Efficient spectrum utilization is obtained by the CR with sensing the surrounding environment to adjust the transmission and receiving parameters, that is transmit power, modulation scheme and frequency etc. The three different features of the spectrum sensing are the interference temperature model, detection of spectral holes and CSS using multiple sensing users.

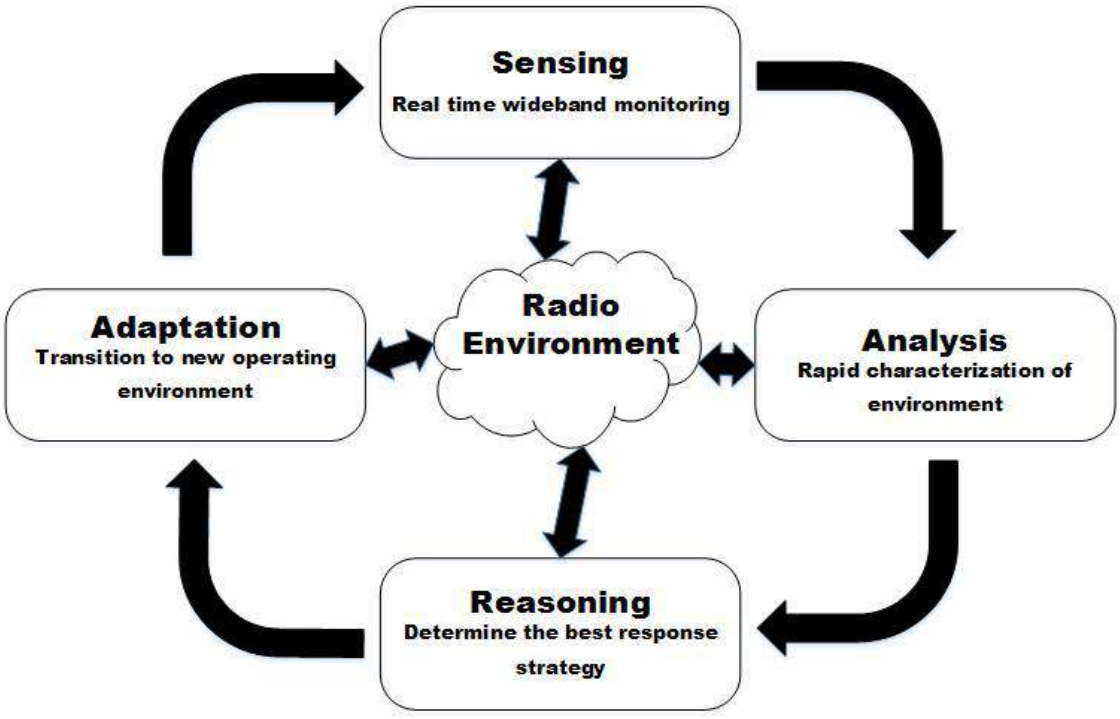

Figure 2. 2 Cognitive Radio Operational Cycle

2.4.2 Spectrum management and handoff

When unlicensed users have knowledge about the available spectrum holes, spectrum management and handoff functions enable these opportunistic users to select the best frequency bands and to hop in the multiple bands according to the time varying channel characteristics to meet various qualities of service needs. If the licensed user starts its transmission in the vacant band, SUs must be intelligent enough to direct and shift its activity to other available frequencies according to capacity of the channel determined by the interference level, noise, channel error rate, path loss and holding time etc.

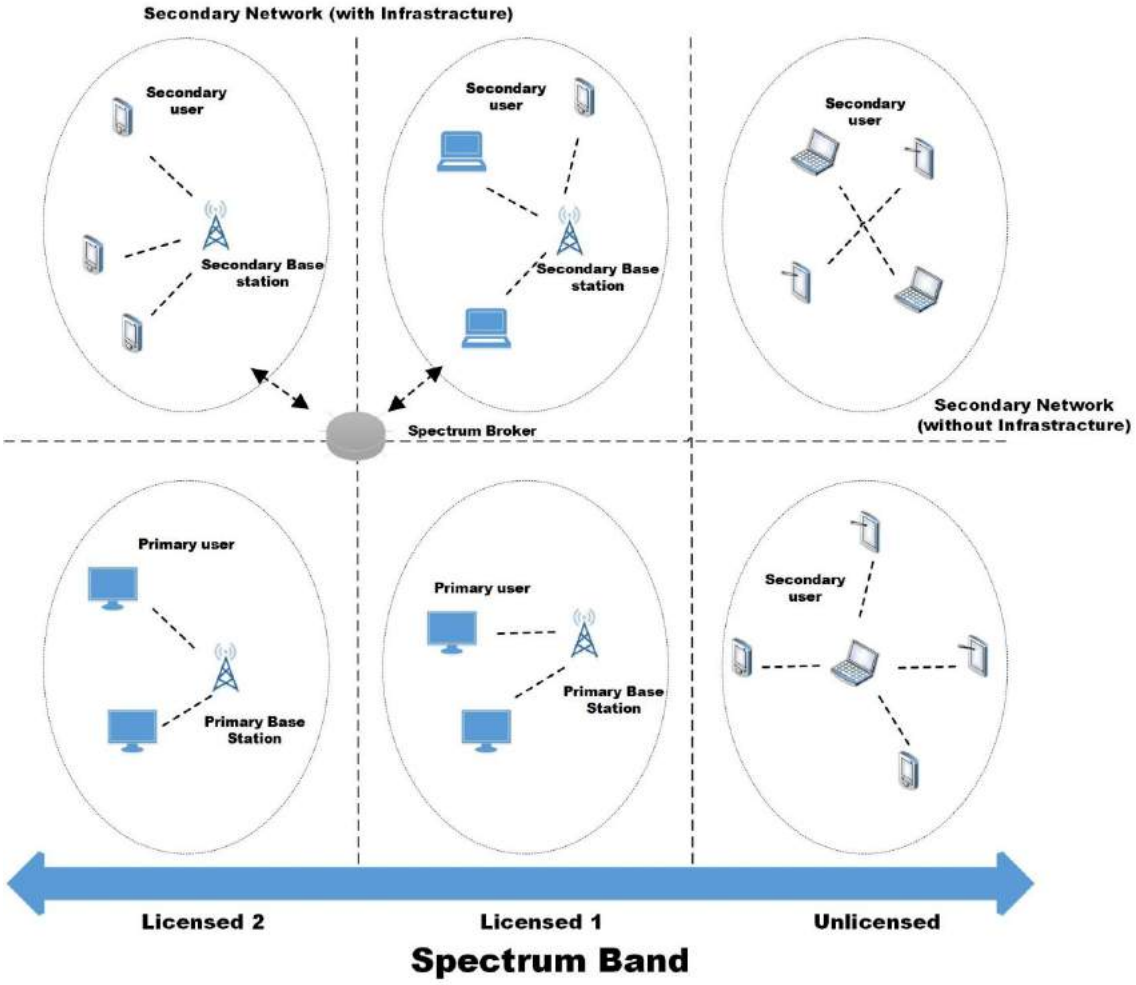

Figure 2. 3 DSA Network architecture

2.4.3 Spectrum allocation and sharing

The DSA allows SUs to share their spectrum resources with other unlicensed users and PUs. But it is difficult to achieve better spectrum allocation for sharing with increased spectral efficiency. As the PU has the right to use the spectrum without any restrictions and disturbances, therefore, interference level due to the transmission of unlicensed users must be limited to a certain threshold. In the process when multiple users try to access the frequency band of the PU, their access needs to be coordinated so that to reduce collision and interference.

2.5 Network architecture of Cognitive Radio

The current fixed spectrum assignment is not able to meet with the growing demands of higher data rate and to accommodate new wireless services. The use of cognitive radio has emerged as a new wireless communication technology to meet up with challenges of the underutilized spectrum resources in the most efficient manner. A CR network architecture is divided into a secondary network with SUs and secondary base station and the primary network with PU and the primary base station in Figure 2. 3 [43].

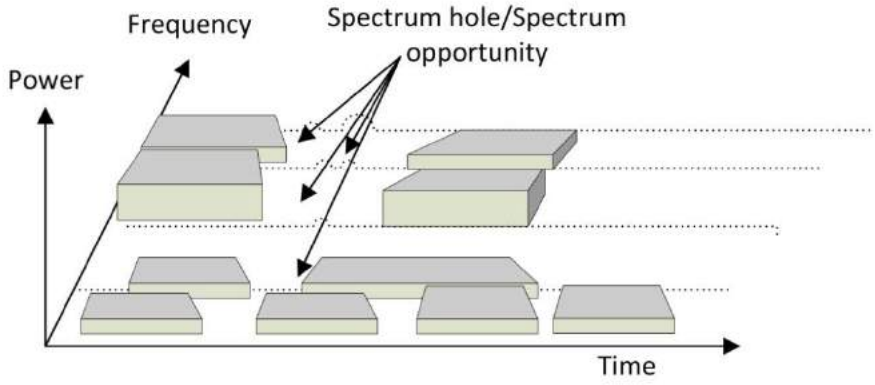

Figure 2. 4 Spectrum holes

The secondary network both with and without any secondary base station, consists of many SUs, all trying to detect the occupancy of the PU spectral hole, when there is no activity of the PU. The secondary base station is serving as a hub for secondary network, having fixed infrastructure components and coordinating the possession of the PU spectrum holes with SUs, when it is not in use of the PU in Figure 2. 4.

The secondary base station and users are both equipped with the features of CR. The spectrum broker manages the transmission of all secondary networks, when large number of secondary networks tries to make use of the same spectral band. This is done with the help of collecting information from each secondary network, so that to assign network resources in the most efficient and fair spectrum sharing manner. The PUs are legal in using the assigned portion of the spectrum band by taking help of the primary network base station. This provides the authenticity such that no interference or interruption is received by these licensed users due to the transmission of secondary network. As the PUs and their base station do not have the properties of CR, therefore, any secondary base station sharing the licensed spectrum band with the PU without determining activity of the PU is certainly generating problems in the PU transmission. It is therefore mandatory for the secondary network to detect immediately the PU activity and to further direct any secondary transmission to other freely available spectral bands [44],[45].

Efficient utilization of the radio spectrum is characterized by overlay and underlay techniques in CR. The underlay cognitive radio is able to sense the radio spectrum and communicate over the vacant channel. Overlay antennas of the CR are using two ports, where one port is narrowband and frequency reconfigurable, while the other port support UWB. A new kind of antennas with challenging and counterintuitive evolutionary computation like GA is used to optimize the antenna geometry for achieving maximum frequency bands with minimum switches [46].

Cognitive Radio is the wireless architecture representation in which fixed band is not assigned to the communication system and that search by itself to find a vacant band to operate. It is shown that the detection performance of an unknown weak signal in a known weak constellation is similar to the energy detector (ED). The use of the pilot signals is introduced in the presence of moderate level of noise uncertainty, which produces improved detection results [47].

2.6 Malicious users in Non-Cognitive Networks

The impacts of malicious users on the performance of cloud computing, internet, WSN and MANET are discussed below.

2.6.1 Cloud Computing

Cloud computing is the type of computing system based on the internet that allows sharing data and resources, in order to create and to configure an application online in Figure 2. 5. The goal of mobile cloud computing is to provide services to users of cloud computing conventionally and efficiently without any limits. Similarly, mobile cloud computing is integrating the mobile internet and cloud computing, in the provision of diverse types of integrated cloud computing services [48].

To overcome the abnormality effects in cloud computing, analyses and behavior of the users traffic is investigated in [49]. At first, whole feature set is constructed by collecting features from the user traffic that helps in the selection of essential and more accurate features to select and predict an abnormal user using Naive Bayes classification.

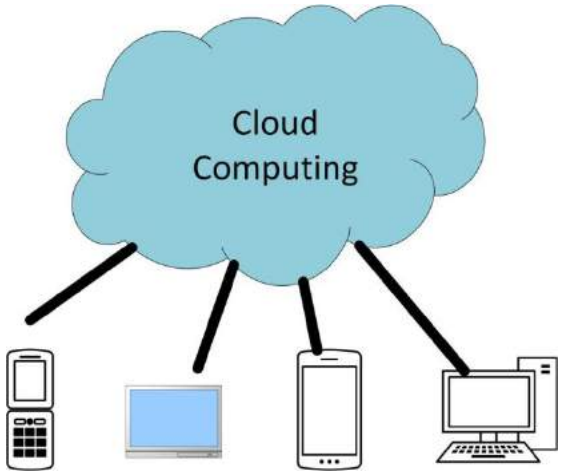

Figure 2. 5 Cloud Computing

2.6.2 Distributed Denial of Service attacks on the Internet

A distributed denial of service (DDOS) attacker denies the licensed user entry in to the service with takeover of the system resources, which leads to congestion in the system. In the intrusion detection framework, network traffic is divided into three types, that is, suspicious, malicious and innocent traffic. The normal user causes the innocent traffic, while the malicious traffic is due to the malicious user. A suspicious traffic is difficult to be categorized as malicious or normal. The normal incoming traffic is transported to the destination, while the malicious users' incoming traffic is dropped. However, suspicious users traffic is a challenge to the system and do not fall precisely into either of the two scenarios of the normal and malicious, therefore, a simple drop out of the suspicious traffic results in a false positive problem at the system.

Participation of the DDoS users have a major impact to affect the network outage, packet transmission delay, economic losses, website disruption, and legitimate user obstruction. The DDoS detection techniques are implemented either at the victim nodes or at many intermediate routers that run DDoS identification algorithms.

A network with a single victim node surrounded by a single hop distance is recognized as protection nodes that form an overlay. The single nodes deployment schemes are not capable enough to detect DDoS attacks with great reliability, as the network traffic is not aggregate enough at the intermediate nodes. Instead of designing systems that work in isolation, utilization of the distributed framework for nodes detection with various systems plugged in and assist to reach to a better overall detection is proposed in [50],[51].

The security areas of the customer network are expanded to include an internet service provider network, in order to effectively handle any suspicious traffic. A DDoS category of attack is discussed [52] that has not only an impact on the QoS of the victim systems, but can also poor down the QoS of the outsider systems. This distributed detection approach detects the DDoS attacks with coordination across the internet. The proposed scheme uses a nonparametric detection technique to improve individual nodes detection precision. Further, a gossip multicast method swap information is made of the individual nodes to get to the accurate detection results.

A semi supervised clustering scheme for intrusion detection is proposed [53]. In this work, the network data flows are first divided into three data types such as ICMP flow, TCP flow and UDP flow according to the network protocols and is next forwarded to the detection agents. The chances of MUs existence increase with the P2P applications and total users that have a negative impact on the performance of the P2P network. In [54] outlier mining based malicious node detection model is proposed for the hybrid P2P networks.

2.6.3 Wireless Sensor Network

Sensor networks have the ability to provide the most feasible/economical solution to challenging problems like defense, traffic observation, weather/pollution monitoring and in wild life tracking

system. Sensor networks allow the rapid deployment of low cost intelligent sensors in an environment of high interest. Along with the process capabilities, wireless sensor network has the important constraints of large memory and bandwidth requirements. It is mainly deployed in the particular environment where the exchange of data is through short range radio technology. Wireless sensor networks have obtained an amazing gratitude and hi-tech progress in recent times. In spite of the easiness in employment and considerable advantages, protection has always been a testing subject due to the environment in which the sensing nodes work. To handle the malicious signals involvement in the wireless sensor network and to keep it secure from viruses and worms, some strong security mechanisms are required. A susceptible infrared vaccinated (SIV) model for analyzing the effects of node injection and worms aggressive dynamics in the wireless sensor network is proposed in [55].

To provide the idea and benefit of the holistic approach to cognition in the sensor network, an inclusion of learning and analysis is performed in the top and physical layer opportunistic spectrum access. The pre attack behavior is recognized using emotional ant based centralized intrusion detection system in [56]. Similarly, the affected sensor nodes can be precisely recognized in the application independent framework. This model establishes unique properties of the sensor network with appropriate generalization of the application specific detection method. Based on the frame, alert reasoning algorithm can easily identify compromised sensor nodes [57]. An extensive literature review is investigated for the trust and reputation-based model in both the sensor and ad-hoc networks. Based on the trust establishment mechanism, state of the art is categorized into two parts, that is, system centric trust model and node centric trust models. Efficacy of the existing schemes is evaluated based on computation, trust evidence initialization, weight assignments and propagation [58].

In the wireless ad-hoc networks, intermediate nodes provide the facility of relay for the nodes to talk with far-off targets. As wireless nodes are limited by the energy constraints, therefore it may not be in the nodes interest to admit relay requests all the times. An assumption is made to state node actions, rigorously determined by the nodes self interest in [59].

2.6.4 Mobile Ad-hoc Network

The advent of intelligent transportation system is on the horizon that leads to safer and more efficient roadways. The automotive industry has begun the deployment of its first intelligent vehicle system that consists of technologies such as route guidance, adaptive cruise control systems, black boxes and night vision systems. Intelligent vehicles get knowledge of the nearby vehicle dynamics and the presence of any roadway risks through the advance wireless communication and sensor technologies [60].

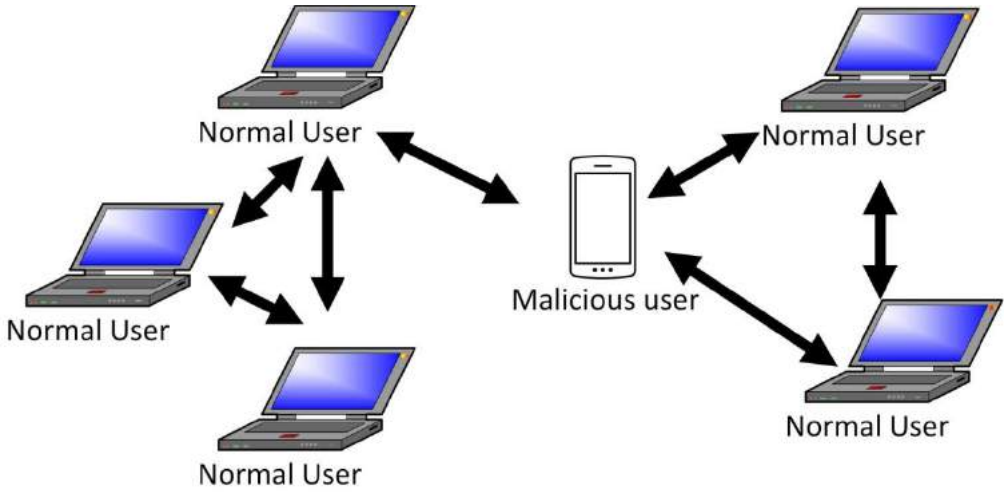

Figure 2. 6 Malicious Users in Mobile Ad-hoc Network

The focus on the fundamental security problem in the MANET as in Figure 2. 6 is to protect multi hope network connectivity of mobile nodes is proposed in [61]. This has identified security issues related to the problem, and discusses the security challenges in the design, and review

state of the art security proposals to protect the mobile ad hoc network link and network layer operations over the multi-hope wireless channel.

The malicious actions make a threat to the general packet radio services (GPRS) network, mobile users with GPRS, and the data transferred through the network. The malicious attacks are carried out by third parties, users or network operators, to exploit the security limitations in the network [62]. An examination of the pivotal security issues in the 5G network is investigated [63], where the wireless communications are essentially susceptible to the security breaks. A physical layer security can safeguard confidentiality of the data with the exploitation of inherent unpredictability of the communications medium with the disruptive technologies.

2.6.5 Wireless Body Area Network

A wireless body area network which is a type of sensor network as in Figure 2. 7, autonomously operate to connect a variety of health check sensors and appliances. These sensors and appliances may be placed either internal or external to human body. The major advantages of the WBAN are to facilitate patients with the handy applications that can move along with the patients. The sensors are placed at accessible distance or on patient body communicate with the local control devices. Local managing devices further talk to the distant targets to share analytical and therapeutic purpose data [64].

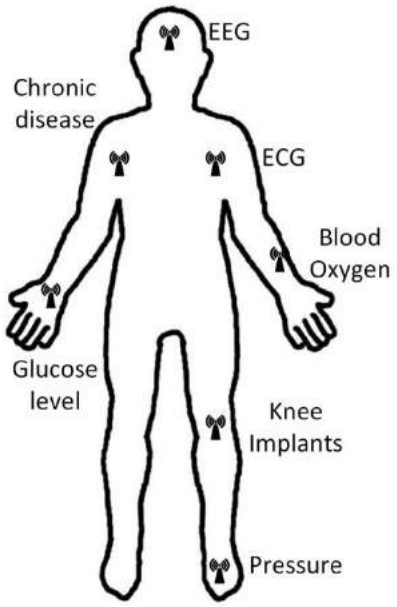

Figure 2. 7 Wireless Body Area Network

A small size and low cost sensor development system is achieved with the advancement in large scale and integrated communication technologies, which can be injected into human body for suitable healthcare applications. Some applications of the wireless sensor network are to provide an all time supervision of the user and also to avoid the risky state. In case of any emergency situations, WSN is cable to take appropriate actions to guarantee full safety for the patients [65]. The theory of Internet of Things (IoT) enables the possible information discovery about a tagged person or tagged object by searching internet address or record entry [66]. The security issue and confidentiality shelter of the WBAN data is a challenging problem, when it is stored either within the WBAN or in their transmission out of WBAN areas. Investigation of the two important data security issues is made such as the fine grained distributed access control and accurate distributed data storage for susceptible and confidential patient therapeutic data [67].

2.7 Malicious Users in Cognitive Network

The existing spectrum sensing schemes are not reliable to mitigate security attacks. Conventional security solutions in the non cognitive networks erroneously operate when faced by the new spectrum sensing attacks. The most considerable features of any WSNs is the facility to gather and practice in parallel with the massive amounts of data using tiny and limited power devices. This may enable their use in target detection, surveillance and monitoring applications. In recent times, some new ideas have been suggested to make best use of the cognitive WSNs (CWSNs), to develop knowledge of the environment, and to further make adjustable decisions based on desired goals [68].

The security issues in cognitive radio mobile ad-hoc network (CR-MANET) are in the greater interest of the research community. The impact of including malicious users in the CR-MANET is investigated and its suitability under the SSDF category of malicious users is illustrated. A consensus based technique for the CR-MANET is discussed to reduce the effects of any SSDF user in [69]. This shows the design of a wideband autonomous CR scheme for jamming and interference avoidance. The cognitive anti-jamming stochastic game model is able to avoid the transmission of other WACRs as well as to predict and evade the dynamic signal of the jammer that sweeps across the desired spectrum [70]. Similarly, vehicular ad-hoc networks (VANETs) can satisfy the demands of high bandwidth requirements in amount of applications to communicate between vehicles using CR features. An assumption is made in this work to declare every vehicle as benign and honest in the network. As reduction of security issues in the CR-MANET is a major issue, therefore, a weighted agreement based sensing scheme is implemented to look after the sensing practice in the belligerent cognitive radio vehicular ad-hoc network (CR-VANET) in [71]. Some of the SUs always report existence of the PU transmission, in order to utilize the spectrum themselves. To protect the system against these challenges, an

abnormality identification algorithm that measure the suspicious level of the users and to further utilize these suspicious levels in eliminating the influence of malicious users is presented in [72].

A single suspicious user elimination in CRN is of high interest in most of the literatures. In case of more than one suspicious users in the network, detection accuracy of the system is degraded considerably. A generalized extreme studentized deviate and adjust box plot schemes handle multiple suspicious users efficiently in the collaborative network in [73].

2.7.1 Selfish Users in Cognitive Network

The CR attacks are classified as: sensing attacks, decision attacks and the spectrum mobility attacks. Similarly, the selfish user attack is studied at various classification standards that increase to share the spectrum resources. An adaptive attacker can adapt its power and channel parameters by employing estimation and learning techniques in [74]. The existing cognitive routing protocols assume the nodes to participate honestly in the packet forwarding. This assumption is no longer authentic due to lack of a trusted centralized authority in the CRNs. A cross layer selfish avoidance routing protocol in the presence of selfish nodes in the dynamic CRNs is proposed in [75].

Various categories of the network attacks such as node masquerading, deliberate packet dropping and packet mislabeling pose challenge to the quality of service (QoS) provisioning in the CRN. The existing work focus in the literature is in the medium access control and physical layer of the CR, however, security threats at the network layer are not being explored well in order to establish communication between different users [76]. Trusted nodes operate normally in the CRN by following the network standards and protocols. The selfish nodes fraudulently increase access to the spectral resources in order to avoid other users access to the channels. Similarly, the

inspiration for malicious users is to obstruct other users from contacting the resources in several ways, such as disturbing and degrading the network performance. This can result in significant reduction of the network performance due to the vulnerabilities of the CR-MAC layer as in [77].

2.7.2 Byzantine Users in Cognitive Network

The Byzantine category of attack is the type of spectrum sensing data falsification (SSDF) attack in the text. Byzantine user is the key adversary to the success of CRNs. The Byzantine category of malicious users and the protection schemes against these attacks has gained increasing awareness in recent times. An abnormality detection approach is proposed to alleviate the unknown strategy of attackers in CRN [20]. The Byzantine user behavior is classified based on the attack parameters, and to determine how, who and where the attack is launched. The increased number of Byzantine users in the network leads data fusion schemes incompetent to decide accurately and most of the reputation based schemes are incapable to attain the desired performance gain [78].

The work demonstrates the susceptibility of two specific cognitive networking schemes in the presence of single Byzantine user. A novel energy well category of attack is discussed against the Q-routing, in which a Byzantine member can draw traffic meant for a sincere contributor. A denial of service attack learning algorithm with the single Byzantine participant degrading network performance for an arbitrary amount of time is investigated in [79]. This technique includes, measurements involving history trust factors, incentive factors, consistency factors and active factors. The doubtful users are recognized and take out of the final decision based on the measured trust factors [80].

The Adaptive cooperative schemes identify attackers along with their attacking plans to estimate the credit value of the users and identify any malicious attacker. In order to do this, a novel ACSS technique is compared with the usual likelihood ratio test and sequential ratio test at different levels of MUs that allocates an appropriate mutual weight to the users, in order to improve the system performance [15].

2.7.3 Jammers and Eavesdroppers in Cognitive Network

The PU activity is often eavesdropped by a number of eavesdroppers, therefore, SUs are required to intelligently interface with these eavesdroppers to minimize their harmful effects and gain transmission opportunities. In order to assure the highest quality service to the users, transmission rate of users must be kept higher than a certain level [81].

The CR system physical layer security under multi-eavesdropper system is investigated, that consists of several SUs transmission to the general cognitive base station (CBS). An optimal and suboptimal arranging algorithm using round robin system improves the security issues of the CBS transmissions in the presence of eavesdropping attacks [82].

Little study is met in the literature regarding the general security areas such as the network reliability in the presence of jamming users. Traditional jamming is targeting frequency band of operating target radio with malicious signals injection to interfere with the desired signal at the receiver. The interference history takes the form of the narrowband continuous wave (CW) jamming, broadband noise jamming, swept CW jamming, narrowband CW jamming or pulsed jamming. There are various objectives a jammer is searching, i.e., network degradation, herding and Intermediate denial of service (IDoS) [83].

The cognitive anti jamming problem in a multi agent environment that is modeled as a general stochastic game is addressed. This work first introduce action and reward definitions for the projected stochastic game and then, an optimal and suboptimal anti jamming and hindrance prevention policies using reinforcement learning (RL) is suggested [84]. The confidential data need to be accessed by the intended users only rather than any intruder. Similarly, eavesdroppers using the attacks of jamming and eavesdropping [85] compromise the physical layer security.

2.7.4 Primary User Emulation Attacks in Cognitive Network

The primary user emulation attack (PUEA) is one of the common security attack that compromise spectrum sensing process. In the PUEA attack, malicious user prevents vacant spectrum bands by masquerading as the primary user in order to prevent other secondary users from accessing the spectrum opportunity. Although, test beds exists in the literature, but no diagnostic models relevant to the various parameters which could cause a PUE attack is studied in the literature [86]. The sensing information of the different SUs is combine at the fusion center and the combine weights are optimized so that to maximize detection probability of available channels with the constraints of required false alarm probability [87].

Most of the previous studies on the PUEA assume that the unique properties of the PU transmitter and its physical location are known at the SU or at the FC. However, an accurate strategy which is capable to accurately detect PU, without the prior information is of high interest. In the study of [12], a new technique called attack aware threshold selection scheme requires no a prior information about the properties and location of the PU. An always present attacker leads to wastage of energy resources and must be ignored at the fusion center. The

PUEA category of MU is disrupting the spectral resources of the PU more hazardously as compared with the always present attackers in [88].

2.8 Sensing schemes in the literature

Spectrum sensing in CR is a demanding research area these days. The unlicensed opportunistic access of the unused frequency bands across the licensed radio spectrum is investigated for increasing the efficiency of the spectrum utilization. As the spectrum access demands protection of the licensed spectrum operations, therefore, sensing based access is the most reliable and simple method to allow the unlicensed users to transmit through the free spectrum bands [2] in Figure 2. 8.

In CRN, SUs are looking out for opportunities to find vacancies in the radio spectrum in order to utilize the spectrum for communication. When the PU rejoins the spectrum, SU has to terminate its connectivity, it is therefore difficult to insure QoS for the SUs. In case of the frequent usage of the channel by PUs, termination probability of SUs is difficult to be ensured. The channel reservation scheme raises the QoS for SUs, where, it enables the terminated SUs to move to the reserved channel and keep communication active [89]. KL divergence based sensing method with the constant false alarm probability in [90] provides reliable sensing results. The detector is based on the distribution analysis of the incumbent user received signal. A theoretical false alarm probability will be derived for fixed threshold using Meijer G-function with the product of p Rayleigh independent random variables.

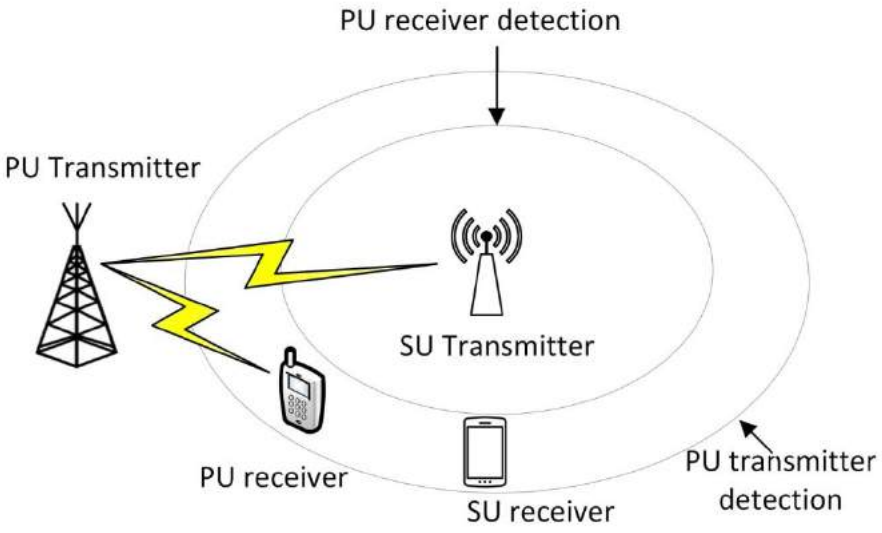

Figure 2. 8 Spectrum sensing concept

The statistical modeling of the network traffic is able to predict behavior of the PU with high performance. In particular, an innovative technique for the detection of an orthogonal frequency division multiplexing (OFDM) based PU signal is discussed in [91], where performance analysis is carried out in comparison with conventional spectrum sensing method that exploits the autocorrelation coefficients. Unlike the conventional method, the strategy is completely blind and can be applied with no a priori knowledge of any characteristics of the signal of interest. The new system implementation challenges involved in the design of CRs is the ability to efficiently sense the spectral environment and to flexibly adapt the transmission parameters in order to maximize the capacity of the system. The critical design problem in such system is the need to process multi-gigahertz wide bandwidth and to reliably detect the presence of the PUs. These requirements put severe limits on the linearity, sensitivity and dynamic ranges in the circuitry of the RF front ends [92]. The use of multiple antennas for spectrum sensing is considered when noise and signal of the PU are considered independent complex zero-mean Gaussian random variables. In the implementation of multiple antennas for spectrum sensing the system get knowledge of the channel gain, PU signal variance and noise variance [93]. The spectrum

sensing process has the main objective of providing more spectrum access opportunities to the cognitive users without making any interference with the licensed users. The transmission efficiency of the current radio frequency front-ends inevitably decreases due to its inability to do the sensing and transmission jobs at the same time. In the solution to cope with both the interference avoidance and spectral efficiency problems, a theoretical framework is built to optimize the sensing parameters and to maximize the sensing efficiency with the constraint on interference avoidance [94]. To consider spectrum sensing of the OFDM signals in an AWGN channel for the completely determined noise and signal power, a vector matrix model setup is made for the OFDM signal using cyclic prefix and optimal Neyman-Pearson detector. The optimal detector results are compared with the ED numerically. It is shown that the ED is near optimal with a gain of 1 dB SNR. To deal with the unknown noise and power of the signal, results are derived for the generalized likelihood ratio test (GLRT) detector based on the second-order statistics of the received data. Detection results of the GLRT detector in unknown noise and signal power are compared with the OFDM based signal detector, producing improved detection performance with 5dB SNR gain [95].

SUs try to sense the primary channel $s(l)$ and make the absence and presence hypothesis assumption about the channel as follows [6]:

$$y_j(l) = \begin{Bmatrix} H_0, & n_j(l) \\ H_1, & h_j s(l) + n_j(l) \end{Bmatrix} \quad (2.1)$$

Where H_0 is the hypothesis about the availability and H_1 is the hypothesis for the occupancy of the PU spectrum by the licensed user. $y_j(l)$ is the received signal of the j^{th} user at the l^{th} time slot.

$n_j(l)$ is the Additive White Gaussian Noise (AWGN) at the j^{th} receiver. h_j is the amplitude of the channel gain, while $s(l)$ denotes the transmit signal of the PU in the l^{th} time slot.

As a consequence of H_1 and H_0 hypothesis, the observed signal energy at the j^{th} receiver can be represented as [6]:

$$E_j(i) = \begin{Bmatrix} \sum_{l=l_i}^{l_i+S-1} \left| n_j(l) \right|^2, & H_0 \\ \sum_{l=l_i}^{l_i+S-1} \left| h_j s(l) + n_j(l) \right|^2, & H_1 \end{Bmatrix} \quad (2.\ 2)$$

GLRT detector for sensing: GLRT detectors have been proposed for multi antenna systems and for sensing OFDM signals by taking some of the system parameters, such as channel gains, noise variance, and PU signal variance as the unknown parameters [93],[95],[96].

Matched Filter Detector: When information of the PU signal is known at the SUs, the optimal detection method is the matched filter detector in Figure 2. 9.

This detector utilizes correlation property to determine, if the known primary and received signals have any correlation to maximize the SNR. This technique work inappropriately when transmits signals of the PUs are unknown at the SUs [47].

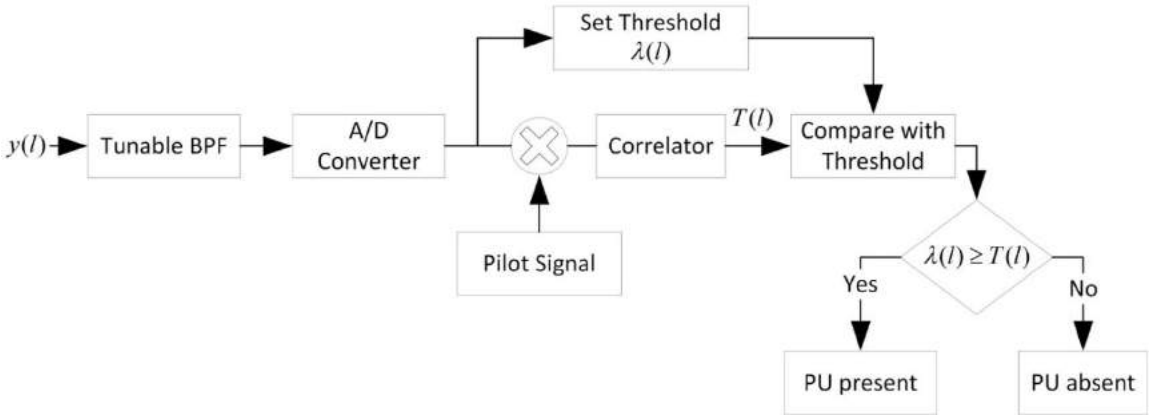

Figure 2. 9 Matched Filter Detector

Energy detector: Energy detector is the most common used option due to its simplicity in Figure 2. 10. In this scheme, the received signal energy is compared with a threshold. If the total energy is greater than threshold, SU take decision to show the PU signal is present; otherwise, it declares that the PU is absent [47],[97].

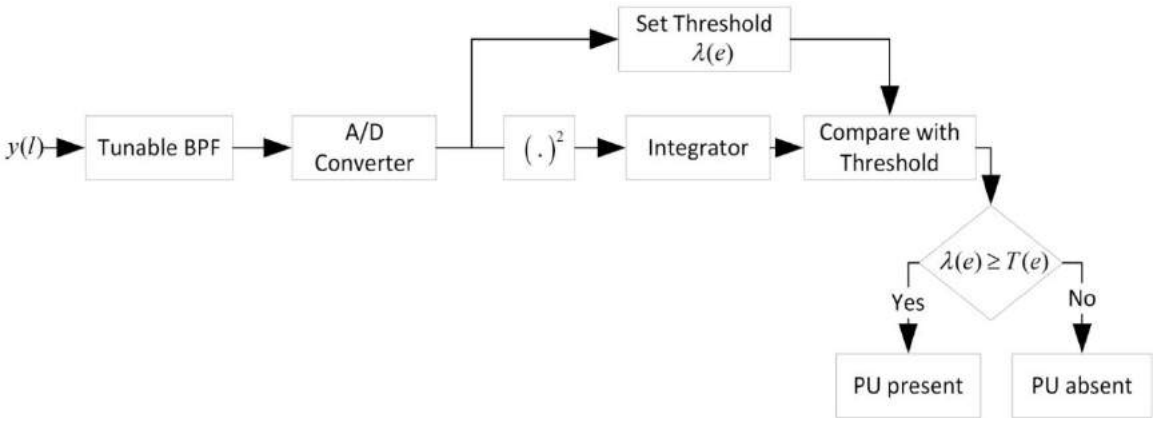

Figure 2. 10 Energy detector

Feature detector: Cyclo-stationary detector is the one that uses cyclo-stationary features of the signal for spectrum sensing [97],[98]. It can distinguish both noise and PU signal and is very helpful in the detection of weak signals under the low SNR, where energy detection and matched filtering detection are not applicable [29].

In the literature cyclo-stationary feature detection is superior of all due to their ability to differentiate modulated signal, noise and interference in the presence of low SNR [99]. The conventional detection solution for spectrum sensing is based on the ED which is completely blind and characterized by the lowest computational complexity of the decision device. Therefore, detector sensing performance is often compared with the ED, but unfortunately, in low SNR regimes and in the presence of noise uncertainty, ED dramatically degrades its performance [100]. An inappropriate detection of the vacant spaces might generate interference

to licensees if misdetection operation is made by the sensing users. To avoid such problems, an alternate series representation of the Marcum Q-function, for the exact detection probability over Nakagami fading channels is discussed in [101], where SUs do not interfere with transmission of the PUs.

The telecommunication signals are often sculptured cyclo-stationary, therefore this problem is translated to the detection of cyclo-stationary attributes over a cyclic scope of frequencies and fixed false alarm rates in [97],[98].

2.9 Cooperative spectrum sensing

Cooperative communication in CRN is a new technology that allows distributed sensors in the wireless network to operate using distributed transmission and signal processing techniques in Figure 2. 11. In the fading environment, detection of white spaces in the licensed user channel is a challenging job for the individuals. The quality of received signal is severely degraded due to path-loss and shadowing in the propagation path from various obstacles. Fading effects due to the constructive/destructive interference in multipath strongly suffered the received signals. The effects of fading can be reduced using diversity schemes in which copies of the received signal are provided to the receiver. Diversity effects are obtained using multiple antenna systems with more than one antenna installed at the transmitter and receiver sides. However, the cost, size and weight constraints make the practical implementation of multi antenna wireless terminal very difficult to insure. Cooperative spectrum sensing guides the sensing process to fight against the fading effects with improved detection performance. The use of cooperation among individual sensors has greatly attracted the research community interest in the wireless network [102].

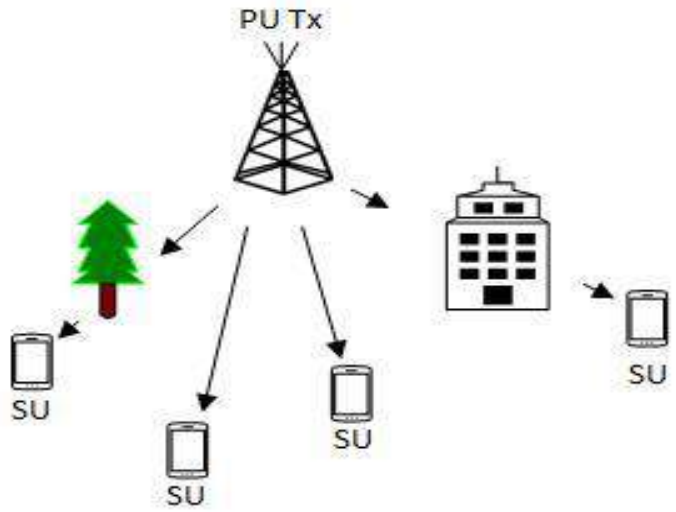

Figure 2. 11 Cooperative spectrum sensing in a shadowed environment.

CSS design consists of designing cooperative model, selection of spectrum sensing techniques, control and reporting channels, data fusion schemes, hypothesis test, selection of user, and knowledge base center as in Figure 2. 12.

- Spectrum sensing techniques are used to monitor PU spectrum band to state its free and occupied information. Individual users cooperation can highly affect the spectrum selections.
- The detection performance of cooperative sensing is supported and improved with the knowledge base. The prior knowledge as well as licensee and unlicensed user locations are stored in the knowledge base.
- Data fusion schemes integrate the shared sensing results to take cooperative decision.
- The control and reporting channels dealt with transferring the sensing data to control coordinator or to other SUs using limited bandwidth.
- Hypothesis testing is used to state the presence and absence information of the PU. This testing is made individually by the control coordinator or by each SU to take cooperative decision.

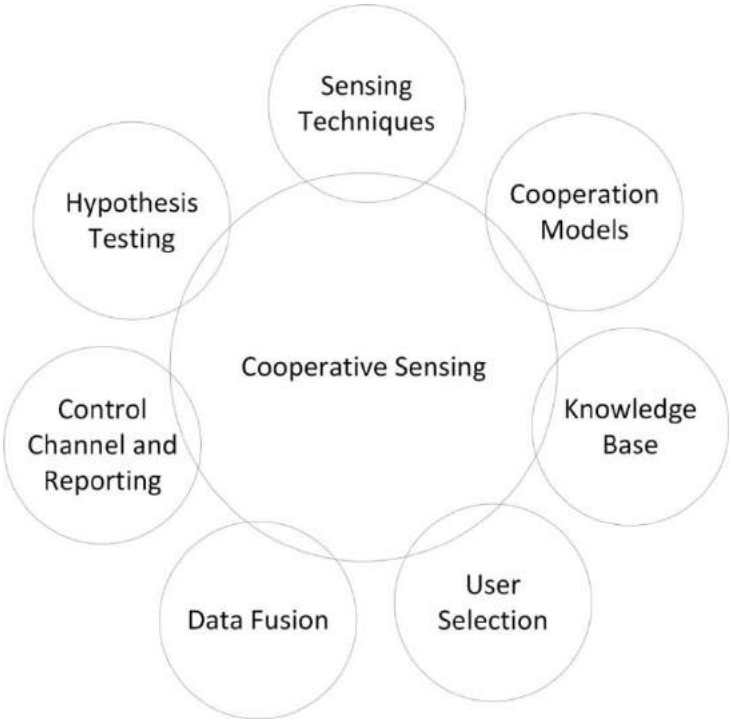

Figure 2. 12 Elements of CSS

Cooperative spectrum sensing consists of a series of actions with centralized and distributed sensing responsibilities.

2.9.1 Centralized and Distributed Spectrum Sensing

Centralized cooperative strategy is the most popular of all cooperative schemes. In the centralized cooperative strategy a central unit, also called FC collect the sensing information from all cooperative users to take the final decision. Either opportunistic information is broadcast to all SUs by the central unit or the FC itself controls the SU traffic by managing the vacant spectrum opportunity in an optimum fashion. The central unit can be an access point (AP) in the wireless local area network (WLAN) or a base station (BS) in a cellular network. Similarly, in the ad hoc network any SU can act as master node to coordinate CSS operation. Hence, the centralized cooperation can take place in both the distributed and centralized network architecture. The cooperative decision made by the distributed scheme is not relying on the FC

decision. Instead, all SUs communicate among themselves to converge to a joint global decision on in an iterative manner. The three basic steps accomplished by the distributed cooperated algorithms are as follows:

1. Local findings of each user are forwarded to the other users in its neighborhood.
2. Cooperative SUs combine their local sensing information with the sensing information reported by other SUs to decide the presence and absence of PU based. The shared sensing results consist of either soft or hard decisions.
3. If the spectrum hole is not identified, SUs forward their combined results to other users in the next iteration. The process continues until the scheme converges and final decision on the availability of the spectrum is achieved.

Table 2. 1 Centralized and Distributed Spectrum Sensing comparison

CSS approach	**Advantages**	**Disadvantages**
Centralized spectrum sensing	This scheme is more bandwidth efficient as compared with the distributed scheme under the same number of cooperative users.	The fusion center becomes very critical and complex to take the burden of all cooperative users.
Distributed spectrum sensing	No requirements of the backbone infrastructure, that results in low implementation cost.	This scheme needs large control bandwidth to share information among the cooperating users. Each CR finds neighborhood for information exchange by itself, which is a challenging job. Large sensing duration resulted due to the iterative nature of the distributed algorithm.

A new form of space diversity in the cooperative sensors is realized to overcome the detrimental effects of the fading channels. The most important challenge for a CR system is the identification

of licensed users on a wide range of frequency spectrum, at a certain time and specific geographic locations. The detection process of the license user is made stronger and effective with CSS in CRN. All cooperative users in [103],[104] make use of equal energy detectors in spectrum sensing, where received energies of the users are modeled as correlated log-normal random variables. Cooperative spectrum sensing employing PSO based threshold adapting technique address the said problem in [10]. The use of iterative property is carried out round wise in the scheme, where in each round, SUs first selects few primary channels as the candidates for sensing based on the primary SNR. Then the users selected the same channels collaboratively form coalitions through coalitional game theory. Multiple games are then played concurrently over multiple channels in terms of the false alarm and miss detection probabilities. After generating stable coalitional structure, the best coalition on each channel is chosen to perform the CSS [105]. The sensitivity requirement in the receiving devices is highly demanded as any local radio can face deep fading environment. This sensitivity requirement of the individual nodes is reduced by following a light weight CSS using hard decision schemes. In the cooperative environment few independent users are almost robust than many of the correlated users participation. The consideration of failure or adverse nodes can strongly affect the cooperative scheme gain. Failure sensing nodes, reporting the absence and presence information of the PU are easily compensated by noting their behavior in [5]. A novel channel assignment scheme in [106], exploits the channel selection dependence on the signal frequency, attenuation, communication range and interference levels. This model is considered more realistic compared to the traditional methods in the mobility pattern of the CR nodes. It adaptively selects the maximal transmission range of each node over which reliable transmission is possible. An adaptive random nature scheme in [107] is able to better estimate about the license user spectrum

and to solve sensing data collection problems in an intelligent manner. This study considered the environment of un-equal SNR values of the primary signal at the local SUs. A random access method is used to collect spectrum sensing data of the users at collection time and the length of collection time is adaptively determined based on the known sensing data. In spectrum sensing CSS has got special attention, but it has shortcomings in terms of energy consumption and sensing overhead. The batteries limited life spans allow individual sensors in CSS to make a balance in the energy consumption of the individual sensors. Different variants of the centralized cooperative sensing techniques such as fuzzy logic, asynchronous cooperative sensing and weighted cooperative sensing of the primary transmitter detection are discussed in [108]. A novel linear combination scheme that requires mean and variance of the individual test statistics in [7] is tested under the block fading, slow fading and fast fading. This introduced a stochastic geometry tool to investigate the performance of CSS. String matching algorithms like Smith Waterman algorithm is widely used in bio-informatics for aligning the biological sequences in [109], to compare the reports of CR users with each other and to measure the similarity index. The sensing information of the users with their similarity index below this threshold value is discarded from the global decision. An energy harvest-based weighed CSS is proposed in [110]-[112] to decrease energy wastage of the users with increased sensing performance. This maximizes the spectrum access probability of the users by jointly optimizing the sensing time and total number of cooperative users. The probabilities of detection and false alarm results are important for the users to guarantee their usage of the channel. Cooperating spectrum sensing sets one of the probabilities as target and optimize the other using cooperative schemes. The derivations in [25],[113] show that in cooperative sensing, not all users participation is necessary, but the users with high SNR information of the PU signal is important. In the presence

of large number of cooperative users, the network latency and sensing traffic forwarded to FC rises quickly. This increase the number of parameters which leads to increase sensing time along-with collision at the control channel between fusion center and SUs. The work in [6] proposed the implementation of extended sequential CSS, in which individual SUs reputation help in efficient collection of local sensing notifications at the FC. A novel Bayesian method in [14] has increased robustness in the presence of abnormal SUs to artificially reduce or increase throughput of the radio network [14] .

2.9.2 Combination schemes at the Fusion Center

Combination schemes are employed at the FC to deal with the received sensing notifications of individual users. The three basic steps to perform fusion combination schemes at the FC are as below:

1. The fusion center selects a channel or frequency band of interest for sensing and requests all cooperative users to individually perform the sensing operation.
2. Cooperating users report their local sensing observations using the control channel.
3. The collection center fuses the local sensing observations of all cooperative users to decide about the presence and absence hypothesis of the PU and also to report back the same to the individual users.

As in Figure 2. 13, cooperative users sense the PU spectrum individually and reports FC about the channel condition. Based on the FC local decision and received observations from all other users, a global decision is obtained about the free and occupied status of the PU spectrum. The history logs of the users also enable FC to identify an MU. The received energy observations $E_j(i)$ of the j^{th} user in equation (2. 2) are further used in the hard and soft fusion combinations in the following sections.

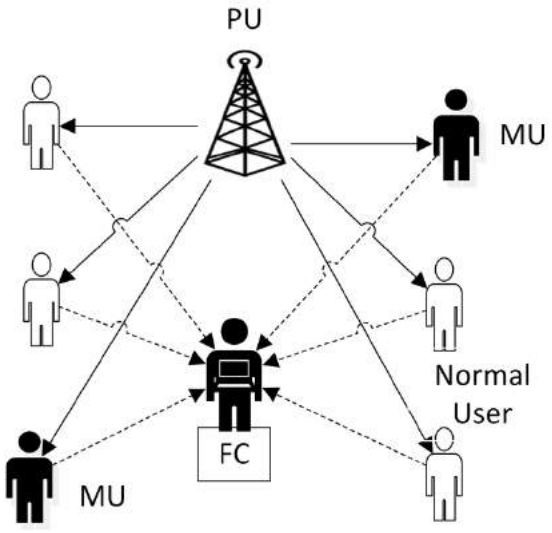

Figure 2. 13 Cooperative users report collection at the FC

2.9.2.1 Hard Fusion Combination schemes

The three most commonly used hard fusion schemes applied by the FC are the voting rule, OR and AND rules. The voting rule decides about the PU activity based on the voting of K SUs decision out of total S cooperative users. If K out of S users decides that a signal is present, then FC takes a global decision H_1. Here S is the total number of cooperative SUs and K is the count of how many of the SUs have reported PU signal presence. The count $K = M/2$ is selected as a special case of the voting rule called the majority decision rule. Similarly, in the majority voting decision if the PU detection reports are less than K then FC takes the global decision as H_0

$$G_{B-MV}(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) \geq K \\ H_0 : \ otherwise \end{Bmatrix} \qquad (2.\ 3)$$

In equation (2. 3), $G_{B-MV}(i)$ is the global decision made by the FC using majority voting scheme. While applying AND rule by the FC, all the M SUs has to provide a unanimous decision of the

PU detection, then the FC declares the channel as occupied by the PU and generate a global decision as H_1 representing the PU signal, otherwise decision H_0 is made by the FC as:

$$G_{B-AND}(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) = M \\ H_0 : \ otherwise \end{Bmatrix} \quad (2.4)$$

On following the OR rule procedure by the FC during each sensing interval, if at least one of the SUs provide local detection information to the FC, then FC decides a global decision H_1, otherwise decision is made in favour of H_0

$$G_{B-OR}(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) \geq 1 \\ H_0 : \ otherwise \end{Bmatrix} \quad (2.5)$$

A CSS based on the counting rule is proposed in [27], where optimal sensing parameters of CSS for minimizing error is derived, and then simple algorithm is proposed to set CSS with the optimal parameters [21]. A closed form expression for the detection, false alarm and misdetection probabilities are derived for the AND and OR fusion schemes in [114]. The literature is following several fusion schemes like majority voting, OR rule and so on, which are special cases of the general k out of n decision rule. A dynamic adjustments of the value k instead of keeping any fixed value for k in [115]-[117] is able to provide more suitable detection results.

2.9.2.2 Soft Fusion Combination schemes

In the soft decision fusion scheme all users inform FC with their local energy statistic without any local processing's. FC further uses soft decision fusion schemes like EGC and MGC to take global decision that could best fit with the licensed user status.

The EGC employed by the proposed method is combining the individual statistical information of all SUs, giving equal weight to each individual SU decision and summed coherently. The result is compared with the threshold to decide the license user spectrum by the EGC as:

$$G_{EGC}(i)=\begin{Bmatrix} H_1:\ \dfrac{\left(\sum_{j=1}^{M} E_j(i)\right)}{M}\geq\gamma \\ H_0:\ otherwise \end{Bmatrix} \tag{2. 6}$$

In MGC scheme, each receiving signal branch is multiplied with a weighed function proportional to the branch gain. Branches with strong signals are further amplified while weak signals get attenuated with these weights. The idea to boost the strong signal components and attenuate the weak ones as in MGC diversity is exactly the same as that of filtering and signal weighting in the matched filter receiver. The MGC scheme at the FC assign higher weights to the decision of the SUs with higher SNR values and low weight to the decision of SUs with low SNR as:

$$G_{MGC}(i)=\begin{Bmatrix} H_1:\ \sum_{j=1}^{M}\left(w_j\times E_j(i)\right)\geq\gamma \\ H_0:\ otherwise \end{Bmatrix} \tag{2. 7}$$

$$\text{Where } w_j=\frac{\eta(j)}{\sum_{j=1}^{M}\eta(j)}$$

An alternate closed form expression for the detection probability over Nakagami channel is presented in the [118]. Square law combining is proposed, when users of the wireless service experience Nakagami fading channel and detection results are obtained with closed form expression of the integral Nakagami parameters [118]. Two simple and computationally efficient spectrum sensing schemes that enable faster decision at the FC using sequential and order transmission schemes in the presence of different SNR distribution assumptions are in [119].

CSS is considering MGC one of the optimal spectrums sensing choice. However, MGC requires the use of SNR information for better operation, therefore the use of the robust KL divergence based soft fusion combination in CSS has enabled FC to obtain almost similar performance to MGC scheme with no requirements of the SNR and no additional steps for the identification of MUs [16]. An optimal soft combination scheme using relay behavior of the cooperative users provides space diversity to the spectrum sensing operation. The optimal soft fusion scheme of the relay observation is derived with the Neyman-Pearson model that maximizes deflection coefficients of the global test statistics at the FC using instantaneous value of the received PU signal power at SUs [120].

Although CRN performance has majorly improved with cooperation, but an increase in the total number of cooperative users is not the best solution, as it can degrade total throughput of the CRN. A multistage cross entropy (MSCE) algorithm is used to optimize the trade-off between the global detection probability and achieved throughput [121]. An ED based cooperative spectrum sensing for CRNs is considered in [122], where Neyman-Pearson criterion is obtained based on the optimal soft combination schemes to maximize the detection probability with a given false alarm probability and establish a suitable trade-off in detection performance and system complexity [22],[122].

2.9.3 Cooperative spectrum sensing schemes against malicious users

Although CSS is providing an efficient solution in CRN spectrum utilization, but the presence of spectrum falsification type of MUs can degrade its performance. Reliability of the CSS is seriously compromised with its exposition to the data spectrum falsification attack that sets vital menace to the reliability of CSS.

The effects of deterministic falsified category of MUs can be ignored by the FC with following traditional static threshold based decision mechanism. This static threshold mechanism is unable to cope with the nature of SSDF users in CSS. A dynamic threshold based strategy help to defend the CSS against the SSDF attacks in [123] . A novel reputation based cooperative scheme first detects, and then reject any malicious user, to improve the system performance. Finally, it compares the results with the well known reputation based methods in a blind or un-blind way [124],[125]. A novel defense scheme that jointly exploits the cognitive process of sensing and spectrum access in a close loop manner without any prior information about the number of attacking users is proposed in [13]. The results obtained are important from two perspectives, efficient spectrum sensing and identification of MUs. The work in [17] make use of the KL divergence method to reduce the spectrum falsification effects of MUs. Outlier detection techniques, such as BWP has its major application in the identification of outlier data components [126]. A combination of DSND and GA proposed reduce the effect of opposite, random opposite, always no and yes nature of malicious users and get superior results in comparison with the simple majority voting and EGC schemes. A traditional static threshold based decision mechanism that uses trust based secure routing model is able to resist the forwarding routing attacks in CRN. The monitoring nodes establish trust against the forwarding nodes and declare the nodes to be malicious based on their trust values. The malicious behavior of the non-trusted nodes is charged with stricter punishment policy that results in better network throughput and end-to-end delay performance [127]. An onion-peeling based approach enables CSS to oppose against multiple un-trusty sensors. A suspicious level is accumulated for all cooperative users based on their reputation. The users with their suspicious level beyond threshold are considered malicious and take out of the final decision [128]. It is necessary in CSS

to detect any abnormal users and to further ignore their sensing reports in spectrum sensing. Many techniques are based on the bias method, which require enough knowledge of the attacker's behavior. It is typically seen that the FC has no information of the attacker tactics. The use of abnormality based approaches in data mining can cope with the unpredictable behavior of the malicious users [16],[129].

To counteract the data falsification attack of MUs, Tietjen-Moore and Shapiro-Wilk based tests are suggested in the literature [25]. This work first considers the basic and statistical falsification attacks from MUs independently, and then proposes a novel SSDF attacks that involve the cooperation in misbehaved users by masking their results. The total number of MUs is further estimated using clustering and largest gap methods. In [21] and [130], the PUEA is nearly placed to the licensed PU and transmit with similar power as that of the PU in a way that it look similar to it [14],[131].

Evolutionary computing has great applications in the wireless communication. Evolutionary computing is used in the spectrum sensing, resource allocation and interference mitigation in CRN. Cooperative spectrum sensing also utilize evolutionary computing, such as GA and PSO to get to a more realistic decision about the license user activity.

Genetic algorithm enables CSS to produce optimized sensing results in order to increase bandwidth efficiency and spectrum utilization. A binary GA based soft combination scheme proposed in [130] produces improved detection results and bandwidth utilization for CSS. Genetic algorithm is analyzed under the impact of correlated user decisions to minimize the sensing error based on the Neyman-Pearson criterion in [132]. An effort is made in CRN to optimize the detection and false alarm probabilities, in order to reduce the error probability of SUs in centralized network using GA with the aim to keep the error probability minimum and to

search for the most optimum values of detection and false alarm probabilities. The GA performance is compared with the differential evolutions and it is obvious that the differential evolution finds a better solution with less number of evolutions [23]. The multi-parent crossover based soft decision fusion scheme in [133] using GA is able to reach to the better detection results as compared to the standard GA and other soft and hard decision fusion schemes.

In [134], a hybridize PSO-OR scheme use the combination of PSO and logical OR hard decision scheme together with double threshold ED to perform spectrum sensing operation. The FC received local decisions and energy observations reported by the users. PSO is then employed to optimize sensing decisions of the fuzzy users. A final global decision is then made by the FC based on the local decisions provided by all SUs. Similarly, the PSO scheme using MINI-MAX criterion is investigated in [135], in order to reduce the error probability more accurately compared with GA using optimized weighting coefficients against cooperative users. The multi objective hybrid invasive weed based PSO scheme, optimize soft combination in selection of the threshold and coefficient vector assignment to various users in order to reduce the probability of error in [136]. An optimal weighted coefficient vector in the soft fusion combination is determined using PSO to improve detection performance. This scheme has better results in achieving desired fitness, stability and convergence speed [112]. The major concern in CRN is to provide protection to the licensee channel against the harmful interference caused by the spectrum access of SUs. Detection error in the soft combinations is bitterly minimized by using imperialist competive algorithm in a structurally centralized CRN. The imperialist competive algorithm enabled CSS to assign optimize weights to the sensing measurements of individual users that established more optimum results compared with other soft and hard fusion combination and evolutionary algorithms [8].

2.10 Summary

The rapid evolutions in wireless communication demand new wireless services in both, the used and vacant parts of the radio spectrum. The FCC exclusively assigns spectrum bands to various services. CR is a smart technique that gains knowledge from the environment and adjust its parameters accordingly. The PUs are free to transmit any time with no restrictions, while the SUs can utilize the spectrum only when the licensee declares it free. In CRN, sensing the incumbent user spectrum is vital. An offensive detection on the PU channel due to false alarm reduces the SUs opportunity to utilize the free spectrum. Similarly, any misdetection in the PU transmission will produce interference in the transmission of legitimate and opportunistic users. In case of the frequent usage of the spectrum by the PUs, the termination probability of SUs is not easy to ensure. The cooperative user devices placed more than a few wavelengths apart experience an independent fading effect. The doubt to efficiently detect the licensed spectrum possession is removed by enabling different users to share their local sensing results and make a cooperative decision. In this dissertation of the Resource Allocation and Spectrum Sensing in Cognitive Radio Network using Soft Computing and Statistical Techniques, KL divergence, GA, PSO, correlation and BWP has been employed to protect the CSS against the spectrum falsification attack (SFA) of the AYMU, ANMU, ROMU and OMU categories of MUs.

In chapter 3, different techniques are investigated for selecting an optimal resource allocation and spectrum sensing policy in the presence of MU's.

Chapter 3

Statistical and Heuristic Algorithms

3.1 Background

In this chapter, we will discuss KL divergence, GA, PSO, BWP and Hampels Test (HT) to detect abnormal activity of the Always Yes, Always No, Opposite and Random opposite categories of MUs. KL divergence is the basic equation in the information theory to measure the similarity in data. KL divergence is the statistical measure that quantifies the closeness of the probability distribution with a model distribution [137]. However, its intuitive understanding arises from the likelihood theory, which shows the probability that one observes a set of data given a particular model is true [138]. This link in the KL divergence and the likelihood arise from the reality in cases where large number of measurements, possibly infinite are performed [137],[139]. The KL divergence provides many applications in the field of statistics and information theory to determine the behaviour of the data [137]. Similarly, in order to judge a model inconsistency, the KL divergence is the most frequently used information principle [140]-[143]. KL divergence is also defined as the logarithmic ratio of the probability density functions (PDFs) of the two models, where one is always considered to be a fitted model and the other model as a reference model. The expectation is always taken in the KL divergence with respect to the reference model. KL divergence is suitable for model comparison in the Bayesian framework, typically involve the integrated likelihood of the competing models [142].

The name heuristic is a Greek word which means ‘to discover’ or ‘to find’ something. It is the terminology used in the algorithms, to solve a problem more quickly and efficiently as compared

with the traditional method of algorithm in the exchange of precision and accuracy with more optimality, completeness and execution time. The optimization problems make good use of the heuristic algorithms (HA), when the optimal solution is not possible or when it is unrealistic. HA can be helpful to speed up the process of finding any satisfactory solution. Different researchers from all over the world have shown their interest in the HA, due to its ease in the perception and implementation and also helpful act against variations in the environment [144]-[147]. Heuristic algorithms are based on the concept of biological evolution, that is, Darwin's theory of evolution, with the population based searching methods using genetic operators, including crossover, mutation, inheritance and selection. Further advantages of the HA as compared with the traditional optimization methods include its broad series of applications, ease of concept, hybridization, parallelism, ability to solve problems with no solution and their adaptability to the dynamical changes [148]-[151]. Among the many HA found in the literature, few of them are listed below.

- Firefly algorithm
- Genetic algorithm
- Cuckoo search algorithm
- Differential algorithm
- Ant colony optimization
- Cultural algorithm
- Particle swarm optimization
- Pattern search algorithm
- Bee colony optimization
- Fire algorithm

- Backtracking search algorithm
- Evolutionary programming
- Self-organizing migration algorithm
- Harmony search algorithm
- Bat algorithm

In this chapter, we will restrict our discussion to the KL divergence, GA, PSO, BWP and HT.

3.2 Kullback Leibler Divergence

As the KL divergence value between the two probability distribution functions (PDFs) $a(x)$ and $b(x)$ both normally distributed as follows [152].

$$K(a \| b) = \int_{-\infty}^{+\infty} a(x) \log\left(\frac{a(x)}{b(x)}\right) dx \tag{3. 1}$$

Similarly, the KL divergence for functions $a(x)$ with mean and variance $\left(\mu_a, \sigma_a^2\right)$ and function $b(x)$ with mean and variance values $\left(\mu_b, \sigma_b^2\right)$ is further calculated as:

$$\begin{aligned} K\left(a \| b\right) &= K\left(\mu_a, \mu_b, \sigma_a^2, \sigma_b^2\right) \\ &= \frac{1}{2}\left(\log\left(\frac{\sigma_b^2}{\sigma_a^2}\right) - 1 + \frac{\sigma_a^2}{\sigma_b^2} + \frac{\left(\mu_a - \mu_b\right)^2}{\sigma_b^2}\right) \end{aligned} \tag{3. 2}$$

The result in Equation (3. 2) clearly shows that for functions $a(x)$ and $b(x)$ with similar PDF occurrence, has "0" KL divergence value. As always Yes and always No MUs are giving identical energy distribution with similar mean and variance values under both H_1 and H_0 as in Figure 3. 1, therefore the KL divergence has a value 0 for always Yes and always No MU. The

opposite MU and random opposite MUs are generating dissimilar KL divergence results in comparison with normal SUs as shown in the energy distribution in Figure 3. 1.

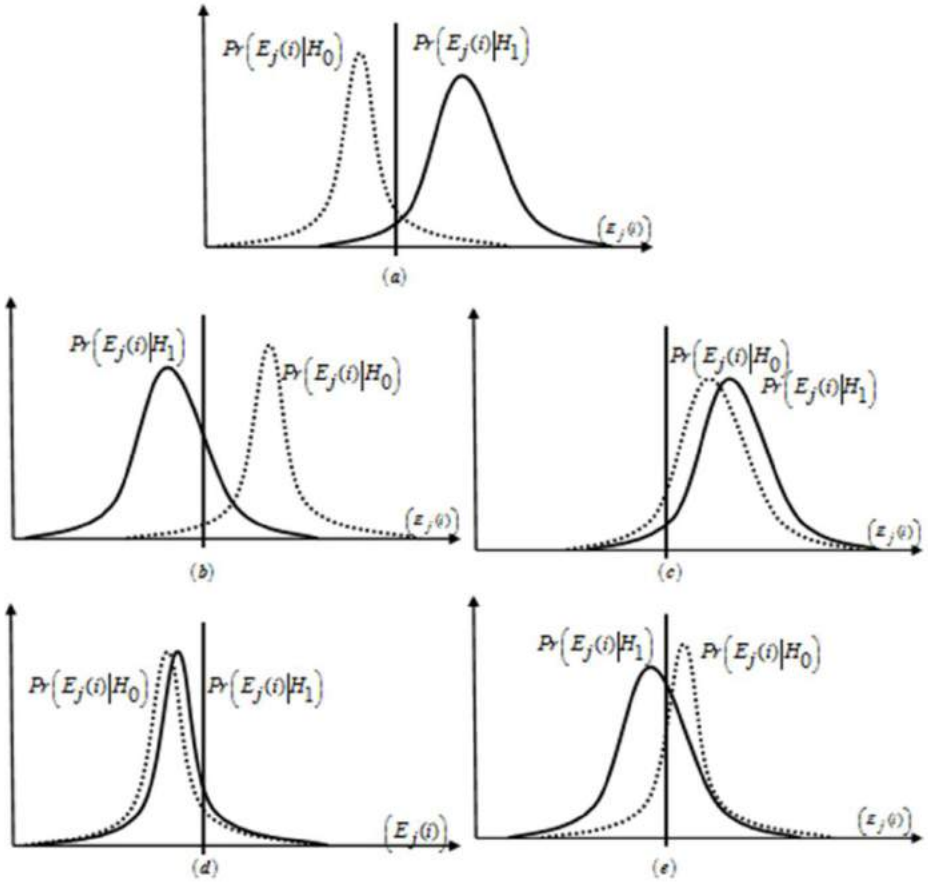

Figure 3. 1 PDF of the energy distribution reported from the CR users under the absence or presence hypothesis of the PU signal: (a) normal user, (b) opposite MU, (c) always Yes MU, (d) always No MU, (e) random opposite MU.

The PDF of the energy distributions received from the normal SU, opposite MU, always Yes MU, always No MU and random opposite MU are shown for comparison in Figure 3. 1. It is to be noted that the energy distribution of these MUs is totally different from the normal SU. These differences in the energy distribution of the SUs are used for the detection of MUs. A normal SU in Figure 3. 1(a) is shown with positive energy distribution under H_1 hypothesis and negative energy distribution under H_0 hypothesis. The opposite MU has opposite energy distribution to

the normal users as in Figure 3. 1(b) under both H_0 and H_1. Always Yes MUs with positive energy distribution under both H_0 and H_1 hypothesis and always No MUs with negative energy distribution under both H_0 and H_1 hypothesis are shown in Figure 3. 1(c)-3.1(d). Random opposite MU has statistically opposite nature to the normal SUs with probability p and results in distributions as in Figure 3. 1(e) in both hypotheses.

3.3 Genetic Algorithm

The idea Genetic algorithm was introduced for the first time in 1975 by John. H. Holland in his work of presenting an easy solution for the natural selection [153],[154]. GA has its major advantage in the fact that it cannot be struck in the local minima and give suitable result to the problems that are difficult to dealt with by other methods, or having no mathematical model, or the problem with complex mathematical model, or when the problem consists of large number of parameters. Nowadays, various fields of engineering make use of the GA in solving diverse optimization problems [155]-[158].

GA technique with its recycling features starts with the randomly generated population having a fixed number of individuals. The population is the representation of the possible solution to the problem in the concern environment. All individuals of the population are known as chromosomes, where each chromosome consists of fixed genes. When the population is formed, selections of the stochastic operator go for the best solution during each generation. A new set of individuals called parents is formed with the selected solutions, which will further participate in the outstanding evolutionary process. The parent chromosomes employ the process of crossover, mutation and elitism, in order to find the best solution, which further constitute a new set of individuals labelled as children (offspring's). This selection of the parents and production of the

offspring's continues until the establishment of given number of iterations or when best individuals are selected. The procedural steps of the GA are depicted in the flow chart diagram in Figure 3. 2.

Step I Initialization: This is the commonly used step in all HA, as the set of individuals that contains a possible solution of a problem being solved is mandatory for every HA. Therefore, this step has no constraint on the size of the individuals that constitute the population.

Step II Fitness Evaluation: The most important part of HA techniques is the design of the fitness function, as the performance and result of any algorithm mainly depends on the particular fitness function, which is specific to a problem. The fitness score is evaluated for all individuals and are placed in descending order of their fitness.

Step III Parent selection and Offspring production: These sorted individuals in the previous step now became parents in the next generation. The probability to generate children population is proportional to the fitness of their parents. Single point and multi point crossover are helpful in this production. Parents with higher fitness score have the opportunity to produce more children's. More children will be produced by parent having higher fitness and vice versa. There are two approaches for doing this:

1. Selecting parents with their probability is inversely related to their fitness and invite them to bring into being.
2. Selecting roulette wheel method with angle of the sector directly associated with the fitness, therefore, the sector with a higher angle has more possibility to be successful as a better parent.

Step IV Generating the new population: Children are selected for the next generation by following three methods such as Generation replacement, Elitism and Survival of the fittest.

(a): Replacement of generation: This step allows the complete replacement of parents by their children. Although a thorough process for mixing of genes is allowed in the practice, even then there is no assurance that all of the children will be better candidates as compared with their parents. Therefore, this will happen in degradation of the fitness due to losing some of the individuals having best genes.

(b): Elitism: Some of the best individuals from the previous should be retained in this process, so that to deal with the handicap of generational replacement.

(c): Survival of fitness: In this process, both the children and parents are sorted in descending order of their fitness results.

Step V Mutation: The process of mutation is the only choice when no development is observed in fitness of the next generation. In mutation individual genes are selected randomly for a change.

Step VI Termination criteria: The GA algorithm will automatically come to an end if the iteration limit is achieved or if the necessary MSE is accomplished. Otherwise, the process will go back to step II as in the GA flow-chart diagram of Figure 3. 2.

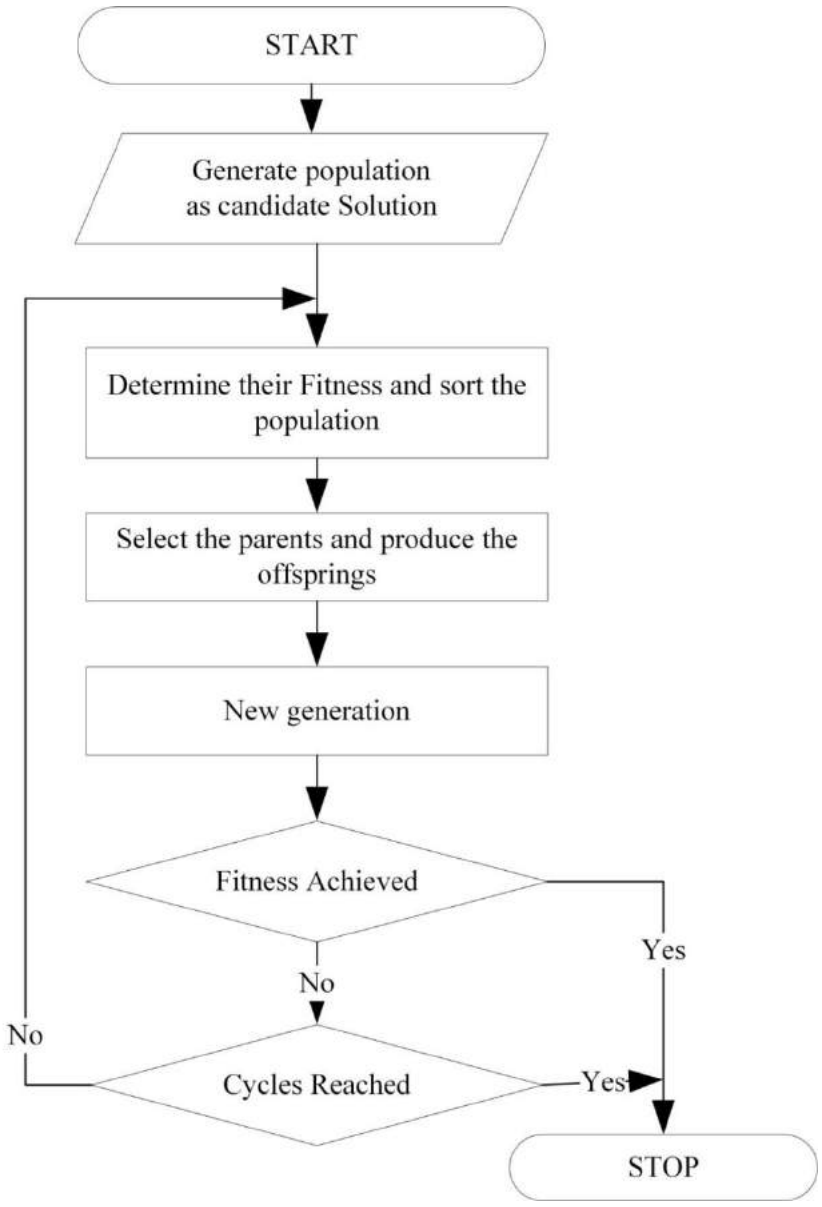

Figure 3. 2 GA Flow chart diagram

3.4 Particle Swarm Optimization

Particle swarm optimization is utilized as a tool for optimization of the threshold point in [159]. Different variants of the PSO are used in [160] to find optimal weighting coefficients against SUs in CSS. PSO with ED having double thresholds for the cooperative SUs is in [161]. An

efficient PSO with optimized throughput and providing high protection to the legitimate user is proposed in [162].

PSO is derived from the bird flocking or fish swarming, and was introduced by Eberhart and Kennedy in 1952. In PSO, individual intelligence as well as collective intelligence is playing a role in finding an enhanced solution. In the GA, it is likely that every novel group is flourishing better than the previous generation. Similarly, in the PSO the same group which has been initially created is likely to become better and better. Each individual establishes his intelligence and improves it with time. The whole group is expected to improve upon its group intelligence. Particles in PSO algorithm utilizes its own and neighbor knowledge to update their position and velocity. The PSO particle exchange information about their best position among each other during a number of iterations. The procedural steps of the PSO are as below in Figure 3. 3.

Step I Initialization: In this step, PSO population is initialized randomly, consisting all possible solutions of the specific problem as in the GA. Where each particle is the candidate solution.

Step II Fitness Evaluation: In this process, the fitness of each particle is determined according to the requirements and suitability to the specific environment.

Step III Local best and global best: After the determination of fitness functions, global best and local best particles are determined. As each PSO particle may improve on its own. If a new version of the particle improves compared with its previous one, it will be taken as the local best. Similarly, the particle with the best fitness out of the population is selected as the global best.

Step IV Update Velocity: In this step particles velocities are updated, which is directly proportional to its previous velocity, its distance from the local best and distance from the global best.

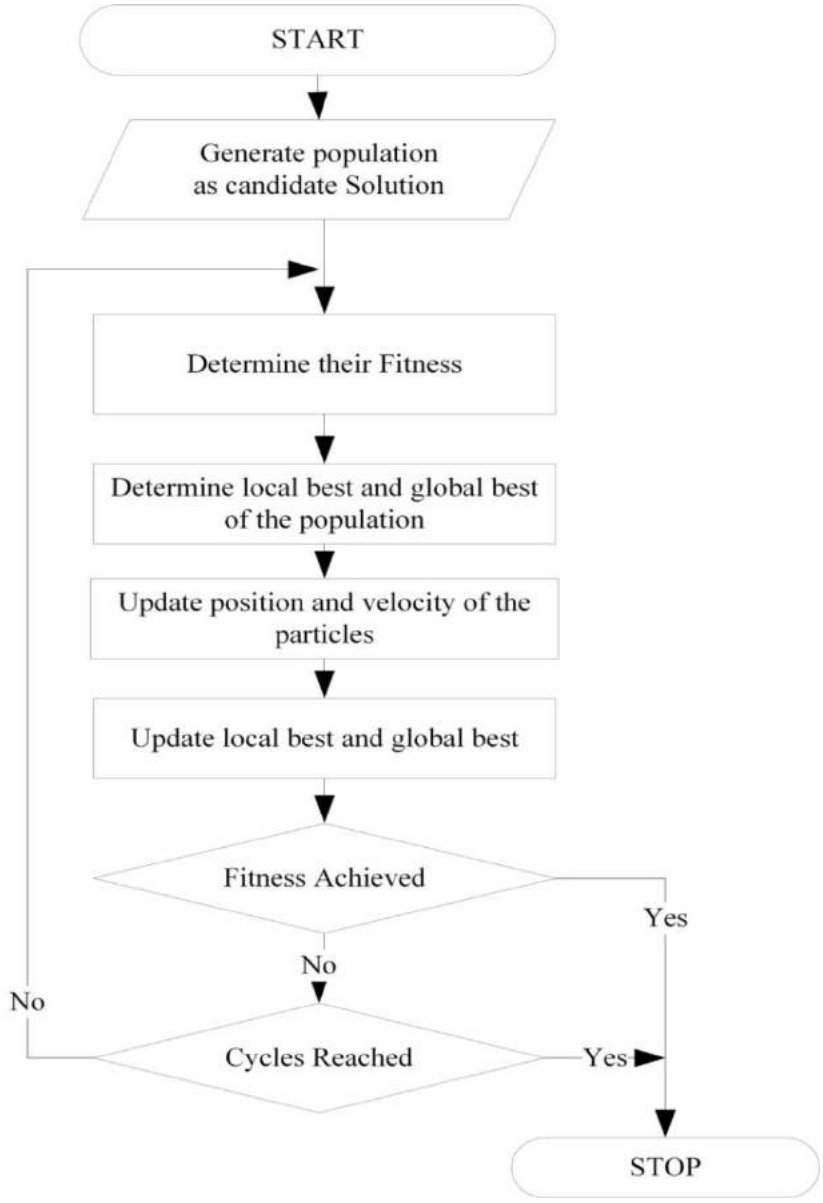

Figure 3. 3 PSO Flow chart diagram

Step V Update Local and Global best particles:

The Fitness function of the new population is determined and its local best and global best results are compared with the previous results of the local and global best particles to search for any improvement in the local best and global best results.

Step VI Termination Criteria: The PSO algorithm is terminated if required solution is met or when the maximum number of iterations is achieved. Otherwise, the program goes back to step II.

3.5 Box-whisker plot and Hampel's Test

A box-whisker plot and Hampel's test are the simple ways for the identification of outliers in any statistical data. Box-whiskers plot is the most commonly and widely used statistical tool for exploratory data analysis. It's a useful method invented in 1969 by John W. Tukey an American mathematician to visualize the data dispersion [26]. Box-whisker plot can instinctively reflect outliers by dividing data into four equal parts

$$\boldsymbol{d} = \left[d_1 \; d_2 \; ... \; d_M \right] \tag{3. 3}$$

First, the result is made in ascending order and the median value is identified that divides the data into upper and lower half using median value. Lower and upper quartile values are determined from the data $\boldsymbol{d}$. An outlier in the data using BWP is a dispersal of the data greater than 1.5 times the box away from either the lower or the upper quartile [163]-[166]. The median value of vector $\boldsymbol{d}$ is determined as:

$$Med = \begin{Bmatrix} d_j\left(\frac{M+1}{2}\right), & d\ odd \\ \frac{1}{2}\left(d_j\left(\frac{M}{2}\right) + d_j\left(\frac{M}{2}+1\right)\right), & d\ even \end{Bmatrix}, \; j \in 1,2,...,M \tag{3. 4}$$

The first and third quartile values that contain 25^{th} and 75^{th} percentile of the data in equation (3. 3) are denoted as Q^1_{Lower} and Q^3_{Upper} . The inter-quartile value for the range of the upper and lower quartile values is measured as:

$$IQR = Q^3_{Upper} - Q^1_{Lower} \tag{3. 5}$$

Similarly, the lower and upper limits are selected to detect MUs as:

$$L_{\lim it} = Q^1_{Lower} - 1.5\left(IQR\right) \tag{3. 6}$$

$$U_{\lim it} = Q^3_{Upper} + 1.5\left(IQR\right) \tag{3. 7}$$

After setting all parameters of the BWP, MUs are identified using the following criteria.

$$Abnormal = \left\{ \begin{matrix} j^{th}\ data & if\ \left(d_j \geq U_{\lim it}\ or\ d_j \leq L_{\lim it}\right) \\ 0, & otherwise \end{matrix} \right\}, j \in 1,2,...,M \tag{3. 8}$$

In equation (3. 8), a user is declared malicious if its correlation score is outside the lower and higher limits of the BWP.

Traditionally, in case of no outlier contamination in the data, location and scatter for the data is efficiently estimated with the sample mean and variance. HT introduced in 1971 by Hampel has the ability that it is not susceptible to the quantity and value of outlier. The HT also shows no limitation to the abundance of the statistical data. Therefore, it is applicable to the data containing abnormalities in order to search for abnormal contributing data [27]-[30]:

First, the value of deviation r^1_j from the median is determined for all data elements as:

$$r^1_j = \left(d^1_j - med(d^1_j)\right) \tag{3. 9}$$

Here $med(d^1_j)$ is the median value of the data in equation (3. 3) d^1_j made by all SU. A data is declared outlier, when the following condition is satisfied:

$$M_{mu} = \begin{Bmatrix} j^{th}, & if \left|r_j^1\right| \geq 4.5 Med\left|r_j^1\right| \\ 0, & otherwise \end{Bmatrix} \quad (3.\ 10)$$

Where $\left|r_j^1\right|$ is the absolute value of the median deviation and $Med\left|r_j^1\right|$ is the median of the absolute median deviation results.

3.5 Summary

This chapter focuses on the heuristic and statistical techniques for detecting abnormal sensing users that misguide other SUs about the licensee activity. It further creates the problem of improper resource allocation and incorrect spectrum sensing in CRN. The chapter is divided into three parts. Part I explains the optimal soft combination scheme, that is, KL divergence, that works on the PDF dissimilarity. The focus in part II is on the GA and PSO algorithms with its flowchart and necessary decision steps. In Part III, a theoretical and mathematical background of the BWP and HT methods are highlighted for detecting an abnormal sensing data among the data provided by all cooperative users. The detected MUs by the BWP and HT are isolated from the normal sensing users in the hard combination schemes that leads to better resource allocation and spectrum sensing in CRN in the presence of MUs.

Chapter 4

Cooperative Spectrum Sensing using Kullback Leibler divergence

4.1 Introduction

In this chapter, we have discussed the KL divergence scheme for MUs detection in CSS. Fading and shadowing in the communication channel degrades the sensing capability of individual users. To resolve this issue CSS is suggested. Although the system reliability is improved with cooperation but the presence of MU in CSS deteriorates the sensing performance. This chapter is divided into two parts. In part I, we have considered history based forward and feedback KL divergence method for minimizing SSDF attack. In the proposed CSS scheme, each SU reports the PU availability to the FC and also keeps the same evidence in its local database. Based on the KL divergence, if the user is acknowledged normal by the FC, then unified energy information is reported to the FC based on its current and previous sensed results. This method leads to high detection probability with optimum transmission energy, thus providing an improvement in performance. Simulation results show that the proposed KL divergence method has performed better than the existing EGC, MGC and simple KL divergence schemes in the presence of MUs at different levels of SNRs, total number of cooperative users and MUs. In part II, unlike the KL divergence in part I, where the individual SU sensing information is utilized for measuring the KL divergence, MUs are identified and separated based on the KL measurements of the individual SU decision and the average sensing statistics received from all other users. The proposed KL divergence scheme allocates lower weights to the MUs sensing and higher weights

to the normal SUs sensing. The proposed method has been tested in the presence of always yes, always no, opposite and random opposite MUs. Simulations confirm that the proposed KL divergence scheme performance has exceeded the existing soft combination schemes in estimating the PU status.

4.2 Data Model

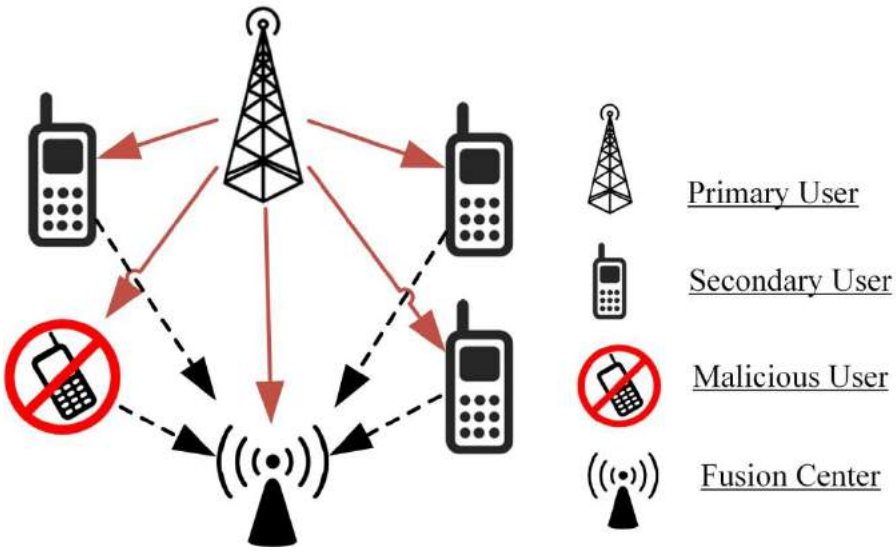

Figure 4. 1 Conventional CSS mechanism.

All SUs in the centralized CSS as in Figure 4. 1 report FC about the existence of PUs with local spectrum sensing information. FC combines the received sensing notifications from all SUs with his own sensing results and generates a global decision about the free and the occupied status of the PU spectrum.

Based on the spectrum sensing information by each SU in a particular band decision between H_1 and H_0 is as follows [6]:

$$y_j(l) = \begin{Bmatrix} H_0,\ n_j(l) \\ H_1,\ h_j s(l) + n_j(l) \end{Bmatrix} \tag{4. 1}$$

Here H_0 and H_1 are the hypothesis about the absence and presence of the PU. $y_j(l)$ is the received signal from the j^{th} SU, $n_j(l)$ is the AWGN at the l^{th} time slot for the j^{th} SU, h_j is the channel gain value between the j^{th} SU and PU and $s(l)$ is the signal transmitted from the PU. According to the hypothesis H_1 and H_0 the received signal energy of the channel by the j^{th} SU user at the i^{th} sensing interval is [6]:

$$E_j(i) = \begin{Bmatrix} \sum_{l=l_i}^{l_i+S-1} \left| n_j(l) \right|^2, & H_0 \\ \sum_{l=l_i}^{l_i+S-1} \left| h_j s(l) + n_j(l) \right|^2, & H_1 \end{Bmatrix} \tag{4. 2}$$

Where S is representation of the number of samples in the i^{th} sensing interval. The number of samples is to be considered large enough so that the energy reported by each SU resembles a Gaussian random variable under both H_0 and H_1 hypotheses.

$$E_j \sim \begin{Bmatrix} N\left(\mu_0 = S, \sigma_0^2 = 2S\right), & H_0 \\ N\left(\mu_1 = S\left(\eta_j + 1\right), \sigma_1^2 = 2S\left(\eta_j + 1\right)\right), & H_1 \end{Bmatrix} \tag{4. 3}$$

Here η_j is the SNR value between the j^{th} SU and the PU. (μ_0, σ_0^2), (μ_1, σ_1^2) are the mean and variance values of the energy under H_0 and H_1 hypothesis.

4.3 Proposed history based Kullback Leibler divergence scheme

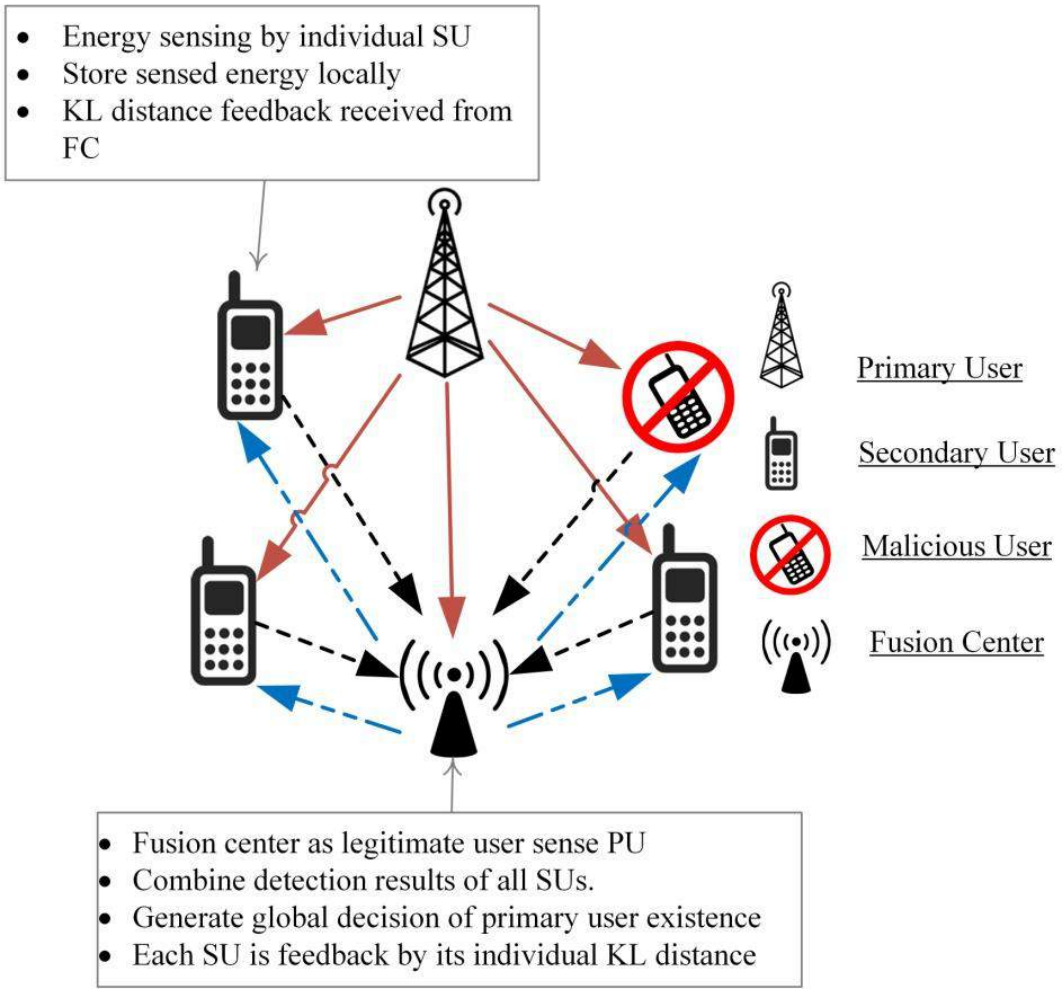

Figure 4. 2 Proposed CSS mechanism in the presence of MUs.

In the proposed work, the total number of MUs considered is less than the total number of cooperating SUs. All SUs report FC about the existence of PUs with local spectrum sensing information and also stores this data locally. FC combines the individual reports and generates a global decision of the PU spectrum. FC also creates a feedback report for each SU about its individual detection performance as in Figure 4. 2 by measuring the KL divergence score for each SU. Before SU reports any sensing information, it compares the detection results feedback received from the FC with a target value. Based on the feedback from the FC, if the detection results are achieved on behalf of a user, then this particular user will further participate in the

sensing process by combining current sensing results with its local history to report a more solid PU status to FC. SUs not declared as normal will forward their current sensing energy of the PU channel to the FC, while the confirmed normal user will sense the channel and forward mean energy of the reports already made under H_1 and H_0 hypothesis.

Pseudo code of the proposed method is as below

For $i = 1$ to sensing limit
For $j = 1$ to number of SU
IF $\left(\sum_i K_j(i-1) < T_1\right) OR\left(i = 1\right)$
$Z_j(i) = E_j(i)$. Where $E_j(i)$ is current sensing energy
Else
$Z_j(i) = M_{1j}(i)$ **or** $M_{0j}(i)$ is the average of the reported energy for the j^{th} SU under H_1 and H_0 Hypothesis.
End If
End of loop
For $j = 1$ to number of SU
Estimate new values of mean and variances under H_1 as $\left(\mu_{j1\_new}, \sigma^2_{j1\_new}\right)$ and under H_0 as $\left(\mu_{j0\_new}, \sigma^2_{j0\_new}\right)$ based on $Z_j(i)$
The difference of the KL distances for the j^{th} SU under H_1 and H_0 is measured as $\Delta K_{L,j}(i)$
Update the KL distance score $K_j(i)$ for the j^{th} SU as
$K_j(i) = \sum_i^N K_j(i-1) + \Delta K_{L,j}(i)$ and send feedback report of $K_j(i)$ to the j^{th} SU.
End of Loop
The combine KL divergence is determined as $\Delta K_T(i) = \sum_j W_j \times \Delta K_{L,j}(i)$. Where W_j is the weighting factor assigned to the j^{th} SU decision.
IF $\Delta K_T(i) > 0$
$G_B(i) = 1$
Else
$G_B(i) = 0$
End If
IF $G_B(i) = 1$
Update mean μ_{j1} and variance σ^2_{j1} for the next iteration.
Else
Update mean μ_{j0} and variance σ^2_{j0} for the next iteration.
End If

End sensing limit

4.3.1 Local decision and history maintenance by the SU

In this step, pre-sensing check is done by each SU, before forwarding, local sensing information to the FC based on its KL distance feedback information received from the FC.

$$Z_j(i) = \begin{cases} E_j(i), & IF\left(i=1\right) OR\left(\sum_i K_j(i-1) < T_1\right) \\ M_{1j}(i)\, or\, M_{0j}(i), & Otherwise \end{cases} \qquad (4.\ 4)$$

Where $\sum_i K_j(i-1)$ is the KL distance value received by the j^{th} SU and $M_{1j}(i)$, $M_{0j}(i)$ are the mean sample values of all sensing energies reported by the j^{th} SUs under H_1 and H_0 hypothesis based on the history results.

If it is the first time, sensing is done by the j^{th} SU or if the KL divergence satisfaction score is not achieved by a particular SU then, according to equation (4. 4) the sense energy $Z_j(i) = E_j(i)$ is reported by the SU to the FC and stores this energy locally for future implication.

Similarly, if detection results for the j^{th} SU are met by achieving the KL divergence satisfaction score, then the user is declared as normal. The normal user will search local history and calculate the mean of all high reporting energies as $M_{1j}(i)$ and of low energies as $M_{0j}(i)$ and will no more send energy $E_j(i)$ to the FC as:

$$Z_j(i) = \left\{ M_{1j}(i)\, or\, M_{0j}(i), \quad IF\left(\sum_i K_j(i-1) \geq T_1\right) \right\} \qquad (4.\ 5)$$

The normal SUs further forward these mean energy samples to the FC during the current and in the following sensing intervals according to the observation of the channel to forward decision M_{1j} or M_{0j} to the FC.

4.3.2 KL Divergence at the FC

Based on the energies reported by the j^{th} SU and the previous mean and variance values, new values of the mean and variances in the i^{th} sensing interval are calculated for all SUs at the FC as follows:

$$\begin{aligned}
\mu_{j1_new}(i) &= z_1\mu_{j1} + z_2 Z_j(i) \\
\sigma^2_{j1_new}(i) &= z_1\sigma^2_{j1} + z_1\left(Z_j(i) - \mu_{j1}\right)^2 \\
\mu_{j0_new}(i) &= z_1\mu_{j0} + z_2 Z_j(i) \\
\sigma^2_{j0_new}(i) &= z_1\sigma^2_{j0} + z_1\left(Z_j(i) - \mu_{j0}\right)^2
\end{aligned} \tag{4. 6}$$

z_1 and z_2 are constants with $z_1 = \frac{k-1}{k}$ and $z_2 = \frac{1}{k}$. Here k is the effecting level of the received energy to corresponding mean and variance of SUs PDF.

The KL divergence value for the j^{th} SU is determined as:

$$K_{j1}(i) = KL\left(\mu_{j1\_new}(i), \mu_{j1}, \sigma^2_{j1\_new}(i), \sigma^2_{j1}\right) \tag{4. 7}$$

$$K_{j0}(i) = KL\left(\mu_{j0\_new}(i), \mu_{j0}, \sigma^2_{j0\_new}(i), \sigma^2_{j0}\right) \tag{4. 8}$$

Where $K_{j1}(i)$ is the KL divergence score for the j^{th} SU under the presence hypothesis and $K_{j0}(i)$ is the KL divergence for the j^{th} SU under the absence hypothesis. The difference in the PDF $\Delta K_{L,j}(i)$ for the j^{th} SU under H_1 and H_0 hypothesis is calculated as:

$$\Delta K_{L,j}(i) = \left(K_{j1}(i) - K_{j0}(i)\right) \tag{4. 9}$$

The total KL divergence value $K_j(i)$ of the j^{th} user is further updated as below:

$$K_j(i) = \sum_i K_j(i-1) + \Delta K_{L,j}(i) \tag{4. 10}$$

This updated value of $K_j(i)$ is sent by the FC to the j^{th} SU in order to utilize this information prior to any further reports.

4.3.3 Global decision at the FC

Based on the KL divergence values of all SUs, the global decision $G_B(i)$ is made at the FC as follows:

$$G_B(i) = \begin{cases} H_1, & IF\left(\Delta K_T(i) = \sum_j W_j \times \Delta K_{L,j}(i)\right) \le 0 \\ H_0, & Otherwise \end{cases} where\, W_j = \frac{1}{\sigma_{j1}^2 \sum_j \frac{1}{\sigma_{j1}^2}} \tag{4. 11}$$

where W_j is the weighting value assigned to the j^{th} SU for data fusion combination. The lower weights are assigned by the FC to the reports of SUs with higher variance under the presence hypothesis before combination. As MUs including always Yes, always No, opposite and random opposite MUs have a dissimilar $K_{j1}(i)$ and $K_{j0}(i)$ in comparison with normal SUs, therefore their contribution in effecting CSS rule is minimized.

4.3.4 Updating mean and variance for the next iteration

As perfect values of the (μ_{j1}, μ_{j0}) and $(\sigma_{j0}^2, \sigma_{j1}^2)$ for calculating KL divergence is not possible due to unavailability of exact information about the PU. Therefore, universal decision $G_B(i)$ value calculated previously is further taken as an estimate of the PU signal for calculating and updating mean and variance values, which is used in the next sensing interval for KL divergence value calculation.

$$Z_{j1} = \left\{ Z_j(i) \middle| H_1 \right\} \approx \left\{ Z_j(i) \middle| G_B(i) = H_1 \right\} \tag{4. 12}$$

$$Z_{j0} = \left\{ Z_j(i) \middle| H_0 \right\} \approx \left\{ Z_j(i) \middle| G_B(i) = H_0 \right\} \tag{4. 13}$$

Therefore, based on the universal decision results generated by the FC updated values of mean and variances are calculated. If the global decision $G_B(i) = 1$, mean and variance μ_{j1} and σ_{j1}^2 are updated as:

$$\begin{aligned} \mu_{j1} &= D_1 \mu_{j1} + D_2 Z_j(i) \\ \sigma_{j1}^2 &= D_1 \sigma_{j1}^2 + \frac{D_1}{D_2} \left(Z_j(i) - \mu_{j1} \right)^2 \end{aligned} \tag{4. 14}$$

Similarly, if $G_B(i) = 0$, then mean and variance μ_{j0}, σ_{j0}^2 are updated for all SUs as:

$$\begin{aligned} \mu_{j0} &= D_1 \mu_{j0} + D_2 Z_j(i) \\ \sigma_{j0}^2 &= D_1 \sigma_{j0}^2 + \frac{D_1}{D_2} \left(Z_j(i) - \mu_{j0} \right)^2 \end{aligned} \tag{4. 15}$$

$D_1 = \frac{d}{d-1}$ and $D_2 = \frac{1}{d}$, where d is window size related to the history of the sensing performance for estimated mean and variance.

A flowchart diagram representing the detail operation of the proposed scheme is shown in Figure 4. 3.

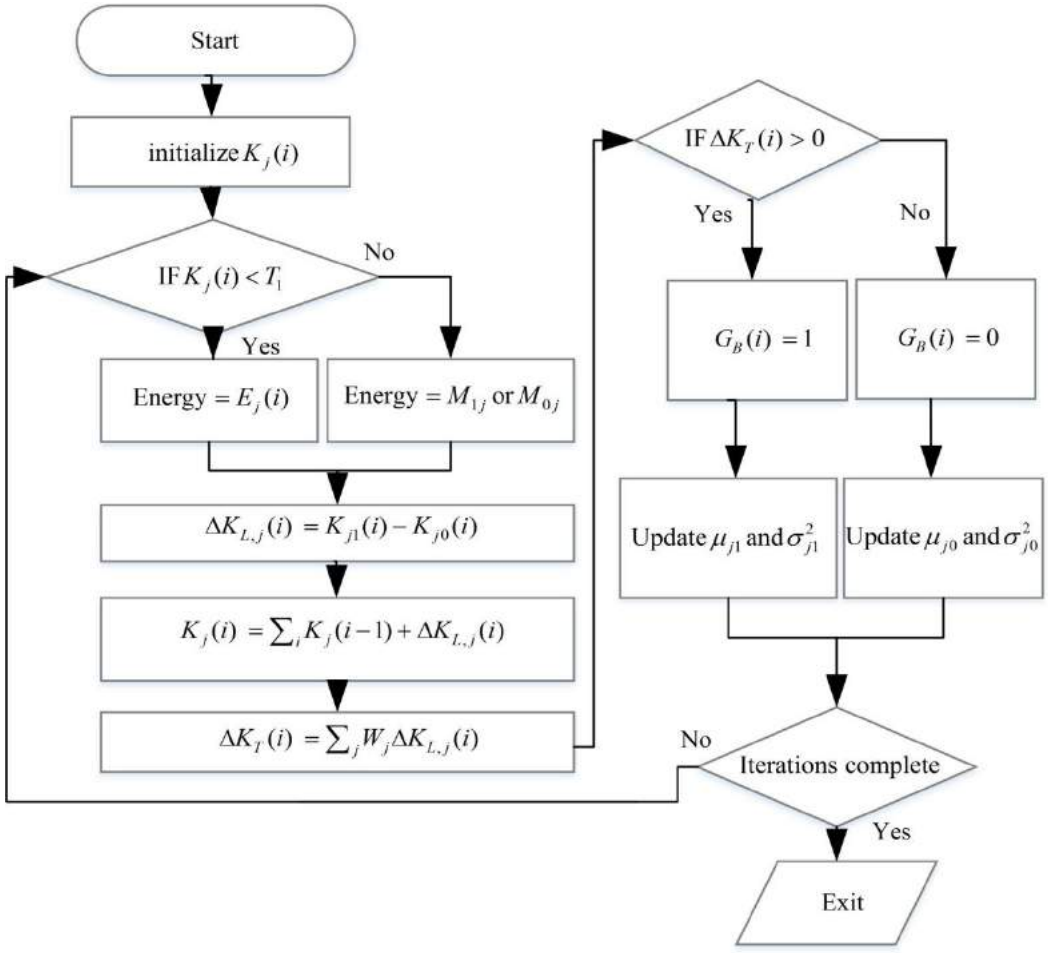

Figure 4. 3 Flowchart diagram of the history based KL divergence

4.3.5 Simulation results of the history based KL divergence scheme

For simulation purposes parameters setting is made for the Cognitive Radio Network with a total number of 16, 20 and 24 SUs at different ratios of MUs. Variation in the SNR for the SUs is

made in a range of -20 dB to -10 dB. The window size d related to the history of the sensing information is kept as 250 and k (energy affecting mean variance values) is elected as 25. The sensing time is taken as 1 ms for each SU and the number of samples in a sensing interval is taken as $M = 270$. Total sensing iterations N in this simulation is 100, and the maximum number of MUs considered for comparison are 4, 8 and 10 with equal distributions of always Yes, always No, opposite and random opposite MUs for comparing the detection performance. The system was simulated under three different cases. In the first phase 4 MUs are selected in 16, 20 and 24 cooperative SUs with an equal percentage of always Yes, always No, opposite and random opposite MUs. Similarly, in the second phase, 8 MUs were equally distributed as always Yes, always No, opposite and random opposite MUs under total 16, 20 and 24 cooperative SUs. In the third phase, the MUs are extended to 10 for a total of 16, 20 and 24 SUs to test the performance. In order to check the performance of the proposed history based KL divergence scheme in searching for optimized resource allocation and spectrum sensing in CRN in the presence of MUs using soft computing and statistical techniques, the detection, false alarm and error results are obtained in Figure 4. 4-Figure 4. 12. The objective of the proposed scheme is to precisely sense the PU channel in the presence of MUs which is possible with high detection and low false alarm probabilities, that ultimately leads to a low error probability in sensing the PU channel. The performance of the proposed methodology is compared with the KL divergence, maximum gain combination (MGC) and equal gain combination (EGC). Receiver operating characteristics (ROC) curve is drawn for proposed method, traditional KL [16], MGC and EGC schemes in Figure 4. 4-Figure 4. 6. Simulation results confirmed that the proposed KL divergence statistical scheme has superior resource allocation and spectrum sensing results in CRN than the previous KL, EGC and MGC schemes at different levels of total cooperative and

MUs. The ROC results collected in these figures show the superiority of the proposed method in comparison with traditional KL, EGC and MGC schemes. In Figure 4. 4 results plotted between false alarms and detection probability for a total of 4 MUs when the total number of SUs varies from 16 to 24. It is clear to see that as the total number of SUs increases in Figure 4. 4, the detection results of all fusion schemes increases with increasing total number of cooperative SUs for a given false alarm and fixed number of MUs. Similarly, ROC results are generated for the proposed and all other fusion schemes i.e. traditional KL, EGC and MGC in Figure 4. 5 and Figure 4. 6 with total 8 and 10 MUs at different levels of cooperative SUs. By comparing the results collected in Figure 4. 4-Figure 4. 6 it is noticeable to change predominant increase in the probability of detection for a given false alarm probability as the total number of cooperative SUs increases from 16 to 24. The results generated in Figure 4. 4-Figure 4. 6 also shows that as the number of total MUs were increased from 4 in Figure 4. 4 to 10 in Figure 4. 6 with 16, 20 and 24 total cooperative users, the proposed method is least affected with the increasing number of MUs in comparison with other soft fusion schemes. In this part of the simulation results, the proposed method is able to provide higher detection results for a given false alarm at different concentration levels of the normal and malicious cooperative users.

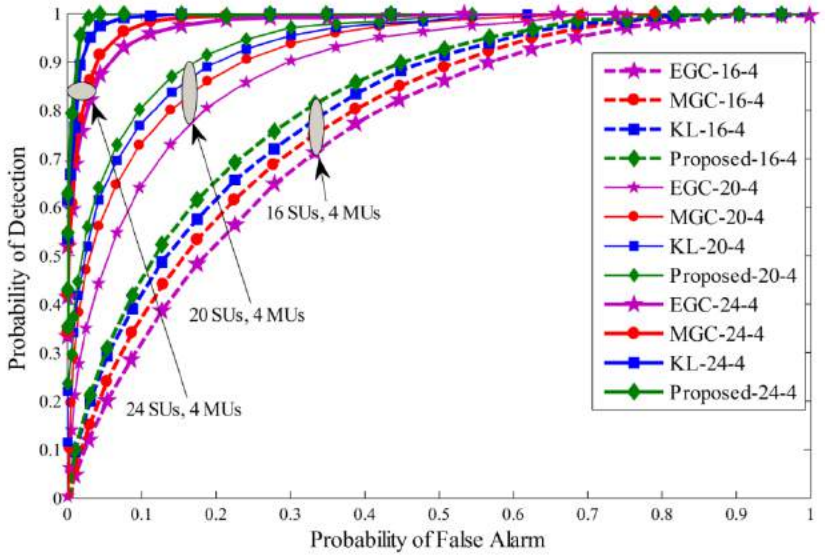

Figure 4. 4 Probability of Detection vs. Probability of False Alarm (ROC) curve for (1) 16 total SUs with 4 MUs (2) 20 total SUs with 4 MUs (3) 24 total SUs with 4 MUs.

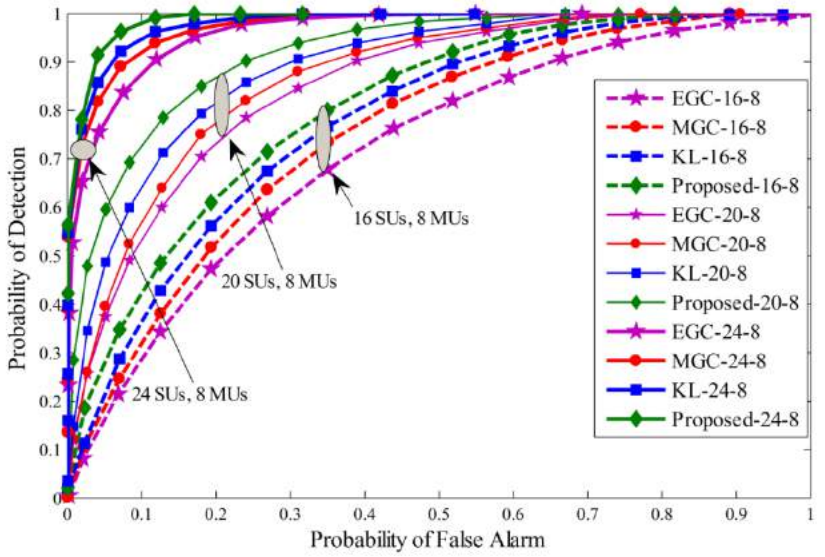

Figure 4. 5 Probability of Detection vs. Probability of False Alarm (ROC) for (1) 16 total SUs with 8 MUs (2) 20 total SUs with 8 MUs (3) 24 total SUs with 8 MUs.

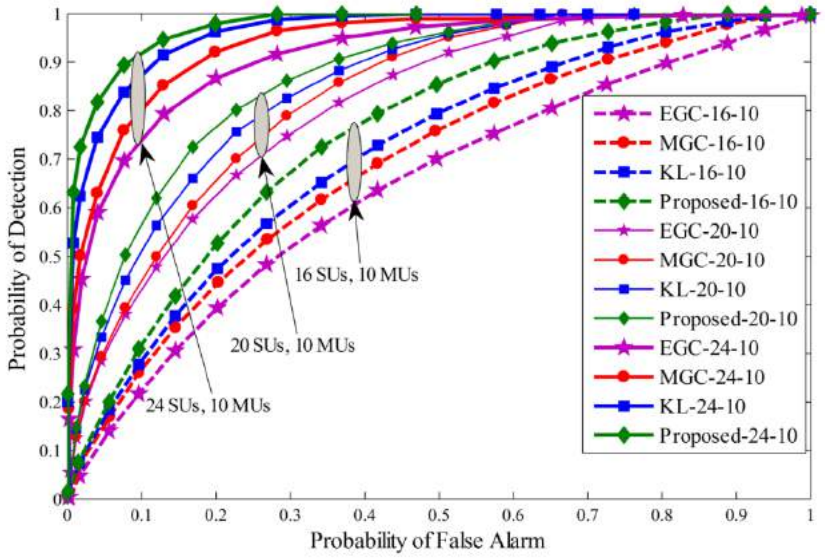

Figure 4. 6 Probability of Detection vs. Probability of False Alarm (ROC) for (1) 16 total SUs with 10 MUs (2) 20 total SUs with 10 MUs (3) 24 total SUs with 10 MUs.

A similar comparison is shown in Figure 4. 7-Figure 4. 9 by drawing the probability of error against the probability of detection for the proposed, KL [16], MGC and EGC schemes. The graphical results showed improved detection results for the proposed scheme against traditional KL, MGC and EGC schemes at all numbers of cooperative and malicious SUs. By inspecting these results, it can be observed that for the proposed scheme, the error probability in detecting PU is lowest in comparison with the previous fusion schemes and has less vulnerability to the increasing MUs.

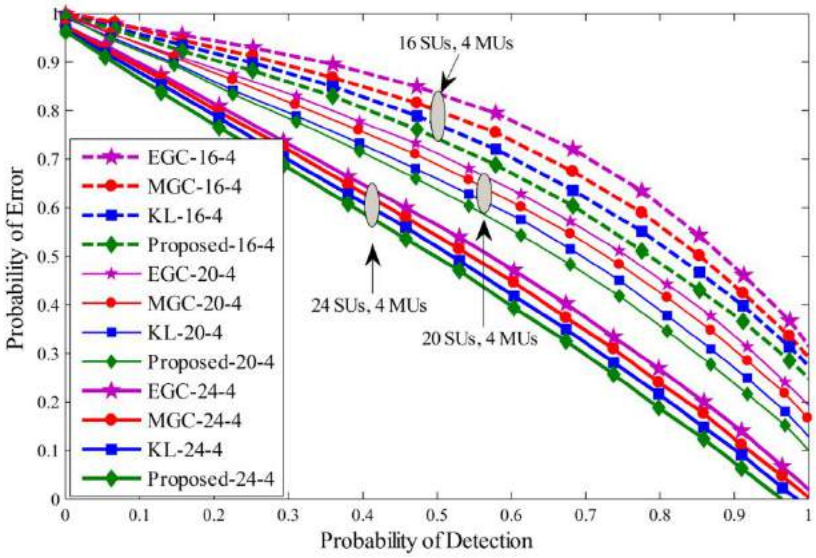

Figure 4. 7 Probability of Error vs. Probability of Detection for (1) 16 total SUs with 4 MUs (2) 20 total SUs with 4 MUs (3) 24 total SUs with 4 MUs.

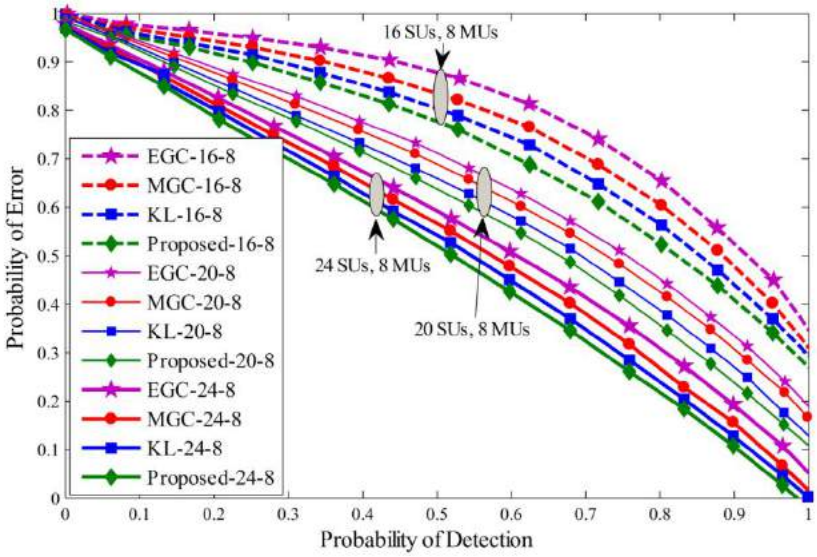

Figure 4. 8 Probability of Error vs. Probability of Detection for (1) 16 total SUs with 8 MUs (2) 20 total SUs with 8 MUs (3) 24 total SUs with 8 MUs.

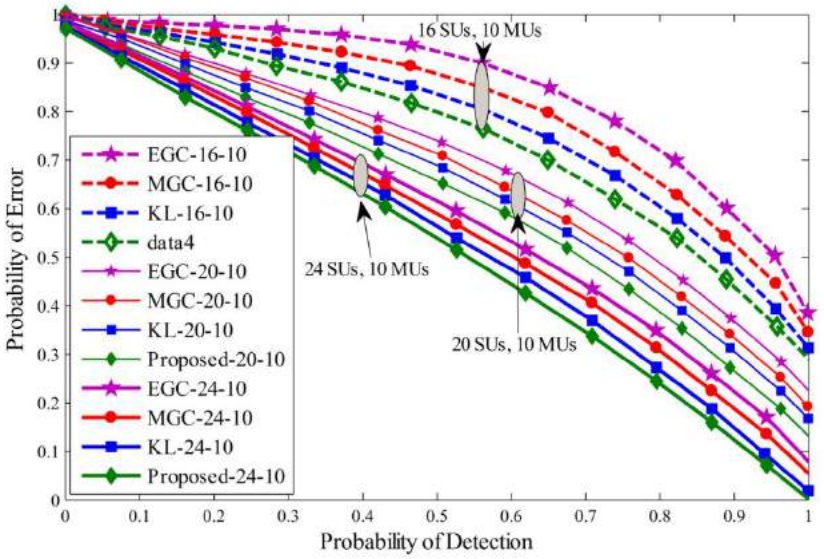

Figure 4. 9 Probability of Error vs. Probability of Detection for (1) 16 total SUs with 10 MUs (2) 20 total SUs with 10 MUs (3) 24 total SUs with 10 MUs.

Probability of error results for each individual SU is drawn against the varying SNRs from -20 dB to -10 dB in Figure 4. 10-Figure 4. 12. The graphical results showed that with the increasing average SNR values, the proposed method results showed sophisticated improvements and is able to reduce the channel sensing error quickly in comparison with all other fusion schemes. Similarly, it can be seen that for a given average SNR value, the probability of error decrease even further by varying the total number of cooperative SUs from 16 to 24 in Figure 4. 10-Figure 4. 12. The efficiency in terms of sensing the licensed user channel reduces with an increase in the total number of MUs from 4 in Figure 4. 10 to 10 in Figure 4. 12 at different level of total SUs. The graphical results demonstrates that the proposed algorithm is least influenced with increasing the number of MUs, while EGC has the worst probability of error.

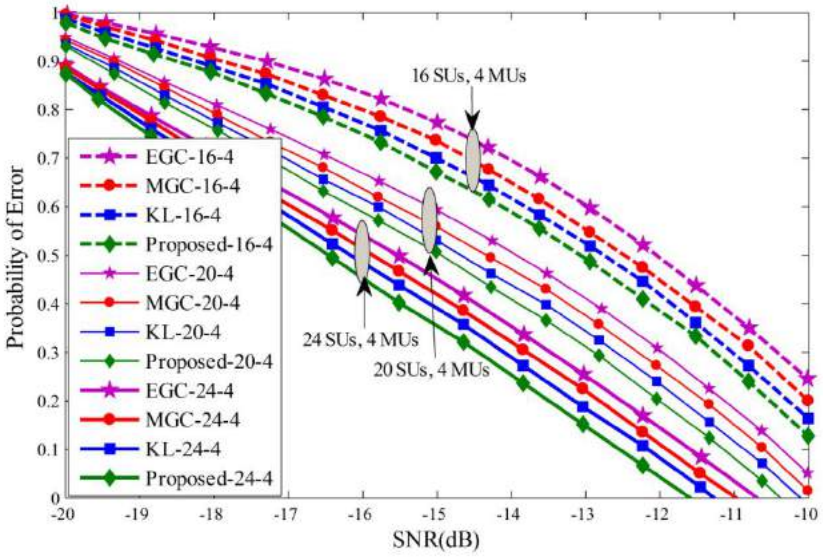

Figure 4. 10 Probability of Error vs. Signal to Noise Ratio for (1) 16 total SUs with 4 MUs (2) 20 total SUs with 4 MUs (3) 24 total SUs with 4 MUs.

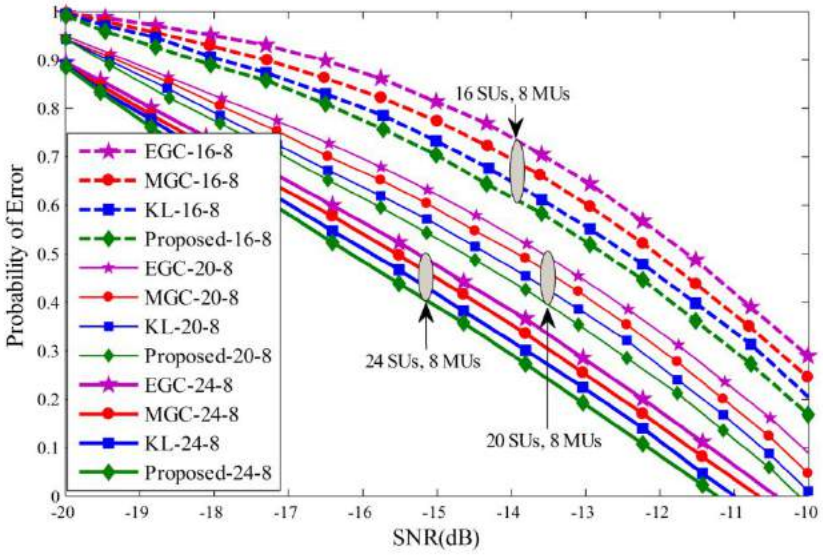

Figure 4. 11 Probability of Error vs. Signal to Noise Ratio for (1) 16 total SUs with 8 MUs (2) 20 total SUs with 8 MUs (3) 24 total SUs with 8 MUs.

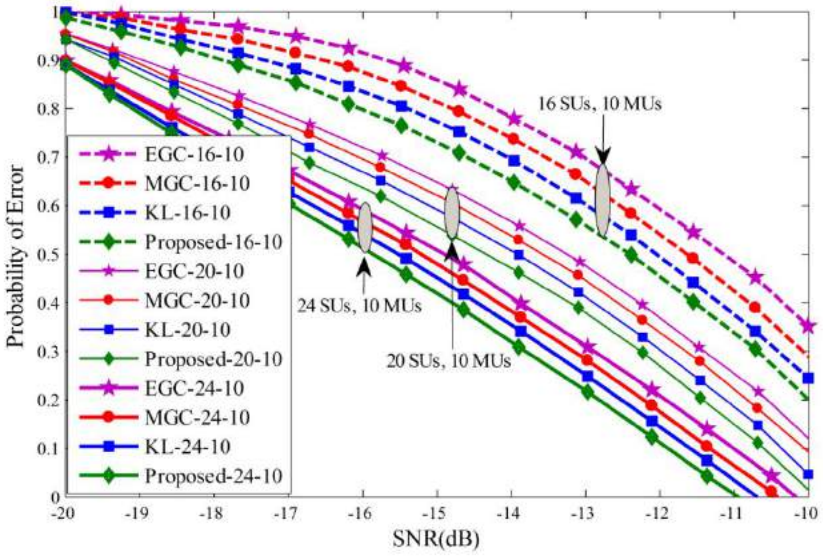

Figure 4. 12 Probability of Error vs. Signal to Noise Ratio for (1) 16 total SUs with 10 MUs (2) 20 total SUs with 10 MUs (3) 24 total SUs with 10 MUs.

For energy comparison of the proposed scheme and traditional KL divergence scheme, simulation results are plotted in Figure 4. 13 among the total average transmitted energy of all SUs and MUs. In Figure 4. 13 the total number of MUs is increased from 4 to 20 and the average transmitted energy of all SUs are collected under 20, 25 and 30 total cooperative SUs. It is obvious from Figure 4. 13 that the proposed scheme is outperforming the traditional KL method in terms of energy utilization in all three cases when 20, 25 and 30 cooperative SUs participate in CSS. The energy transmitted by all SUs increases when the number of cooperative SUs is increased from 20 to 30 for a given total number of MUs. The MUs are selected for energy comparison with 25% always Yes, 25% always No, 25% opposite and 25% random opposite MUs. These energy plots display that the proposed scheme results in overall savings of the transmitting energy for the proposed scheme under all 20, 25 and 30 total cooperative SUs. The simulation results show effectiveness of the proposed scheme in getting optimized resource allocation and spectrum sensing in cognitive radio network with malicious users using KL

divergence statistical technique with higher detection results of the PU, which results in lower error with optimize transmission energy.

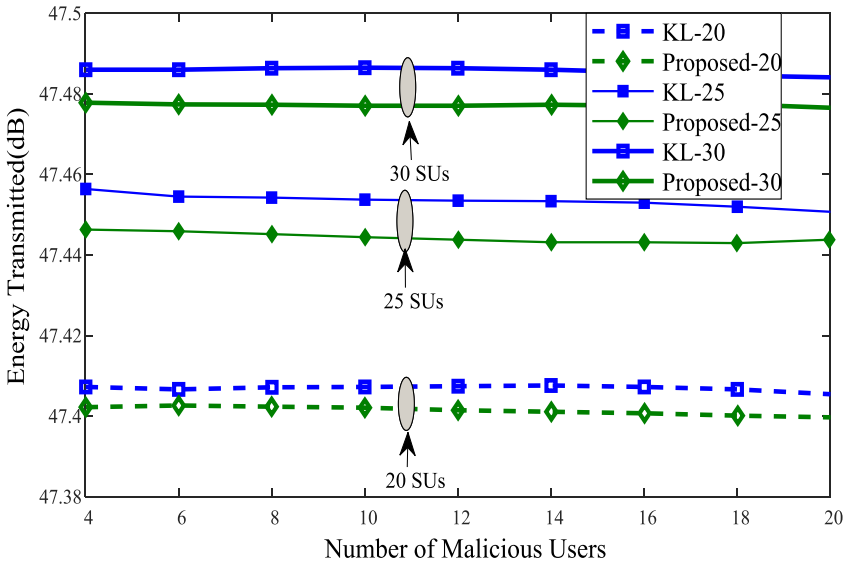

Figure 4. 13 Energy Transmitted vs. Number of MUs for (1) total 20 SUs (2) total 25 SUs (3) total 30 SUs.

4.4 Proposed one-to-many relations based KL divergence

The proposed work considers total cooperative users larger in number compared with MUs. All the cooperative users inform FC with their local spectrum observations of the primary channel. FC collects and takes its global decision based on the received energy statistics of the reporting users. Before making any global decision about the licensed user spectrum, FC is able to assign weights to the local sensing of SU reports with the proposed KL divergence method. The resultant weights illustrate reliability of the local spectrum sensing information of the individual cooperating users prior to making any final decision at the FC.

A pseudo code showing the proposed KL divergence algorithm for the local detection, determining KL divergence score using one-to-many relationship based energy statistics and taking global decision based on the received energy and measured weights are as given below:

For $i = 1$ **to limit**
For $j = 1$ **to SU**
Local detection $E_j(i)$ by the j^{th} user
New values of mean and variance $\left(\mu_{ja}(i), \sigma^2_{jb}(i)\right)$ based on $E_j(i)$
Average means and variance values while taking out the j^{th} user energy statistics.

$$\mu_{ja'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \mu_{ja}(i)\right) - \mu_{ja}(i)}{(M-1)} \right), i \in 1,...,N$$

$$\sigma^2_{jb'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \sigma^2_{jb}(i)\right) - \sigma^2_{jb}(i)}{(M-1)} \right), i \in 1,...,N$$

One-to-many relationship based KL divergence
$K_j(i) = KL\left(\mu_{ja'}(i), \mu_{ja}(i), \sigma^2_{jb'}, \sigma^2_{jb}\right)$
Weights for the j^{th} user in the i^{th} interval

$$c_j(i) = \left(\frac{1}{K_j(i)} \right), w_j(i) = \left(\frac{c_j(i)}{\sum_{j=1}^{M} c_j(i)} \right), i \in 1,...,N$$

End SUs
IF $\sum_{j=1}^{M} w_j(i) * E_j(i) > \varepsilon$
Global decision, $G_B(i) = H_1$
Else
Global decision, $G_B(i) = H_0$
End
End limit

4.4.1 Data collection and mean variances adjustments by the FC

FC receives the individual soft energy information $E_j(i)$ in the i^{th} interval from all the j^{th} cooperating SUs as:

$$\boldsymbol{e} = \left[E_1(i)\ E_2(i)\ E_3(i)\ ...\ E_M(i)\right], i \in 1,...,N \tag{4. 16}$$

Where M is a row vector containing the soft spectrum sensing data of all M users during the i^{th} interval. The soft energy report $E_j(i)$ has mean and variance $\left(\mu_1, \sigma_1^2\right)$ under hypothesis H_1 and $\left(\mu_0, \sigma_0^2\right)$ under the H_0 hypothesis.

FC further determines new values of the mean and variance for all users in the i^{th} sensing interval based on the received energy observations in equation (4. 16) as:

$$\boldsymbol{a}(i) = \left[\mu_{1a}(i)\ \mu_{2a}(i)\ \mu_{3a}(i)...\mu_{Ma}(i)\right], i \in 1,...,N \tag{4. 17}$$

$$\mu_{ja}(i) = \begin{Bmatrix} z_1\mu_{j1} + z_2E_j(i), & H_1 \\ z_1\mu_{j0} + z_2E_j(i), & H_0 \end{Bmatrix} \tag{4. 18}$$

Here $\mu_{ja}(i)$ is the new value of the mean for the j^{th} SU in the i^{th} sensing interval, which is updated according to the received energy $E_j(i)$ and (z_1, z_2) preselected constants.

Similarly, new variance values are determined and collected based on the received energy $E_j(i)$ as:

$$b(i) = \left[\sigma_{1b}^2\ \sigma_{2b}^2\ \sigma_{3b}^2 ... \sigma_{Mb}^2\right], i \in 1,...,N \tag{4. 19}$$

$$\sigma_{jb}^2(i) = \begin{Bmatrix} z_1\sigma_{j1}^2 + z_1\left(E_j(i) - \mu_{j1}\right)^2, & H_1 \\ z_1\sigma_{j0}^2 + z_1\left(E_j(i) - \mu_{j0}\right)^2, & H_0 \end{Bmatrix} \quad (4.\ 20)$$

In the new mean and variance measurements in equation (4. 18) and equation (4. 20) the constants $z_1 = (k-1)/(k)$ and $z_2 = (1/k)$, where the constant k is the effecting level of the mean and variance by the received energy $E_j(i)$.

4.4.2 One-to-many relationship based KL divergence measurement

After the collection of mean and variance information on behalf of all M users in the i^{th} sensing intervals, FC measures a difference in the mean and variance of the j^{th} user energy statistics with all other users. The average mean values are measured on behalf of all M SUs based on the new mean values of equation (4. 18) as:

$$\mu_{ja'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \mu_{ja}(i) \right) - \mu_{ja}(i)}{(M-1)} \right) \quad (4.\ 21)$$

The one-to-many difference results of the mean for all M SUs are collected as:

$$\boldsymbol{a}'(i) = \left[\mu_{1a'}(i)\, \mu_{2a'}(i) \ldots \mu_{Ma'}(i) \right], i \in 1, \ldots, N \quad (4.\ 22)$$

Similarly, the average variance values are measured on behalf of all M SUs based on the new variance values of equation (4. 20) as below:

$$\sigma^2_{jb'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \sigma^2_{jb}(i) \right) - \sigma^2_{jb}(i)}{(M-1)} \right) \tag{4. 23}$$

$$\boldsymbol{b}'(i) = \left[\sigma^2_{1b'}(i)\, \sigma^2_{2b'}(i)\, \sigma^2_{3b'}(i) \ldots \sigma^2_{Mb'}(i) \right], i \in 1, \ldots, N \tag{4. 24}$$

Here $\mu_{ja'}(i)$ is the average mean and $\sigma^2_{ja'}(i)$ is the average variance value of the energy samples provided by all other users while ignoring the mean and variance results of the j^{th} user. These mean and variance values are obtained by excluding the j^{th} user. The result in equation (4. 22) and equation (4. 24) determines the impact of not including each cooperative user during the average mean and variance observation measurement. As all MUs including always yes (AY), always no (AN), always opposite (AO) and random opposite (RO) have dissimilar results of the mean and variance in comparison with normal SUs, therefore the average results attained against these users is different from the normal SUs in equation (4. 22) and equation (4. 24).

The KL divergence value for the j^{th} SU is determined between the individual sensing results in equation (4. 17), equation (4. 19) and the information provided by all other SU information as in equation (4. 22) and equation (4. 24) as:

$$K_j(i) = KL\left(\mu_{ja'}(i), \mu_{ja}(i), \sigma^2_{jb'}(i), \sigma^2_{jb}(i) \right) \tag{4. 25}$$

Where $K_j(i)$ denotes the KL divergence result in the presence and absence hypothesis of the j^{th} SU in the i^{th} interval. These KL divergence scores against each SU sensing are modified as:

$$c_j(i) = \left(\frac{1}{K_j(i)} \right), i \in 1,...,N,\ j \in 1,...,M \tag{4. 26}$$

The result in equation (4. 26) is normalized for assigning weights to each SU decision as:

$$w_j(i) = \left(\frac{c_j(i)}{\sum_{j=1}^{M} c_j(i)} \right), i \in 1,...,N,\ j \in 1,...,M \tag{4. 27}$$

In equation (4. 27) the users with abnormal behavior acquire lower weights in comparison with normal users.

Table 4.1 shows the weight measurement for the normal and malicious users against various SNRs. These weights are obtained for the case when one of the four categories of MUs participates in CSS. In Table 4.1 as the value of SNR increase, the weight assigned to these MUs decreases while the normal user's weights increase.

Similarly, Table 4.2 shows the weights for the case when all four categories of MUs participate in CSS. In Table 4.2, the weight results assigned to each MU along with the average weights received by all the normal cooperative SUs are. In this case, the different weights received by these MUs approaches near to zero with increasing SNR while the normal SUs weights increase with increasing SNR.

Table 4. 1. KL weights assigned by the FC under one category of MU participation.

SNR (dB)	**Weights**				
	AY only	**AN only**	**AO only**	**RO only**	**Normal User**
-20	0.006757	0.006553	0.016615	0.008775	0.080399

-19	0.006750	0.006551	0.008679	0.006123	0.080798
-18	0.006745	0.006547	0.008341	0.005763	0.081049
-17	0.006740	0.006544	0.008341	0.005757	0.081110
-16	0.006737	0.006539	0.006206	0.005616	0.081198
-15	0.006731	0.006537	0.006186	0.005537	0.081231
-14	0.006722	0.006532	0.006164	0.005393	0.081266
-13	0.006717	0.006530	0.005722	0.005295	0.081306
-12	0.006715	0.006526	0.005722	0.005290	0.081324
-11	0.006711	0.006525	0.005629	0.004688	0.081428
-10	0.006709	0.006521	0.005629	0.004318	0.081441
-9	0.006706	0.006518	0.005190	0.003863	0.081545
-8	0.006704	0.006516	0.004947	0.003836	0.081636
-7	0.006701	0.006510	0.003674	0.003773	0.081739
-6	0.006692	0.006505	0.001509	0.003198	0.081777
-5	0.006687	0.006502	0.001507	0.001335	0.082069

Table 4. 2. KL weights assigned by the FC when all categories of MUs participate.

SNR (dB)	**Weights**				
	1 AY	**1 AN**	**1 AO**	**1 RO**	**Normal User**
-20	0.000682	0.000359	0.001661	0.065425	0.077865
-19	0.000523	0.000331	0.001155	0.012339	0.082344
-18	0.000466	0.000319	0.001085	0.006149	0.082800
-17	0.000379	0.000277	0.001037	0.005841	0.082875
-16	0.000287	0.000212	0.000825	0.005060	0.082967

-15	0.000229	0.000169	0.000817	0.004495	0.082984
-14	0.000175	0.000159	0.000766	0.004449	0.083008
-13	0.000160	0.000139	0.000645	0.004355	0.083035
-12	0.000137	0.000113	0.000637	0.003774	0.083047
-11	0.000112	0.000080	0.000477	0.002980	0.083048
-10	0.000096	0.000079	0.000469	0.002719	0.083058
-9	0.000095	0.000070	0.000285	0.002563	0.083061
-8	0.000094	0.000069	0.000242	0.002524	0.083136
-7	0.000082	0.000066	0.000222	0.002486	0.083254
-6	0.000055	0.000039	0.000137	0.001171	0.083307
-5	0.000010	0.000008	0.000057	0.000266	0.083694

4.4.3 Global statement by the FC

Grounded on the weighted results measured to guarantee the authenticity sensing information in equation (4. 27), the global statement $G_B(i)$ is declared by the FC as:

$$G_B(i) = \begin{Bmatrix} H_1, & \sum_{j=1}^{M} \boldsymbol{w}_j(i) * E_j(i) \geq \varepsilon \\ H_0, & otherwise \end{Bmatrix}, i \in 1,...,N \qquad (4.\ 28)$$

Where $\boldsymbol{w}_j$ is the weight assigned to the j^{th} user energy in the data fusion at the FC and ε is the threshold value for the detection of the PU. The lesser weight results are charged by the FC against the sensing information of a user with malicious behavior, while the normal user sensing report is assigned a higher weight value. All MUs including AY, AN, AO and RO are easily identified by the proposed scheme with their KL divergence behavior. The normal SUs have a

higher KL divergence result because they have less inconsistency from the average of all other users sensing information. The MUs receive minimum weight because the information provided by MUs deviates more from the average sensing information provided by all other SUs. It is therefore noticeable that these MUs get lower weights as compared with normal SUs.

4.4.4 Next iteration mean and variance based on the global statement

Due to the non-availability of the exact information about the PU, perfect values of the means $\left(\mu_{j1}, \mu_{j0}\right)$ and variances $\left(\sigma_{j0}^2, \sigma_{j1}^2\right)$ for measuring KL divergence are not possible. It is therefore good to consider the global decision $G_B(i)$ results as an estimate of the primary signal. The updated mean and variance will be used by the FC in the KL divergence calculation in the next sensing interval.

$$E_{j1} = \left\{E_j(i) \middle| H_1\right\} \approx \left\{E_j(i) \middle| G_B(i) = H_1\right\} \tag{4. 29}$$

$$E_{j0} = \left\{E_j(i) \middle| H_0\right\} \approx \left\{E_j(i) \middle| G_B(i) = H_0\right\} \tag{4. 30}$$

The global decision $G_B(i) = 1$ at the FC will update mean μ_{j1} and variance σ_{j1}^2 under the H_1 hypothesis as follows:

$$\begin{aligned} \mu_{j1} &= B_1 \mu_{j1} + B_2 Z_j(i) \\ \sigma_{j1}^2 &= B_1 \sigma_{j1}^2 + \frac{B_1}{B_2}\left(Z_j(i) - \mu_{j1}\right)^2 \end{aligned} \tag{4. 31}$$

Similarly, the decision $G_B(i) = 0$ will update mean μ_{j0} and variance σ_{j0}^2 under the H_0 hypothesis for all cooperative users as:

$$\mu_{j0} = B_1\mu_{j0} + B_2E_j(i)$$
$$\sigma^2_{j0} = B_1\sigma^2_{j0} + \frac{B_1}{B_2}\left(E_j(i) - \mu_{j0}\right)^2 \quad (4.\ 32)$$

In equation (4. 32) $B_1 = \frac{z}{z-1}$ and $B_2 = \frac{1}{z}$, where z indicate the window size of the sensing history for the estimated mean and variance.

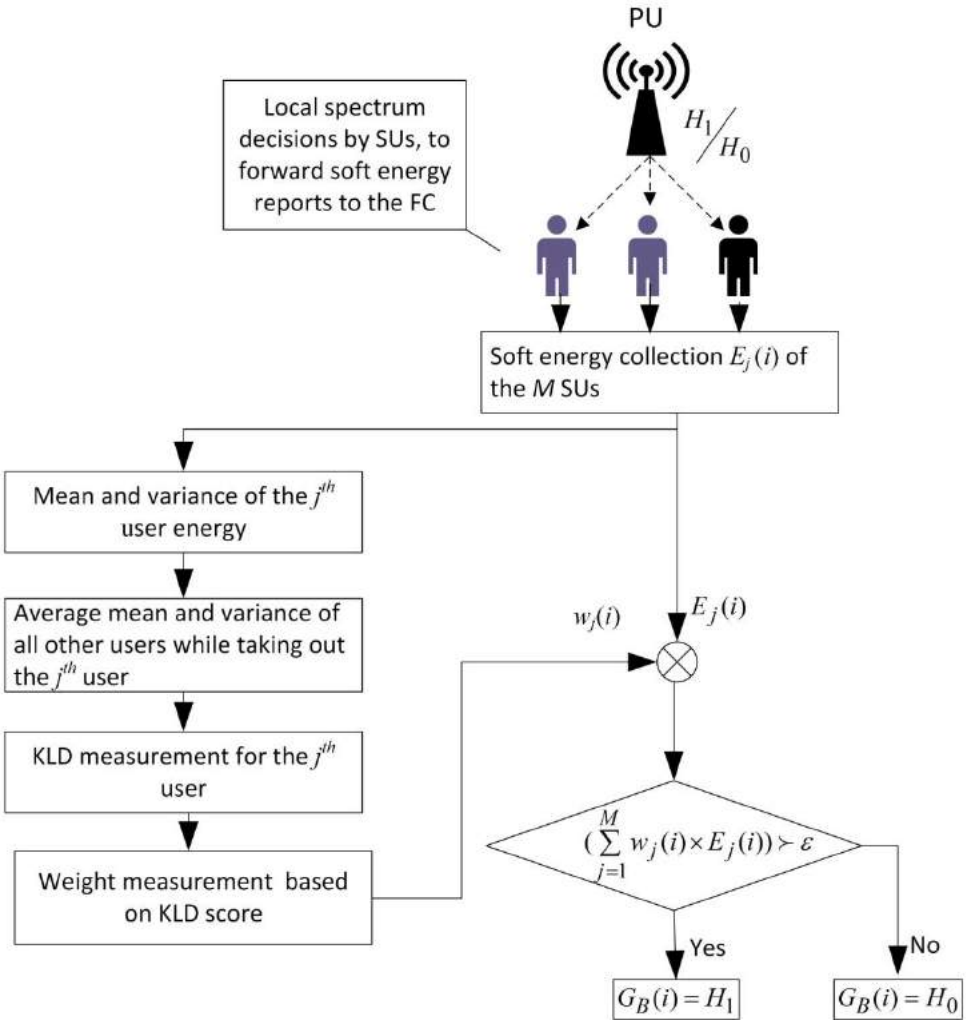

Figure 4. 14 Flowchart diagram of the proposed weighted KL divergence scheme.

The proposed scheme flowchart diagram in Figure 4. 14 illustrates the local detection, KL divergence measurement based on the weight assignments and global decision establishment by the FC.

4.4.5 Simulation results of the one to many relations based KL divergence scheme

In order to get simulation results for the CRN parameter settings are made with 10, 16, 20 and 30 total cooperative users. Out of the total cooperative SUs, four users are intentionally selected as AY, AO, RO and AO nature of MUs. The average SNRs for the simulation are selected as -20 dB to -5 dB for all SUs. The sensing time for each SU is selected as 1 ms containing 270 samples in each sensing interval. Total sensing intervals for the cooperative users are selected as 200. The RO users perform malicious acts probabilistically in the intervals 1 to N . The window size (z) for updating mean and variance is selected as 270. In the study, all 4 categories of MUs i.e. AY, AN, AO and RO are spread evenly. In order to check the performance of the proposed weighted KL divergence scheme in determining optimized solution of resource allocation and spectrum sensing in CRN with MUs using soft computing and statistical techniques the PU activity detection and false alarm results are collected in Figure 4. 15-Figure 4. 20. The MUs task in CSS is to minimize the detection probability and maximize the false alarm probability. The proposed weighted KL divergence scheme can smartly overcome these issues.

The proposed KL divergence performance is compared with traditional KL and EGC schemes in 6 different cases as below.

Case 1: In this case ROC results are drawn between the proposed method, traditional KL and EGC scheme under various SNR values of -20 dB to -5 dB as displayed in Figure 4. 15. MUs are selected as AY only in the first part of the comparison in Figure 4. 15. Results are obtained for all combinations by taking the total number of AY as 1, 2, 3 and 4 subsequently. The results

illustrate that the KL divergence scheme is more secure against the increasing number of AY users 1 to 4 and has better detection probability results in comparison with all other schemes. In Figure 4. 15 when there is only 1 AY user active in CSS the ROC results of all fusion schemes are less affected, but as the total number of AY users is increased to 3 and 4 the proposed KL results dominate the traditional KL and EGC schemes by producing a high detection with less false alarms. The EGC scheme is more affected by the increasing number of AY users because EGC gives equal weight to the detection performance of normal and AY users. The proposed KL is able to assign less weight to the AY users in comparison with normal SUs as it is clear from the average weight value measured against each AY in Table 1. The less weight assigned to the AY reduces the false data effect of the AY participation in CSS. The harmful effect of the AY contribution in CSS is further reduced with increasing average SNR by lowering the weight assignment to them in the global decision.

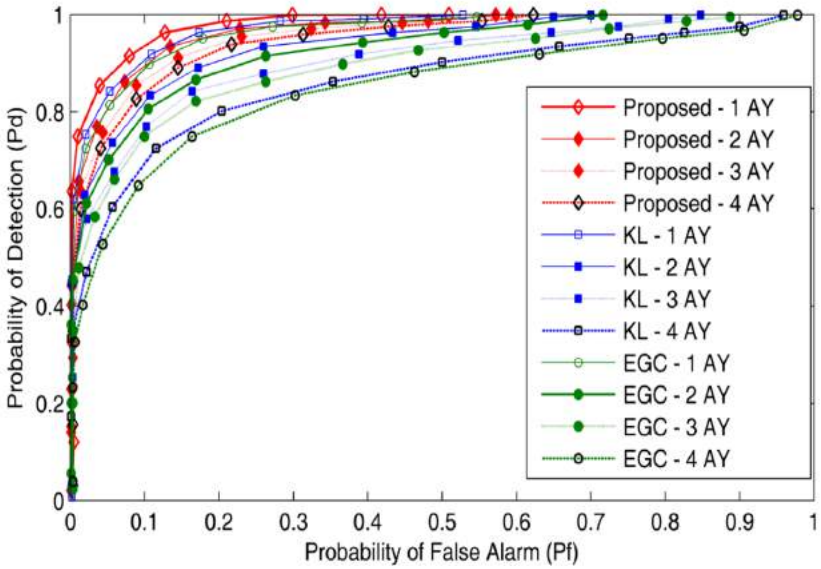

Figure 4. 15. Detection vs. False Alarm results with 1, 2, 3 and 4 (AY) malicious users.

Case 2: In this part of the simulation, all parameters are kept similar to case 1 with changing only the nature of MUs from AY to AN user. Comparison is made between proposed KL,

traditional KL and EGC scheme by testing the system against increasing number of AY from 1 to 4 as in Figure 4. 16.

Since the proposed KL is treating AY and AN users similar in determining the KL divergence, therefore using proposed KL divergence the weight that AN user receives is almost equal to the AY user weights in case 1. The ROC performance of the proposed and all other schemes against the AN scenario is very similar to case 1, due to the likely behavior of the AN user to that of the AY user. As it was in case 1, when the numbers of AN user are increased from 1 to 4, the proposed KL is less affected by this increment in Figure 4. 16. All AN users receive lower weight while the normal SUs receive higher weights in comparison with AN users, which results in better performance of the proposed KL scheme. The traditional KL and EGC schemes performance in detecting the licensed PU channel reduces more quickly in comparison with the proposed technique as the total AY increases from 1 to 4. The gap in the ROC curves of the traditional fusion schemes becomes wider for a total of 4 AN users from the one when only 1 AN user participates in sensing as shown in Figure 4. 16.

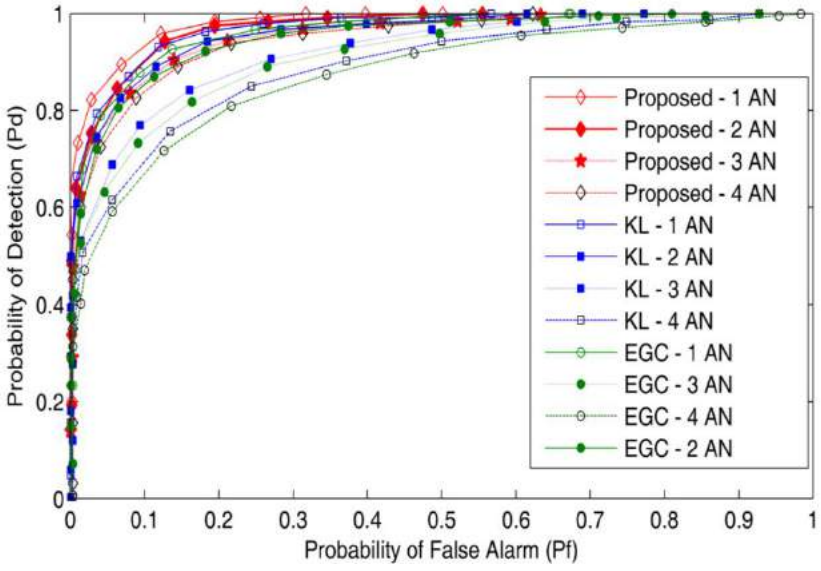

Figure 4. 16 Detection vs. False Alarm results with 1, 2, 3 and 4 (AN) malicious users.

Case 3: In the third scenario, simulation results are obtained for the increasing number of AO users from 1 to 4 in Figure 4. 17 with the same parameters in case 1 and case 2. Since the AO users have its mean and variance results opposite to the average mean and variance values provided by all other users, therefore, the proposed KL method is able to generate lower reliability report in terms of weight for the AO user in comparison with normal cooperative users. The results show that as AO user's increases to 4 few drops is observed in the ROC curve of the proposed scheme as compared with the traditional KL and EGC scheme. In comparison with case 1 and case 2, the traditional soft combination schemes like KL and EGC performance degrade even more. The existence of AO users results in less correct detection and high false alarm rate of the PU spectrum for the EGC and KL scheme. Proposed method results in Figure 4. 17 are followed by the KL while EGC has shown its worst performance among all fusions.

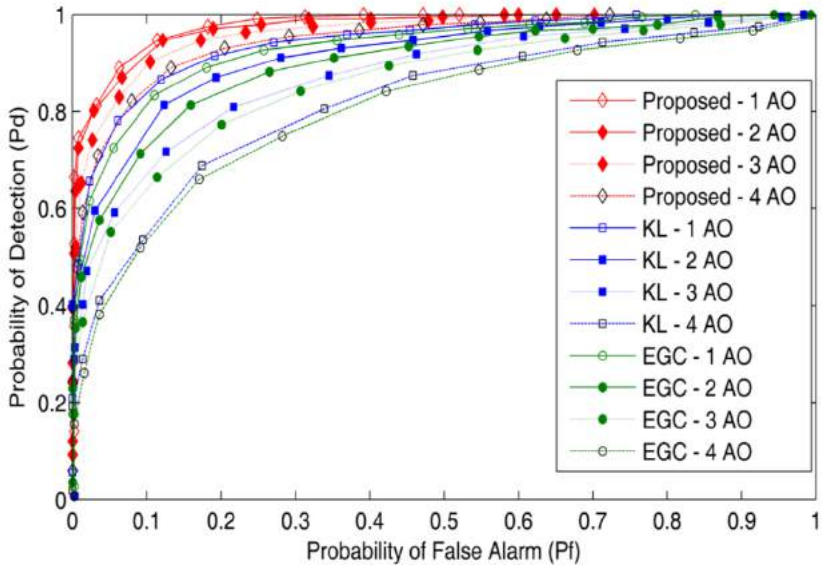

Figure 4. 17 Detection vs. False Alarm results with 1, 2, 3 and 4 (AO) malicious users.

Case 4: The ROC results in which only RO user participates in CSS are depicted in Figure 4. 18. The RO user hides its malicious identity by acting probabilistically as AO at randomly selected sensing intervals in the N total intervals and is difficult to catch with the provided statistics.

The traditional KL and EGC schemes are not able to handle the RO user information intelligently and their ROC results degrade severely with the increased number of RO participations in Figure 4. 18.

The proposed KL scheme is able to identify the RO users when they perform malicious acts probabilistically and generate better detection and false alarm results in Figure 4. 18 compared with the traditional KL and EGC schemes. Results show that unlike the traditional EGC and KL divergence schemes, increasing number of RO users less affects the proposed KL divergence. All the RO nature users in the proposed CSS receive lesser weights in comparison with weights obtained by the normal SUs because their malicious behavior is easily caught by the proposed KL scheme.

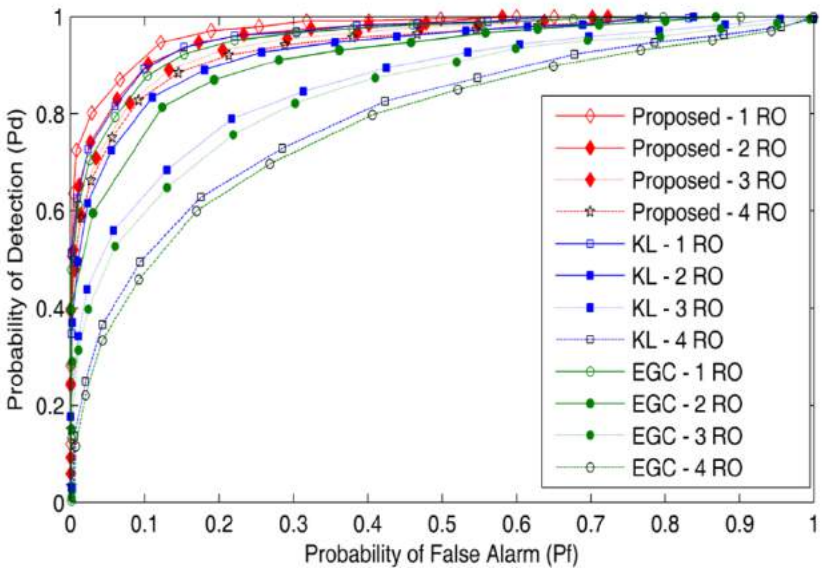

Figure 4. 18. Detection vs. False Alarm results with 1, 2, 3 and 4 (RO) users.

Case 5: In this part of the simulation as in Figure 4. 19, 8 MUs are equally selected in numbers as AY, AN, AO and RO categories. The simulation is performed against an average signal-to-noise ratio of -12.5 dB.

The detection and false alarm probability results are obtained for the proposed, traditional KL and EGC schemes for a total of 10, 20 and 30 cooperative SUs in Figure 4. 19. The average signal-to-noise ratio is kept -12.5 dB with total 4 MUs. Figure 4. 19 show that one-to-many relation based KL divergence scheme has better ROC performance than all other schemes. It is noticeable that all combination schemes detection performance improves with the increasing number of total cooperative and fixed MUs. The proposed method ROC results are more precise and superior to the traditional schemes i.e. KL and EGC schemes at all levels of the total sensing users.

Case 6: In this case, the number of AY, AO, AN and RO is kept the same. The total number of participating SUs in CSS is kept fixed at 16 and different ROC results are plotted for the one-to-many relations based KL divergence and other soft combination schemes at different levels of the averages signal-to-noise ratios.

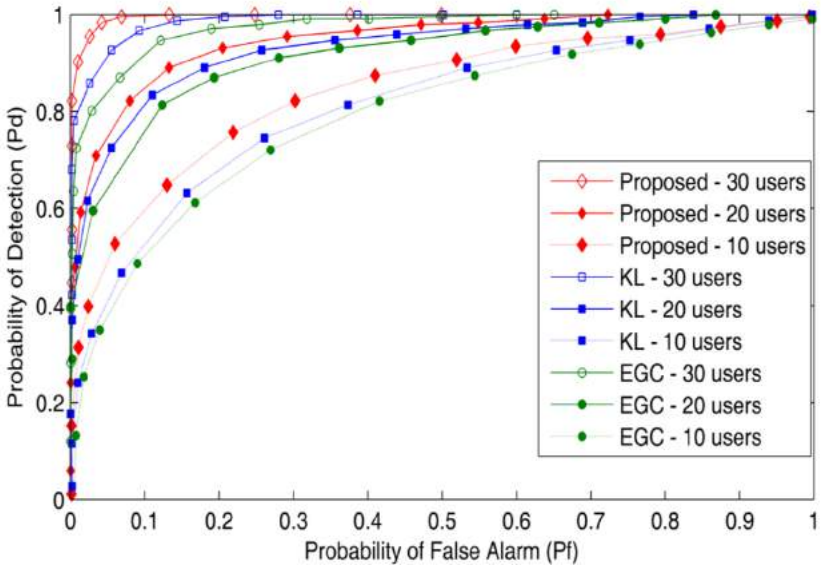

Figure 4. 19. Detection vs. False Alarm results with all MUs and 10, 20, 30 total reporting users.

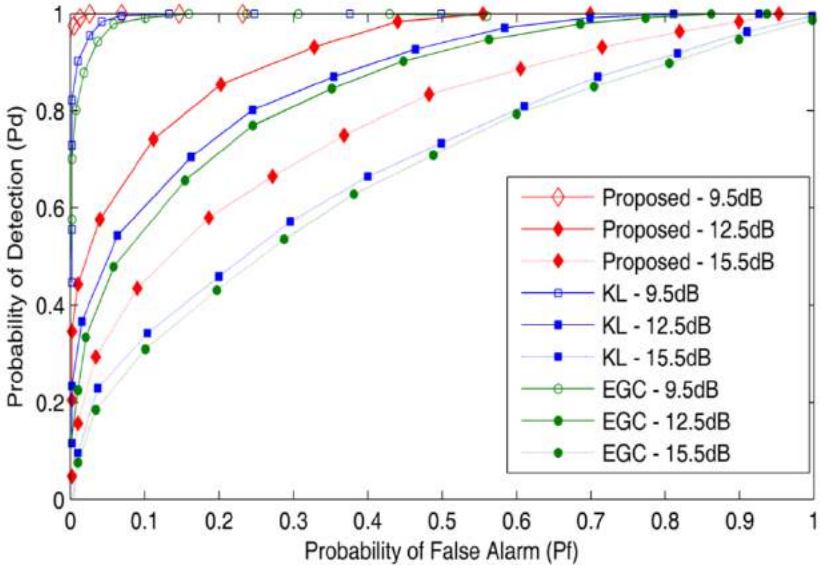

Figure 4. 20. Detection vs. False Alarm results with all MUs and different levels of signal-to-noise ratios (-9.5 dB, -12.5 dB, -15.5 dB).

The simulation results in Figure 4. 20 shows that under fixed malicious and total cooperative users the ROC performance rises with increasing SNRs for all combination schemes. As the signal-to-noise ratio increases from -15.5 dB to -9.5 dB, proposed scheme ROC results are more accurate and precise than the traditional combination schemes at both SNR levels. The proposed method ROC improvement with increasing signal-to-noise ratio is due to more clear distinction on the energy distribution of the absence and presence hypothesis information provided by the normal and MUs. These results also show that the CSS performance improves more with the increasing signal-to-noise ratio information in case 6 as compared with the increasing number cooperative users in case 5.

All the above experimental results clarify the fact that by following the proposed one-to-many relations based KL divergence method an improvement is obvious in the sensing performance at the FC. This improvement is achieved by raising the detection probability and lowering the false alarm results leading to a reduction in the error probability of the system. The proposed fusion combination scheme shows optimum and accurate resource allocation and spectrum sensing

results in cognitive radio network with malicious users using one to many relationship based KL divergence statistical technique. The use of the proposed method for calculating weights following by soft combination scheme makes the proposed CSS results more valid in the presence of malicious users. The simulation results show that the risk of AY, AN, RO and AO users with CSS significantly reduces by adopting the proposed scheme. It is clear from the graphical result that cooperation turns out to be more precise by using the suggested methodology. The one to many relation based KL divergence is able to generate better resource allocation and spectrum sensing results in cognitive radio network with malicious users using one to many relationship based KL divergence statistical technique, by assigning lower weights to the MUs information and is able to eliminate the effect of MUs in CSS.

4.5 Summary

As MUs mislead other users to access the license user spectrum, it is therefore, mandatory in CSS to filter the MU sensing information. The KL divergence tool is used to detect MU in CSS based on the PDF dissimilarity of a normal and MU. The proposed KL divergence scheme in part I is following a modified pre-sensing check by the users before forwarding the spectrum information to the FC. SUs with their KL divergence reputation score feedback by the FC attained, will report PU activity with the sensed energy based on the current and past results from its local database. Simulations exhibit the proposed scheme's effectiveness in terms of sophisticated detection while exercising comparatively less total transmission energy.

In part II, the efficiency degrading effects due to the presence of abnormal users in CSS is minimized using one-to-many relationship based KL divergence method for the PU detection. Functionality of the proposed scheme is verified in the presence of AY, AN, AO and RO type

MUs. FC first receives the individual sensing information of all SUs and then applies the proposed method for measuring weights against each SU. MUs with abnormal behavior as compared with normal SUs are given lower weights by the proposed scheme, while the normal SUs receive higher weights. FC further employs these weights in combining the sensing information of all SUs in predicting a global decision. The results show that the user with abnormal behavior has less impact on the global decision as compared to a normal SU decision. Simulation result reflects the superiority and authenticity of the proposed scheme in producing more accurate, precise and reliable decisions as compared with EGC and traditional KL fusion schemes.

Chapter 5

Malicious user detection using soft computing techniques

5.1 Introduction

In this chapter, we have discussed heuristic techniques such as GA and PSO for determining optimal cooperative decision in the presence of malicious activity. This chapter is divided into three parts. In part I, FC apply GA using DSND method to detect abnormal users and then with the help of crossover and mutation, best fitness is selected. These results are then used in a hard fusion combination scheme such as logical AND, OR and majority voting to declare final decision of the PU status. In part II, GA used one-to-many hamming distance and Z-score outlier factors in determining suitable PU detection information in the presence of MUs. At last detection, false alarm and error probabilities of the proposed GA based majority voting hard decision fusion (GAMV-HDF) scheme is compared with the majority voting hard decision fusion (MV-HDF), EGC based soft decision fusion (EGC-SDF) and MGC based soft decision fusion (MGC-SDF) schemes at different levels of the SNRs and cooperative users. In part III, PSO is employed to take global decision at the FC based on the soft energy reports of all cooperative users. In this part, users send their sensing statistics to the FC for a number of observations. Simulation results are obtained for the proposed PSO-Hard, PSO-EGC and PSO-MGC schemes and are compared with the traditional Hard, EGC and MGC schemes. Results illustrate that the proposed scheme outperformed all other techniques in detection, false alarm and error probabilities for different number of MUs.

5.2 Data Model for DSND based GA

5.2.1 Local spectrum decisions

SUs take its local decision by comparing the observed energy of the PU channel with a threshold in order to send a hard decision "1" or "0" to the FC as

$$y_j(i) = \begin{Bmatrix} 1, & if\ E_j(i) \geq \gamma_j \\ 0, & Otherwise \end{Bmatrix} \tag{5. 1}$$

where $E_j(i)$ is the receive energy in the i^{th} sensing interval by the j^{th} SU, γ_j is the threshold value set for the j^{th} SU. If energy of the received signal by the j^{th} SU is greater than the threshold, then it declares PU existence by forwarding a binary decision "1" to the FC otherwise decision "0" is forwarded to the FC to state the channel as open of the incumbent authorized user.

The probability of detection P_d^j and probability of false alarm P_f^j of the j^{th} SU are defined as [22]:

$$P_d^j = \Pr\left\{ y_j(i) = 1 \middle| H_1 \right\} = \Pr\left\{ E_j(i) \geq \gamma_j \middle| H_1 \right\} \tag{5. 2}$$

$$P_f^j = \Pr\left\{ y_j(i) = 1 \middle| H_0 \right\} = \Pr\left\{ E_j(i) \geq \gamma_j \middle| H_0 \right\} \tag{5. 3}$$

The probability of detection, probability of false alarm and probability of miss-detection over an AWGN channel is expressed as

$$P_d^j = Q_k\left(\sqrt{2\eta_j}, \sqrt{\gamma_j} \right) \tag{5. 4}$$

$$P_f^j = \frac{\Gamma\left(K, \gamma_j / 2\right)}{\Gamma(K)} \tag{5. 5}$$

$$P_m^j = 1 - P_d^j \tag{5. 6}$$

where η_j is the SNR, $K = TW$ is the time bandwidth product. $Q_K(.,.)$ is the generalized Marcum Q-function, $\Gamma(.)$ and $\Gamma(.,.)$ are complete and incomplete gamma functions respectively [21].

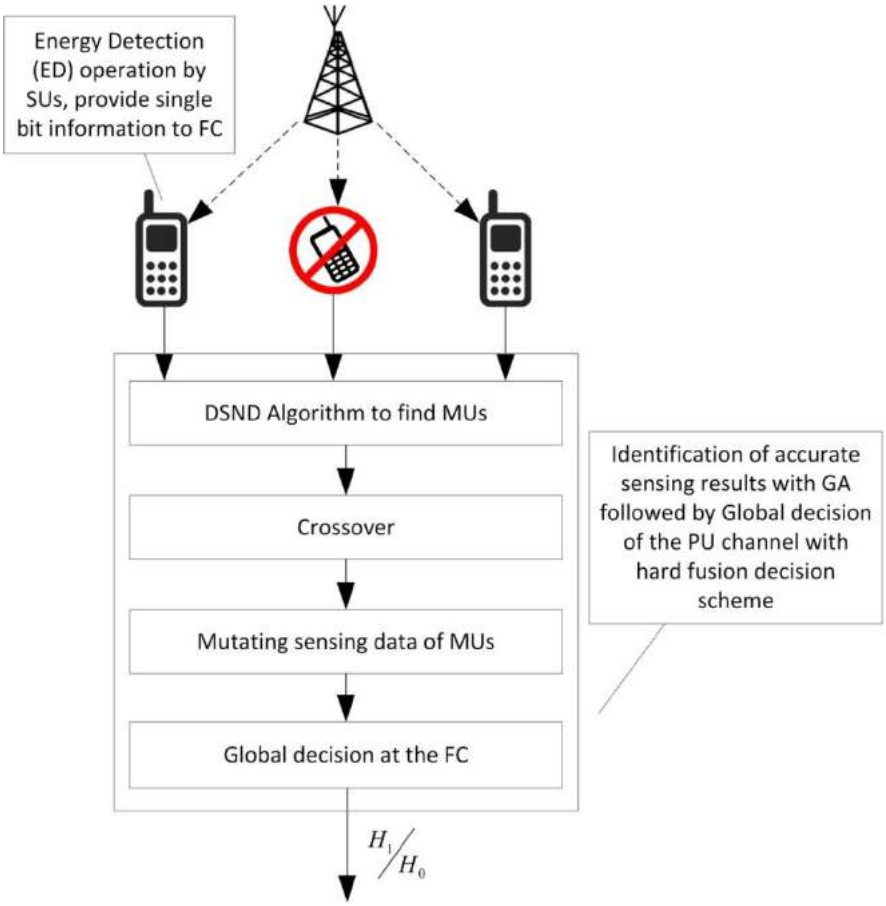

Figure 5. 1 Proposed CSS Model of the DSND based GA scheme

FC collects the spectrum sensing decisions of individual SUs to form a history reporting matrix consisting individual hard decision of all SUs as below:

$$\boldsymbol{Y} = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1M} \\ y_{21} & y_{22} & \cdots & y_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ y_{N_0 1} & y_{N_0 2} & \cdots & y_{N_0 M} \end{bmatrix} \quad (5.\ 7)$$

Where $\boldsymbol{Y}$ is a population matrix of size $N_0 \times M$ consists of the spectrum sensing information accumulated in the database of FC by all M SUs in the N_0 sensing reports, made by normal and malicious users. The SSDF effects of always yes MU (AYMU), always no MU (ANMU), opposite MU (OMU) and random opposite MU (ROMU) in CSS is minimized with the following algorithm.

5.2.2 Genetic Algorithm at the Fusion Centre

The DSND Algorithm utilizes by GA for the detection of abnormalities in the CSS system at the FC is as below:

5.2.2.1 DSND for catching Malicious Users

Based on the local sensing information received from all SUs in the N_0 sensing intervals, FC is able to identify all abnormal SUs i.e. AYMU, ANMU, OMU and ROMU with DSND.

The DSND algorithm is based on the history of SUs reports made to the FC. After the collection of N_0 reports from all M SUs as in equation (5. 7), indices K_1 and K_2 are selected such that $K_1 < K_2$. The indices K_1 and K_2 are chosen such that $M_0 < K_1 << M$ and $M_0 << K_2 < M$. The K_1 and K_2 values are the gauges for the detection of MUs in CSS with M_0 total number of MUs out of total M cooperative SUs. The DSND algorithm is based on comparing the history information of the users. In case the inter-user distance is greater than a certain limit K_1 or less than the limit

K_2, then the user is termed as malicious. A user cannot exist which is malicious in both K_1 and K_2 senses. As the method is based on the history of the user reports the more information the system has about a user the more accurately this algorithm work.

The distance between the reports of the "j^{th}" user and all other users show how many bits are different in the reports made by the "j^{th}" user with other users. N_0 shows the total reports made by all "j^{th}" users.

$$d_{ij} = \sum_{k=1}^{M} \left| y_{ij} - y_{ik} \right|, where\, i \in 1,...,N_0 \; and \; j,k \in 1,...,M \tag{5. 8}$$

Where d_{ij} is the sum of absolute distance of the "j^{th}" user sensing report with all M SUs reports in the i^{th} sensing interval.

$$\boldsymbol{D} = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1M} \\ d_{21} & d_{22} & \cdots & d_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ d_{N_0 1} & d_{N_0 2} & \cdots & d_{N_0 M} \end{bmatrix} \tag{5. 9}$$

The distance matrix $\boldsymbol{D}$ shows the distances calculated for all the j^{th} SUs during each sensing interval. The sorted results of $\boldsymbol{D}$ is used to set the upper and lower limits in equation (5. *10*) as follows:

$$Limit = \mu \pm C \times \sigma^2 \tag{5. 10}$$

where μ is the mean and σ^2 is the variance value measurement of the distance matrix. The constant consider is $10/N_0$, with N_0 shows history length of the total reports. Upper and lower limits are further defined as below:

$$I_1^H = \mu + 10 \times \sigma^2 / N_0 \tag{5. 11}$$

$$I_1^L = \mu - 10 \times \sigma^2 / N_0 \tag{5. 12}$$

After setting upper and lower limits values I_1^H and I_1^L from the sorted results of the distance matrix $\boldsymbol{D}$ and selection of K_1^{st} and K_2^{st} for detecting abnormalities, if K_1^{st} entry is greater than I_1^H the user is declaring malicious in K_1 sense and if K_2^{st} entry is less than I_1^L the user is declared malicious in K_2 sense.

$$MU = \begin{cases} j^{th}\ user & if\ \left(K_1^{st} > I_1^H\ or\ K_2^{st} < I_1^L\right) \\ 0, & Otherwise \end{cases} \tag{5. 13}$$

After identification of any abnormal behavior as above, the sensing data from such abnormalities is randomly mutated and crossover operation is performed as below, to make the final decision authentic and error proof.

5.2.2.2 Crossover and Mutation

Reference to the GA population, this work refers to the gathering of SU sensing information collected for certain sensing intervals, with rows of the population is the representation of the sensing information reported by all SUs. As fitness function is a representation of the utility of each chromosome, fit chromosomes are able to pass through heredity, while unhealthy chromosomes are deceased due to the natural phenomenon of the survival of the fittest.

The fitness function in this work is selected based on the results in equation (5. 9) as:

$$F = \left[F_1 \; F_2 \; F_3 \; ... \; F_{N_0} \right] \tag{5. 14}$$

where each fitness function value is calculated as:

$$F_i = \sum_{j=1}^{M} d_{ij} \tag{5. 15}$$

The information with minimum total neighbor distances for all users is selected as the best chromosome. Based on the result of equation (5. 15) the top two chromosomes are selected as the parent chromosome and crossover operations are done among the rest to determine new offspring.

Crossover: The crossover exploits the best behaviors of the current chromosomes and mixes them in a bid to increase their appropriateness. This operator randomly selects a locus and exchanges the sub-sequences before and after that locus between two parent chromosomes to build a pair of children. A crossover point is randomly selected in this work.

The fitter chromosomes likely passes to the next generation and the population is sorted in ascending order of fitness values.

Mutation: The process of mutation represents a random change of the value of the gene, which shows the change in the sensing data for the selected user. The mutation operation is performed on the sensing information provided by abnormal users. The reported information of abnormal detected user is randomly inverted. If the genome bit is 0, it is changed to 1 and vice versa.

After the random mutation and crossover operation, a new population matrix is obtained which results in a neighbor distance matrix $\boldsymbol{D}^{'}$ as follows:

$$\boldsymbol{D'} = \begin{bmatrix} d'_{11} & d'_{12} & \cdots & d'_{1M} \\ d'_{21} & d'_{22} & \cdots & d'_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ d'_{N_0 1} & d'_{N_0 2} & \cdots & d'_{N_0 M} \end{bmatrix} \tag{5. 16}$$

Therefore, new fitness function values are determined as:

$$F'_i = \sum_{j=1}^{M} d'_{ij} \tag{5. 17}$$

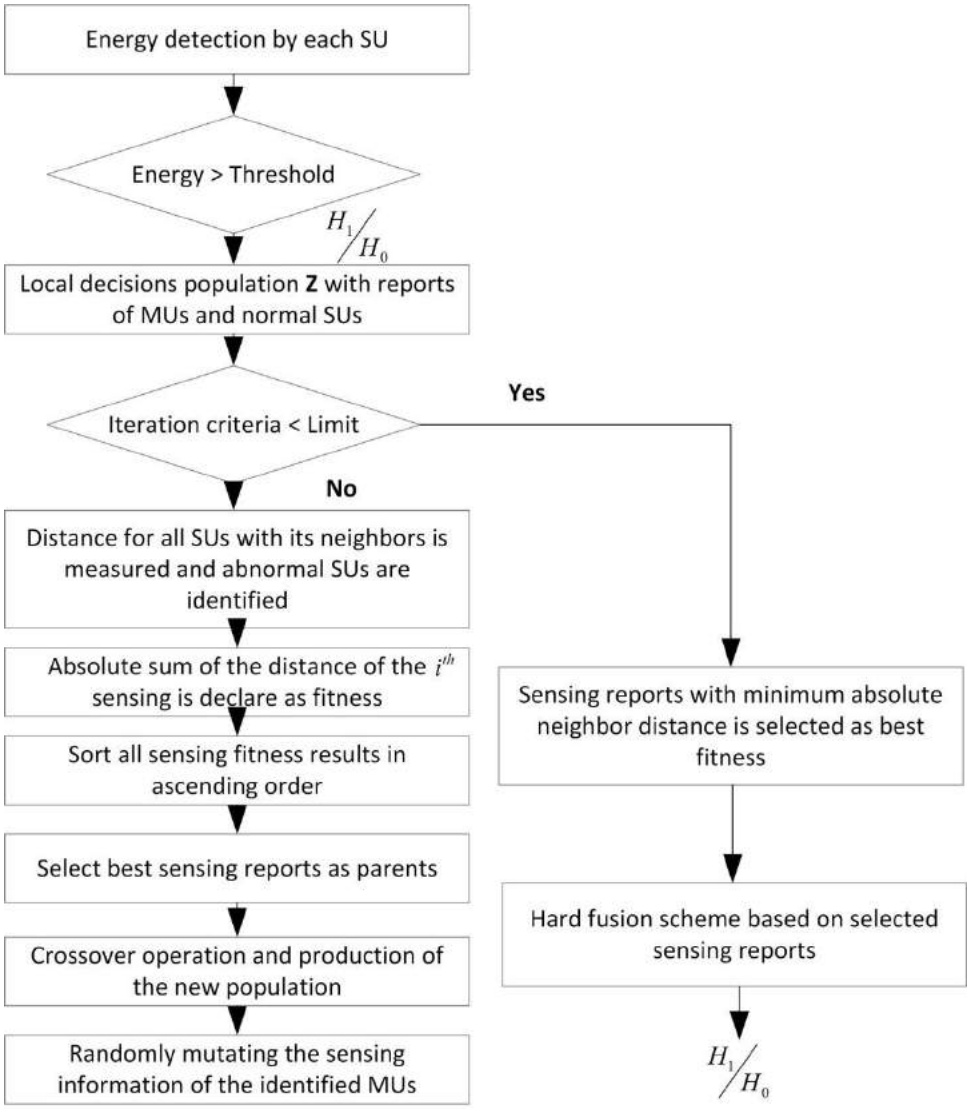

Figure 5. 2 DSND based GA scheme Flowchart

Fitness values in equation (5. 17) are further sorted in ascending order and the minimum is selected as the best fitness. Sensing reports in $\boldsymbol{Y}$ with similar index to the best fitness is selected final recommendation of the GA. The recommended sensing information is further utilizes in the hard fusion combination scheme as in section 3.3 to finalize a unified global decision.

A flow chart diagram with step wise operation is shown in Figure 5. 2.

5.2.2.3 Counting rule as hard decision rule at the FC

The three most commonly used hard fusion combination schemes are the Voting scheme (majority decision here), OR scheme and AND fusion scheme. After the identification of abnormal users by the DSND algorithm GA is utilized to make the final decision as free of these abnormal users and to make the sensing decision more reliable and accurate.

In the voting decision scheme an unanimous decision on the PU existence H_1 is made if K out of total M users make a decision of the PU presence. Similarly, if the number of SUs with PU detection information is less than K then decision is made in favor of H_0 to declare the license channel as free. In the proposed work, majority voting scheme is selected with $K = M/2$ as a special case

$$\begin{aligned} H_1 &: \ \sum_{j=1}^{M} y_j(i) \geq \left(\frac{M}{2} \right) \\ H_0 &: \ otherwise \end{aligned} \tag{5. 18}$$

Here M is the total number of SUs reports made to the fusion center.

Cooperative detection and false alarm probabilities of the DSND based GA is represented at the FC based on the local detection made by individual SUs as follow:

$$P_d = \Pr\{Y=1|H_1\} = \Pr\left\{\sum_{j=1}^{M} y_j(i) \geq \frac{M}{2}|H_1\right\}$$
$$P_f = \Pr\{Y=1|H_0\} = \Pr\left\{\sum_{j=1}^{M} y_j(i) \geq \frac{M}{2}|H_0\right\} \quad (5.19)$$

Where P_d and P_f are the cooperative detection and false alarm probabilities of the majority voting scheme when DSND based GA mechanism is used to detect the licensed user spectrum.

5.2.3 Simulation Results of the DSND based GA scheme

For simulation purposes, parameters are set for the cognitive radio network with total 10 cooperative users. Out of the total M users in cooperation, 6 users are selected as honest SUs and 4 of the users as AYMU, ANMU, OMU and ROMU. The SNRs varies from -20 dB to 10 dB. The sensing time is taken as 1 ms and number of samples K in each sensing interval is selected 270. The number of sensing iterations are considered 100 and sensing intervals during which ROMU act maliciously are selected randomly from 1 to N. Similarly, a crossover locus point is randomly selected from 1 to $(M-1)$. The crossover and mutation operation is observed for 10 cycles. Performance of the system is verified and checked by keeping the number of OMU, ROMU, AYMU and ANMU users same. The sensing population size of the GA is selected $N_0 \times M$ with N_0 is the total number of chromosomes, selected as 16 in this study, which shows the sensing history information for the M SUs.

Simulation results collected shows the ROC curve of the proposed method along-with EGC and simple majority voting decision. Probability of detection against probability of false alarm and probability of miss detection versus probability of false alarm is shown in Figure 5. 3 and Figure 5. 4, respectively. The proposed majority voting with prior identification of MUs using DSND

followed by crossover and mutation regarding the PU status is giving sophisticated detection results against EGC and simple majority voting schemes. Probability of detection and probability of miss detection results in both the cases when MUs are taken into account and the one without the consideration of these MUs are drawn. In both cases detection and false alarm results of the proposed scheme is outperforming the simple majority voting and EGC with almost same probability of false alarm.

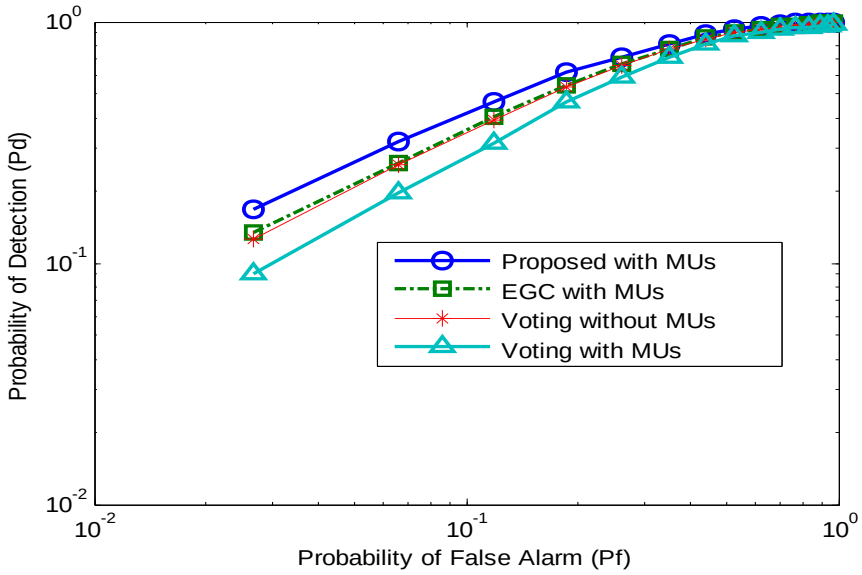

Figure 5. 3 Probability of Detection vs. Probability of False Alarm for the proposed voting, EGC, voting without MUs and simple voting schemes

Results for the probability of detection and probability of miss-detection are obtained against the SNRs in Figure 5. 5 and Figure 5. 6, it is clear to see improvement in the detection and miss-detection results with an increase in SNR. In both Figure 5. 5 and Figure 5. 6 results of the proposed majority voting scheme are suitable against EGC and simple majority voting scheme even when MUs are included in majority voting CSS.

Finally, the probability of error (P_e) results vs. SNR is drawn between the simple majority voting, Proposed DSND based GA and EGC

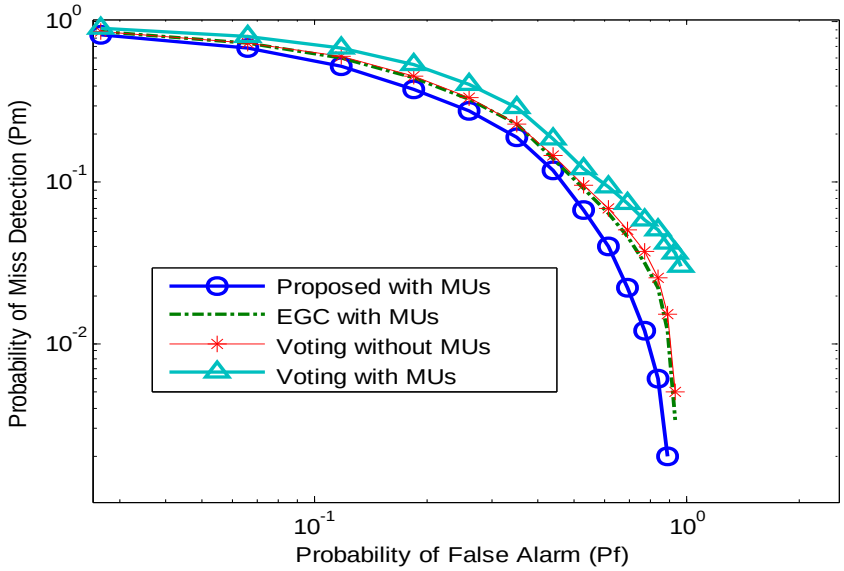

Figure 5. 4 Probability of Miss Detection vs. Probability of False Alarm for the proposed voting, EGC, voting without MUs and simple voting schemes

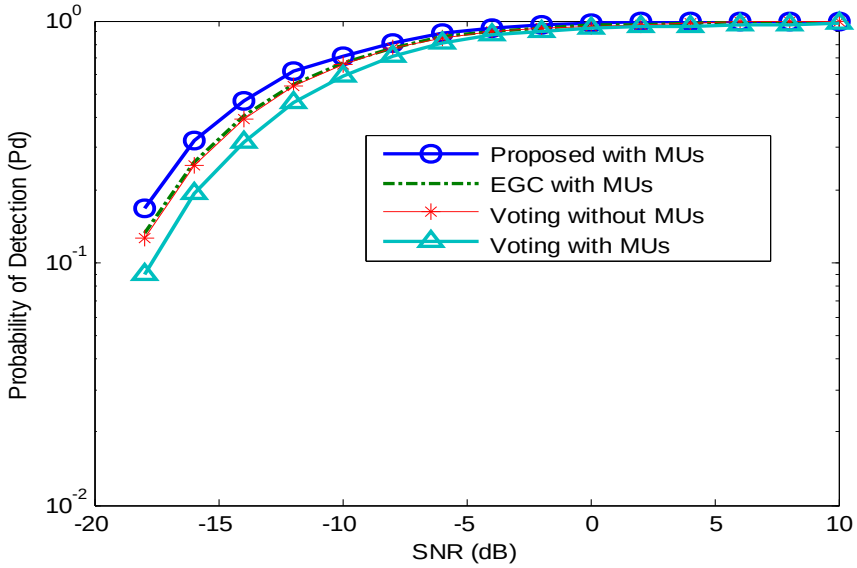

Figure 5. 5 Probability of Detection vs. Signal to Noise Ratio for the proposed voting, EGC, voting without MUs and simple voting schemes

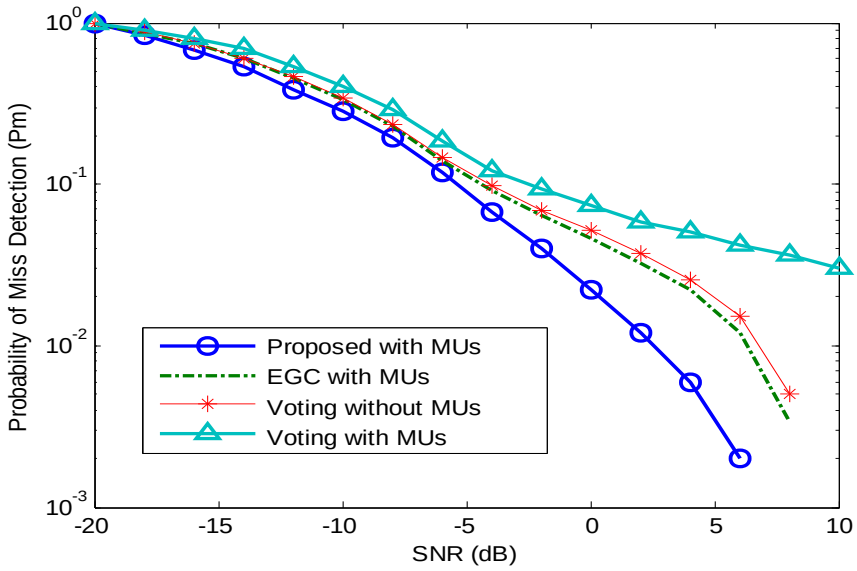

Figure 5. 6 Probability of Miss Detection vs. Signal to Noise Ratio for the proposed, EGC, voting without MUs and simple voting schemes

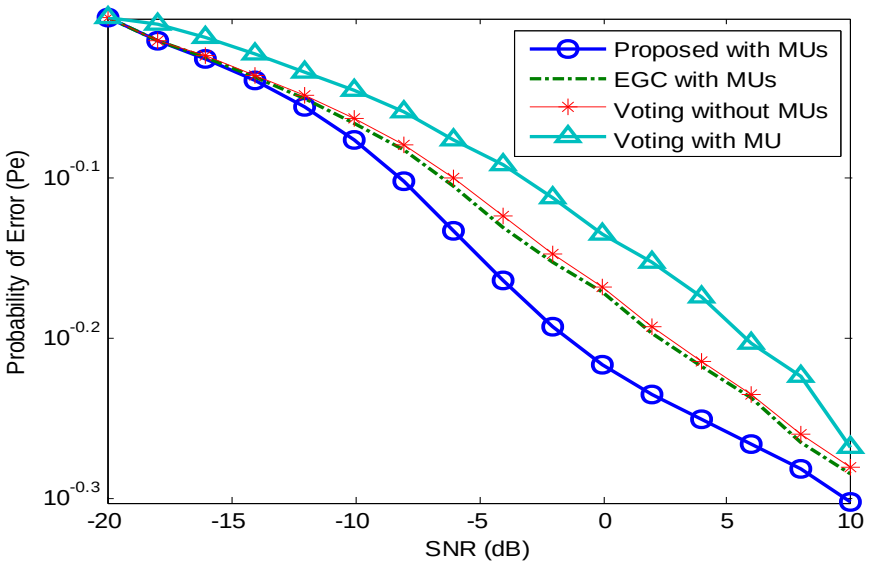

Figure 5. 7 Probability of Error vs. Signal to Noise Ratio for the proposed voting, EGC, voting without MUs and simple voting schemes

The graphical results in Figure 5. 7 shows that the probability of error of the proposed scheme is below the simple majority voting and EGC schemes at the same level of SNR.

It is clear from the simulation results that the combination of DSND with GA followed by the majority voting hard fusion scheme makes the performance of CSS more authentic and valid in the presence of AYMU, ANMU, ROMU and OMU.

5.3 Data Model for majority voting GA scheme

Model of the proposed CSS is shown in Figure 5. 8. SUs sense the licensed channel and take a local decision to forward either H_1 or H_0 decision to the FC. The rule of FC is divided into two parts. First, it collects local spectral observations from all SUs and applies GA using one-to-many hamming distance along with z-score as a total outlier factor for determining the fitness of all sensing reports. The final sensing selection is made for the sensing report with minimal total outlier score results at the end of desired iterations. In the second part it uses majority voting hard decision fusion (MV-HDF) scheme to declare the final status of the PU channel based on the selection results of the GA.

5.3.1 Local Spectrum Decisions

Based on the hard binary sensing decisions by all users in equation (5. 1), FC collects their local sensing reports and form a reporting matrix as below:

$$\boldsymbol{Y} = \left[y_{ij} \right], i \in 1,...,N,\ j \in 1,...,M \tag{5. 20}$$

Where $\boldsymbol{Y}$ is a population matrix of size $N \times M$ containing the hard binary decisions at the FC by all M users in the N sensing reports of the PU channel. The population is built for both the NSUs and MUs. Furthermore, GA is used as a tool for minimizing the SSDF effects of MUs and any imperfections by the normal SU (NSU) in the following section.

5.3.2 Best sensing report selection using GA

On the basis of all the sensing information of SUs during each sensing interval as above, FC further utilizes GA for determining the best sensing results out of the local decision reports provided by all SUs for taking out a global decision.

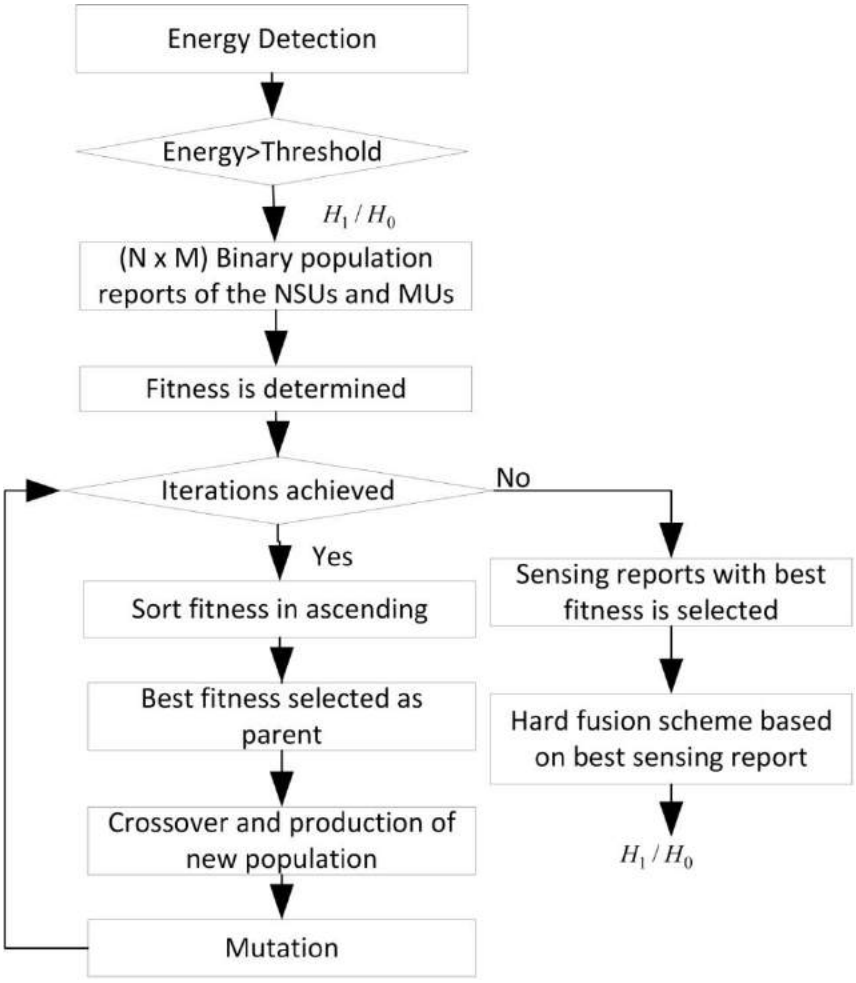

Figure 5. 8 GA based CSS Flowchart.

FC determines absolute differences of the j^{th} user sensing with the average sensing energy reported by all other SUs based on the result in equation (5. 20). Average of all SU decisions is calculated by neglecting the j^{th} SU results in the i^{th} sensing interval to find out the impact of not

including this particular user in the collective sensing result. A similar procedure is followed for the reports of all M users in the N sensing interval as:

$$\boldsymbol{A} = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1M} \\ m_{21} & m_{22} & \dots & m_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ m_{N1} & m_{N2} & \cdots & m_{NM} \end{bmatrix} \tag{5. 21}$$

$$\text{where } m_{ij} = \left\{ \frac{\left(\sum_{j=1}^{M} y_{ij} \right) - y_{ij}}{M-1} \right\}$$

In equation (5. 21) m_{ij} is the average value of energy reports of all other SUs in the i^{th} sensing interval while keeping away the sensing results of the j^{th} SU out of the average measurement. The PU spectrum reports of the MUs are different from the NSUs, therefore taking these MUs out during each sensing interval is generating dissimilar averaging results for the OMU, ROMU, AYMU and ANMU compared with NSUs.

5.3.2.1 Outlying using One-to-many sensing distance

To figure out how much the individual sensing results of each SU "y" are behaving differently from the average sensing results "m" of all other users. Outlying factors are determined for the sensing reports of SUs based on the one-to-many sensing distances $\boldsymbol{o}_j^1(i)$ for the j^{th} user in the i^{th} sensing interval as:

$$\boldsymbol{o}_j^1(i) = \left| y_{ij} - m_{ij} \right|, i \in 1,...,N,\ j \in 1,...,M \tag{5. 22}$$

Based on the results in equation (5. 22) the outlier score $\boldsymbol{o}_j^1(i)$ of the NSUs and MUs are added to discover the total one-to-many hamming distance score under each sensing interval as:

$$\boldsymbol{o}_i^1 = \sum_{j=1}^{M} \left(\boldsymbol{o}_j^1(i) \right),\ j \in 1,...,M \tag{5. 23}$$

Where $\boldsymbol{o}_i^1$ in equation (5. 23) is the total outlier score representing the absolute sum of the hamming distances of the individual user detection y_{ij} with the average detection m_{ij} of all other SUs.

The calculations in equation (5. 23) are made for all the N intervals and results are collected as:

$$\boldsymbol{o}^1 = \left[\boldsymbol{o}_1^1 \ \ \boldsymbol{o}_2^1 \ \ ... \ \ \boldsymbol{o}_N^1 \right] \tag{5. 24}$$

Here $\mathbf{o}^1$ in equation (5. 24) is the outlier score result for all the N sensing intervals. This score is a measurement of how far the report of each SU is lying away from the average sensing reports provided by all other SUs by making separable those sensing intervals during which MUs and the imperfection of the NSU were misguiding the FC's final decision about the PU channel.

5.3.2.2 Outlying using z-score

Similarly, the other outlier score measurement for each user report is made with the help of the **z-score** measurement in comparison with the sensing report received from each SU as:

$$\boldsymbol{o}_j^2(i) = \left| \frac{\left(y_{ij} - \mu(i) \right)}{\sigma(i)} \right|, i \in 1,...,N,\ j \in 1,...,M \tag{5. 25}$$

Where $\mu(i) = \sum_{j=1}^{M} \frac{y_{ij}}{M}$ is the mean value of the sensing reports of all M users in the i^{th} sensing interval. $\sigma(i) = \sqrt{\frac{\sum_{j=1}^{M} \left(y_{ij} - \mu(i) \right)^2}{M}}$ is the standard deviation of the i^{th} interval reports and $\boldsymbol{o}_j^2(i)$ is the z-score outlying of the j^{th} user report in the i^{th} interval of the historical formation.

The result for $\boldsymbol{o}_j^2(i)$ in equation (5. 25) shows how much local sensing observation of the j^{th} user is detached away from the group observations provided by all other users using z-score.

Now for guaranteeing the authenticity of each of the i^{th} reports, a sum of the z-score results for all intervals is made as:

$$\boldsymbol{o}_i^2 = \sum_{j=1}^{M} \left(\boldsymbol{o}_j^2(i) \right), i \in 1, ..., N \tag{5. 26}$$

The total $\boldsymbol{o}^2$ score result for all N sensing reports are collected as:

$$\boldsymbol{o}^2 = \left[\boldsymbol{o}_1^2 \;\; \boldsymbol{o}_2^2 \;\; ... \;\; \boldsymbol{o}_N^2 \right]^T \tag{5. 27}$$

As fitness function is the representation for the suitability of each sensing reports, the final selection of the fitness of each sensing reports from both the NSU and MU reports is determined. The best selection results having less abnormal behavior on behalf of the NSU and MU users are calculated.

In order to select the best sensing reports received from the normal and MUs, fitness function is calculated based on the result in equation (5. 23) and equation (5. 26) as:

$$\boldsymbol{f}(i) = \left(\boldsymbol{o}_i^1 + \boldsymbol{o}_i^2 \right) \tag{5. 28}$$

The result of equation (5. 28) is able to make clear separation between reports under the predominant impact of MUs and NSU malfunctioning from the one containing less effect of these abnormalities. The fit chromosomes in equation (5. 28) are allowed to pass through

heredity, while the unhealthy chromosomes with higher abnormalities deceased due to the natural phenomenon of the survival of the fittest.

The sensing results in $\boldsymbol{Y}$ with the minimum total outlier score in equation (5. 28) are selected as the best chromosome and considered to be accurate sensing information on behalf of the NSU and MUs. The top chromosomes based on the fitness results in equation (5. 28) are selected as the parent chromosomes and crossover operation is performed in the rest to determine new offsprings.

The crossover operator randomly selects a locus and exchanges the sub-sequences before and after that locus between two parent chromosomes to build a pair of children. A crossover point is randomly selected here in this thesis. The fitter chromosomes are more likely to be passed on to the next generation. The population is then sorted in ascending order of fitness values.

The process of mutation represents a random change in the bit values of the gene. The mutation operation is performed on the sensing information of the least fit chromosome. Genome bits of the least fit chromosome are inverted after random selection.

After the random mutation of genome bits and crossover operation, a new population matrix $\boldsymbol{Y}$ is obtained and the same procedure as in equations (5. 22) to (5. 27) is repeated for the determination of best fitness which results in new values of the fitness function as in equation (5. 28). After achieving the desired iteration criteria, the sensing reports $y_j(b)$ with minimum outlier score in equation (5. 28) is selected for a global decision.

A flowchart diagram with detailed operation of the proposed scheme from local binary decisions by the SUs following by the data collection at the FC and GA operation for the identification of best sensing reports selection on behalf of NSUs and MUs is shown in Figure 5. 8.

5.3.3 Counting rule as Hard decision Rule at the FC

After the selection of best sensing reports $y_j(b)$ in $\boldsymbol{Y}$ with minimal outlier value as in equation (5. 28), FC applies one of the hard fusion combination schemes to take a global decision of the primary user status. The three most commonly used hard fusion schemes applied by the FC are the voting rule, OR and AND rules.

The voting rule decides about the PU activity based on the voting of K SUs decision out of total M cooperative users. If K out of M users decides that a signal is present, then FC takes a global decision H_1. Here M is the number of cooperative SUs and K is the count of how many of the SUs have reported PU signal presence. The count $K = M/2$ is selected as a special case of the voting rule called the majority decision rule. Similarly, in the majority voting decision if the PU detection reports are less than K then FC takes the global decision as H_0

$$G_B(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) \geq K \\ H_0 : otherwise \end{Bmatrix} \quad (5.\ 29)$$

While applying AND rule by the FC, all the M SUs has to provide a unanimous decision of the PU presence, then the FC declares the channel as occupied by the PU and generate a global decision as H_1 representing the PU signal, otherwise decision H_0 is made by the FC as:

$$G_B(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) = M \\ H_0 : otherwise \end{Bmatrix} \quad (5.\ 30)$$

On following the OR rule procedure by the FC during each sensing interval if at least one of the SUs provide local detection information to the FC, then FC decides a global decision H_1, otherwise decision is made in favour of H_0

$$G_B(i) = \begin{Bmatrix} H_1 : \sum_{j=1}^{M} y_j(b) \geq 1 \\ H_0 : \textit{otherwise} \end{Bmatrix} \tag{5. 31}$$

The results of the cooperative detection and false alarm probability for the voting rule based on the local detection of all the M SUs is demarcated at the FC as [22]:

$$\begin{aligned} P_d &= \Pr\left\{G_B(i) = 1 \middle| H_1\right\} = \Pr\left\{\sum_{j=1}^{M} y_j(b) \geq K \middle| H_1\right\} \\ P_f &= \Pr\left\{G_B(i) = 1 \middle| H_0\right\} = \Pr\left\{\sum_{j=1}^{M} y_j(b) \geq K \middle| H_0\right\} \end{aligned} \tag{5. 32}$$

Here FC declares a global decision as $G_B(i) = 1$of the PU status if K out of total M SUs are reporting in favour of H_1. The majority voting decision is taken as a special case of the voting rule with $K = M/2$. Both OR and AND rules are also special cases of the voting rule with $K = 1$ for the OR and $K = M$ for the AND category of the hard combination schemes.

Similarly, the results of the cooperative detection and false alarm probabilities for the OR and AND rules are as given below:

$$\begin{aligned} P_{d\_OR} &= 1 - \prod_{j=1}^{M} \left(1 - P_{d,j}\right) \\ P_{f\_OR} &= 1 - \prod_{j=1}^{M} \left(1 - P_{f,j}\right) \end{aligned} \tag{5. 33}$$

$$P_{d\_AND} = \prod_{j=1}^{M}\left(P_{d,j}\right)$$
$$P_{f\_AND} = \prod_{j=1}^{M}\left(P_{f,j}\right) \quad (5.\ 34)$$

where P_{d_OR} and P_{f_OR} are the cooperative spectrum detection and false alarm probabilities, respectively while applying OR rule, while P_{d_AND} and P_{f_AND} are the detection and false alarm results, respectively when AND hard fusion scheme is applied. A pseudo code demonstrating a procedure of the proposed scheme is given below.

For $k = 1$ to sensing limit
For $i = 1$ to iterations
For $j = 1$ to total SUs
If $E_j(i) > Threshold$
$y_j(i) = 1$, hard decision "1"
Else
$y_j(i) = 0$, hard decision "0".
End
End
For $j = 1$ to total SUs

$$m_{ij} = \left\{ \frac{\left(\sum_{j=1}^{M} y_{ij}\right) - y_{ij}}{M-1} \right\}$$

$$\mathbf{o}_j^1(i) = \left| y_{ij} - m_{ij} \right|, i \in 1,...,N,\ j \in 1,...,M$$

$$\mathbf{o}_j^2(i) = \left| \frac{\left(y_{ij} - \mu(i)\right)}{\sigma(i)} \right|, i \in 1,...,N,\ j \in 1,...,M$$

End

$$\mathbf{o}_i^1 = \sum_{j=1}^{M}\left(\mathbf{o}_j^1(i)\right), i \in 1,...,N$$

$$\mathbf{o}_i^2 = \sum_{j=1}^{M}\left(\mathbf{o}_j^2(i)\right), i \in 1,...,N$$

$$\mathbf{f}(i) = \left(\mathbf{o}_i^1 + \mathbf{o}_i^2\right)$$

Crossover the new population
Randomly mutation of the least fit
End iterations
Best sensing sample $y_j(b)$ out of Y
If $\sum_{j=1}^{M} y_j(b) \geq K$
Global decision $G_B(i) = H_1$

Else
Global decision $G_B(i) = H_0$
End
End sensing limit

5.3.4 Simulation Results of the majority voting GA scheme

For simulation purposes cognitive radio network parameters are set with total M cooperating SUs including NSUs, MUs and FC. Out of the M users, 4 users are selected as AYMU, ANMU, OMU and ROMU nature of MUs. Performance of the proposed and other schemes is tested under various simulation conditions. At first the total number of cooperating SUs is taken as 12 at different average SNR values (-9.5 dB, -13.5 dB, -15.5 dB). In this study MUs were observed under low and higher SNR values compared with NSUs. In the second part the simulation is done for the proposed and all other schemes at different ratios of cooperative SUs with 8, 12 and 16. The sensing time is taken as $1\,ms$ and the number of samples M in each sensing interval is 270. The total number of sensing iterations is taken as 1000. The sensing intervals during which ROMU perform a malicious act is selected randomly from 1 to 1000.The crossover points for the GA is randomly selected from 1 to M . The crossover operation in the chromosomes and the production of new offspring is observed for 10 cycles. MUs are equally distributed as OMU, ROMU, AYMU and ANMU. The GA population consists of $N = 10$ chromosomes with a total of M number of SUs in each chromosome. The GA population represents the sensing information of the M users in the N trials.

The simulation results collected in Figure 5. 9-5. 12 show the ROC curves for the GAMV-HDF, MV-HDF, EGC-SDF and MGC-SDF schemes. The results collected in Figure 5. 9 and Figure 5. 10 shows that as the average SNR raises from -17.5 dB to -9.5 dB, the ROC curves of all fusion

schemes enhance. In Figure 5. 9 cooperating users are kept 12 and simulation is done for the proposed GAMV-HDF, MV-HDF, EGC-SDF and MGC-SDF at different average SNRs. In this part of the simulation MUs are observed with low SNR values compared with normal cooperating SUs. The results demonstrate that the proposed scheme has improved ROC results at all average SNR values. This is followed by the MGC-SDF, EGC-SDF and simple MV-HDF schemes. The outcomes in Figure 5. 10 shows the ROC results against different average SNR values for a total of 12 cooperative SUs with malicious behaviour changed for the abnormal SUs. In this part MUs are taking higher SNR values compared with normal cooperating SUs. In Figure 5. 10 when MUs are having higher SNR values compared with normal cooperating SUs, the results of the EGC-SDF and MGC-SDF is getting worse among all schemes. The proposed method has improved performance at all values of SNR in Figure 5. 10 compared with other combination schemes.

Similarly, Figure 5. 11 and Figure 5. 12 show probability of detection versus probability of false alarm under -10.5 dB average SNR value. In Figure 5. 11 the system is tested against 8, 12 and 16 cooperative SUs with low SNR by MUs compared with NSUs while in Figure 5. 12 the system was observed when MUs participate with higher SNR values against the NSUs. It is clear of the results in Figure 5. 11 and Figure 5. 12 that cooperation has resulted in improved performance for all fusion schemes with the increased number of cooperative stations from 8 to 16.

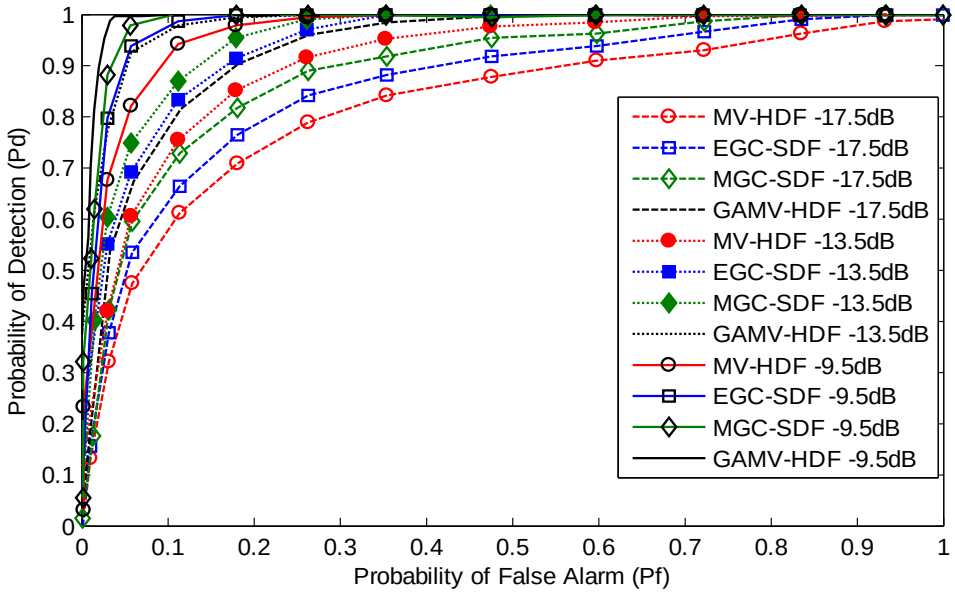

Figure 5. 9. Probability of Detection vs. Probability of False Alarm (ROC) at different SNR values (-9.5 dB, -13.5 dB, -17.5 dB) with MUs having low SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

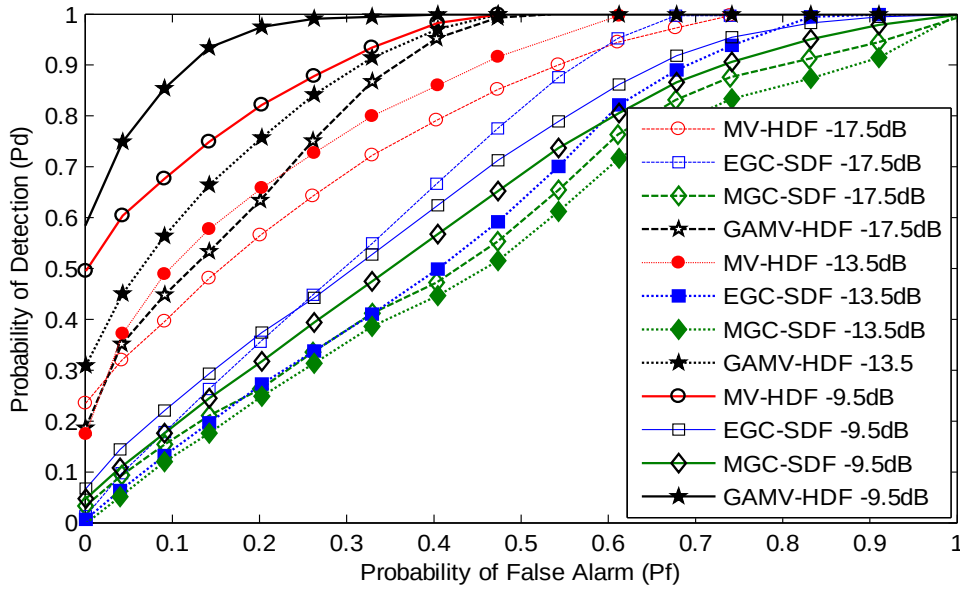

Figure 5. 10. Probability of Detection vs. Probability of False Alarm at different SNR values (-9.5 dB, -13.5 dB, -17.5 dB) with MUs having high SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

The proposed GAMV-HDF method in Figure 5. 11 are able to surpass all other schemes in this low SNR situation of MUs. In case of higher SNR participation from MUs compared with NSUs

as in Figure 5. 12, ROC results of the MGC-SDF is weak under all 8, 12 and 16 total number of cooperating SUs cases when MUs taking higher SNR values. The simple MV-HDF is able to produce improved ROC performance in comparison with EGC-SDF and MGC-SDF schemes in Figure 5. 12.

Results for the probability of detection are obtained against the varying SNR values in Figure 5. 13 and Figure 5. 14 at different ratios of cooperating SUs. In Figure 5. 13 detection results are collected when MUs are observed with low SNR and in Figure 5. 14 with higher SNR values for MUs compared with normal cooperative users. It is good to see development in the detection results for the proposed GAMV-HDF scheme with increasing SNR in both results. Figure 5. 13 shows that when MUs have a low SNR compared with normal SUs proposed method has better detection results at all SNRs and all cases of 8, 12 and 16 cooperating users. The proposed method detection results are followed by the MGC-SDF and EGC-SDF schemes at different contributions of 8, 12 and 16 cooperating users, while the detection results obtained for the simple MV-HDF scheme is the lowest of all in Figure 5. 13. In Figure 5. 14 when MUs have higher SNR values the propose method detection results is less vulnerable. The simple MV-HDF is able to surpass both the EGC-SDF and MGC-SDF schemes at all values of SNRs and different ratios of cooperating SUs.

Finally the probability of error results of the PU detection is shown in Figure 5. 15 and Figure 5. 16. The result shows minimum error in the proposed GAMV-HDF scheme against the simple MV-HDF, EGC-SDF and MGC-SDF schemes. In both Figure 5. 15 and Figure 5. 16 results are drawn with a total of 8, 12 and 16 users under low SNR observed in Figure 5. 15 and with higher SNR in Figure 5. 16.

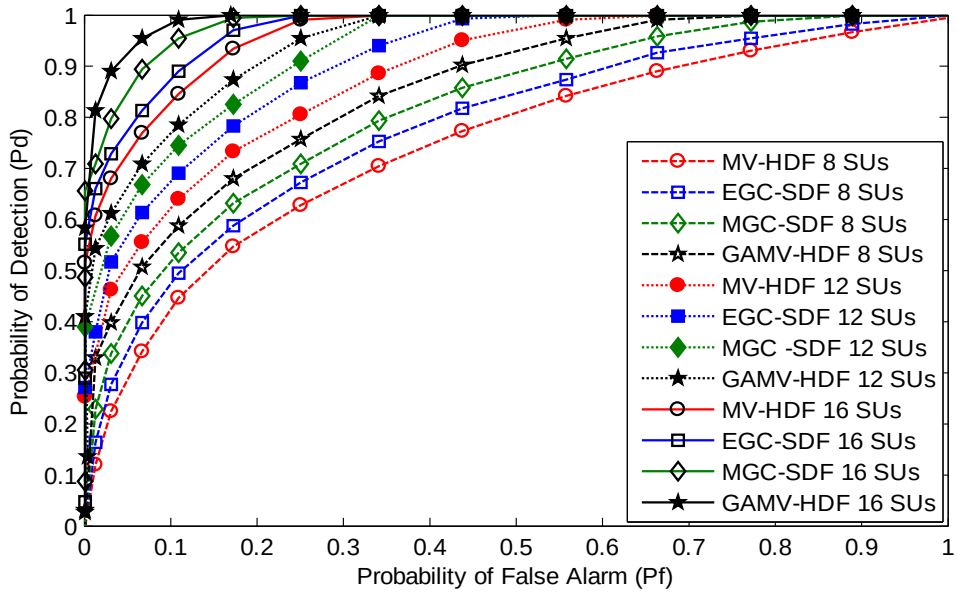

Figure 5. 11. Probability of Detection vs. Probability of False Alarm at different ratio of cooperating SUs (8, 12, 16) with MUs having low SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF

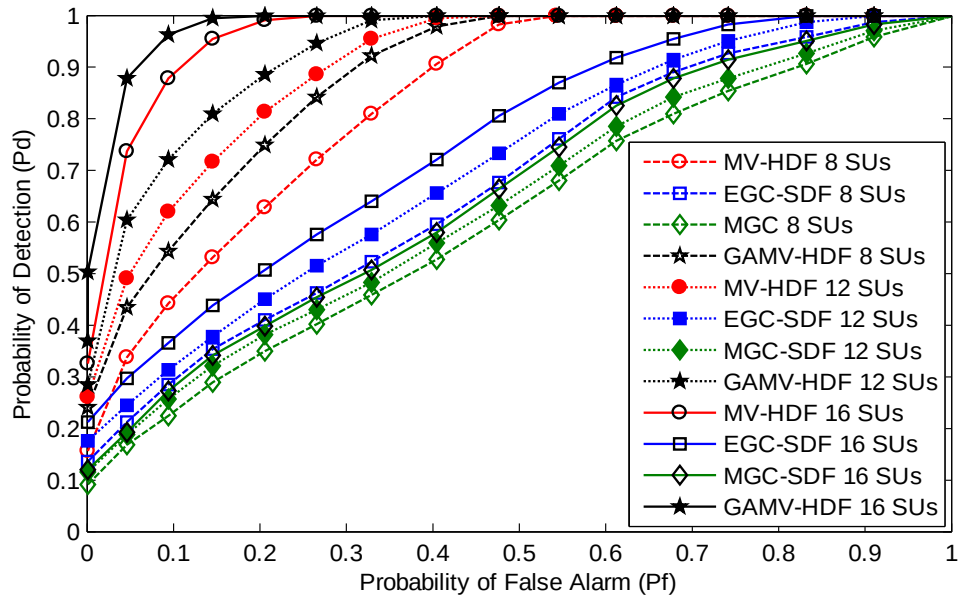

Figure 5. 12. Probability of Detection vs. Probability of False Alarm (ROC) at different ratio of cooperating SUs (8, 12, 16) with MUs having high SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

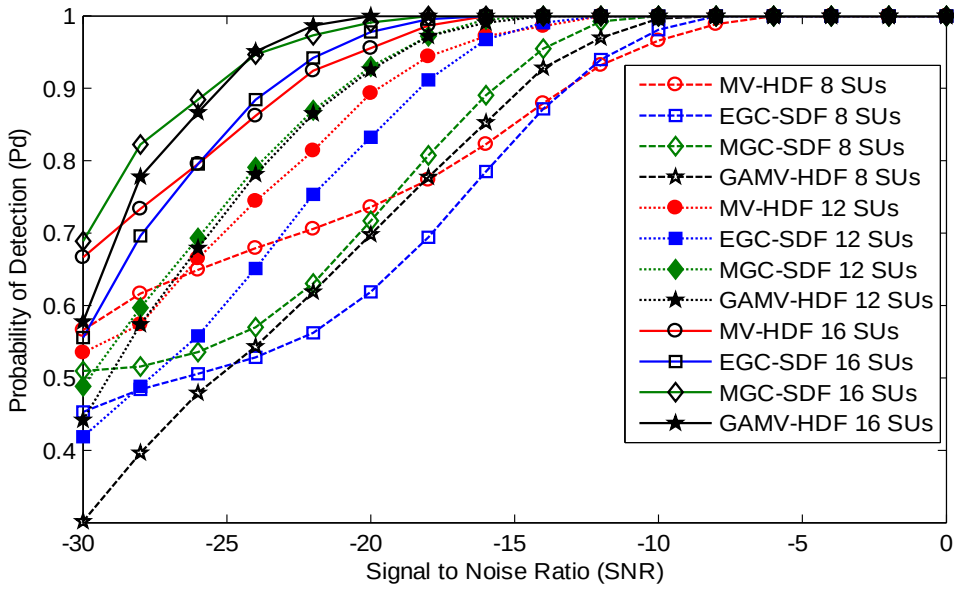

Figure 5. 13. The Probability of Detection vs. Signal to Noise Ratio at different ratio of cooperative SUs (8, 12, 16) with MUs having low SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

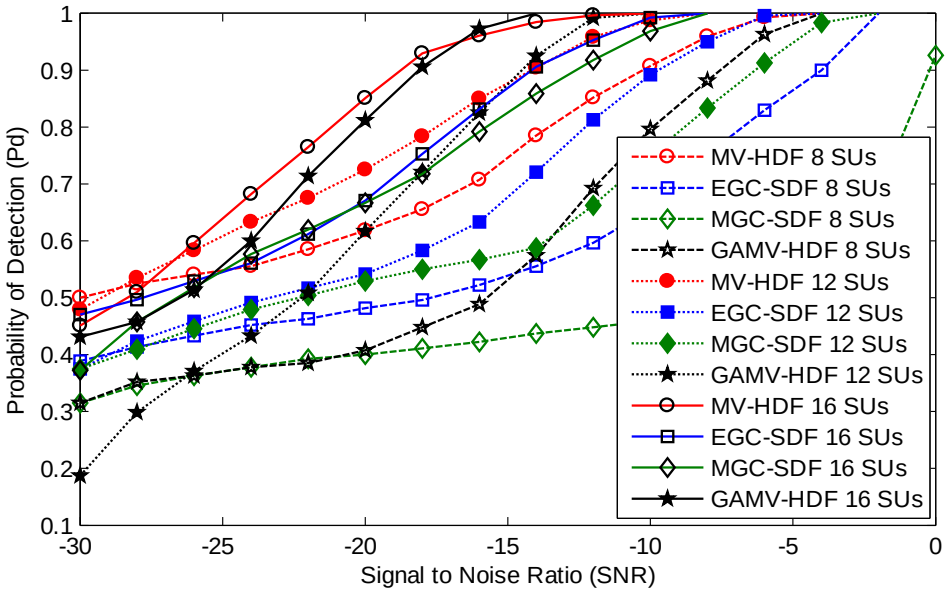

Figure 5. 14 The Probability of Detection vs. Signal to Noise Ratio at different ratio of cooperative SUs (8, 12, 16) with MUs having high SNR compared with SUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes

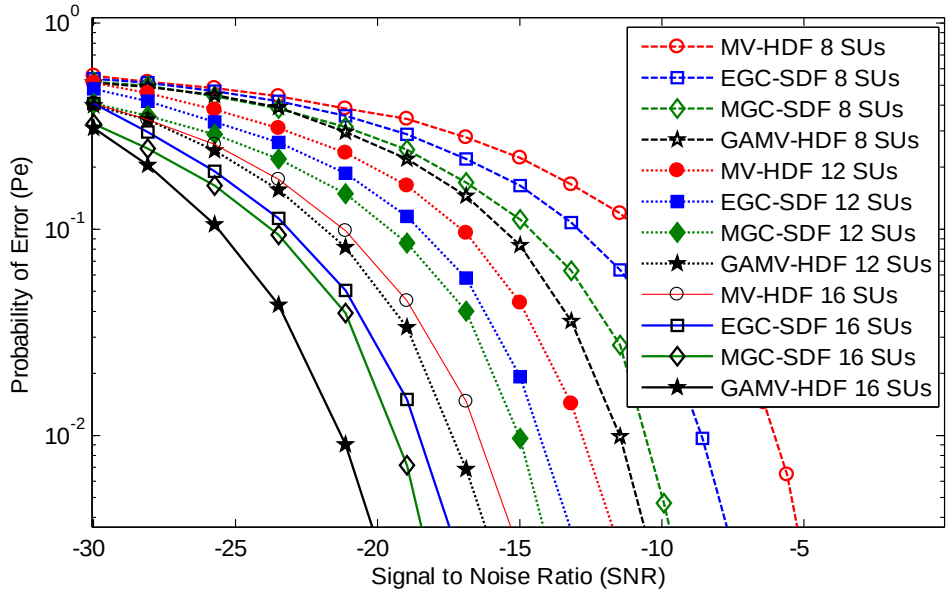

Figure 5. 15. Probability of Error vs. Signal to Noise Ratio at different ratio of cooperative SUs (8, 12, 16) with MUs having low SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

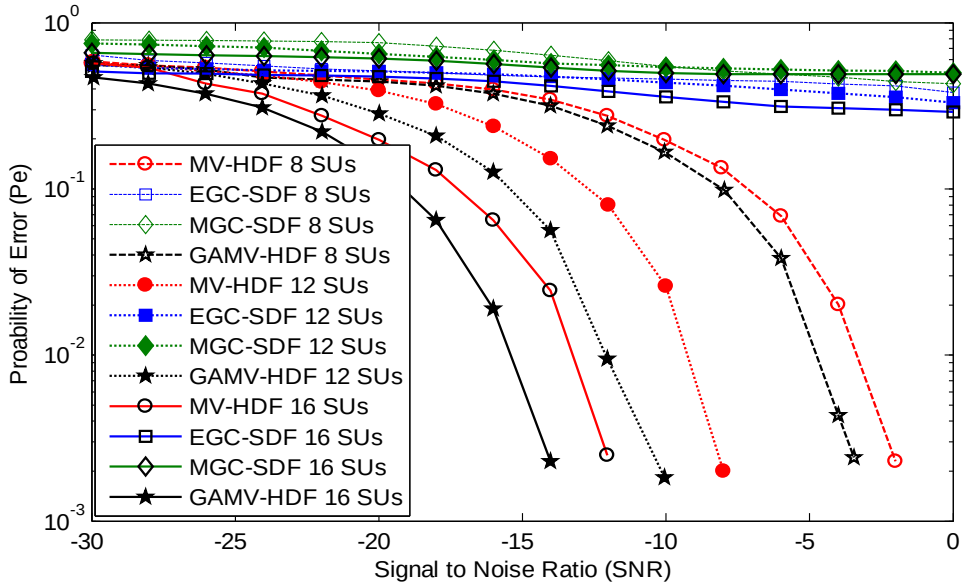

Figure 5. 16. Probability of Error vs. Signal to Noise Ratio at different ratio of cooperative SUs (8, 12, 16) with MUs having high SNR compared with NSUs for the MV-HDF, EGC-SDF, MGC-SDF and GAMV-HDF schemes.

The proposed scheme is able to produce less detection error in terms of sensing the licensed user channel followed by the MGC-SDF scheme in Figure 5. 15. Furthermore, the simple MV-HDF scheme has resulted in high probability of error in Figure 5. 15. From the results in Figure 5. 16 when MUs have higher SNR values as compared with NSUs, the error probability of the MGC-SDF and EGC-SDF increases compared with simple MV-HDF and proposed GAMV-HDF method. The MGC-SDF performance degrades in this case because MGC-SDF is giving higher preference to the detection of SUs with higher SNR information. As MUs are considered with higher SNR, therefore MGC-SDF decision about the PU channel is strongly misguided by the MUs. Similarly, EGC-SDF performance is also affected by the higher SNR of the MUs because it is equally considering the reported information of all SUs for a global decision.

It is clear from these simulations that the use of GA followed by the MV-HDF scheme makes the performance of CSS more authentic and valid in the presence of MUs at various numbers of cooperating SUs and SNR ratios.

The harmful risk of AYMU, ANMU, ROMU and OMU user participation in CSS is reduced with the usage of the recommended technique. From the graphical results of the proposed scheme, simple MV-HDF, EGC-SDF and MGC-SDF schemes it is clear that the cooperation process turn out to be more solid and systematic by following the proposed methodology.

5.4 Data Model for PSO based scheme

PSO is derived from the bird flocking or fish swarming, and was introduced by Eberhart and Kenedy in 1952. In PSO, individual intelligence as well as collective intelligence plays a role in finding an enhanced solution. In the GA, it is likely that every novel group is flourishing better than the previous generation. Similarly, in the PSO the same group is likely to become better and

better. In PSO each individual establishes his local intelligence and improves it with time. The whole group is expected to improve upon its group intelligence. Particles in PSO algorithm utilizes its own and neighbor knowledge to update their velocity and position. The PSO particle exchange information about their best position among each other during a number of iterations.

The proposed CSS model using PSO is in Figure 5. 17. In this model SUs senses the licensed PU channel, and forward their local energy statistics information to the FC for a number of observations to form a PSO population. FC then applies the PSO method for identifying that sensing report, which has a better resemblance with the actual status of the PU transmission activity. The decision center measure the fitness score under all sensing iterations and declare the minimum total outlying score particle as the actual channel information of the PU for a final decision. Fusion combination schemes are applied by the FC, based on the selected global best particle of the population to generate a more accurate and reliable final decision of the PU channel.

5.4.1 Local Spectrum decisions

FC receives the soft energy reports of all users and form a history matrix consisting energy statistics observed by each user during the N_0 sensing intervals as below:

$$\boldsymbol{E} = \left[E_{ij} \right] = \begin{bmatrix} E_{11} & E_{12} & \cdots & E_{1M} \\ E_{21} & E_{22} & \cdots & E_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ E_{N_0 1} & E_{N_0 2} & \cdots & E_{N_0 M} \end{bmatrix}, i \in 1,...,N_0, j \in 1,...,M \qquad (5.\ 35)$$

Where E_{ij} is the energy information of the j^{th} SU in the i^{th} interval. Spectrum sensing information is gathered in the FC database for all M SUs including both normal and malicious users.

The sensing falsification effects of the MUs as discussed are minimized using the following steps of the proposed method.

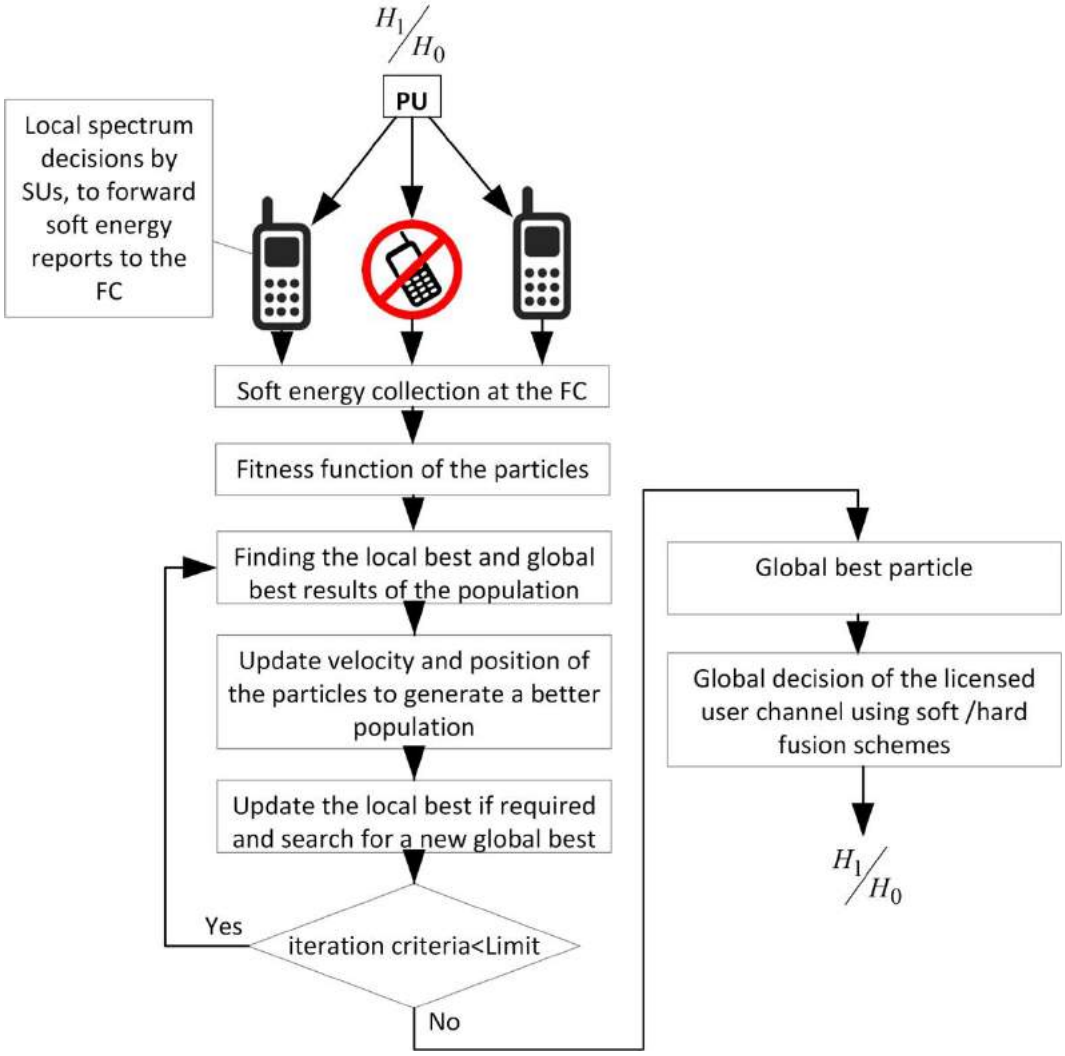

Figure 5. 17 PSO based CSS Model.

5.4.2 Finding the fitness of particles

After the collection of energy information from all M SUs for the N_0 sensing intervals as in equation (5. 35), FC modifies the particle positions to observe the differences in each individual

sensing report with the reports provided by all other SUs. A new population is formed on behalf of all users based on the information already collected in equation (5. 35) as below:

$$\boldsymbol{E'} = \left[E_{ij}^{'} \right] = \begin{bmatrix} E_{11}^{'} & E_{12}^{'} & \cdots & E_{1M}^{'} \\ E_{21}^{'} & E_{22}^{'} & \cdots & E_{2M}^{'} \\ \vdots & \vdots & \ddots & \vdots \\ E_{N_0 1}^{'} & E_{N_0 2}^{'} & \cdots & E_{N_0 M}^{'} \end{bmatrix}, i \in 1,...N_0, j \in 1,...,M \tag{5. 36}$$

$$\text{Where } E_{ij}^{'} = \left| \left\{ \frac{\left(\sum_{j=1}^{M} \left(E_{ij} \right) - E_{ij} \right)}{\left(M - 1 \right)} \right\} \right|$$

Here $E_{ij}^{'}$ is the average of the individual soft energies reports provided by all other users while taking out the report of the j^{th} user in this averaging.

5.4.2.1 Outlying using one-to-many sensing distance

In order to determine how much individual sensing reports of each SU is behaving differently from the average sensing results, an outlying factor is measured based on the one-to-many sensing distance $\boldsymbol{d}_j(i)$ for the j^{th} user in the i^{th} sensing particle as:

$$\boldsymbol{d}_j(i) = \left| E_{ij} - E_{ij}^{'} \right|, i \in 1,..., N_0, j \in 1,..., M \tag{5. 37}$$

Based on the results in equation (5. 37) the outlier score $\boldsymbol{d}_j(i)$ of the normal SUs and MUs are added to discover the total one-to-many hamming distance score under each sensing interval

$$\boldsymbol{d}_i = \sum_{j=1}^{M} \left(d_j(i) \right), i \in 1,..., N_0, j \in 1,..., M \tag{5. 38}$$

Where $\boldsymbol{d}_i$ in equation (5. 38) is the total outlier score representing the absolute sum of the hamming distances of the one individual SU detection "E_{ij}" with the average detection $E_{ij}^{'}$ of all other SUs in the i^{th} sensing interval.

The measurement in equation (5. 38) is made for all the N_0 intervals and results are collected as:

$$\boldsymbol{d} = \left[d_1 \; d_2 \; d_3 \; ... \; d_{N_0} \right]^T \tag{5. 39}$$

Here $\boldsymbol{d}$ is the outlier score result for all the N_0 sensing intervals. This score is a measurement of how far, the report of each SU is lying away from the average sensing reports provided by all other SUs by making separate those sensing intervals during which MUs and the imperfection of the normal SU were misguiding the FC final decision about the PU channel.

5.4.2.2 Outlying using z-score

Similarly, the other outlier score measurement for each user report is made with the help of the **z-score** measurement in comparison with the sensing report received from each SU as:

$$\boldsymbol{o}_j(i) = \left| \frac{\left(E_{ij} - \mu(i) \right)}{\sigma(i)} \right|, i \in 1,...,N_0, \; j \in 1,...,M \tag{5. 40}$$

Where $\mu(i) = \dfrac{\left(\sum_{j=1}^{M} E_{ij} \right)}{M}$ is the mean and $\sigma(i)$ is the standard deviation of the i^{th} particle in the PSO population. $o_j(i)$ is the z-score outlying of the j^{th} report in the i^{th} interval of the historical information. The result of $o_j(i)$ in equation (5. 40) shows how much local sensing observation of

the j^{th} user is detached away from the group observations provided by all other users using z-score.

Now for guaranteeing the authenticity of each of the i^{th} reports, a sum of the z-score results for all particles is made as:

$$\boldsymbol{o}_i = \sum_{j=1}^{M} \left(\boldsymbol{o}_j (i) \right), i \in 1,..., N_0, \, j \in 1,..., M \tag{5. 41}$$

The total z-score of all N_0 PSO particles of the PSO population are collected as:

$$\boldsymbol{o} = \left[o_1 \;\; o_2 \;\; o_3 \;\; ... \;\; o_{N_0} \right]^T \tag{5. 42}$$

As fitness function is the representation for the suitability of each sensing reports, the final selection of the fitness of each sensing reports from both the normal SU and MU is determined and the best selection of the sensing results having less abnormal behavior of the cooperative SUs is calculated.

The suitability criteria for the selection of particles of the PSO according to their fitness values are declared according to equation (5. 39) and equation (5. 42) as:

$$\boldsymbol{f}(i) = \left(\boldsymbol{d}_i + \boldsymbol{o}_i \right) \tag{5. 43}$$

The result in equation (5. 43) shows the minimum score of the sensing reports containing fewer abnormalities in comparison to those reports that are badly affected due to the abnormal behavior of the MUs.

5.4.3 Update Population

The global best position "$\boldsymbol{g}$" is the particle in $\boldsymbol{E}$ which results in a minimum outlying score among all particles according to equation (5. 43). Each particle may improve on its own if its new version improves compared to the previous one. Local best particles of the population are selected as $\boldsymbol{P} = \boldsymbol{E}$.

The positions and velocities of the particles are initially set to zero. The particle velocities are further updated with individual and collective intelligences as:

$$V_{(i+1)j} = V_{ij} + C_1 \times R_1 \times \left(P_{ij} - E_{ij} \right) + C_2 \times R_2 \times \left(\boldsymbol{g}_j - E_{ij} \right) \tag{5. 44}$$

Here C_1 and C_2 are the learning acceleration coefficients used to describe individual and social contributions of each particle, R_1 and R_2 are uniformly distributed random numbers in the range "0" to "1" which present stochastic component to the algorithm.

After calculations of velocities for each particle with the local and global intelligence of the particles, these velocities are rounded to the two extremes as:

$$V_{(i+1)j} = \begin{Bmatrix} \max(V), V_{ij} > \max(V) \\ \min(V), V_{ij} < \max(V) \end{Bmatrix} \tag{5. 45}$$

The j^{th} particle position representing the soft energy information at the $(i+1)^{th}$ iteration is updated with the measured velocities just as:

$$E_{(i+1)j} = E_{ij} + V_{(i+1)j} \tag{5. 46}$$

Where $E_{(i+1)j}$ are the reports of the modified population, E_{ij} is the initial report of the j^{th} user in the i^{th} interval and $V_{(i+1)j}$ are the measured velocities in equation (5. 46).

5.4.4 Update local best and global best

Fitness values for the new population in equation (5. 46) are determined by following the same procedure as in equation (5. 43).

Fitness values of the novel particles are compared with the fitness values of the previous population to search for the local best and global best positions to determine any improvements in the updated energy reports in comparison with earlier energy reports. The local best positions of the population are updated as:

$$P_i = \begin{Bmatrix} E_i, & f(E_i) < f(P_i) \\ P_i, & otherwise \end{Bmatrix}, i \in 1,...,N_0 \qquad (5.\ 47)$$

In equation (5. 47) results of the local best particles are updated by comparing the fitness of the new population equation (5. 46) to that of the local best particles "P" fitness. The local best particles are updated and take the values of the new population if it gives highest outlying results according to equation (5. 43) as compared to the newly created population.

Similarly, a search is made to identify new global best particle for the entire population by cross analysis of the fittest. Fitness of the updated local best particles as in equation (5. 47) is placed for comparison in order to search for any improvement in the selection of the global best particle as follows:

$$\boldsymbol{g} = \begin{Bmatrix} P_i, & f(P_i) < f(\boldsymbol{g}) \\ \boldsymbol{g}, & otherwise \end{Bmatrix}, \forall i \in 1,...,N_0 \qquad (5.\ 48)$$

In equation (5. 48), outlying score of each particle from the local best population is compared with the global best particle determined earlier. If any particle of the local best population has a fitness function found to be more optimum in comparison with the global best particle with the minimum outlying score as in equation (5. 43), then global best particle is replaced by that particle.

Here the new global best particle is selected as "$\boldsymbol{g}$" representing particle with the best fitness function having minimum outlying results in the current and previous PSO population.

The PSO production of the new population and search of the global best results continues until the stopping criterion is met. At the end of desired number of iterations, the final global best particle containing soft energy reports made by all M cooperative SUs is elected for a final decision by the FC about the PU channel.

5.4.5 Global decision of the licensed channel

Based on the final selection of the global best particle "$\boldsymbol{g}$" as the soft energy reports on behalf of all M cooperative SUs, FC utilizes soft and hard fusion combination schemes as in section 2 for declaring a unanimous decision about the license user spectrum. The EGC, MGC and majority voting hard fusion combination schemes are used as a decision criterion in this section.

The EGC is combining the individual statistical information of all SUs by giving equal weight to each individual SU decision and summed coherently. The summed is compared with the threshold to decide the license user spectrum by the EGC as:

$$EGC = \begin{Bmatrix} H_1: & \dfrac{\left(\sum_{j=1}^{M} g_j\right)}{M} \geq \gamma \\ H_0: & otherwise \end{Bmatrix} \tag{5. 49}$$

The cooperative detection and false alarm probabilities P_{d_EGC} and P_{f_EGC} made by the EGC scheme based on the global decision made about the PU spectrum are as:

$$\begin{aligned} P_{d\_EGC} &= \Pr\left(\frac{\left(\sum_{j=1}^{M} \boldsymbol{g}_j\right)}{M} \geq \gamma \middle| H_1 \right) \\ P_{f\_EGC} &= \Pr\left(\frac{\left(\sum_{j=1}^{M} \boldsymbol{g}_j\right)}{M} \geq \gamma \middle| H_0 \right) \end{aligned} \tag{5. 50}$$

In MGC scheme, each receiving signal branch is multiplied with a weighed function proportional to the branch gain. Branches with strong signal are further amplified while weak signals are attenuated by these weights. The idea to boost the strong signal component and attenuating weak components as in MGC diversity is exactly the same as that of filtering and signal weighting in the matched filter receiver. Similarly, the MGC scheme at the FC is giving higher weights to the decision of the SUs with higher SNR values and low weight to the decision of SUs with low SNR values as:

$$MGC = \begin{Bmatrix} H_1: & \sum_{j=1}^{M} \left(w_j \times \boldsymbol{g}_j \right) \geq \gamma \\ H_0: & otherwise \end{Bmatrix} \tag{5. 51}$$

$$\text{Where } w_j = \frac{\eta(j)}{\sum_{j=1}^{M} \eta(j)}$$

The cooperative detection and false probabilities of the MGC scheme are measured based on the soft energy received as:

$$\begin{aligned} P_{d\_MGC} &= \left\{ \left(\sum_{j=1}^{M} \left(w_j \times \boldsymbol{g}_j \right) \geq \gamma \right) | H_1 \right\} \\ P_{f\_MGC} &= \left\{ \left(\sum_{j=1}^{M} \left(w_j \times \boldsymbol{g}_j \right) \geq \gamma \right) | H_0 \right\} \end{aligned} \tag{5. 52}$$

In the count fusion combination schemes, FC counts the total number of SUs with their energy value greater than the threshold as:

$$\begin{Bmatrix} H_1 : \sum_{j=1}^{M} \left(\boldsymbol{g}_j \geq \gamma_j \right) \geq k \\ H_0 : \textit{ otherwise} \end{Bmatrix} \tag{5. 53}$$

The three most commonly used HFC schemes are the majority voting, OR and AND fusion schemes. In the count HFC scheme a unanimous decision on the PU existence is made if k out of total M SUs make a decision of the PU detection with their energies larger than a threshold. FC declares a final decision of the PU channel as H_1 if k SUs reported about the PU existence. Similarly, if the number of SUs with PU detection information is less than k then the decision is made in favor of H_0 to declare an idle condition of the license channel. The counting score "k" is taken as "1" for the OR fusion rule and "M" for the AND rule. In the study of the proposed work, the majority voting scheme is selected with $k = \frac{M}{2}$. M is the total number of SUs reports

forwarded to FC for PU detection. In the majority voting scheme, if half cooperative users have decided in favor of H_1, global decision is made as H_1, otherwise decision is made in favor of H_0.

The detection and false alarm probabilities of the majority voting decision based on the best selection of the PSO at the FC are as follows:

$$P_{d\_MV} = \Pr\left\{\sum_{j=1}^{M} g_j \geq \frac{M}{2} \middle| H_1\right\}$$
$$P_{f\_MV} = \Pr\left\{\sum_{j=1}^{M} g_j \geq \frac{M}{2} \middle| H_0\right\} \quad (5.54)$$

Where P_{d_MV} and P_{f_MV} are the results of cooperative detection and false alarm probabilities of the majority voting when PSO is used as a detection mechanism for sensing the licensed user spectrum.

5.4.6 Simulations Results of the PSO scheme

For simulation purposes, parameter setting is made for the cognitive radio network with total $M = 11$ cooperating SUs. Out of the total M cooperating users 7 of the users are selected as honest SUs and 4 of them are randomly selected as AYMU, ANMU, OMU and ROMU malicious users. Variation in the SNR for the SUs is made in the range of -30 dB to -2 dB. The sensing time is kept as $1ms$ for each SU with total $K = 270$ samples in each sensing period. The number of sensing iterations N is considered as 100. Sensing intervals during which ROMU perform a malicious act is selected randomly from 1 to N. The performance of the system is verified and checked by distributing equally the MUs as OMU, ROMU, AYMU and ANMU. The sensing reports of the SUs are accumulated into the PSO population of size $N_0 \times M$ with total N_0 number of particles representing sensing information of all M cooperating SUs.

In the first part of the simulation as in Figure 5. 18, results are drawn to compare the performance of EGC, MGC and majority voting hard fusion combination schemes. In this part of the simulation first all the MUs are selected as AYMU and then as ANMU users. From the simulation results in Figure 5. 18 it is obvious to see an improvement in the detection results of the PSO based EGC, MGC and majority voting schemes against traditional combination schemes. The cooperative system performance experienced under all AYMU and all ANMU is more optimized and suitable for the proposed PSO based soft and hard combination schemes. It is also observable from the graphical results that the detection response of the CSS in both the cases when only AYMU and the one with only ANMU users were taken into considerations is identical. The equal consideration of AYMU and ANMU user situations are similarly treated by system with almost identical probability of detection (P_d) for a given false alarm (P_f). The graphical results in Figure 5. 18 shows the higher ROC results for the PSO based MGC scheme followed by the EGC while the majority voting hard fusion combination presented is producing less detection results compared with other two schemes. It is also obvious from Figure 5. 18 that both the PSO based soft and hard fusion combination schemes are able to outperform the simple MGC, EGC and hard fusion combinations for any given value false alarm.

In the second part, authenticity of the system is verified by comparing the results of the proposed PSO based soft and hard combinations with traditional schemes. In this case, first all MUs were selected as OMU and then all of them were taken as ROMU. From the simulation results, it is clear to see that the detection results for MGC scheme is higher compared with its EGC and majority voting counterparts. The ROC plots of the schemes are shown in Figure 5. 19 for the traditional fusion schemes and proposed PSO based fusion schemes. The plotted results of all the three schemes under proposed and traditional method show the reliability of the PSO based

combination technique against the traditional method. In Figure 5. 19, ROMU is affecting the cooperative sensing environment more hazardously unlike OMU and show that the ROMU presence is more dangerous. The proposed scheme is superseding the traditional fusion combination schemes in both OMU and ROMU considerations.

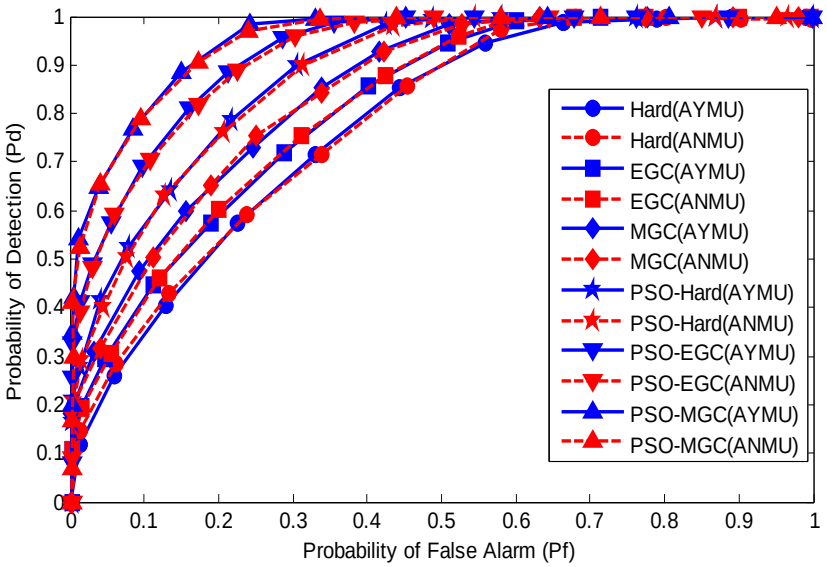

Figure 5. 18 Probability of Detection vs. Probability of False Alarm for the Hard, EGC, MGC, PSO-Hard, PSO-EGC and PSO-MGC schemes in the presence of AYMU and ANMU malicious users.

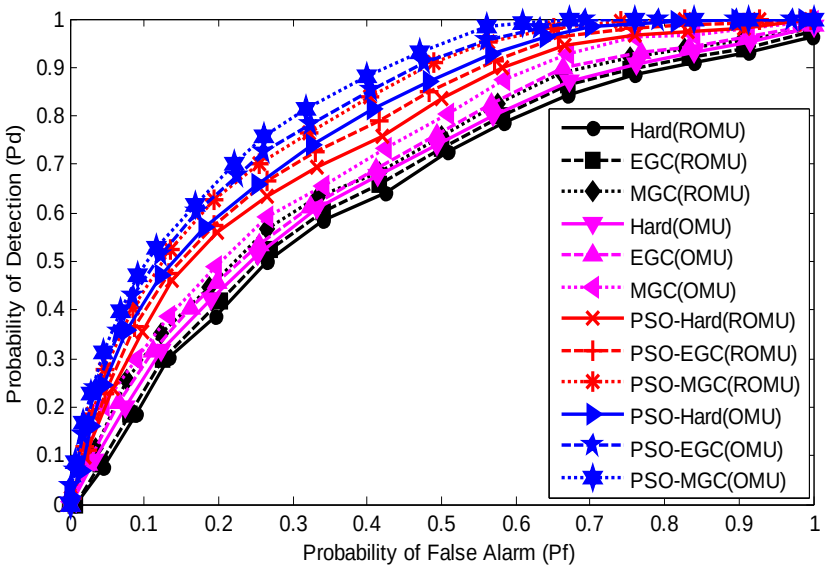

Figure 5. 19 Probability of Detection vs. Probability of False Alarm for the Hard, EGC, MGC, PSO-Hard, PSO-EGC and PSO-MGC schemes in the presence of OMU and ROMU malicious users.

In the third part of the simulation results, the performance of the traditional and proposed PSO based fusion combination schemes is tested when malicious users are distributed equally as AYMU, ANMU, OMU and ROMU in Figure 5. 20.

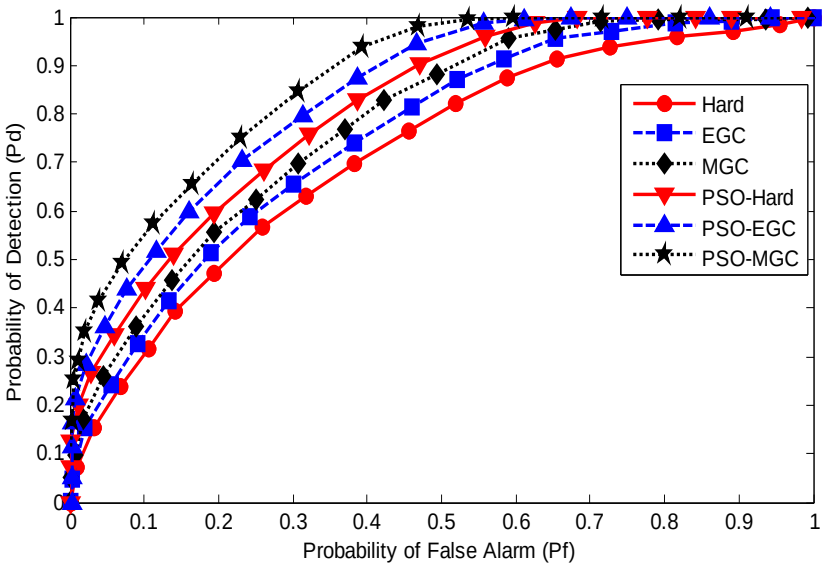

Figure 5. 20 Probability of Detection vs. Probability of False Alarm for the Hard, EGC, MGC, PSO-Hard, PSO-EGC and PSO-MGC schemes in the presence of AYMU, ANMU, OMU and ROMU malicious users.

The lower three ROC plots in Figure 5. 20 show the performance of the traditional fusion schemes under the consideration of all 4 MUs, while the upper three ROC curves show the results of the PSO fusion combination schemes under the same parameter settings. The plots show an improvement in the detection performance of the PSO based fusion combination schemes compared with traditional combination schemes. It is also noticeable that the MGC fusion combination scheme is giving more sophisticated detection results compared with all other fusion schemes.

The performance of the proposed method is further verified by drawing probability of error (P_e) results against average SNR values for the traditional and proposed PSO based fusion combination schemes in Figure 5. 21. The probability of error results in sensing the licensed user channel for the proposed scheme are less and with increased SNR values the proposed method error reduces more quickly as compared to the simple combination schemes.

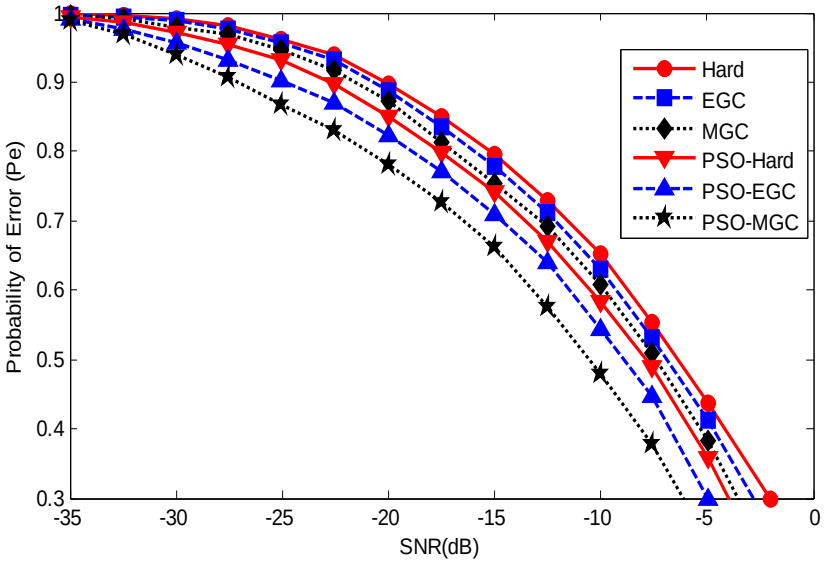

Figure 5. 21 Probability of Error vs. Signal to Noise Ratio for the Hard, EGC, MGC, PSO-Hard, PSO-EGC and PSO-MGC schemes in the presence of AYMU, ANMU, OMU and ROMU malicious users

It is clear from the simulation results that with the use of PSO algorithm the sensing performance achieved by the proposed fusion combination schemes is more optimized and accurate in the presence of MUs. The best sensing report selection of the PSO following by soft and hard fusion combinations makes the CSS results more authentic and valid in the presence of MUs. The risk of considering AYMU, ANMU, ROMU and OMU users in CSS is significantly reduced with the use of the proposed method.

5.5 Summary

The focus in part I, is to improve the majority voting hard combination scheme using GA in the presence of abnormalities. DSND algorithm is employed by the GA for the detection of abnormalities and then applies crossover and mutation operations to provide more verified information of the PU spectrum to FC. The FC further takes its global decision about the license spectrum using majority voting hard fusion decision. At the end FC is able to produce reliably and authentic PU detections in the presence of AYMU, ANMU, ROMU and OMU malicious users.

The focus in part II is to improve the performance of CSS using GA. FC is taking sensed information from all cooperating SUs, including normal and malicious users, and combining them for a more concrete decision about the licensed user spectrum using MV-HDF with GA. The decision results of the MV-HDF are shaped more reliable with GA by identifying optimum sensing results with selection and crossover in the presence of MUs.

Part III, based on the energy statistics received from all SUs, PSO is able to reduce the effect of the MUs in authenticating the global decision of the PU existence. FC combines the diversify sensing reports of all SUs using proposed EGC, MGC and the majority voting decision to take a global decision of the licensed user spectrum. The PSO scheme is able to overcome the effects of OMU, ROMU, AYMU and ANMU categories of MUs followed by soft and hard combinations to decide accurately. Simulation results reflect the superiority and authenticity of the proposed scheme in producing more accurate and reliable decisions for both soft and hard fusion combination schemes at the FC.

Chapter 6

Statistical methods against malicious users in cooperative spectrum sensing

6.1 Introduction

In this chapter, we employed statistical techniques to detect and evade MU out of the FC global decision. The chapter is divided into two parts. In part I, the FC collects local binary decisions of the cooperative SUs until the establishment of enough statistics. Correlations are calculated between the sensing information of individuals and other SUs. The BWP is used for identifying MUs and omitting them from the AND-HFC, OR-HFC, and MV-HFC before taking any global decision of the legitimate user spectrum. In part II, OTMSD and ZS measurements are used by the HT to detect the AYMU, ANMU, OMU and ROMU at the FC. In this part, ROC comparison is made between the proposed EGC using OTMSD (EGC-OTMSD), EGC using ZS (EGC-ZS), MGC using OTMSD (MGC-OTMSD) and MGC using ZS (MGC-ZS) with the traditional EGC and MGC schemes at different historical levels of the reporting users, SNRs and total number of cooperative users. Results demonstrate effectiveness of the proposed soft combination schemes in comparison with the traditional combination schemes.

6.2 Proposed Hard Fusion Scheme using Statistical Features

In the proposed CSS, FC collects and combine spectrum sensing decisions of all individual SUs with its local decision as in equation (5. 20). Where $\boldsymbol{Y}$ is a local decision matrix of size $N \times M$,

which represents the sensing energies accumulated at the FC database by all SUs hard decisions. The value N is the total sensing intervals with M users, including normal, malicious and FC. Furthermore, correlation is used as a tool for the detection of harmful AO and RO users.

Correlation is a statistical exercise that shows how intense the pair of testers are related to each other. Correlation ends with value -1 when both variables are in the opposite direction from perfect negative correlation to $+1$ with a strong correlation.

When all SUs reports FC, the relation in the sensing decision of each SU is made with all other users, to determine any abnormal SU with its false data collected at the FC. The FC takes a global decision on the PU status and after enough statistic collection about each SU, it is able to easily identify and mitigate the effect of both AO and RO categories of MUs in the global decision by the following steps.

6.2.1 Hard decision before system development

In step first of the detection process FC collects and store spectrum information of the users for declaring the user as AO, RO and normal. Before the establishment of enough statistics about the users, FC apply one of the HFC schemes to take a global decision of the primary user status. The three most commonly used HFC schemes applied by FC are the MV-HFC, OR-HFC and the AND-HFC.

The Voting rule decides about the PU signal based on the voting of K SUs decisions out of total M users. If K out of M SUs decides that a signal is present, then FC declares the global decision H_1, where K is the total count of how many of the SUs are in favour of PU presence. Here $K = M/2$ is selected as a special case of the voting rule called the majority decision rule. If the PU detection reports at the FC are less than K then FC takes the global decision as H_0

$$H_1 : \sum_{j=1}^{M} y_j(i) \geq K$$
$$H_0 : otherwise \quad (6.\ 1)$$

While applying AND-HFC rule by the FC, all the M SUs has to deliver a similar conclusion of the PU activity. The FC is able to declare the channel as occupied by the PU and generate a global decision H_1 when all users report PU activity in the given spectrum. Similarly, the decision H_0 is made by the FC to state the free condition of the PU spectrum when less than M users report about the PU activity in the given spectrum:

$$H_1 : \sum_{j=1}^{M} y_j(i) = M$$
$$H_0 : otherwise \quad (6.\ 2)$$

On following the OR-HFC rule procedure by the FC if at least one of the SU provide a local detection information of the PU to the FC, then FC decides H_1 otherwise, the decision is made in favour of H_0 as;

$$H_1 : \sum_{j=1}^{M} y_j(i) \geq 1$$
$$H_0 : otherwise \quad (6.\ 3)$$

Similarly, the results of the cooperative detection $P_{d,MV-HFC}$ and false alarm probabilities $P_{f,MV-HFC}$ for the MV-HFC rule based on the local detections of all M users is demarcated at the FC as [22]:

$$P_{d,MV-HFC} = \Pr\left\{Y = 1 \middle| H_1\right\} = \Pr\left\{\sum_{j=1}^{M} y_j(i) \geq K \middle| H_1\right\}$$
$$P_{f,MV-HFC} = \Pr\left\{Y = 1 \middle| H_0\right\} = \Pr\left\{\sum_{j=1}^{M} y_j(i) \geq K \middle| H_0\right\} \quad (6.\ 4)$$

Where the global decision $Y = 1$ illustrates that the total detection reports of the M users is

exceeded K. As OR-HFC and AND-HFC rules are the special cases of the voting rule with $K=1$ for the OR-HFC and $K=M$ for the AND-HFC category of the HFC. The cooperative detection and false alarm probabilities of the OR-HFC and AND-HFC rules are determined as below

$$\begin{aligned} P_{d,MV-HFC} &= 1-\prod_{j=1}^{M}\left(1-P_{d,j}\right) \\ P_{f,OR-HFC} &= 1-\prod_{j=1}^{M}\left(1-P_{f,j}\right) \end{aligned} \tag{6. 5}$$

$$\begin{aligned} P_{d,AND-HFC} &= \prod_{j=1}^{M}\left(P_{d,j}\right) \\ P_{f,AND-HFC} &= \prod_{j=1}^{M}\left(P_{f,j}\right) \end{aligned} \tag{6. 6}$$

Where $P_{d,OR-HFC}$ and $P_{f,OR-HFC}$ are the results of the cooperative detection and false alarm probabilities of the OR-HFC rule, while $P_{d,AND-HFC}$ and $P_{f,AND-HFC}$ are the detection and false alarm results when AND-HFC is applied.

A detailed operation of the proposed scheme in the form of flowchart diagram representation is shown in Figure 6. 1. The FC collects local binary decisions of the cooperative SUs until the establishment of enough statistics about the SUs. Correlation measurements are made in the sensing information of the individual SUs with the sensing information received on behalf of all other SUs. The BWP is used for the identification of MUs and is taken out of the AND-HFC, OR-HFC, and MV-HFC before taking any global decision of the legitimate user spectrum. The global decision made by the FC is more similar to the actual condition of the PU activity resulting in maximum utilization of the available spectrum with minimum disturbances for the PU.

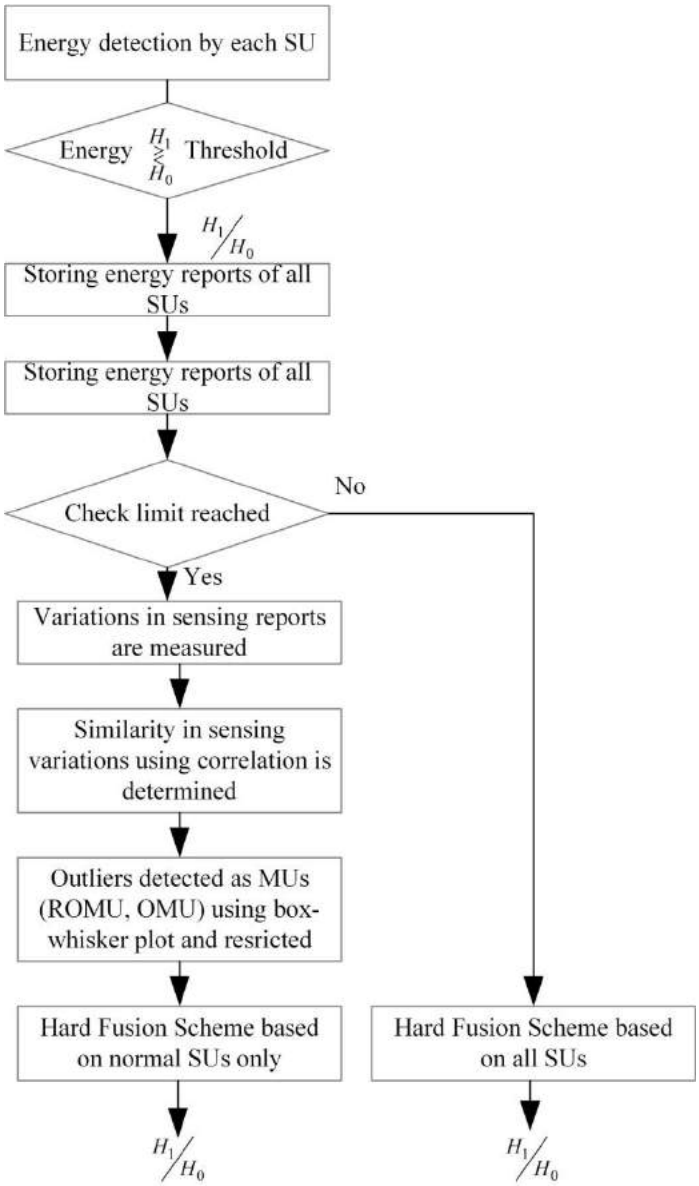

Figure 6. 1 Flow chart diagram representation of the proposed model.

6.2.2 Statistical Results for the detection of AO and RO Secondary Users

After the collection of spectrum sensing reports from all users by the FC, relation is determined in the spectrum sensing results of all users to identify abnormal sensing reports of the AO and RO users at the FC using the following steps.

6.2.2.1 Variation in the sensing intervals

In the first step, FC measures differences in the sensing results provided by one user to all other users for a total of N_0 sensing intervals. The average sensing measurement is made for all other SUs while ignoring sensing results provided by the j^{th} SU in the i^{th} interval. The j^{th} user is neglected to determine the impact of not including this particular user in the combine sensing result. A similar measurement for all other SUs during each of the N_0 sensing intervals is made as:

$$V_{ij} = \left[m_{ij} \right], where\, m_{ij} = \left\{ \frac{\left(\sum_{j=1}^{M} y_{ij} \right) - y_{ij}}{M - 1} \right\} \tag{6. 7}$$

Where V_{ij} is a matrix of size $N_0 \times M$ with M total number of SUs and N_0 is the total sensing intervals under which the system is building statistics. Value for m_{ij} is calculated as the collective energy reports of all SUs in the i^{th} sensing interval while ignoring the sensing results of the j^{th} SU. The result obtained in equation (6. 7) for both the AO and RO users has a different response than normal SUs due to differences in their sensing information. Taking these MUs out of the average value in each sensing interval result in different results for MUs against the normal SUs. Now the difference in the sensing results of each individual SU Y_{ij} is made with the average sensing reports m_{ij} measured on behalf of all other users as:

$$\Delta D_{ij} = Y_{ij} - V_{ij} \tag{6. 8}$$

$$\Delta \boldsymbol{D} = \begin{bmatrix} \Delta d_{11} & \Delta d_{12} & \cdots & \Delta d_{1M} \\ \Delta d_{21} & \Delta d_{22} & \cdots & \Delta d_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta d_{N_0 1} & \Delta d_{N_0 2} & \cdots & \Delta d_{N_0 M} \end{bmatrix} \tag{6. 9}$$

Where $\Delta \boldsymbol{D}$ is a resultant difference matrix of size $N_0 \times M$, which shows the difference in the energy reports of the j^{th} user Y_{ij}, and the average sensing results V_{ij} of all other users in the i^{th} interval.

6.2.2.2 Correlation as similarity tool

The correlation method is applied to the variation results in equation (6. 9) to find a relation in the users sensing information. Correlation operation is performed between the sensing variations of each SU with all other SUs as:

$$r_{\Delta d_j \Delta d_k} = r_{\Delta d_k \Delta d_j} = \frac{\sum_{i=1}^{N} \left(\Delta d_{ij} - \mu_j \right) \left(\Delta d_{ik} - \mu_k \right)}{\sqrt{\sum_{i=1}^{N} \left(\Delta d_{ij} - \mu_j \right)^2 \sum_{i=1}^{N} \left(\Delta d_{ik} - \mu_k \right)^2}}, \; j,k \in 1,...,M \tag{6. 10}$$

In equation (6. 10) $r_{\Delta d_j \Delta d_k}$ and $r_{\Delta d_k \Delta d_j}$ are correlation coefficients of the sensing variations between the j^{th} and k^{th} user. The Δd_{ij} and Δd_{ik} are variants of the j^{th} and k^{th} user samples in the i^{th} sensing interval, while μ_j and μ_k are mean values of the variation samples for the j^{th} and k^{th} user sensing reports in equation (6. 9)

$$\boldsymbol{R} = \begin{bmatrix} r_{\Delta d_1 \Delta d_1} & r_{\Delta d_1 \Delta d 2} & \cdots & r_{\Delta d_1 \Delta d_M} \\ r_{\Delta d_2 \Delta d_1} & r_{\Delta d_2 \Delta d_2} & \cdots & r_{\Delta d_2 \Delta d_M} \\ \vdots & \vdots & \ddots & \vdots \\ r_{\Delta d_M \Delta d_1} & r_{\Delta d_M \Delta d_2} & \cdots & r_{\Delta d_M \Delta d_M} \end{bmatrix} \tag{6. 11}$$

All correlation results are collected in matrix $\boldsymbol{R}$ of size $M \times M$, which shows correlation in the differences of each SU with all other SUs. Total similarity score for each SU is determined by adding the correlation results of all M SUs as:

$$\boldsymbol{r} = \left[\sum_{i=1}^{M} \left(r_{\Delta d_i \Delta d_1} \right) \ \sum_{i=1}^{M} \left(r_{\Delta d_i \Delta d_2} \right) \ldots \sum_{i=1}^{M} \left(r_{\Delta d_i \Delta d_M} \right) \right] \tag{6. 12}$$

The result of the vector $\boldsymbol{r}$ is a $1 \times M$ matrix, which shows the likeliness results of each SU with all other SUs. Values that are more negative in equation (6. 12) show dissimilarity of the sensing information of the user with the other users. The final correlation results make the behavior of all three categories of SUs dissimilar to each other. Correlation results of the AO and RO users largely deviate from the normal users and lie as an outlier in the result of equation (6. 12). The outlier values of MUs are further separated from the normally reporting users by using BWP method as.

6.2.2.3 BWP for MUs identification

A BWP is a simple way for the identification of outliers in any statistical data. It divides correlation values in equation (6. 12) into four equal parts. First, the result is made in ascending order and the median value is identified so that the data is divided into upper and lower half with the help of the median value. Lower and upper quartile values are calculated. An outlier in equation (6. 12) is a dispersal of data greater than 1.5 times the box away from either the lower or the upper quartile. The median value of vector $\boldsymbol{r}$ is determined as:

$$Med = \begin{Bmatrix} r_j \left(\dfrac{M+1}{2} \right), & M \ odd \\ \dfrac{1}{2} \left(r_j \left(\dfrac{M}{2} \right) + r_j \left(\dfrac{M}{2} + 1 \right) \right), & M \ even \end{Bmatrix} \tag{6. 13}$$

The first and third quartile values that contain 25^{th} and 75^{th} percentile of the data in equation (6. 12) are denoted as Q^1_{Lower} and Q^3_{Upper}. The inter-quartile value for the range of the upper and lower quartile values is measured as:

$$IQR = Q^3_{Upper} - Q^1_{Lower} \tag{6. 14}$$

Similarly, the settlements of the lower and upper limits for the detection of MUs are below:

$$L_{\lim it} = Q^1_{Lower} - 1.5(IQR) \tag{6. 15}$$

$$U_{\lim it} = Q^3_{Upper} + 1.5(IQR) \tag{6. 16}$$

After setting all parameters of the BWP, MUs are identified using the following criteria.

$$MU = \begin{Bmatrix} j^{th}, & if\ (r_j \geq U_{\lim it}\ or\ r_j \leq L_{\lim it}) \\ 0, & Otherwise \end{Bmatrix} \tag{6. 17}$$

In equation (6. 17), a user is declared malicious if its correlation score is outside the lower and higher limits of the BWP. Table 6.1-6.3, shows a BWP results of the local sensing information provided by each SU under different SNR values. The AO and RO user's present dissimilar sensing results of the PUs against the normal SUs and are easily identified and separated as MUs from the normal SUs category using BWP criteria in equation (6. 17).

Table 6. 1. Box plot of correlation result under both AO and RO users

SNR (dB)	**Min**	Q^1_{Lower}	**Median**	Q^3_{Upper}	**Max**	**IQR**	**Lower Limit**	**Upper Limit**
-30	-0.1233	0.01559183	0.02097	0.023847	0.025981	0.008255	0.003209	0.03623
-28	-0.1241	0.01502566	0.02049	0.022928	0.033197	0.007903	0.003172	0.034782
-26	-0.1296	0.01767262	0.02225	0.026410	0.029608	0.008738	0.004566	0.039517
-24	-0.1460	0.02419445	0.02566	0.030521	0.031995	0.006327	0.014703	0.040013
-22	-0.1515	0.01600466	0.02709	0.031661	0.035777	0.015657	-0.00748	0.055146
-20	-0.1768	0.0300924	0.03288	0.033382	0.038434	0.00329	0.025158	0.038317

Table 6. 2. Box plot data of correlation results under AO users only

SNR (dB)	Min	Q^1_{Lower}	Median	Q^3_{Upper}	Max	IQR	Lower Limit	Upper Limit
-30	-0.1187	0.027923	0.029733	0.033575	0.036673	0.005652	0.019445	0.042053
-28	-0.1136	0.024431	0.029003	0.032603	0.038683	0.008172	0.012172	0.044861
-26	-0.1143	0.023746	0.026274	0.033884	0.043767	0.010139	0.008538	0.049092
-24	-0.1354	0.028492	0.035867	0.040777	0.041255	0.012285	0.010063	0.059205
-22	-0.1442	0.03397	0.040021	0.042547	0.045457	0.008577	0.021104	0.055413
-20	-0.1765	0.04133	0.048643	0.052537	0.061966	0.011206	0.024521	0.069346

Table 6. 3. Box plot data of correlation results under RO users only

SNR (dB)	Min	Q^1_{Lower}	Median	Q^3_{Upper}	Max	IQR	Lower Limit	Upper Limit
-30	-0.0420	0.004687	0.00771	0.013285	0.020143	0.008598	-0.00821	0.026181
-28	-0.0418	0.006307	0.009428	0.011756	0.016341	0.005449	-0.00187	0.019929
-26	-0.0504	0.003967	0.010962	0.01545	0.021564	0.011483	-0.01326	0.032674
-24	-0.0499	0.01026	0.01173	0.013742	0.018565	0.003482	0.005036	0.018966
-22	-0.0572	0.007603	0.013448	0.017124	0.022818	0.009521	-0.00668	0.031406
-20	-0.0672	0.009589	0.017555	0.019618	0.021469	0.010028	-0.00545	0.03466

6.2.3 New Hard Fusion Decision

The detection results of MUs and system maturity in the N_0 sensing intervals leads FC to take a new hard decision in the subsequent sensing intervals.

A new MV-HFC rule based on the sensing results of the normal cooperative users by taking the detected MUs out of the global decision is given below:

$$H_1 : \sum_{\substack{j=1 \\ j \neq MU}}^{M} y_j(i) \geq K_{NEW}$$
$$H_0 : Otherwise \qquad (6.\ 18)$$

Where K_{NEW} is the new value of the MV-HFC criteria, based on the result of the normal SUs only. The FC decides in favor of H_1 based on the normal users with their detections score greater than K_{NEW}, otherwise, decision H_0 is made by the FC.

Similarly, the new AND-HFC rule is restricted to the condition based on the normal SUs reports as;

$$\begin{aligned} H_1 &: \sum_{\substack{j=1 \\ j \neq MU}}^{M} y_j(i) = M_{NEW} \\ H_0 &: Otherwise \end{aligned} \tag{6. 19}$$

The new AND-HFC rule in equation (6. 19) shows that M_{NEW} SUs has to provide PU detection information to the FC out of the M SUs to decide H_1, otherwise decision is made in favor of H_0. Here M_{NEW} is the normal SUs participation in the global decision without any RO and AO user.

A new criteria of the OR-HFC scheme after the identification and elimination of MUs at the FC is below

$$\begin{aligned} H_1 &: \sum_{\substack{j=1 \\ j \neq MU}}^{M} y_j(i) \geq 1 \\ H_0 &: Otherwise \end{aligned} \tag{6. 20}$$

Similarly, the results of the cooperative detection and false alarm probabilities $C_{d,MV-HFC}$ and $C_{f,MV-HFC}$ of the MV-HFC scheme after taking out MUs is measured as

$$C_{d,MV-HFC} = \Pr\left\{Y=1 \middle| H_1\right\} = \Pr\left\{\sum_{\substack{j=1 \\ j\neq MU}}^{M} y_j(i) \geq \left(K_{NEW}\right) \middle| H_1\right\}$$
$$C_{f,MV-HFC} = \Pr\left\{Y=1 \middle| H_0\right\} = \Pr\left\{\sum_{\substack{j=1 \\ j\neq MU}}^{M} y_j(i) \geq \left(K_{NEW}\right) \middle| H_0\right\} \quad (6.\ 21)$$

Where Y is the final decision made by the FC regarding the PU spectrum. As the OR rule take into account the value of $K_{NEW}=1$, hence

$$C_{d,OR-HFC} = 1 - \prod_{\substack{j=1 \\ j\neq MU}}^{M} \left(1-P_{d,j}\right)$$
$$C_{f,OR-HFC} = 1 - \prod_{\substack{j=1 \\ j\neq MU}}^{M} \left(1-P_{f,j}\right) \quad (6.\ 22)$$

The AND rule can be evaluated by setting $K_{NEW} = M_{NEW}$

$$C_{d,AND-HFC} = \prod_{\substack{j=1 \\ j\neq MU}}^{M} \left(P_{d,j}\right)$$
$$C_{f,AND-HFC} = \prod_{\substack{j=1 \\ j\neq MU}}^{M} \left(P_{f,j}\right) \quad (6.\ 23)$$

6.2.4 Simulation Results of the Statistical Features based technique

The simulation parameter settings are made for the CRN with total 10 cooperative SUs including both normal and malicious. Out of the two MUs, one is taken as AO and the other of the RO nature. The SNR values for simulation vary from -30 dB to -20 dB in Figure 6. 2. Duration of the sensing time interval is selected as 1 ms which is divided into 270 samples. The system was simulated for $N=1000$ sensing iterations out of which in the initial N_0 intervals FC collects information about each SU and take HFC decisions normally. MUs both AO and RO are identified in the first N_0 sensing intervals and then FC applies new criteria to detect PU based on

the selection results of the normal SUs. The RO user performed performing malicious act randomly in the $N/2$ selected sensing intervals. The system was simulated under the conditions when both AO and RO in equal numbers participate in CSS. In the first part of simulation results criteria's for the MUs detection are collected in Figure 6. 2 at different SNR regions. Figure 6. 2 shows the upper and lower limits with the result of the AO and RO users not within the range while the normal SUs results lie within the upper and lower limitation criteria set by the BWP. The correlation results of the RO user are closer to the lower limits set by the BWP which is considered to be more dangerous, while the results of the AO user is very far distant away from the lower limits set by the BWP. Detection results of these MUs were further used in improving the detection results of the PU for all three categories of HFC schemes i.e. MV-HFC, OR-HFC and AND-HFC schemes.

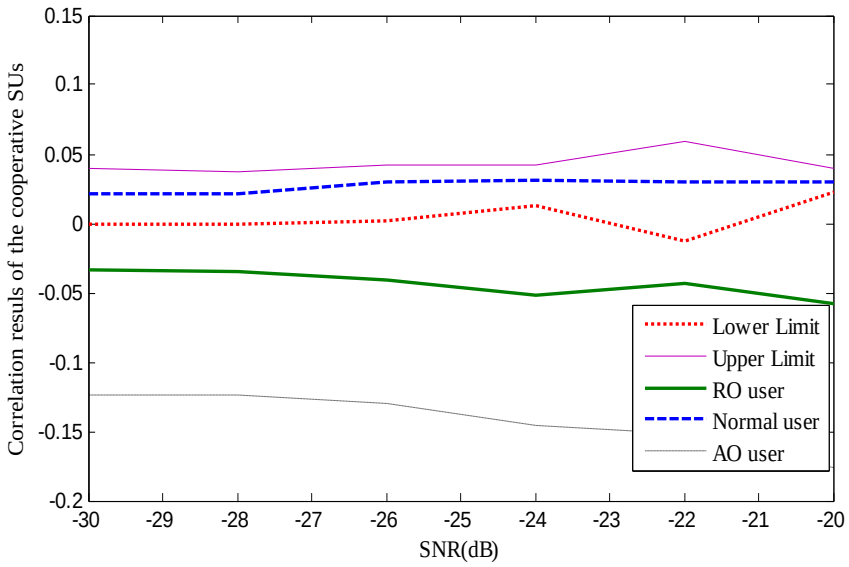

Figure 6. 2 Correlation results vs. SNR for the RO user, normal user and AO user when both RO and AO users were taken.

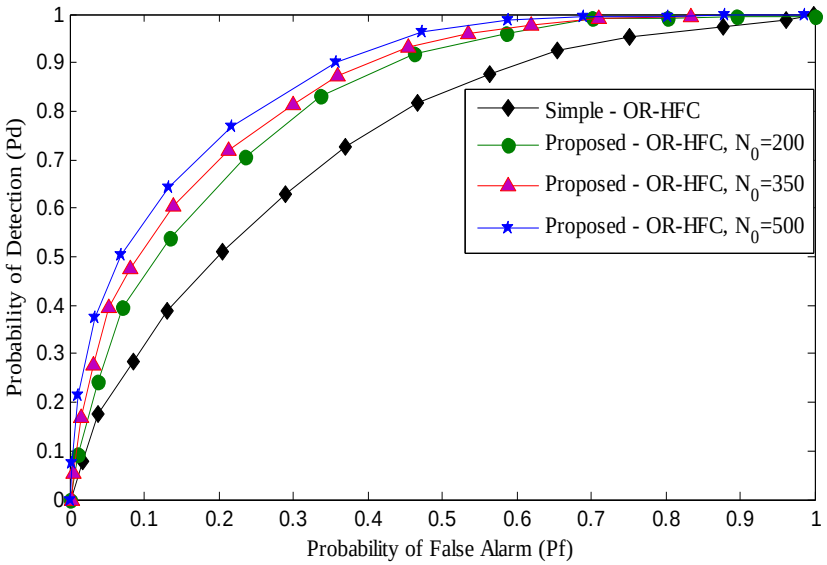

Figure 6. 3 ROC results for the simple OR-HFC and proposed OR-HFC schemes at history levels of 200, 350 and 500

ROC curve results are drawn for the OR-HFC scheme in Figure 6. 3 between the simple OR-HFC and proposed OR-HFC scheme at the different considerations of N_0. Graphical results show better detection results of the proposed OR-HFC compared with simple OR-HFC. In Figure 6. 3, performance of proposed OR-HFC scheme was compared with OR-HFC by varying the length of the user history. Results show that as the user reporting history N_0 increases from 200 to 500 the ROC result performance of the proposed OR-HFC scheme also increases. This improvement in the detection results of the proposed scheme is achieved due to more information collected about the nature of MUs at the FC. The experimentation in Figure 6. 4 is performed by testing the CSS scheme using traditional and proposed MV-HFC schemes to plot the results for the detection probability against the false alarm probability. In the given MV-HFC scheme, the total number of SUs is selected as $M/2$ at the FC, in order to take a global decision about the PU spectrum. Results collected in Figure 6. 4 show improved ROC performance of the proposed MV-HFC scheme compared with simple MV-HFC scheme at all levels of the history

collections at the FC. The proposed MV-HFC scheme is able to take both the MUs out of the voting rule in the following sensing intervals after their identifications. After the identification of abnormal SUs, if half of the normally reported users report in favor of H_1 a global decision H_1 is made, otherwise H_0 is decided by the FC. By inspecting both the results collected in Figure 6. 3 and Figure 6. 4 it is noticeable that the proposed MV-HFC scheme has better ROC results as compared with simple OR-HFC, proposed OR-HFC and simple MV-HFC schemes. The proposed MV-HDF takes global decision based on the majority of the normal SUs after discarding all the detected MUs.

The final ROC comparison in the detection and false alarm results is made in Figure 6. 5 for the proposed AND-HFC and simple AND-HFC. A significant improvement in performance is achieved for the proposed AND-HFC scheme in Figure 6. 5, which follows the proposed method for the identification and elimination of MUs out of the final AND rule. This improvement in performance is further made stronger with increasing history N_0 about the cooperative users.

Figure 6. 6, Figure 6. 7 and Figure 6. 8 compare the error probability results of the OR-HFC, MV-HFC and AND-HFC rules at different levels of average SNR. In this part of the simulation the total number of cooperative SUs is kept at 10 in the presence of 2 MUs including both AO and RO users with varying SNR. The results collected in Figure 6. 6 for the simple OR-HFC and proposed OR-HFC schemes show a reduction in the error probability of the proposed method based OR-HFC rule. The proposed OR-HFC scheme allows the FC to produce accurate decision about the PU activity with minimum error in terms of inaccurate detection of the PU. This inappropriate detection at the FC is further reduced at the FC as the SNR value increases from -30 dB to 0 dB. For a given SNR value in Figure 6. 6 these error chances further reduced with increasing number of reports about the normal and malicious users. The error probability results

are drawn for the simple MV-HFC and proposed MV-HFC schemes in Figure 6. 7. The results show better performance for the proposed MV-HFC scheme in comparison with the simple MV-HFC rule in Figure 6. 7 at all levels of the SNRs and historical information about the cooperative users. The error probability of the proposed MV-HFC scheme reduces more quickly with increasing SNR values and all levels of the historical reports about the cooperative users. The proposed method performance is more improved with increasing history reports of the users from $N_0 = 200$ to $N_0 = 500$.

At last, the error probability results are drawn for the proposed AND-HFC and simple AND-HFC against varying SNR values at different levels of the history reports. The proposed AND-HFC scheme has the ability to produce improvement in the performance against the simple AND-HFC all levels of SNR.

The error results collected in Figure 6. 6, Figure 6. 7 and Figure 6. 8 for the OR-HFC, MV-HFC and AND-HFC confirmed the superiority of the proposed MV-HFC scheme on the given environment of AO and RO category of MUs in CSS. By inspecting results in Figure 6. 6 to Figure 6. 8, performance of the proposed MV-HFC as in Figure 6. 6 is followed by an accurate sensing decision of the proposed OR-HFC scheme in Figure 6. 7, while the AND-HFC scheme in Figure 6. 8 shows the worst performance in the given environment of CSS against AO and RO categories of MUs.

Tabular and graphical results declare that the HFC outcomes are improved by using the proposed method at the FC. MUs are first identified by the proposed scheme and then take out of the global decision, in order to make the global decision more authentic with accurate decision about the PU channel.

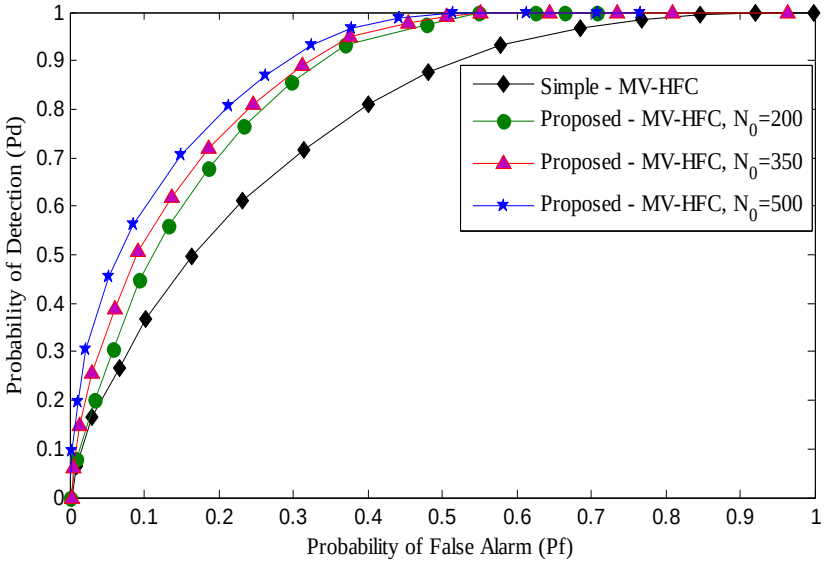

Figure 6. 4 ROC results for the simple MV-HFC and Proposed-MV-HFC schemes at different history levels of 200, 350 and 500

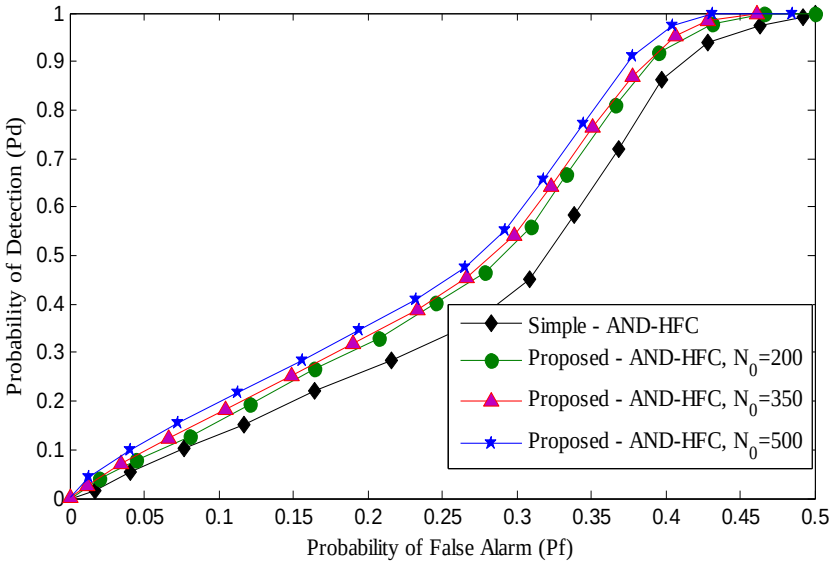

Figure 6. 5 ROC results for the simple-AND-HFC and proposed-AND-HFC schemes at different history levels of 200, 350 and 500

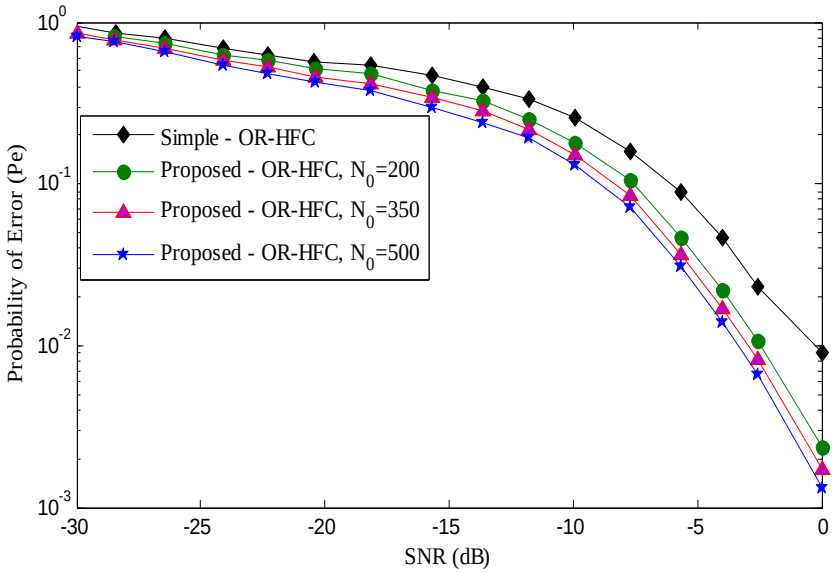

Figure 6. 6 Probability of Error (P_e) vs. SNR for the simple-OR-HFC and proposed-OR-HFC schemes at different history levels of 200, 350 and 500

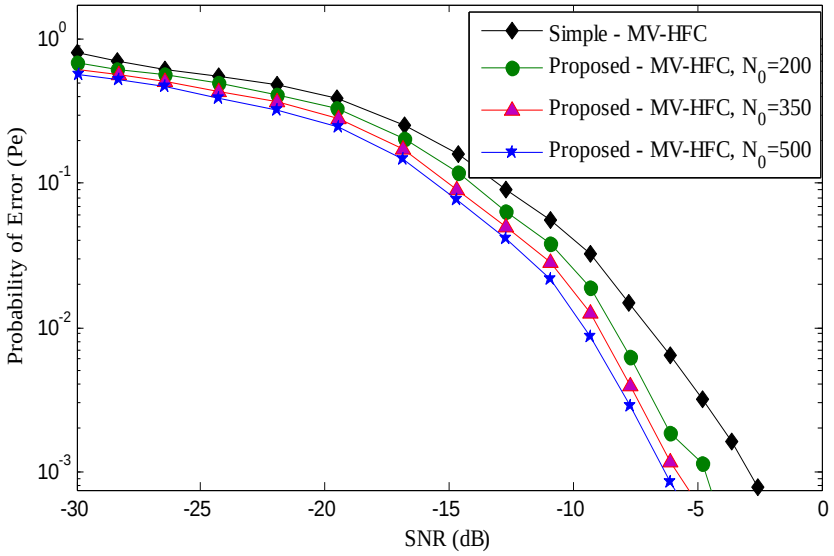

Figure 6. 7 Probability of Error (P_e) vs. SNR for the simple MV-HFC and proposed-MV-HFC schemes at different history levels of 200, 350 and 500

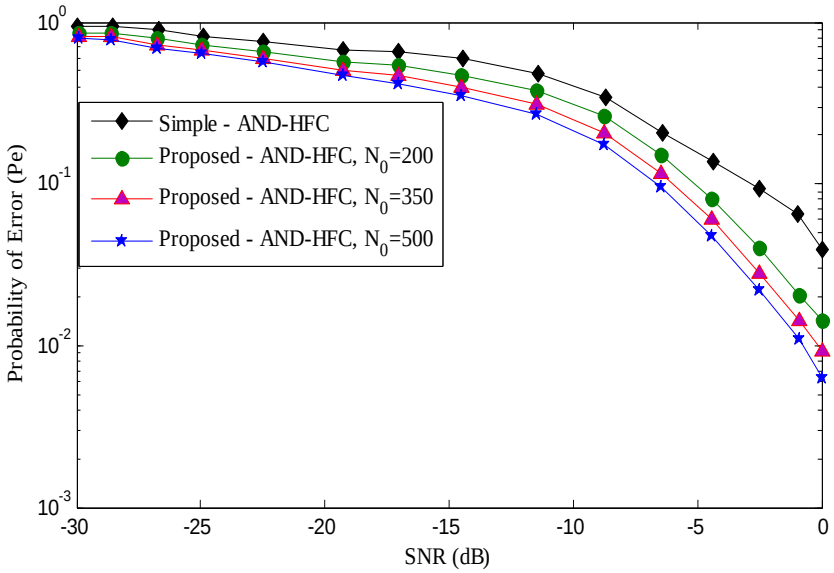

Figure 6. 8 Probability of Error (P_e) vs. SNR for the simple AND-HFC and proposed AND-HFC schemes at different history levels of 200, 350 and 500

The proposed HFC schemes are able to identify response for the detection of MUs and are able to easily distinguish both AO and RO users from the normal category of cooperative users. The FC detects and declare a user as malicious based on the BWP when correlation results are less than the lower or higher than the upper limits. The detection results for the AO user are more negative as compared with the RO and can be easily caught by the proposed scheme. RO user behavior is closer to that of the normal user, therefore, great sensitivity care for the detection of such MUs is demanding. Correlation results of the normal users are always within the limitations of the BWP under all SNR values.

6.3 Proposed system model of the OTMSD and ZS process at the FC

The flowchart of the proposed CSS model using OTMSD and ZS is shown in Figure 6. 9. In Figure 6. 9, SUs senses the certified PU channel, and forward their local energy statistics information to the FC.

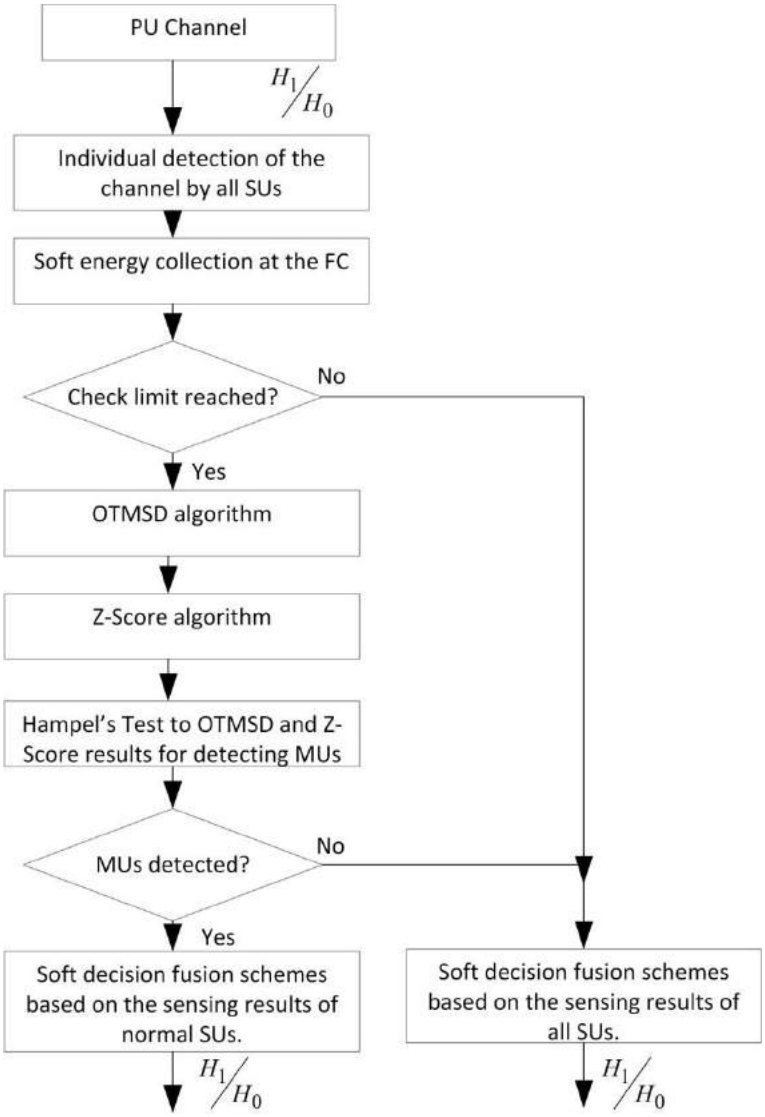

Figure 6. 9 OTMSD and ZS scheme flowchart using HT.

The center takes a global decision taking into considerations the received energy statistics of all SUs and also stores these energy observations until the establishment of enough information about each user. The OTMSD and ZS are applied to each user reports to conclude the normal and abnormal behavior of all cooperative users. The OTMSD and ZS measurement enables FC to make the results of the normally reporting users separate of all MUs. In this model we are

considering the number of normally reporting users larger in comparison with MUs, therefore, based on the OTMSD and ZS results, reported data of the AYMU, ANMU, OMU and ROMU are easily identified as outlier values. It is further noticeable that the reports of MUs were made more dissimilar as outlier values when OTMSD based scheme is utilized as compared with ZS. After the determination of OTMSD and ZS values, outlier data are picked off by following HT. The detection results of the HT declare the user as MU and a new global decision is made by the FC, with the combination of normally cooperative users to establish more accurate and reliable global decision of the PU channel.

A pseudo code of the proposed method is shown below, where each user first performs local detection. Cooperative user's score is determined using one-to-many relationship sensing distance and Z-score algorithms along-with HT for the detection of MUs and finally FC takes global decision based on the normal user reports:

For $i = 1$ **to sensing limit**
For $j = 1$ **to** M
Local detection $E_j(i)$ by the j^{th} user to the FC
End j
If $i = N_0$
---- *OTMSD and ZS at the FC*---
For $j = 1$ **to** M

$$E_{ij}^{'}(i) = \left| \left\{ \frac{\left(\sum_{j=1}^{M} (E_{ij}) - E_{ij} \right)}{(M-1)} \right\} \right|$$

$$\boldsymbol{o}_j^1 = \left| E_{ij} - E_{ij}^{'} \right|, i \in 1,...,N_0, j \in 1,...,M$$

$$\boldsymbol{o}_j^2(i) = \left| \frac{\left(E_{ij} - \mu(i) \right)}{\sigma(i)} \right|, i \in 1,...,N_0, j \in 1,...,M$$

End j
For $j = 1$ **to** M

$o_j^1 = \sum_{i=1}^{N_0}\left(o_j^1(i)\right),\ j \in 1,...,M,\ o_j^2 = \sum_{i=1}^{N_0}\left(o_j^2(i)\right),\ j \in 1,...,M$

End j

----Hampel's Test to determine MUs in $\boldsymbol{o}^1$ *and* $\boldsymbol{o}^2$ *results----*

Medians of $\left(\boldsymbol{o}^1, \boldsymbol{o}^2\right)$ as $\left(Med(\boldsymbol{o}^1), Med(\boldsymbol{o}^2)\right)$

For $j = 1$ **to** M

The median deviation of r_j^1 is determined as $\left(o_j^1 - med(\boldsymbol{o}^1)\right)$

The median deviation of r_j^2 is determined as $\left(o_j^2 - med(\boldsymbol{o}^2)\right)$

OTMSD declares the j^{th} user MU, if $\left|r_j^1\right| \geq 4.5 Med\left|r_j^1\right|$

ZS declares the j^{th} user MU, if $\left|r_j^2\right| \geq 4.5 Med\left|r_j^2\right|$

End j

End If

----EGC global decision----------

If $\dfrac{\left(\sum_{j=1,\, j\neq M_{mu}}^{M} E_j(i)\right)}{M - M_{mu}} \geq threshold$

Global decision, $G_{EGC}(i) = H_1$

Else

Global decision, $G_{EGC}(i) = H_0$

End

---MGC global decision----------

If $\sum_{j=1,\, j\neq M_{mu}}^{M} \left(w_j \times E_j(i)\right) \geq threshold$

Global decision, $G_{MGC}(i) = H_1$

Else

Global decision, $G_{MGC}(i) = H_0$

End

End sensing limit

6.3.1 Local Spectrum decisions

The sensing, statistics of all M users are stored at the FC for the N_0 sensing intervals to get more information about the nature of participating users. The history reporting matrix is the soft energy statistics observed by each SU during the N_0 intervals on behalf of all SUs as below:

$$E = \left[E_{ij} \right], i \in 1,..., N_0, j \in 1,..., M \tag{6. 24}$$

In equation (6. 24), E_{ij} is the energy statistic of the j^{th} user during the i^{th} sensing interval. The sensing information E_{ij} is the collection of the normal and MUs observations for the N_0 intervals.

6.3.2 Outlying using one-to-many sensing distance (OTMSD)

After the collection of energy information of the M users for the N_0 intervals as in equation (6. 24), FC modifies these energy reports to observe the differences in each individual sensing report with the reports provided by all other SUs. A new reporting matrix is formed on behalf of all users based on the information already collected in equation (6. 25) as:

$$E' = \left[E'_{ij} \right], i \in 1,..., N_0, j \in 1,..., M \tag{6. 25}$$

$$\text{Where } E_{ij}^{'} = \left| \left\{ \frac{\left(\sum_{j=1}^{M} E_{ij} \right) - E_{ij}}{(M-1)} \right\} \right|$$

Here $E_{ij}^{'}$ is the average of the individual soft energies reports provided by all other users while taking out the report of the j^{th} user in this averaging.

In order to determine how much the individual sensing reports of each SU is behaving differently from the average sensing results, outlying factors are measured based on the one-to-many sensing distance $\boldsymbol{o}_j^1(i)$ for the j^{th} user in the i^{th} sensing particle as:

$$\boldsymbol{o}_j^1(i) = \left| E_{ij} - E_{ij}^{'} \right|, i \in 1,...,N_0,\ j \in 1,...,M \tag{6. 26}$$

Based on the results in equation (6. 26) the total outlier scores $\boldsymbol{o}_j^1(i)$ of the j^{th} user are added to discover the total one-to-many hamming distance score for the j^{th} user in the total N_0 intervals

$$\boldsymbol{o}_j^1 = \sum_{i=1}^{N_0} \left(\boldsymbol{o}_j^1(i) \right),\ j \in 1,...,M \tag{6. 27}$$

Where $\boldsymbol{o}_j^1$ in equation (6. 27) is the total outlier score representing the sum of the absolute values of the hamming distances of the individual SU soft detection "E_{ij}" with the average detection "$E_{ij}^{'}$" of all other SUs in the i^{th} sensing interval.

The measurement in equation (6. 27) is made for all the M cooperative users and the results are collected as:

$$\boldsymbol{o}^1 = \left[\boldsymbol{o}_1^1\ \boldsymbol{o}_2^1\ \boldsymbol{o}_3^1\ ...\ \boldsymbol{o}_M^1 \right]^T \tag{6. 28}$$

Here $\boldsymbol{o}^1$ is the outline score measured on behalf of all the M users in the N_0 sensing intervals. This score is a measurement of how far the report of each SU is lying away from the average sensing reports provided by all other SUs. The result in equation (6. 28) has enabled the FC to discover the score of malicious and imperfect sensing reports of the normal SU which tries to misguide the FC final decision about the PU channel.

The HT is not susceptible to the quantity and value of outlier values, similarly it shows no limitation to the abundance of the statistical data. Therefore, HT is applied to the result of the OTMSD in equation (6. 28) to search for the false reports of MUs:

First, the value of deviation r_j^1 from the median is determined for all users as:

$$r_j^1 = \left(\boldsymbol{o}_j^1 - med\left(\boldsymbol{o}_j^1\right)\right) \tag{6. 29}$$

Here $med(o_j^1)$ is the median value of the OTMSD score o_j^1 made by all SU. A user is declared outlier (malicious user), when the following condition is satisfied:

$$M_{mu} = \begin{Bmatrix} j^{th}, & if\ \left|r_j\right| \geq 4.5Med\left|r_j^1\right| \\ 0, & otherwise \end{Bmatrix} \tag{6. 30}$$

Where $\left|r_j^1\right|$ is the absolute value of the median deviation and $Med\left|r_j^1\right|$ is the median of the absolute median deviation results.

6.3.3 Outlying using z-score

Similarly, the other outlier score measurement for each user report is made with the help of the **ZS** measurement based on the sensing report received from each SU as:

$$\boldsymbol{o}_j^2(i) = \left|\frac{\left(E_{ij} - \mu(i)\right)}{\sigma(i)}\right|, i \in 1,...,N_0,\ j \in 1,...,M \tag{6. 31}$$

Where $\mu(i) = \dfrac{\left(\sum_{j=1}^{M} E_{ij}\right)}{M}$ is the mean and $\sigma(i)$ is the standard deviation of the i^{th} energy observations of all users. $\sigma_j^2(i)$ is the z-score outlying for the j^{th} report in the i^{th} sensing interval. The result of $o_j^2(i)$ in equation (6. 31) shows how much local sensing observation of the j^{th} user is detached away from the group observations provided by all other users using z-score.

Now for guaranteeing the authenticity of each of the i^{th} reports, z-score results of the M SUs are summed for all N_0 intervals as:

$$\boldsymbol{o}_j^2 = \sum_{i=1}^{N_0} \left(\boldsymbol{o}_j^2(i) \right),\ j \in 1,...,M \tag{6. 32}$$

The total z-score of all M SUs are collected as:

$$\boldsymbol{o}^2 = \left[\boldsymbol{o}_1^2 \ \ \boldsymbol{o}_2^2 \ \ \boldsymbol{o}_3^2 \ ... \ \boldsymbol{o}_M^2 \right] \tag{6. 33}$$

The HT scheme is applied to the result of ZS in equation (6. 33) to search for the false reports of the MUs. Similarly, the value of deviation r_j^2 from the median is resolute for all cooperative users as:

$$r_j^2 = \left(o_j^2 - med\left(o_j^2 \right) \right) \tag{6. 34}$$

Here $med(o_j^2)$ is the median value of the ZS score o_j^2 made by all SUs. A user is declared outlier (malicious user), when the following condition is satisfied.

$$M_{mu} = \begin{Bmatrix} j^{th}, & if \left| r_j^2 \right| \geq 4.5 Med \left| r_j^2 \right| \\ 0, & otherwise \end{Bmatrix} \tag{6. 35}$$

Where $\left| r_j^2 \right|$ is the absolute value of the median deviation and $Med\left| r_j^2 \right|$ is the median of the absolute median deviation results.

The false data provided by all MUs are separated from the normal user data using the OTMSD and ZS proposed methods.

6.3.4 Global decision of the licensed channel

The FC combines the soft energy collection reports of all SUs before the identification of any MU for a global decision about the channel. Various soft and hard combination schemes used by the FC are EGC, MGC and majority voting as a decision criteria of the channel.

The EGC employed by the proposed method is combining the individual statistical information of all SUs by giving equal weight to each individual SU decision and summed coherently. The proposed scheme enables EGC to ignore energy statistics of the identified MU in the combination. The summation is compared with the threshold to decide the license user spectrum by the EGC as:

$$G_{EGC}(i)=\begin{Bmatrix} H_1: \dfrac{\left(\sum\limits_{j=1,\, j\neq MU}^{M} E_j(i)\right)}{M-MU} \geq \gamma \\ H_0: \ otherwise \end{Bmatrix} \tag{6. 36}$$

The cooperative detection and false alarm probabilities P_{d_EGC} and P_{f_EGC} made by the EGC scheme based on its global decision about the PU spectrum are as:

$$\begin{aligned} P_{d\_EGC} &= \Pr\left\{ \frac{\left(\sum\limits_{j=1,\, j\neq MU}^{M} E_j(i)\right)}{M-MU} \geq \gamma \,\middle|\, H_1 \right\} \\ P_{f\_EGC} &= \Pr\left\{ \frac{\left(\sum\limits_{j=1,\, j\neq MU}^{M} E_j(i)\right)}{M-MU} \geq \gamma \,\middle|\, H_0 \right\} \end{aligned} \tag{6. 37}$$

In MGC scheme, each receiving signal branch is multiplied with a weighed function proportional to the branch gain. Branches with strong signal are further amplified while weak signals are attenuated by these weights. The idea to boost the strong signal component and attenuating weak components as in MGC diversity is exactly the same as that of filtering and signal weighting in the matched filter receiver. Similarly, the MGC scheme at the FC assign higher weights to the decision of the SUs with higher SNR values and low weight to the decision of SUs with low SNR values as:

$$G_{MGC}(i) = \begin{Bmatrix} H_1: & \sum_{j=1, j\neq MU}^{M} \left(w_j \times E_j(i) \right) \geq \gamma \\ H_0: & otherwise \end{Bmatrix} \tag{6. 38}$$

$$\text{Where } w_j = \frac{\eta(j)}{\sum_{j=1}^{M} \eta(j)}$$

The cooperative detection and false probabilities of the MGC scheme are measured based on the individual sensing reports as:

$$\begin{aligned} P_{d\_MGC} &= \left\{ \left(\sum_{j=1, j\neq MU}^{M} \left(w_j \times E_j(i) \right) \geq \gamma \right) \middle| H_1 \right\} \\ P_{f\_MGC} &= \left\{ \left(\sum_{j=1, j\neq MU}^{M} \left(w_j \times E_j(i) \right) \geq \gamma \right) \middle| H_0 \right\} \end{aligned} \tag{6. 39}$$

6.3.4 Simulations Results of the OTMSD and ZS process

For simulating the Cognitive Radio Network, parameters are set with 10 and 14 total cooperative SUs. The MUs participating in the CSS are deliberately selected as to the nature of AYMU, OMU, ROMU and OMU. The system is simulated under the average SNR -30 dB to 9 dB and -

36 dB to 3dB. The sensing time for each SU is selected as 1 ms containing 270 samples in each sensing interval. Total sensing intervals for the cooperative users are selected as 200. The ROMU users in this work are performing malicious behavior probabilistically in the sensing N intervals.

The performance of the proposed soft combination scheme is compared with traditional soft combination schemes like EGC and MGC schemes in 6 different cases as below.

Case 1: In the first case ROC performance of traditional EGC and MGC schemes is compared with the proposed EGC and MGC using OTMSD and ZS methods for the detection and avoidance of MUs in the global decision. The total number of cooperative SUs is selected 10 in the presence of AYMU users only. First, the number of the AYMU user has taken 1 in the total 10 SUs and then the total AYMU user number has increased to 2. Results show that in the presence of 1 AYMU user out of total M SUs ROC result of the proposed EGC using OTMSD scheme is for the detection of MUs is the highest of all. The result of the proposed EGC-OTMSD is followed by the MGC-OTMSD with better ROC performance in comparison with simple EGC and MGC schemes. The EGC and MGC schemes using ZS method produce high detection and less false alarm results in comparison with simple EGC and MGC in the presence of 1 AYMU user. Among the simple EGC and MGC schemes, the EGC performance is dominating the ROC of the simple EGC in Figure 6. 10 when only 1 AYMU user delivers always yes reports to the FC. When the number of MUs has increased to 2 in Figure 6. 10 the simple EGC and MGC with no mechanism of MUs is highly affected by the increasing number of AYMU users. In the presence of 2 AYMU users in Figure 6. 10, OTMSD based EGC and MGC schemes showed better detection results with minimum false alarm. The OTMSD based EGC and MGC results are followed by the soft combination schemes using the ZS method in detecting MUs and taking

a global decision about the channel. The ROC performance of the traditional EGC and MGC schemes is getting worse among all with increasing number of MUs. This case also clarifies the fact that EGC scheme produces suitable PU detection results under both OTMSD and ZS schemes. The proposed EGC scheme performance using OTMSD and ZS is followed by the MGC scheme using OTMSD and ZS schemes. The simple EGC and MGC performance is the lowest of all simulation results under both 1 and 2 AYMU users.

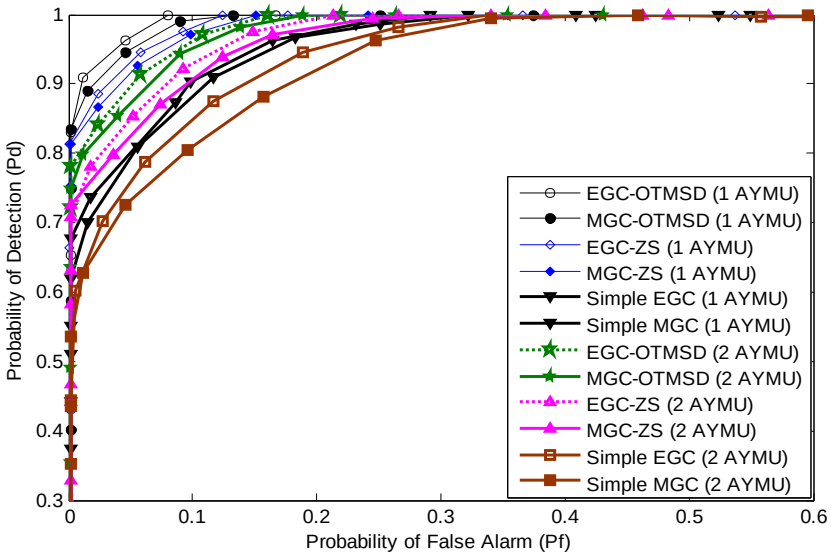

Figure 6. 10 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS schemes with 1 and 2 AYMU user only

Case 2: In this part of the simulation, ROC comparison is made between the traditional EGC and MGC schemes with proposed OTMSD and ZS based EGC and MGC schemes in Figure 6. 11. The nature of malicious users is considered an ANMU user in this work sending an always free status of the PU channel to the FC. The system was simulated with detection and false alarm results obtained in presence of both 1 and 2 ANMU users with a total of 10 cooperative SUs. The ROC performance of the proposed EGC and MGC schemes using OTMSD and ZS schemes and simple EGC and MGC schemes in the presence of AYMU is almost similar to that of case 1. In

the presence of ANMU the first case ROC performance of traditional EGC and MGC schemes are compared with the soft combination schemes using OTMSD and ZS methods. When there is 1 and 2 ANMU participate in the CSS, the performance of the EGC scheme using OTMSD and ZS is superior to the MGC scheme using OTMSD and ZS. The result obtained for the EGC-OTMSD is followed by the MGC-OTMSD under both 1 and 2 ANMU users. The proposed EGC-OTMSD and MGC-OTMSD are closely matched by the proposed EGC-ZS and MGC-ZS schemes that use the ZS score for the detection of MUs and to further take final decision based on the soft energy information of the normally reporting users only.

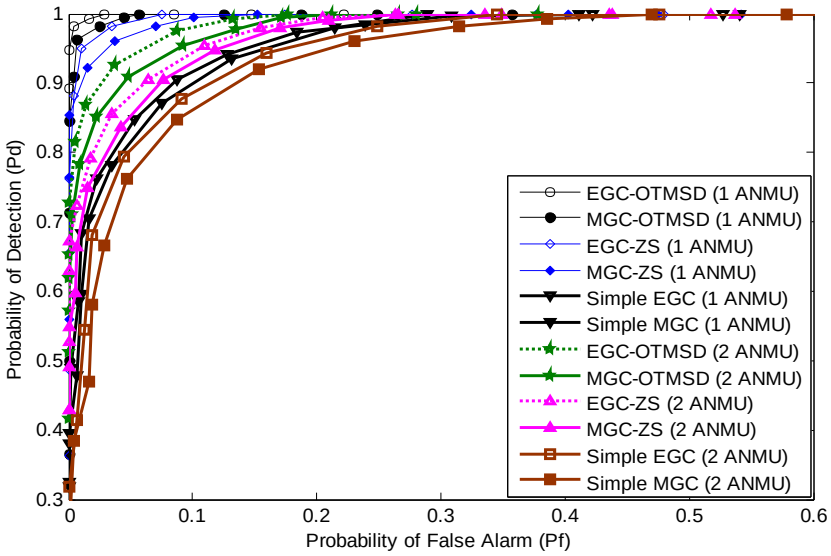

Figure 6. 11 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS schemes with 1 and 2 ANMU users only

Case 3: In the third case as in Figure 6. 12 the nature of MUs is changed to OMU which always negate the actual status of the PU activity. Detection probability results are plotted against the false alarm probability for the traditional schemes, proposed OTMSD and ZS based schemes in Figure 6. 12. In Figure 6. 12 the simple EGC has shown better performance in comparison with simple MGC scheme in the presence of both 1 and 2 OMU category of MUs. The MGC scheme

following OTMSD and ZS method for the avoidance of MUs in CSS showed improved ROC results among all with better defense against the activity of the OMU users. MGC-OTMSD and MGC-ZS results were closely matched by the EGC-MMZ and EGC-ZS schemes during both 1 and 2 OMU user scenario. The result in Figure 6. 12 also shows the effect of OMU users affecting the performance of simple EGC and MGC schemes in which simple MGC has shown poor performance in the presence of OMU users unlike the case when AYMU and ANMU user were participating in CSS.

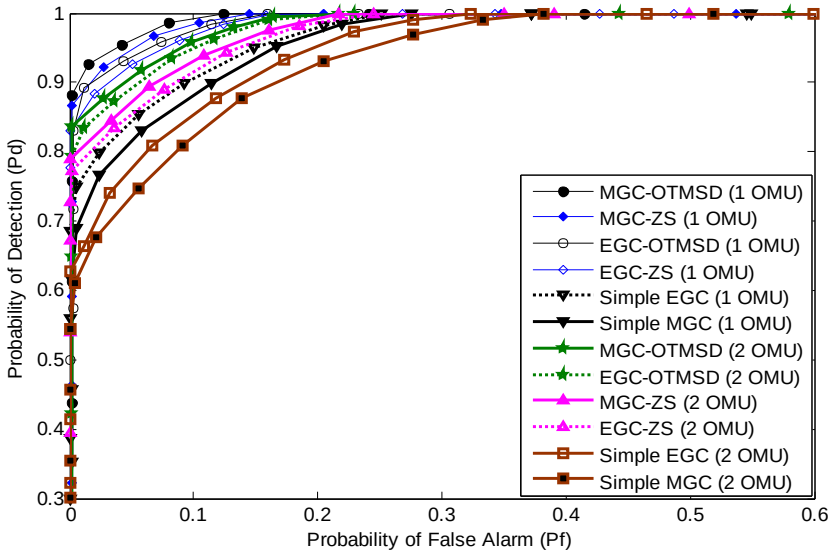

Figure 6. 12 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS schemes with 1 and 2 OMU users only

Case 4: Here detection and false alarm results are obtained for the simple soft combination schemes and proposed OTMSD and ZS based soft fusion combination schemes in the presence of ROMU category of MUs. Results are obtained for the proposed and traditional soft combination schemes in Figure 6. 13 under both 1 and 2 ROMU cooperative users. In Figure 6. 13 the OTMSD based MGC has better ROC results among all under both 1 and 2 ROMU user scenario. The MGC-OTMSD results are followed by the EGC-OTMSD results producing better

ROC results in comparison with MGC-ZS and EGC-ZS schemes. Unlike the participation of the AYMU, ANMU and OMU participation in CSS the simple MGC scheme shows better detection and minimize false alarm results in comparison with simple EGC schemes under both 1 and 2 ROMU participation in the CSS.

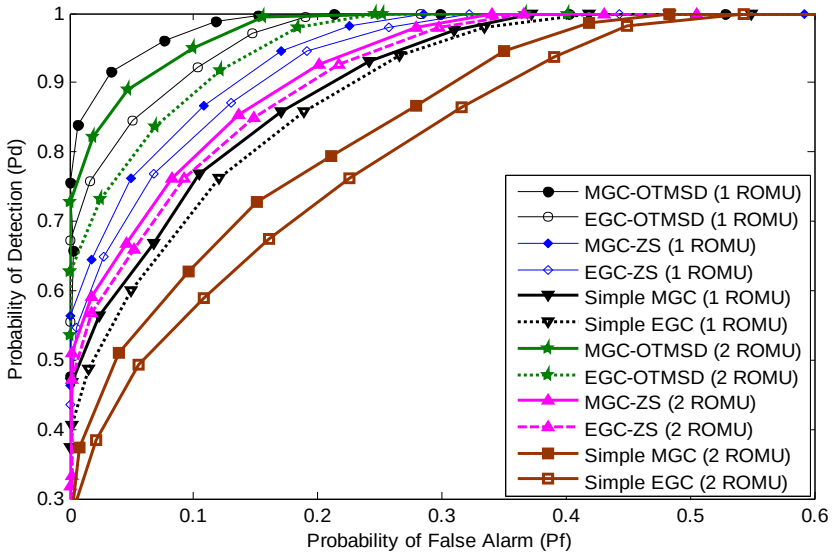

Figure 6. 13 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS schemes with 1 and 2 ROMU users only

Case 5: In this case, detection and false alarm results are obtained for the proposed and simple soft combination schemes in the presence of all MUs in Figure 6. 14. In this part of the simulation the total number of MUs is selected as 4 i.e. AYMU, ANMU, OMU and ROMU delivering false spectrum reports to the FC among the total of 10 cooperative SUs. ROC results are obtained first with an average SNR of -10.5 dB and -16.5 dB under a fixed total number of 10 cooperative SUs. At the average SNR of -16.5 dB, MGC showed superior performance to EGC scheme while using both OTMSD and ZS. Similarly, in Figure 6. 14 at -16.5dB ROC results of the MGC-MMZ and MGC-ZS are followed by the EGC-MMZ and EGC-ZS. The simple EGC scheme provides the lowest performance of the ROC among all. When the average

SNR is increased from -16.5 dB to -10.5 dB results of the proposed MGC-OTMSD and MGC-ZS schemes degrade in comparison with proposed EGC-OTMSD and EGC-ZS scheme. In Figure 6. 14 increasing average SNR from -16.5 dB to -10.5 dB results in improving detection probability and lowering false alarm for the simple EGC scheme in comparison with the simple MGC scheme.

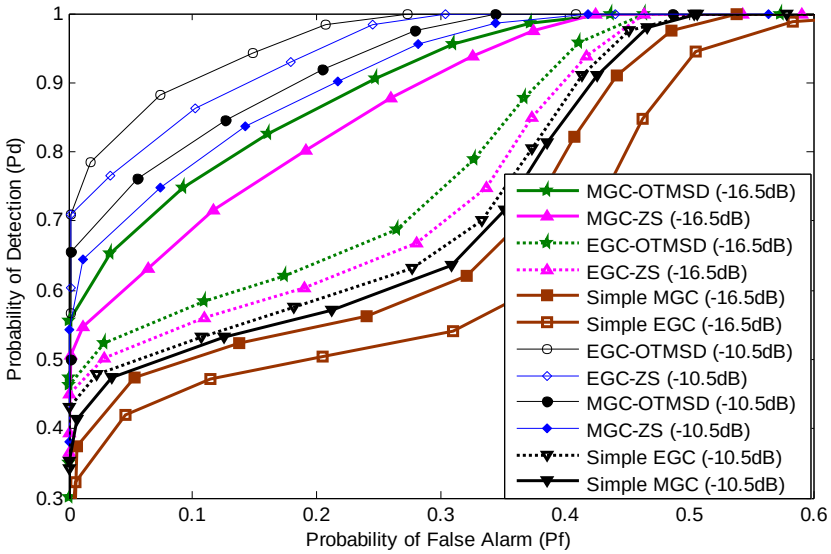

Figure 6. 14 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS with all MUs and different average SNRs (-10.5 dB, -16.5 dB)

Case 6: In Figure 6. 15 a comparison is made for all schemes at different level of cooperative SUs. The results are plotted for the CSS in the presence of 4 MUs including AYMU, ANMU, OMU and ROMU. First detection and false alarm comparison in the presence of total 10 cooperative SUs and 4 MUs and then the total number of cooperative SUs are increased to 14. The ROC results in Figure 6. 15 when total 10 cooperative SUs participate in CSS in the presence of 4 MUs generate better results for the EGC-OTMSD and EGC-ZS in comparison with MGC-OTMSD and EGC-ZS. The Simple MGC is able to provide, the better ROC results as compared with the simple EGC scheme in this part of the simulation. When the number of total

cooperative SUs was increased to 14 performances of the MGC-OTMSD and MGC-ZS improves in comparison with EGC-OTMSD and EGC-ZS with increasing number participating users. Similarly, with increasing number of total cooperative users' performance of the simple EGC scheme degrades as compared with a simple MGC scheme which provides an improvement in the detection performance with a reduced in the false alarm probability.

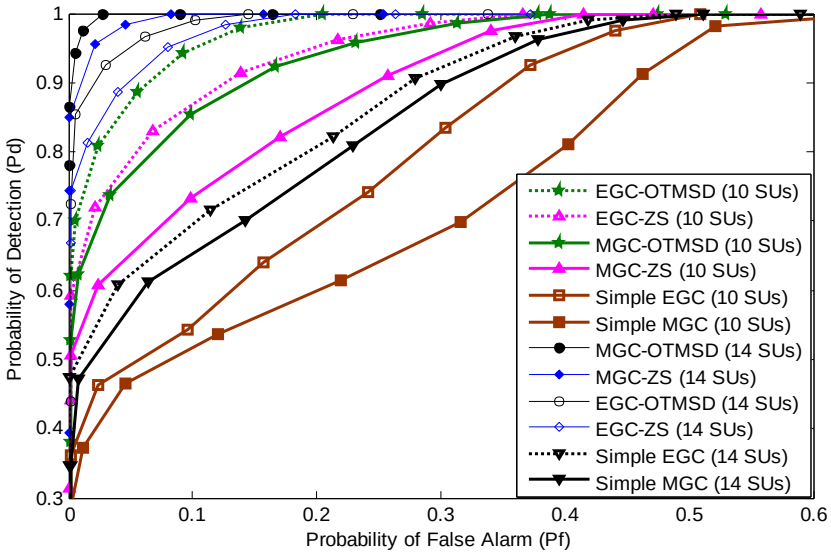

Figure 6. 15 Probability of Detection vs. Probability of False Alarm for the simple EGC, simple MGC, EGC-OTMSD, EGC-ZS, MGC-OTMSD and MGC-ZS with all MUs and different number of cooperative SUs (10, 14)

6.4 Summary

Efficient and on-time detection of MUs in a CSS environment is necessary, in order to avoid FC to conclude erroneous recommendations regarding the PU spectrum occupancy. The proposed AND-HFC, OR-HFC and MV-HFC schemes used by the FC take sensing reports from all SUs and combine them for a more concrete decision in the presence of MUs. Decision results of these HFC schemes are shaped more reliable by identifying first AO and RO using combination of

correlation and BWP to declare new criteria for the detection of PUs without consideration of abnormal users.

This work focuses on improving the functioning of the cooperative spectrum using OTMSD and ZS methods. Based on the received energy statistics of all users, OTMSD and ZS schemes at the FC are able to reduce the effect of the MUs in authenticating the FC decision of the PU existence. FC combines the diversify sensing reports of all SUs using proposed EGC and MGC decision to take a global decision about the licensed user activity. The OTMSD and ZS are able to overcome the effects of OMU, ROMU, AYMU and ANMU categories of MUs followed in the soft and hard combinations to decide accurately. Simulation consequences reflect the superiority and authenticity of the proposed methodology in producing more accurate and reliable decisions for the EGC and MGC soft fusion combination schemes in CSS.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

Cognitive radio enables SUs to utilize vacant spectral holes of the PUs. SUs have to effectively detect activity in the license user spectrum to declare the spectrum as free or occupied by the licensed users. An improper detection of the PU spectrum may result in interference to the PU transmission by the opportunistic SUs.

The sensing ability of SU is severely reduced in the fading and shadowing environment. Therefore, it is possible that the decision made by an individual SU may not be able to produce accurate sensing performance. Few SUs cooperatively sensing and sharing their individual sensing with a common point, that is, fusion center, leads to best estimation outcomes. CSS allows more than one receiver few wavelengths apart under different fading environment to sense the license user spectrum. These cooperative schemes are able to create detection results with high authenticity in the fading and shadowing environment.

Although CSS can accurately sense compared to an individual SU, but the performance of cooperation is reduced when MUs in cooperation share false spectrum information with the FC. Therefore, proper detection and deletion of MU reports at the FC is necessary for improved performance.

This dissertation is divided into three parts: In the first part of the dissertation an old technique of the KL divergence [16],[17],[152] with added analysis is proposed along with a novel one-to-many relationship based KL divergence to mitigate the effect of MUs at the FC. The proposed work considered the participation of always yes, always no, opposite and random opposite categories of MUs in a CSS. PDF of all cooperative users are determined first. The probability distribution measured based on the received energy of the MUs is not similar to the distribution of the normally cooperative users. In the first part of the KL divergence method, FC measures the KL divergence against each user and informs FC about its KL divergence measurements. Each cooperative user compares the KL divergence score achieved by its sensing performance with a threshold and report mean samples of the previous reported energies under both the present and absence hypothesis. In the next section of this part, as the KL divergence measurement of an individual user is not reliable, therefore, KL divergence is determined based on the mean and variance results of the one to many relationship based sensing notifications. The final KL measurement is utilized to assign weights to the SUs reports, which allow MUs to receive lower weights as compared to the normally cooperative users.

In the second part, heuristic techniques are used, i.e. GA and PSO algorithms [23],[24] as a novel techniques to make a decision of the PU channel in the presence of MUs. DSND algorithm [20] is first employed to determine abnormal SUs and minimum mean and z score is used as a fitness function for identifying accurate spectrum sensing information received from all cooperative users. Simulation results demonstrate effectiveness of the proposed soft and HFC schemes using GA and PSO with high detection and minimum false alarm, which results in an overall reduction in the error probability with improved spectrum sensing in cognitive radio network with

malicious users using soft computing as compared with the traditional EGC, MGC and MV-HFC schemes [9],[18],[19],[21],[22].

The impact of MUs in CSS is further reduced in the third part by using a novel statistical methods for the identification before taking any global decision. In this part, correlation is determined between the sensing statistics of individual user and the sensing information provided by all other users. As MUs provide dissimilar sensing data to the FC compared to the normal users, therefore, the correlation measured against MUs is notified as an outlier in the sensing information received from all SUs. The outliers are further separated and identified using BWP and HT methods [25]-[30]. Simulation results shows improved performance for the OTMSD-MGC, OTMSD-EGC, ZS-EGC, ZS-EGC, logical OR, logical AND and majority voting schemes with high detection and low false alarms at different levels of MUs, SNRs and history levels of the participating users [9],[18],[19], [21],[22].

7.2 Future works

Future directions for extending the work are as follows.

1. This study focuses on the spectrum sensing in cognitive radio network with malicious users using soft computing and statistical techniques, further analysis of the spectrum resource allocation in the presence of malicious users is not investigated
2. To highlight avenues for further research in the same area this study has limited analysis of the different fusion schemes in the presence of always Yes, always No, opposite and random opposite categories of MUs to sense merely one PU spectrum. The proposed scheme could be further enhanced for sensing more than one PU spectrums with

introducing PUEA category of MU, resembling behavior of the PU to misguide other SUs.

3. An Adaptable and dynamic threshold adjustment scheme can be utilized for PU detection instead of keeping static threshold scheme that may give a more optimized result.
4. Results obtained for the GA and PSO algorithms can be compared with other heuristic techniques i.e. Differential Evolution (DE), Cuckoo search algorithm, fuzzy logic and neural computing methods.
5. Defense of the cluster based CSS in the presence of MUs can also be investigated. Compressed sensing can be utilized in the future work to reduce the sensing time with better detection results in the presence of MUs.
6. An OFDM based CSS using different number of the orthogonal subcarrier for sensing and transferring the reports to other SUs and FC can also be investigated. The employment of OFDM in CSS is useful as each subcarrier in use by the SUs experience different effects under the fading and shadowing environment.

References

[1]. S. Haykin, “Cognitive radio: Brain-empowered Wireless Communications,” *IEEE J. Sel. areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[2]. A. Ghasemi and E. S. Sousa, “Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs,” *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 32–39, 2008.

[3]. S. Haykin, D. J. Thomson, and J. H. Reed, “Spectrum Sensing for Cognitive Radio,” *Proc. IEEE*, vol. 97, no. 5, pp. 849–877, 2009.

[4]. E. Axell, G. Leus, E. G. Larsson, and H. V. Poor. "Spectrum Sensing for Cognitive Radio : State-of-the-art and Recent Advances," In *IEEE Signal Processing Magazine*. 2012; vol. 29, no. 3, pp.101–116. DOI:10.1109/MSP.2012.2183771.

[5]. S. M. Mishra, A. Sahai, and R. W. Brodersen, “Cooperative Sensing among Cognitive Radios,” in *Proc. IEEE International Conference on Communications*, 2006, vol. 4, no. c, pp. 1658–1663.

[6]. H. V. Van and I. Koo, “A Sequential Cooperative Spectrum Sensing Scheme Based On Cognitive User Reputation,” *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1147–1152, 2012.

[7]. H. Guo, S. Member, W. Jiang, and W. Luo, “Linear Soft Combination for Cooperative Spectrum Sensing in Cognitive Radio Networks,” *IEEE Communications Letters*, vol. pp, no. 99, pp. 1–1, 2017.

[8]. M. Akbari and M. Ghanbarisabagh, “A Novel Evolutionary-Based Cooperative Spectrum Sensing Mechanism for Cognitive Radio Networks,” *Wireless Personal Communications*, vol. 79, no. 2, pp. 1017–1030, 2014.

[9]. J. So, W. Sung. Group-based Multibit Cooperative Spectrum for Cognitive Radio Networks. *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp.10193–10198, 2016. DOI:10.1109/TVT.2016.2536659

[10]. Y. L. Lee, W. K. Saad, A. A. B. El-Saleh, and M. . Ismail, “Improved Detection Performance of Cognitive Radio Networks in AWGN and Rayleigh Fading Environments,” *Journal of Applied Research and Technology*, vol. 11, no. 3, pp. 437–446, 2013.

[11]. W. Ejaz, G. Hattab, T. Attia, M. Ibnkahla, F. Abdelkefi, and M. Siala" Joint Quantization and Confidence-based Generalized Combining Scheme for Cooperative Spectrum Sensing" *IEEE Systems Journal*, vol. 12, no. 2, pp.1909–1920, 2018. DOI: 10.1109/JSYST.2016.2615019.

[12]. A. A. Sharifi, M. Sharifi, and M. J. M. Niya, "Secure Cooperative Spectrum Sensing Under Primary User Emulation Attack In Cognitive Radio Networks: Attack-Aware Threshold Selection Approach," *AEU - International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 95–104, 2016.

[13]. L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending Against Byzantine Attack in Cooperative Spectrum Sensing : Defense Reference and Performance Analysis," *IEEE Access*, vol. 4, pp. 4011–4024, 2016.

[14]. F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and Counteracting Statistical Attacks in Cooperative Spectrum Sensing," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1806–1822, 2012.

[15]. A. A. Sharifi and J. M. Niya, "Securing Collaborative Spectrum Sensing Against Malicious Attackers in Cognitive Radio Networks," *Wireless Personal Communications*, vol. 90, no. 1, pp. 75–91, 2016.

[16]. I. Koo, Vu-Van Hiep, "A Robust Cooperative Spectrum Sensing Based on Kullback-Leibler Divergence," *IEICE Transactions on Communications*, vol. E95–B, no. 4, pp. 1286–1290, 2012.

[17]. I. Koo, "Malicious User Suppression Based on Kullback-Leibler Divergence for Cognitive Radio," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 6, pp. 1133–1146, 2011.

[18]. D. Hamza, S. Aïssa, and G. Aniba, "Equal Gain Combining for Cooperative Spectrum Sensing In Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4334-4345, 2014. DOI: 10.1109/TWC.2014.2317788

[19]. M. Emami, H. Zarrabi, J. J. Jung, "A Soft Cooperative Spectrum Sensing in the Presence of most Destructive Smart PUEA Using Energy Detector, " *Concurrency Computation Practice and Experience* 2018, vol. 30: e4524. DOI:10.1002/cpe.4524.

[20]. H. Li and Z. Han, "Catch Me if You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Transactions on*

Wireless Communications, vol. 9, no. 11, pp. 3554–3565, 2010.

[21]. T. Jiang and D. Qu, "On Minimum Sensing Error with Spectrum Sensing Using Counting Rule in Cognitive Radio Networks," in *Proceedings of the 4th International ICST Conference on Wireless Internet*, 2008, pp. 1–9.

[22]. D. B. Teguig, B. Scheers, and V. L. Nir, "Data Fusion Schemes for Cooperative Spectrum Sensing in Cognitive Radio Networks," in *2012 Military Communications and Information Systems Conference, MCC 2012*, 2012, no. 1, pp. 104–110.

[23]. S. Bhattacharjee, "Optimization of Probability of False alarm and Probability of Detection in Cognitive Radio Networks Using GA," in *Proc. of ReTIS'15 - 2nd IEEE International Conference on Recent Trends in Information Systems*, 2015, pp. 53–57.

[24]. M. Taha, D. Alnadi. "Threshold Adaptation in Spectrum Sensing for Cognitive Radio Using Particle Swarm Optimization, "In *International Conference On Control, Engineering & Information Technology (Ceit'14) Proceedings*, 2014; pp. 223-228.

[25]. S. S. Kalamkar, P. K. Singh, and A. Banerjee, "Block Outlier Methods for Malicious User Detection in Cooperative Spectrum Sensing," in *IEEE Vehicular Technology Conference*, 2015, vol. 2015–Janua, no. January, pp. 1–5.

[26]. A. Li, M. Feng, Y. Li, and Z. Liu, "Application of Outlier Mining in Insider Identification Based on Boxplot Method," in *Procedia Computer Science, Elsevier*, vol. 91, no. May 2010, pp. 245–251, 2016.

[27]. H. Liu, S. Shah, and W. Jiang, "On-line Outlier Detection and Data Cleaning," *Computers and Chemical Engineering*, vol. 28, no. 9, pp. 1635–1647, 2004.

[28]. F. R. Hampel, "The influence curve and its role in robust estimation," *Journal of the American Statistical Association*, vol. 69, no. 346, pp. 383–393, 1974.

[29]. F. R. Hampel, "A General Qualitative Definition of Robustness," *The Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1887–1896, 1971.

[30]. R. K. Pearson, "Outliers in Process Modeling and Identification," *IEEE Transactions on Control Systems Technology*, vol. 10, no. 1, pp. 55–63, 2002.

[31]. M. A. McHenry and D. McCloskey, "Spectrum Occupancy Measurements: Chicago, Illinois, *Technical report*, November 16-18, 2005.

[32]. T. Erpek, K. Steadman, and D. Jones, "Spectrum Occupancy Measurements: Dublin, Ireland," *Technical Report, Shared Spectrum Company* Nov 2007. Available at:

http://www. sharedspectrum. com, April 16-18, 2007.

[33]. T. A. Weiss and F. K. Jondral, "Spectrum Pooling: an Innovative Strategy for the Enhancement of Spectrum Efficiency," *IEEE. Commun. Mag*, vol. 42, no. 3, pp. S8–14, 2004.

[34]. J. Zander, "Radio Resource Management in Future Wireless Networks: Requirements and Limitations," *IEEE Commun. Mag*, vol. 35, no. 8, pp. 30–36, 1997.

[35]. S. Sengupta and M. Chatterjee, "Designing Auction Mechanisms for Dynamic Spectrum Access," *Mob. Networks Appl.*, vol. 13, no. 5, pp. 498–515, 2008.

[36]. F. C. C. S. P. T. Force, "FCC Report of the Spectrum Efficiency Working Group, November 2002." 2009.

[37]. A. Elahi, "Interference Issues in Cognitive Radio Networks," *Ph.D. dissertation, Department of Elect. Eng., International Islamic University*. Islamabad, 2017.

[38]. M. H. Rehmani, Cognitive Radio Sensor Networks: Applications, Architectures, and Challenges. *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, 2014.

[39]. M. Bkassiny, Y. Li, and S. K. Jayaweera, "A Survey On Machine-Learning Techniques in Cognitive Radios," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1136–1159, 2013.

[40]. K. Kumar, A. Prakash, and R. Tripathi, "Spectrum Handoff in Cognitive Radio Networks: A Classification and Comprehensive Survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 161–188, 2016.

[41]. J. Mitola and G. Q. Maguire, "Cognitive radio: Making Software Radios more Personal," *IEEE Pers. Commun*, vol. 6, no. 4, pp. 13–18, 1999.

[42]. J. Mitola, "Cognitive radio for Flexible Mobile Multimedia Communications," in *Mobile Multimedia Communications, 1999.(MoMuC'99) 1999 IEEE International Workshop*, 1999, pp. 3–10.

[43]. B. Wang and K. J. R. Liu, "Advances in Cognitive Radio Networks: A Survey," *IEEE J. Sel. Top. Signal Process*, vol. 5, no. 1, pp. 5–23, 2011.

[44]. K. C. Chen, Y. J. Peng, N. Prasad, Y. C. Liang, and S. Sun, "Cognitive Radio Network Architecture: Part I-General Structure," in *Proceedings of the 2nd international conference on Ubiquitous information management and communication*, 2008, pp. 114–119.

[45]. J. Mitola, "Cognitive Radio Architecture Evolution," *Proc. IEEE*, vol. 97, no. 4, pp. 626–

641, 2009.

[46]. P. S. Aizaz Zainab, "A Survey of Cognitive Radio Reconfigurable Antenna Design and Proposed Design using Genetic Algorithm," in *2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2016, pp. 1–6.

[47]. A. Sahai, N. Hoven, and R. Tandra, "Some Fundamental Limits on Cognitive Radio," in *Allerton Conference on Control, Communications, and Computation*, 2004, pp. 1662–1671.

[48]. R. Zheng, J. Chen, M. Zhang, Q. Wu, J. Zhu, and H. Wang, "A Collaborative Analysis Method of User Abnormal Behavior Based on Reputation Voting in Cloud Environment," *Future Generation Computer Systems*, vol. 83, pp. 60–74, 2018.

[49]. G. Vinodhini and V. Meena, "Detection and Prediction of Abnormal Users in Cloud Network," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 1–7, 2016.

[50]. S. Bhattacharya, S. H. Qazi, J. S. Surekha, J. G. Shruthi, and R. Sanjeetha, "DDoS Attack Detection Using Cooperative Overlay Networks and Gossip Protocol," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 6, pp. 3614–3617, 2015.

[51]. G. Zhang and M. Parashar, "Cooperative Mechanism Against DDoS attacks," in *Proceedings of IEEE International Conference on Information and Computer Science (ICICS 2004)*, 2004, pp. 1–14.

[52]. G. An and J. S. Park, "Packet Marking Based Cooperative Attack Response Service for Effectively Handling Suspicious Traffic," *LNCS, Springer*, vol. 4318, pp. 182–195, 2006.

[53]. S. Teng, H. Du, W. Zhang, X. Fu, and X. Li, "A Cooperative Network Intrusion Detection Based on Heterogeneous Distance Function Clustering," in *14th International Conference on Computer Supported Cooperative Work in Design*, 2010, pp. 140–145.

[54]. X. Meng and S. Ren, "An Outlier Mining-Based Malicious Node Detection Model for Hybrid P2p Networks," *Computer Networks*, vol. 108, no. 2016, pp. 29–39, 2016.

[55]. R. K. Upadhyay and S. Kumari, "Detecting Malicious Chaotic Signals in Wireless Sensor Network," *Physica A: Statistical Mechanics and its Applications*, vol. 492, pp. 1129–1152, 2018.

[56]. G. Vijay, E. B. A. Bdira, and M. Ibnkahla, "Cognition In Wireless Sensor Networks: A Perspective," *IEEE Sensors Journal*, vol. 11, no. 3, pp. 582–592, 2011.

[57]. Q. Zhang, T. Yu, and P. Ning, "A Framework for Identifying Compromised Nodes in Wireless Sensor Networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, no. 3, pp. 1–35, 2006.

[58]. A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A Survey on Trust Based Detection and Isolation of Malicious Nodes in Ad-Hoc And Sensor Networks," *Frontiers of Computer Science*, vol. 9, no. 2, pp. 280–296, 2014.

[59]. V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in Wireless Ad Hoc Networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, 2003, vol. 2, pp. 808–817.

[60]. J. Blum and A. Eskandarian, "The Threat of Intelligent Collisions," *IT Professional*, vol. 6, no. 1, pp. 24–29, 2004.

[61]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *Wireless Communications, IEEE*, vol. 11, no. February, pp. 38–47, 2004.

[62]. C. Xenakis, "Malicious Actions Against the GPRS Technology," *Journal in Computer Virology*, vol. 2, no. 2, pp. 121–133, 2006.

[63]. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G Wireless Communication Networks using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[64]. I. M. Khan, N. Jabeur, M. Z. Khan, and H. Mokhtar, "An Overview of the Impact of Wireless Sensor Networks in Medical Health Care," in *1st International Conference on Computing and Information Technology (ICCT), Al-Madinah Al-Munawwarah, Saudi Arabia*, 2012, pp. 576–580.

[65]. D. Chaudhary and L. M. Waghmare, "Design Challenges on the Impact of Wireless Sensor Network in Applications for Corporate Social Responsibility," *International Journal of Latest Research in Science and Technology*, vol. 3, no. 2, pp. 110-114, 2015.

[66]. V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*, 2011, pp. 1–6.

[67]. M. Li, W. Lou, and K. Ren, “Data Security and Privacy in Wireless Body Area Networks,” *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[68]. A. Haque, M. Faizanuddin, and N. K. Singh, “A Study of Cognitive Wireless Sensor Networks : Taxonomy of Attacks and Countermeasures,” *World Applied Programming*, vol. 2, no. 11, pp. 477–484, 2012.

[69]. F. R. Yut, H. Tang, M. Huang, Z. Lit, and P. C. Mason, “Defense Against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios,” in *IEEE Military Communications Conference*, 2009, pp. 1–7.

[70]. M. A. Aref and S. K. Jayaweera, “A Cognitive Anti-jamming and Interference-avoidance Stochastic Game,” in *2017 IEEE 16th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC)*, 2017, pp. 520–527.

[71]. Z. Wei, F. R. Yu, and A. Boukerche, “Cooperative Spectrum Sensing with Trust Assistance for Cognitive Radio Vehicular Ad hoc Networks,” in *Proceedings of the 5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications - DIVANet ’15*, 2015, pp. 27–33.

[72]. V. Ramani and S. K. Sharma, “Cognitive radios: A Survey on Spectrum Sensing, Security and Spectrum handoff,” *China Communications*, vol. 14, no. 11, pp. 185–208, 2017.

[73]. S. Srinu and S. L. Sabat, “Cooperative Wideband Sensing based on Cyclostationary features with Multiple Malicious User Elimination,” *AEU - International Journal of Electronics and Communications*, vol. 67, no. 8, pp. 702–707, 2013.

[74]. Y. Zhang, G. Xu, and X. Geng, “Security Threats in Cognitive Radio Networks,” *10th IEEE International Conference on High Performance Computing and Communications*, 2008, pp. 1036–1041.

[75]. K. C. How, M. Ma, and Y. Qin, “A Cross-layer Selfishness Avoidance Routing Protocol for the Dynamic Cognitive Radio Networks,” in *2011 IEEE GLOBECOM Workshops*, GC Wkshps 2011, 2011, pp. 942–946.

[76]. M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, “Network Layer Attacks and Countermeasures in Cognitive Radio Networks: A survey,” *Journal of Information Security and Applications*, vol. 38, no. 2018, pp. 40–49, 2018.

[77]. M. R. Manesh and N. Kaabouch, “Security Threats and Countermeasures of MAC Layer in Cognitive Radio Networks,” *Ad Hoc Networks*, vol. 70, no. 2018, pp. 85–102, 2017.

[78]. A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, “Collaborative Spectrum Sensing in the presence of Byzantine Attacks in Cognitive Radio Networks,” *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[79]. J. Herzog, G. Wachman, D. Liu, W. Street, and D. Liu, “On the Robustness of Cognitive Networking Mechanisms to Malicious Insiders,” *Defense Technical Inforamtion Center*, vol. 298, no. 704, 2011.

[80]. S. Kar, S. Sethi, and R. K. Sahoo, “A Multi-factor Trust Management Scheme for Secure Spectrum Sensing in Cognitive Radio Networks,” *Wireless Personal Communications*, vol. 97, no. 2, pp. 2523–2540, 2017.

[81]. Q. Li and D. Xu, “Minimizing Secrecy Outage Probability for Primary Users in Cognitive Radio Networks,” *AEU - International Journal of Electronics and Communications*, vol. 83, no. July 2017, pp. 353–358, 2018.

[82]. Y. Zou, X. Li, and Y.-C. Liang, “Secrecy Outage and Diversity Analysis of Cognitive Radio Systems,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222–2236, 2014.

[83]. J. L. Burbank, A. R. Hammons, and S. D. Jones, “A Common Lexicon and Design Issues Surrounding Cognitive Radio Networks Operating in the Presence of Jamming,” in *Proceedings - IEEE Military Communications Conference MILCOM*, 2008, pp. 1–7.

[84]. M. A. Aref and S. K. Jayaweera, “A Novel Cognitive Anti-jamming stochastic Game,” in *2017 Cognitive Communications for Aerospace Applications Workshop, CCAA 2017*, 2017, pp. 1–4.

[85]. Y. S. Shiu, S. Chang, H. C. Wu, S. Huang, and H. H. Chen, “Physical Layer Security in Wireless Networks: a tutorial,” *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[86]. S. Anand, Z. Jin, and K. Subbalakshmi, “An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks,” in *Third IEEE International Symposium on Dynamic Spectrum Access Networks 2008 (DySPAN 2008)*, 2008, pp. 1–6.

[87]. C. Chen, H. Cheng, and Y. Yao, “Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[88]. M. Haghighat and S. M. S. Sadough, “Cooperative Spectrum Sensing for Cognitive Radio

Networks in the presence of Smart Malicious Users," *AEU - International Journal of Electronics and Communications*, vol. 68, no. 6, pp. 520–527, 2014.

[89]. L. Zhai, H. Wang, and C. Gao, "A Spectrum Access Based on Quality of Service (QoS) in Cognitive Radio Networks," *PLOS ONE*, vol. 11, no. 5, pp. 2005–2009, 2016.

[90]. B. Zayen and A. Hayar, "A Performance Study of Kullback-Leibler Distance-based Spectrum Sensing Algorithm," in *2011 3rd International Conference on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2011, pp. 1–5.

[91]. E. Guzzon, F. Benedetto, and G. Giunta, "Performance Performance improvements of OFDM Signals Spectrum Sensing in Cognitive Radio," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, 2012, pp. 1–5.

[92]. Y. Eghbali, H. Hassani, A. Koohian, and M. Ahmadian-attari, "Improved Energy Detector for Wideband Spectrum Sensing in Cognitive Radio Networks," *Radioengineering*, vol. 23, no. C.1, pp. 430–434, 2014.

[93]. A. Taherpour, M. Nasiri-kenari, and S. Gazor, "Multiple Antenna Spectrum Sensing in Cognitive Radios," *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 814–823, 2010.

[94]. W. Lee, S. Member, and I. F. Akyildiz, "Optimal Spectrum Sensing Framework for Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, 2008.

[95]. E. Axell and E. G. Larsson, "Optimal and Sub-Optimal Spectrum Sensing of OFDM Signals in Known and Unknown Noise Variance," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 290–304, 2011.

[96]. Z-D Lei, FPS Chin, "Sensing OFDM Sytems, under Frequency Selective Fading Channels," *IEEE Trans Veh Technol*, vol. 6, no. 4, pp. 1960-1968, 2010.

[97]. M. Ghozzi, F. Marx, M. Dohler, and J. Palicot, "Cyclostatilonarilty-Based Test for Detection of Vacant Frequency Bands," in *2006 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2006, no. 1, pp. 1–5.

[98]. P. D. Sutton, K. E. Nolan, and L. E. Doyle, "Cyclostationary Signatures in Practical Cognitive Radio Applications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 13–24, 2008.

[99]. S. P. Herath and N. Rajatheva, "Analysis of Equal Gain Combining in Energy Detection

for Cognitive Radio over Nakagami Channels," in *IEEE GLOBECOM*, 2008, pp. 1–5.

[100]. F. Benedetto, G. Giunta, and M. Renfors, "A Spectrum Sensing Algorithm for constant Modulus Primary Users Signals," *IEEE Communications Letters*, vol. 20, no. 2, pp. 400–403, 2016.

[101]. S. P. Herath, N. Rajatheva, and C. Tellambura, "On the Energy Detection of Unknown Deterministic Signal Over Nakagami Channels with Selection Combining," in *Canadian Conference on Electrical and Computer Engineering*, 2009, pp. 745–749.

[102]. M. Nabil, "A Cooperative Spectrum Sensing Scheme based on Task Assignment Algorithm for Cognitive Radio Networks," in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2014, pp. 151–156.

[103]. B. Khaled, B. Letaief, and W. Zhang, "Cooperative Communications for Cognitive Radio Networks," in *Proceedings of the IEEE*, 2009, vol. 97, no. 5, pp. 878–893.

[104]. J. Unnikrishnan and V. V. Veeravalli, "Cooperative Spectrum Sensing and Detection for Cognitive Radio," in *IEEE Global Telecommunications Conference ({GLOBECOM})*, 2007, pp. 2972–2976.

[105]. W. Wang, B. Kasiri, J. Cai, and A. S. Alfa, "Distributed Cooperative Multi-channel Spectrum Sensing Based on Dynamic Coalitional Game," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2010, pp. 1–5.

[106]. C. Telecommunication, "A New Protocol for Cooperative Spectrum Sharing in Mobile Cognitive Radio Networks," *Radioengineering*, vol. 24, no. 3, pp. 757–764, 2015.

[107]. D. Lee, "Adaptive Random Access for Cooperative Spectrum Sensing in Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, 2015, vol. 14, no. 2, pp. 831–840.

[108]. K. Ahmed and F. Bashir, "Comparative Study of Centralized Cooperative Spectrum Sensing in Cognitive Radio Networks," in *2010 2nd International Conference on Signal Processing Systems*, 2010, vol. 0, no. 1, pp. V3-246-V3-249.

[109]. H. A. Shah and I. Koo, "Optimal Quantization and Efficient Cooperative Spectrum Sensing in Congnitive Radio Networks," in *2015 International Conference on Emerging Technologies (ICET)*, 2015, pp. 1–6.

[110]. X. Liu, J. Yan, and K. Chen, "Optimal Energy Harvest-based Weighed Cooperative Spectrum Sensing in Cognitive Radio," in *2016 International Workshop on Sustainability,*

Implementation and Resilience of Energy-Aware Networks, ICNC Workshop, 2016, no. 2, pp. 16–20.

[111]. F. Benedetto, G. Giunta, A. Tedeschi, and E. Guzzon, "Performance Improvements of Cooperative Spectrum Sensing in Cognitive Radio Networks with Correlated Cognitive Users," *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, Prague, 2015, pp. 1-5.

[112]. F. Eg, A. F. Ge, D. K. Ge, D. K. Ge, and A. D. Ea, "On the Detection Performance of CSS Based on PSO," in *2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT)*, 2014, vol. 67, pp. 110–114.

[113]. W. Zhang, R. K. Mallik, and K. B. Letaief, "Cooperative Spectrum Sensing Optimization in Cognitive Radio Networks," in *IEEE International Conference on Communications*, 2008, pp. 3411–3415.

[114]. R. Bouraoui and H. Besbes, "Cooperative Spectrum Sensing for Cognitive Radio Networks : Fusion Rules Performance Analysis," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016, pp. 493–498.

[115]. N. Marchang, R. Rajkumari, S. B. Brahmachary, and A. Taggu, "Dynamic Decision Rule for Cooperative Spectrum," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2015, no. 1, pp. 1–5.

[116]. L. Ling, L. Yin, and Z. Hongbo, "Half-Voting Based Twice-Cooperative Spectrum Sensing in Cognitive Radio Networks," in *5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, no. 3, pp. 1–3.

[117]. T. Jiang and D. Qu, "On Minimum Sensing Error with Spectrum Sensing Using Counting Rule in Cognitive Radio Networks," in *Proceedings of the 4th International ICST Conference on Wireless Internet*, 2008, pp. 1–9.

[118]. Y. Liu, D. Yuan, M. Jiang, W. Fan, G. Jin, and F. Li, "Analysis of Square-Law Combining for Cognitive Radios over Nakagami Chananels," in *5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, pp. 1–4.

[119]. H. Yang, Z. Zhao, and H. Zhang, "Hard Combining Based Energy Efficient Spectrum Sensing in Cognitive Radio Network In this section, " in *Globecom 2013-Cognitive Radio and Networks Symposium*, 2013, pp. 1038–1043.

[120]. B. Shen, T. Cui, and K. Kwak, “An Optimal Soft Fusion Scheme for Cooperative Spectrum Sensing in Cognitive Radio Network,” in *2009 IEEE Wireless Communications and Networking Conference*, 2009, pp. 1–5.

[121]. B. Environment and W. Innovation, "Multi-stage cross entropy optimization algorithm for hard combining schemes in cognitive radio network," *2015 IEEE 12th Malaysia International Conference on Communications (MICC)*, Kuching, 2015, pp. 113-118.

[122]. J. Ma, G. Zhao, and Y. Li, “Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4502–4507, 2008.

[123]. L. Wang, L. Zhang, and X. Chen, “A Dynamic Threshold Strategy Against SSDF Attack for Cooperative Spectrum Sensing in Cognitive Radio Networks,” in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1–5.

[124]. F. Benedetto, A. Tedeschi, G. Giunta, and P. Coronas, “Performance Improvements of Reputation-Based Cooperative Spectrum Sensing,” in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1–6.

[125]. F. Benedetto, G. Giunta, E. Guzzon, and M. Renfors, “Effective Monitoring of Freeloading User in the Presence of Active User in Cognitive Radio Networks,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2443–2450, 2014.

[126]. H. C. Caswell, “Analysis of Catastrophic Events Using Statistical Outlier Methods,” in *Transmission and Distribution Conference and Exposition (T&D)*, 2012 *IEEE PES*, 2012, pp. 1–3.

[127]. G. Zhang, Z. Chen, L. Tian, and D. Zhang, “Using Trust to Establish a Secure Routing Model in Cognitive Radio Network,” *PLOS One*, vol. 10, no. 9, pp. 1–15, 2015.

[128]. W. Wang, H. Li, Y. Sun, and Z. Han, “CatchIt: Detect malicious nodes in collaborative spectrum sensing,” in *GLOBECOM - IEEE Global Telecommunications Conference*, 2009, pp. 1–6.

[129]. P. Kaligineedi, S. Member, and M. Khabbazian, “Malicious User Detection in a Cognitive Radio Cooperative Sensing System,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2010.

[130]. A. A. El-Saleh and K. Hussain, “Cognitive Radio Engine Model Utilizing Soft Fusion

based Genetic Algorithm for Cooperative Spectrum Optimization," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 2, no. 3, pp. 169–173, 2013.

[131]. K. Zeng, P. Pawełczak, and D. Čabrić, "Reputation-based Cooperative Spectrum Sensing with Trusted Nodes Assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226–228, 2010.

[132]. L. Khalid and A. Anpalagan, "Cooperative Sensing With Correlated Local Decisions in Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 2, pp. 843–849, 2012.

[133]. M. A. Alrefaei, T. M. Shami, and A. A. El-saleh, "Genetic Algorithm with Multi-Parent Crossover for Cooperative Spectrum Sensing," in *2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN)*, 2015, vol. 1, pp. 17–21.

[134]. F. Mohammed and M. Deriche, "A Two-Threshold Cooperative Spectrum Sensing Algorithm using Swarm Intelligence," in *2013 Computing, Communications and IT Applications Conference (ComComAp)*, 2013, pp. 59–62.

[135]. M. Akbari and M. R. Manesh, "Minimizing the Detection Error of Cognitive Radio Networks Using Particle Swarm Optimization," in *2012 International Conference on Computer and Communication Engineering (ICCCE)*, 2012, no. July, pp. 3–5.

[136]. D. Das and S. Das, "A Cooperative Spectrum Sensing Scheme Using Multiobjective Hybrid IWO/PSO Algorithm in Cognitive Radio Networks," in *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 2014, pp. 225–230.

[137]. T. Cover, and J. Thomas, Elements of Information Theory. *New York: Wiley*. ISBN 0-471-06259-6, 1991.

[138]. O. Richard, Duda, E. H. Petert, G. S. David, Pattern Classification, *2nd Edition, Wiley*, 2000, ISBN 978-0-471-05669-0

[139]. J. Shlens, G. D. Field, J. L. Gauthier, M. I. Grivich, D. Petrusca, A. Sher, A. M. Litke, E. J. Chichilnisky, "The Structure of Multi-neuron Firing Patterns in Primate Retina,"*J Neurosci*, vo. 26, pp. 8254 – 8266, 2006.

[140]. C. E. Shannon, "A Mathematical Theory of Communication,". *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948. doi:10.1002/j.1538-7305.1948.tb01338.x.

[141]. S. Kullback, R. A. Leibler "On Information and Sufficiency", *Annals of Mathematical*

Statistics, vol. 22, no. 1, pp. 79–86, 1951. doi:10.1214/aoms/1177729694.

[142]. D. V. Lindley, "On a Measure of the Information Provided by an Experiment", *Annals of Mathematical Statistics*. vol. no. 4, pp. 986-1005, 1956.

[143]. H. Akaike, "A New Look at the Statistical Model Identification," in *IEEE Transactions on Automatic Control*, vol. 19, no. 6, pp. 716-723, Dec 1974.

[144]. D. B. Fogel and L. J. Fogel, "Using Evolutionary Programming to Schedule Tasks on a Suite of Heterogeneous Computers," *Comput. Oper. Res.*, vol. 23, no. 6, pp. 527–534, 1996.

[145]. P. J. Angeline, G. M. Saunders, and J. B. Pollack, "An Evolutionary Algorithm that Constructs Recurrent Neural Networks," *IEEE Trans. Neural Networks*, vol. 5, no. 1, pp. 54–65, 1994.

[146]. D. Dasgupta and Z. Michalewicz, "Evolutionary Algorithms in Engineering Applications," *Springer Science & Business Media*, 2013.

[147]. M. C. Bhuvaneswari, Application of Evolutionary Algorithms for Multi-objective Optimization in VLSI and Embedded Systems. *Springer*, 2015.

[148]. H. P. Schwefel, "Evolution and Optimum Seeking. Sixth-Generation Computer Technology Series," *Wiley, New York*, 1995.

[149]. M. Pelikan, "NK landscapes, problem difficulty, and hybrid evolutionary algorithms," in *Proceedings of the 12th annual conference on Genetic and evolutionary computation*, 2010, pp. 665–672.

[150]. C. Blum and A. Roli, "Hybrid Metaheuristics: An Introduction," in *Hybrid Metaheuristics, Springer*, 2008, pp. 1–30.

[151]. D. Ashlock, "Evolutionary computation for modeling and optimization," *Springer Science & Business Media*, 2006.

[152]. F. Mostseller, J. W. Tukey. Data analysis and regression. *A Second Course in Statistics. MA: Addison-Wesley*, 1977.

[153]. J. Hollahd, Adaptation in Natural and Artificial Systems. *University of Michigan Press*, 1995.

[154]. J. H. Holland, "Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence", *U Michigan Press*, 1975.

[155]. J. B. Grimbleby, “Hybrid Genetic Algorithms for Analogue Network Synthesis,” in *Proceedings of the 1999 Congress on Evolutionary Computation-CEC99*, 1999, vol. 3, pp. 1781–1787.

[156]. U. Maulik, “Analysis of Gene Microarray Data in a Soft Computing Framework,” *Appl. Soft Comput.*, vol. 11, no. 6, pp. 4152–4160, 2011.

[157]. L. M. O. Queiroz and C. Lyra, “Adaptive Hybrid Genetic Algorithm for Technical Loss Reduction in Distribution Networks under Variable Demands,” *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 445–453, 2009.

[158]. S. U. Khan, I. M. Qureshi, F. Zaman, and A. Naveed, “Null Placement and Sidelobe Suppression in Failed Array Using Symmetrical Element Failure Technique and Hybrid Heuristic Computation,” *Prog. Electromagn. Res. B*, vol. 52, pp. 165–184, 2013.

[159]. A. Rauniyar, S. Y. Shin, "Improved Detection Performance of Energy Detector by Optimization of Threshold Using BPSO Algorithm for Cognitive Radio Networks," in *The Proceedings of the 2nd International Conference on Industrial Application Engineering*; 2015, pp. 179-183.

[160]. F. Eg, A. F. Ge, D. K. Ge, A. D. Ea, “On the Detection Performance of CSS Based on PSO, ” *2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT)*, Langkawi, Malaysia, Nov 2014, pp. 110–114

[161]. F. Mohammed and M. Deriche, "A two-threshold cooperative spectrum sensing algorithm using swarm intelligence," *2013 Computing, Communications and IT Applications Conference (ComComAp)*, Hong Kong, 2013, pp. 59-62

[162]. R. A. Rashid, F. Bin, "Efficient In-Band Spectrum Sensing Using Swarm Intelligence for Cognitive Radio Network," in *Canadian Journal of Electrical and Computer Engineering*, vol. 38, no. 2, pp. 106-115, Spring 2015

[163]. V. Vignesh, D. Pavithra, K. Dinakaran, and C. Thirumalai, “Data analysis using box and whisker plot for stationary shop analysis,” *Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017*, vol. 2018–January, pp. 1072–1076, 2018.

[164]. S. Suresh, S. Lal, C. S. Reddy, and M. S. Kiran, “A Novel Adaptive Cuckoo Search Algorithm for Contrast Enhancement of Satellite Images,” *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 10, no. 8, pp. 3665–3676,

2017.

[165]. C. Zhang, G. Li, and W. Cui, “High-Resolution Remote Sensing Image Change Detection by Statistical-Object-Based Method,” *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, pp. 1–8, 2018.

[166]. H. C. Caswell, “Analysis of Catastrophic Events Using Statistical Outlier Methods,” in *Transmission and Distribution Conference and Exposition (T&D), 2012 IEEE PES*, 2012, pp. 1–3.