An Authentication Based Approach for Prevention of Spectrum Sensing Data Falsification Attacks in Cognitive Radio Network

Nikhil Marriwala (nikhilmarriwala@gmail.com)
University Institute of Engineering and Technology https://orcid.org/0000-0002-1093-630X
Himanshu Punj
ICL Group of Colleges, Village Sountil, Naraingarh
Sunita Panda
GITAM School of Technology, Bengaluru Campus
Inderjeet Kaur
Ajay Kumar Garg Engineering College Ghaziabad
Deepak Rathore
Guru Ghasidas Vishwavidyalaya Bilaspur

Research Article

Keywords: Cognitive Radio Network, Spectrum Sensing Data Falsification, Cyclo-feature Detection, Radio Matrix Theory, Iterative State Estimation, Distance Ratio Test, K- mean Clustering.

Posted Date: August 10th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-749602/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on November 13th, 2021. See the published version at https://doi.org/10.1007/s11277-021-09329-8.

An Authentication based Approach for Prevention of Spectrum Sensing Data Falsification attacks in Cognitive Radio Network

[1]Nikhil Marriwala [0000-0002-1093-630X]
Assistant Professor, Electronics and Communication Engineering Department, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, Email:-nikhilmarriwala@gmail.com
[2]Himanshu Punj,
ICL Group of Colleges, Village Sountil, Naraingarh, Ambala, punjhimanshu21@gmail.com
[3]Dr. Sunita Panda,
Assistant Professor, Department of Electrical, Electronics and Communication Engineering, GITAM School of Technology, Bengaluru Campus, Karnataka, spanda3@gitam.edu
[4]Inderjeet Kaur
Associate Professor, Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College Ghaziabad, Inderjeetk@gmail.com
[5]Deepak Rathore,
Assistant professor, Department of Electronics and Communication Engineering, Guru Ghasidas Vishwavidyalaya Bilaspur, erdeep2020@gmail.com

Abstract

This is the era of Intelligent cognitive radio network technology that provides the available spectrum with efficient utilization. Cognitive Radio technology must promise to allow interference-free spectrum access by users. The paper discusses the several attacks and motives of attacks. The authentication mechanism role to prevent the attacks for hassle-free spectrum utilization is demonstrated. In this paper, resolving the cognitive network security issues by the authentication mechanism and the methods and need of authentication is discussed. This paper addresses the research challenges in the way of securing the cognitive radio network and countermeasures in CRN security strategies. Cognitive radio is an empowering innovation that guarantees to achieve spectrum utilization. In cognitive radio networks, several security threats affect the process of cognitive radio. Spectrum sensing data falsification (SSDF) attack is most disruptive in which the malicious users degrade the decision-making process by sending the false sensing reports to data fusion centres thus preventing honest users from utilizing the spectrum. Hence, security is a very important issue in cognitive radio networks that needs to be addressed for proper utilization of available spectrum by the users. Cognitive radio technology must promise secure spectrum dynamic access to users. In this paper, to counter the SSDF attack, the trust-based security mechanism is demonstrated to authenticate the honest users and it is observed that the proposed framework in the MATLAB environment is efficient and able to detect malicious users. Cognitive radio technology is the strategy applied to the spectrum to make it efficient for wireless communication. The strategy is an intelligent way to access the spectrum as it can learn its environment and make decisions by easy adaptation of operating parameters. The multiple nodes scenario is a good perspective. Software-defined radio is an

essential component of cognitive radio Here, secondary users can access the spectrum to primary users whenever their vacant spectrum is available. The initial step is to sense the spectrum available further steps are spectrum decision making, spectrum management, and spectrum mobility. The network is vulnerable to various attacks on spectrum sensing and policy protocols which lead to disturbing functionality of cognitive radio technology. The defence mechanism based on public-key cryptography is proposed in which PU is authenticated by appending signature provided to PU signal. Authentication with a tag to the primary users is another perspective proposed. CRN technology should provide integrity, confidentiality and authenticity to the users.

Keywords: Cognitive Radio Network, Spectrum Sensing Data Falsification, Cyclo-feature Detection, Radio Matrix Theory, Iterative State Estimation, Distance Ratio Test, K- mean Clustering.

1.1 Introduction to Cognitive Radio Network

The Cognitive Radio, the term given by Joseph Mitola III in 1998 presented the concept for wireless technologies that "the related networks are sufficiently computationally intelligent about radio resources and related computer-to-computer communications to detect user communications needs as a function of user context and to provide radio resources and wireless services most appropriate to those needs". Therefore, cognitive radio techniques are strategies that are only available for the efficient and effective use of the spectrum. [1]. This strategy is a smart way to get access to the spectrum, as it can learn the environment of the classes by analyzing the series and make a decision by adjusting the operating parameters. The main task of the user of the network who wants to access the spectrum is to detect the presence of licensed users known as primary users (PUs), and if PU is absent, then to sense the RF environment to know the available spectrum. This process is important and called spectrum sensing. The goal of spectrum sensing is interference-free access to PUs by either switching to an available band or limiting its interference with PUs at an acceptable level and, second, secondary users must efficiently detect and utilizes the spectrum holes[2]. Thus, the detection performance in spectrum sensing is important to the performance of both primary and cognitive radio networks.

On average, users can first get a feel for what needs to be done before they try to get a minimum of intervention from the initial to the user. The first step is to sense the spectrum available, the next step is deciding on the range, the spectrum and range of movement. The network is primarily exposed to different types of attacks in spectrum sensing, which led to a violation of the functionality of the equipment as the mind. Spectral sensing to inform the user that the information which is provided is that the work is important for the CRN performance. As part of the process of exploration and to the average user, who is working to cognitive, to the stations in the memory location, to make sure that there is no harmful interference to the original user. Cognitive radio is sometimes a very difficult period to investigate the spectrum from the sources you trust. This is because, the signals will tend to have, the effect of the shade of the decline of the multipath decay. And there is the possibility for the user to repeat, as well as the reveal of the user of the original is set based on any unwanted noise or interference. These problems can be resolved by re-synchronizing the multiple of the average users work together in the spectrum of

the probe. Each of the average users of the spectrum, it will serve as a sensitive terminal, from which the local spectrum sensing.

While the traditional attacks in wireless networks, there is still, however, a knowledge of radio technology, it can receive a different kind of vulnerability. The enemies in an aggressive environment, try out the node-management systems to attack a single query protocol, for example, the false sense that the reporting of the results will directly affect the group's final decision. Such an attack is known as a Spectral Probe, Data Manipulation (SSDF) attack. Spectral detection of data tampering attack (SSDF) is an attack in which the underlying spectral sensing data is sent to the collector of the data, which affects the decision-making process. A security mechanism based on public-key cryptography, New York City, which is authenticating with the addition of the signature, gave a signal, at the New York city identification are then used to find the early adopters are the most likely. CRN's engineering needs to look into the user's territorial integrity, personal identity and the authenticity of the documents. The primary research is on security attacks based on the categories name, user name, and then the attack response. The studies in the literature, which shows that the result of the co-operative probing can be greatly diminished by the falsified reports of malicious nodes. The existing SSDF attack, the studies tend to look at the presence of a fusion centre, how people interact with local measurements, and, therefore, the final decision about the presence or absence of the primary user.

The need for a fusion centre has its reasons such as:

1. Centralized schemes tend to suffer from a high consumption between the mind of the channels that needed to remember the places, and the connector center area. They are the channels of communication between the connection to the centre and the secondary users are subject to fading, the results are not reliable.
2. All of the detection system, which is based on the spatial relationship, and assuming that the centre of the compound prior to the start of the calling process, it will be Geo-locations of all cognitive radios.[3].
3. Malicious websites can also colour the links between the city centre and thus paralyze the entire system. The Fusion centre, which is engaged in further information, is the most beautiful place to visit on a secret spy attack. The single point of failure can lead to accidents relating to the leaking of personal information.
4. Introduction of the higher level, that is, the users need to get started and to get in contact with the integration centre. Also, if the node is non-stationary, a stable connection requires the large-scale deployment of the network protocol.

5. Another disclosure of your personal information on the site is a part of security, and this is usually necessary to protect the privacy of the CRNS. With self-serving end-users is a matter of concern, CRNS. Everyone is getting ready to take part in the co-detection process. includes individual sensors, and the interaction of neighbouring nodes, and, therefore, the power consumption and CPU cycles (CPU) [4].

On average, the users that are owned by different measures for the different base stations in the case of a distributed CRN is likely to reduce the self-serving goal is to make an individual decision to work together with the other secondary users to act on their own or with the help of distributes. Effective control of such self-serving actions and the need to ensure the fairness of the network and help honest users to compare, in order to achieve a better touch of the features is the requirement. Therefore, an interesting and important field of research is both to encourage,

rather than the bad, but the selfish, the user, to take part in the collaborative search process. Without a central authority, as well as stimulating the cooperative sensing process needs to be fully implemented. Violate the privacy of the main and regular users of certain security systems is, once again, a limitation of the literature. The obligation of professional secrecy, which typically requires a Wi-Fi network is of particular importance in heterogeneous environments such as the CRNS. Any service or program that can not be controlled, but of this information. The shortcomings of the existing systems, existing security mechanisms, as well as the problems and opportunities of the future, can improve the safety and security of cognitive radio networks, which are necessary for the creation of an effective system of trust, in order to prevent the attacks in cognitive radio networks, SSDF.

Therefore, a reliable mechanism, which is very important to ensure the smooth operation of the main users is ruled by the malicious users who send false information on the range of the average user is. To change the offer-acceptance policies as a natural defence mechanism, CRN, and authentication of users, helping to achieve a trust-based mechanism, and prevents the attackers from violating the decisions of the module. The strong security mechanisms that are based on trust, it can serve CRN. Creating trust is a complex task that requires consideration of several terms. A possible way to integrate the CRNS confidence in the modelling involves identifying the identity of the user[5].

1.2 Cognitive Radio Functioning

Cognitive radio follows a particular approach for spectrum utilization inefficient manner. It has the ability to know the surrounding environment and recognize the useful spectrum bands with the implementation of intelligent algorithms it detects the suitable spectrum hole appropriate for work. It can adapt to the varying environment making the operation of the network easier. This approach is the essential feature of cognitive radio which makes it a promising technology. Figure 1.1 demonstrates the functions of CR and the features on which the CRN relies[2].

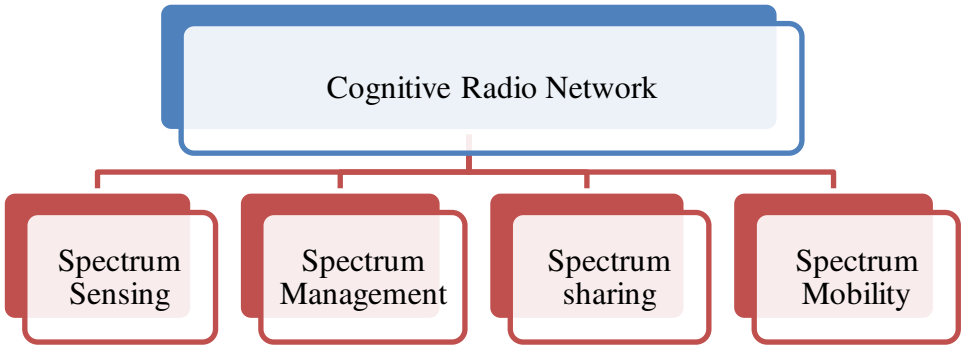

Figure 1.1 Functions of Cognitive Radio

- Spectrum sensing: To sense the RF environment and be aware of the available spectrum.

- Spectrum management: To get the Selection of the present channels depending on their signal strength, efficiency etc.
- Spectrum sharing: To share the licensed-band user's spectrum bands.
- Spectrum mobility: To provide the features permitting the cognitive-radio user changing of its operational frequency.

1.3 Spectrum Sensing Techniques

The first task of cognitive radio is too aware of the surrounding environment by knowing the available spectrum that can be utilized for transmission. It refers to the objective of estimating the parameters of the radio channel, such as the characteristics of the transmission channel, level of interference, noise level, availability of spectrum, availability of power, etc. Spectrum sensing is performed predominantly in the time and frequency domain. It can also be done, however, in code and phase domains, as well as. Figure 1.2 below represents the various sensing techniques there for the spectrum[6].

A number of different sizes, to be in a particular range, as it was felt by many of the parameters of the signal is cyclostationary, the parameters, the modulation parameters, etc, the problem is that the mechanism for the detection of the spectral sensing is a delay in the decision-making process, due to the high complexity of the signal processing. In the case of the transient detection is based on the sample distribution, and modification analysis[7].

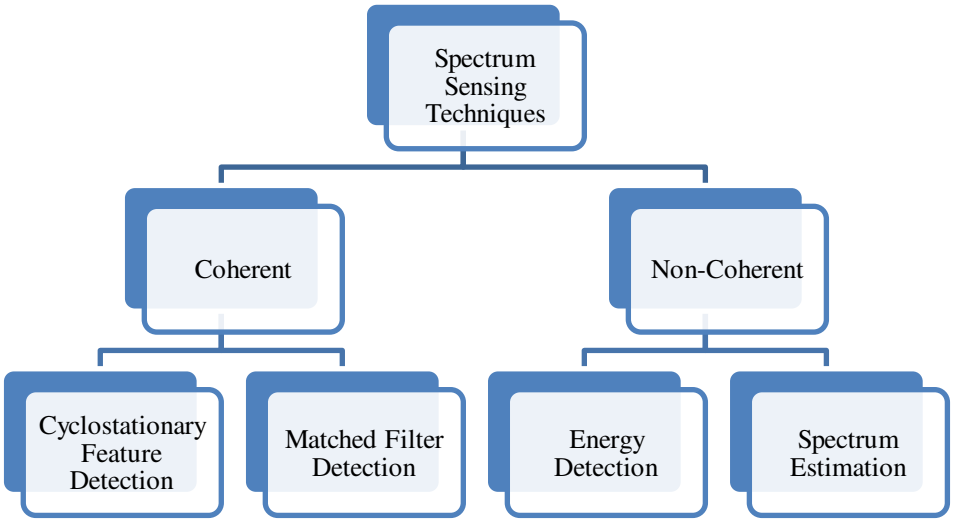

Figure 1.2 Classification of Spectrum Sensing Techniques

1.4 Functionalities of Cognitive Radio Network

The functionalities of several layers of CRN are explored in the literature. Figure.1.3 describes the functionalities of important layers of the cognitive radio network.

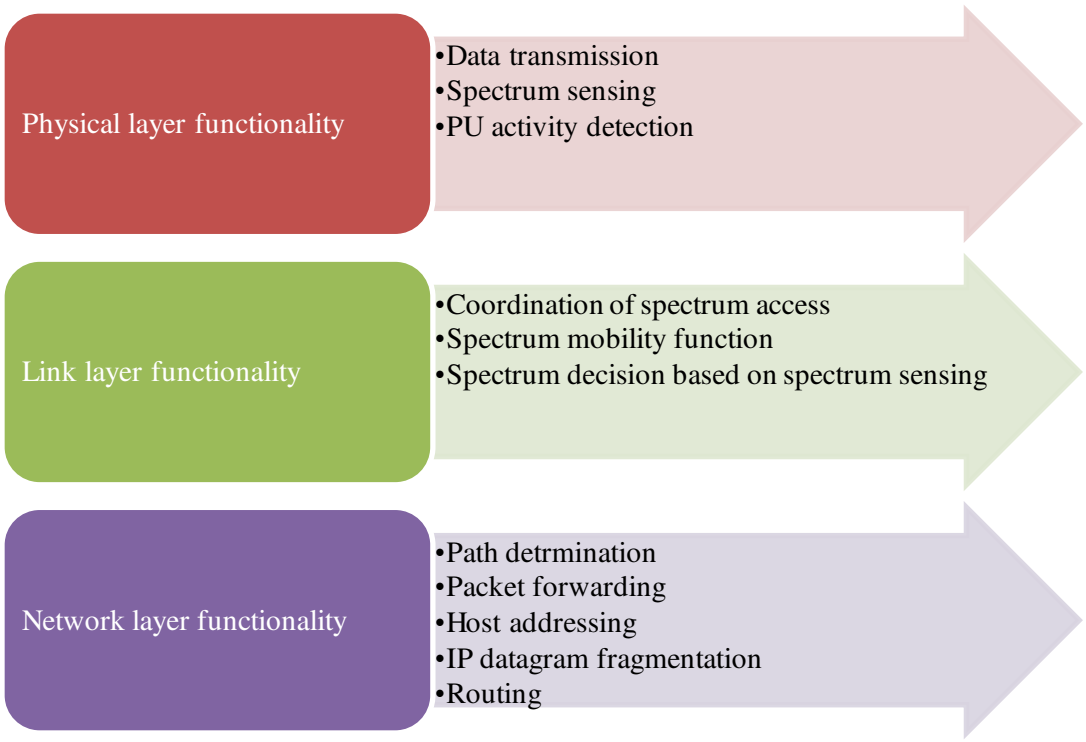

Figure.1.3. Functionalities of Layers of Cognitive Radio

1.5 Addressing Security Issues

- A number of the multiplication methods are used in such a way that the PD-broadcast is not to be considered as the noise of the licensed users[5]. This technology makes it possible to use a higher throughput at the expense of a small increase in the complexity of the issue. Bearing in mind that there is a trade-off, the hybrid methods can be considered to be that of the existing spectrum technology, with the PD-networks.

Finally, the spectrum sharing approaches usually focus on two types of systems: networks to share it in a different system (intra-network spectrum sharing among multiple coexisting CR networks), or online, for the parts of the series, as shown below.

- **Primary Emulation Attack**: A number of the multiplication methods are used in such a way that the PD-broadcast is not to be considered as the noise of the licensed users. This technology makes it possible to use a higher throughput at the expense of a small increase in the complexity of the issue. Bearing in mind that there is a trade-off, the hybrid methods can be considered to be that of the existing spectrum technology, with the PD-networks. Finally, the spectrum sharing approaches usually focus on two types of systems: networks in order to share it in a different computer system (intra-network spectrum sharing among multiple coexisting CR networks), or online, for the parts of the series, as shown below.
- **Spectrum sensing data falsification attack**: It is important in the security of cognitive radio. It is a belief manipulation attack as it is caused by manipulation of parameters by malicious users degrades the decision ability of the decision centre.
- **SSDF attack:** The behaviour of the malicious user in this attack will be classified under this. This attack is studied in terms of user accuracy to repeat based on the run-up you choose. To protect the information system to ensure security, availability of information, integrity and confidentiality in terms of functionality of different levels, are the activities that are planned.

- SSDF attack affects the availability of radio networks and speed of knowledge. To measure the integrity of the principle, the level-based safety method, fur is more effective, based on evidence, which significantly reduces cooperation[5].
- The effective defence against SSDF is based on the balance between hardware cost and method of user authentication and non-denial. It will be necessary to verify the identity and territorial integrity of the system item.
- Users with supply-based schedules, increase their ability to make decisions. If security is breached, the burden on services is increasing rapidly. The detection of attacks increases the development of the structure.
- Of the cluster, the mechanism isn't difficult to detect the malicious users in each cluster to detect reliable clusters and authenticates the user.
- The attackers ' goal is to analyze the nature of the approach, in order to avoid being aided by other factors, and can be easy to judge the intentions of the user.

1.6 Attacks on Cognitive Radio Network

The high demand for wireless network services has made the security factor increasingly difficult. Though vulnerable to most security threats due to the nature of CRN and its critical applications. Ensuring security is a major challenge for these networks, despite such a great advantage.

Table I Attacks identification and mitigation mechanisms

Sr.no.	Author's name	Proposed algorithm	Security attacks	Authentication
1	Wanga et al.[7]	Physical layer network coding	Primary user emulation attack (PUEA)	A hash function can be used to evaluate the trusted sender's list
2	Zenget al. [5]	Authentication of spectrum sensing outcomes using data collector as well as fusion scheme	Mitigation of Spectrum sensing data falsification (SSDF) attacks	Evaluation of data collector
3	Bennaceur et al. [8]	mechanism based on determining cognitive trust value	PUEA and SSDF attacks	User identity authentication
4	Fatemieh et.al.[9]	Cross-layer confirmation scheme	Primary emulsion attack fetching the cross-layer network	recognition on basis of cross-layer authentication
5	Zeng et al.[10]	Game theory scheme	Primary user emulation attack (PUEA)	A clustering scheme is introduced in each of the clusters in order to identify the needs of the user

Table II Layers Attacks and Countermeasures

Sr.no.	**Layer**	**Attack and its Effects**	**Countermeasures**
1.	Physical Layer	• Jamming affects sensing • PU Emulation- affects PU detection • Overlapping SU	• Escape the denial of service, changing the spatial location of a legitimate user, Periodic scanning and cyclostationary parameters metrics[5] • Cryptographic authentication, biometric techniques[11] game theory[12] • Trust approach, game theory
2.	Data Link layer	• SSDF- affects spectrum decision • Common Control Channel jamming • Common Control Channel saturation	• User's authentication, reliability score identification of SU's. • Trust node detection mechanism[12]
3	Network layer	• Hello flood - affects routing • Teardrop- IP datagram fragmentation • Sinkhole-affects routing • Sybil -affects host addressing • Wormhole -effects routing	• Asymmetric key cryptographic approach • Cyclostationary parameters based routing protocols.[13]
4	Transport Layer	• Key depletion- data, services and protocol	• Cryptographer algorithm[2]
5	Application layer	• Malicious software injection-effects decisions • Policy attacks-effects quality of services	• Game theory[5]
6	Cross-Layer	• Jellyfish -affects network mechanism • Lion attack -affects transmission control protocol • Routing information jamming	• Detection mechanisms[5]

2.1. Literature Review

Chen et.al.[2]**,** proposed a reputation-weighted method, to combine the information is based on the sequential testing of the hypothesis that a relationship with him. The test is made up of two parts: the reputation of the maintenance, and hypothesis testing. Reputation is determined by the effect of the local-sounding statement on the final sound of a decision. Hypothesis testing is an enhanced version of the following Probability Ratio Test (SPRT) - Weighted, and the Sequential Probability Ratio Test (WSPRT). The idea of the WSPRT is the change in the likelihood of the SPRT so that the good reputation of the individual nodes is also taken into account. This system depends on the a priori knowledge of the radio, the value of the membership. It also doesn't take into account the spatial variation of the spectrum of the sun. Please note that this is only to be used on a small surface is detected. In addition, the attack is not removed, by the end of the process, even if, the estimation of the weight is not much. The speed in order to get to a steady-

state is not satisfactory. Another limitation is the fact that it can be used to get a stable connection, with an average user will only have to report on a double income, in addition to the first user to report or not, but classy, get together, where the average level of the users is reporting that the measured energy of the primary user. This limit reduces to the exact solution.
Yang et al.[3], proposed a game-theoretical anti-jamming scheme and modelled the jamming and anti-jamming process as a Markov decision process. With this approach, secondary users can avoid the jamming attack launched by external attackers.

Zeng et al. [5], suggested grouping the sensors that are close to the group, and then uses the correlation of the filter in order to exclude or minimize the impact of adverse events. They are stylish, with a view of the relation of the shade, and in the shadows between the adjacent sensors. A sensor of the message, which differs significantly in other communication is deemed to be suspicious and will have to be disposed of, or sanctioned by the fusion center. However, the system only works, when you are attacking, organize at least 13 of the cluster nodes, and identifying the regions in which the attack is paramount.

Kim et al.[11], proposed the reliable attack detection system is cooperative sensing via the recursive State estimation (IRIS). This approach takes into account the network topology. However, the network topology is subject to change in cognitive radio networks, so that the proposed course of action is not always promising.

Change, etc.

Bian et al.[6], for the first time, to go into the analysis of the systems, the distribution, the spectrum, the IEEE 802.22 standard. The security sub-menu to protect the operation of a computer network, an additional message authentication codes to operate your devices. However, the security sub-menu is only to protect the control messages to the mobile phone, and protect the beacon between the throws that are there.

Li et al.[12] , propose an approach that detects anomalies, and detect harmful to repeat the behaviour. They suggested that a two-way algorithm is used to determine the distance to your neighbours are still far away from the user, which is by far and away the most the average user, date, amount of space. However, their approach assumes that the Np, which means that the majority of nodes are honest. In addition, he suggests that if history repeats, the user is very close to that of the story of the other, and his behaviour is normal. This is likely to determine the normal of the spatial correlation of attack, therefore, it may not be the one that could be applied in cognitive radio networks. These controls may not be used in a dynamic network, in which the discovery of the history of the various miles is not too close to each other.

Wang et al.[13], An algorithm has been proposed for the detection of malicious users, who expect the suspicion of the average level of the users, on the basis of their previous reports. However, enough of an attack, the damage to property (IV), after an attack, the reports of the absence of a primary user, and they don't exist, and perhaps in the right way, otherwise, the effect of the attack. They don't just identify the false alarms of attacks, and the attacks, the identification of false alarms and misses. An attack against a false positive outcome is the same as the exploit attack (EA), after an attack on information about the presence of the greatest of the user when not in use. However, the false-alarm and miss detection of attacks is a combination of EA and BF. If you do accept a power of the detection threshold, the report of an attack on a

lower energy level; otherwise, it indicates that the higher the energy level is not present. While this is still a primary user, the attack may not create false alarms, increase the detection report. The false-alarm and miss-detection scenarios should be analyzed in two different cases.

Kaligineedi et al. [14], proposed to offer a simple, detection system for primary filtration of the extreme values in order to query the data. The use of a medium of the constraint system, to simplify the decision-making process, and in the centre of a community. However, it has only a limited capacity to detect, and only in an extreme adverse report, the indicator light may be on for this period of time, always has been, the user, and is not always an identified customer. As an extension to this approach, once again, to be examined by the external factors and suggests a different kind of approaches in order to improve the detection of malicious code on it. They also suggested that the use of the number of observations in the immediate neighbourhood, to further improve the detection rate. If the user's spatial information is available in the transfer centre, there are the outliers, the coefficient may be, for each node, based on the results of the energy detector, and its nearest neighbour in space. It can detect the malicious user is able to manipulate the distribution and the density of the cognitive radio.

Xiea and Wanga[14]**,** proposed a PUE identification system for cognitive radio networks based on physical layer network coding. The analysis showed that the gap between the starting points of interference between the two receivers is limited by the senders' positions. Using a trustworthy node as the reference sender multiple hyperbolas on which the interested sender resides are calculated. SDR is implemented and trial of the system is done in actual network surrounding is presented

Sakran et al.[15], the proposed protected in style the selection of schools, who choose a trusted, decoding, and direct style in order to help the Hustle, and the highest attainable standard of integrity, level, limit, are subject to the PU interference of the power of the number of parties, and the PUs, when the information is in the channel, with the limited CRNs security.

Yan et al.[16] , discuss to a series of attacks over the distribution of information, the lack of access to common sense. They provide a sense of security, which is still being distributed, as the hash-based data. These controls may not be used in a dynamic network, in which the discovery of the history of the various miles is not too close to each other.

Gopinathan et al.[10], focused on the guarantee of truthfulness through bid independent prices. However, most of them do not provide a security guarantee for the spectrum auctions. This scheme provides security to the users with the verification of their identity.

networks, either.

Fatemieh et al[9]**,** identified the measurement of an equal split in the square, the mobile areas, as well as confirm that, as between the adjacent rushing it like it is, in the hierarchical structure of certain cells, with a significant lot of malicious nodes. Single-cell compared to the reports, it can be compared to as a couple. Only in the run-up to the acceptance or receipt is to have a node is moved, which is determined by the Sprinkling, and is excluded from further calculations. A balanced strategy is presented for those who have been appointed by the central government as the deviants. They are given a low and high points. On average, the value of the cell discharge is

considered to be very low, as compared to its competitors, as mentioned, is a low-VF, a high-top. After the detection of outliers, and the average weight of the nodes is up to date. This work provides a basis for taking into account the uncertainty that it brings. However, it is assumed that the legitimate and malicious websites are mobilizing together. When a malicious website interacts in order to modify the distribution system, the system will be compromised.

Chari et al. [17]**,** demonstrated an efficient authentication protocol to upgrade the security of the Cognitive Radio Network. The strategy for recognizing the Primary client Emulation Attacks in a CRN using cross-layer approached and an authentication scheme to detect PUEA has been presented. It is identified that the physical layer authentication method can serve as a faster authentication method but with low accuracy in detection and a cryptography-based authentication protocol can serve as a slower authentication method but with high accuracy in detection.

Subbulakshmiet al.[18]**,**demonstration of a nonparametric multivariate method, the fastest, the detection of a radio receiver, the measure of energy and cyclostationary properties. The proposed method can be used to trace the dynamics of the state of the communication channels. This feature can be useful for dynamic spectrum sharing (DHS), and the future of the system, because it is, in practice, the centralized channel, the synchronization is real, and the first information on the channel statistics are usually difficult to access. It is referred to as a multivariate non-parametric average of the sampling, the power of a cyclostationary system to enable more rapid detection, is proposed, with a higher level of performance compared to traditional systems.

Pei et al. [19]**,** demonstrated the requirement that is the required features in order to work in a mobile Ad hoc network (MANET) environment, as well as detection and response mechanism, should be set up. In operation, each node has an independent agent of the ID detection and response. The identification is carried out in response to the detection. The nodes that have not been authenticated, or the network. In this scheme, every node in the local planning system. Each system can work independently and with others, and retain the information. This information will apply to notices of alleged copyright and the security of information that is being discovered as a result of co-operation with other organizations.

Pietro et al.[20], presented an anti-jamming technology that is defined on delay in time broadcast scheme which opens up a new area for CRN security. With the help of this mechanism envious malicious users are eliminated who are accessing the spectrum opportunities through misconduct.

Mirza et al[21], presented the trust-based observations of the Access control mechanism(TEAM). It offers a full-featured and distributed access control mechanism, which is based on the trust model, safety, security, and cooperation in a network location. This segment of access control and the management of the process into two parts: the local and the global. The mission of the local context is to check global information about distrustful behaviour.

Jarawaheh et al [22]**,** presented the reputation-based representations of the shared spectrum sensing scheme for ad hoc CRN. The system can reliably protect the secondary users and decide

on an SSDF attack. The device is designed for scenarios in which the IP is not in scope when compared with those of the CRNs of a network.

Khan et al.[23], presented a survey on wireless sensor networks (WSNs) and elaborated on the next generation of WSNs, utilizing the advantages of cognitive radio (CR) technology for identifying and accessing the free spectrum bands. For the successful adoption of CWSNs, they have to be trustworthy and secure. The area of security and privacy was explored.

Gul et al. [24], presented an approach to countermeasure with PUEA attack in CRN. The author demonstrated that in the absence of Primary Users (PU), the attackers mimic PUs' signals characteristics to fool legitimate Secondary Users (SU) that evacuate the channel for them. Localization and encryption are the best approaches in this area. The author proposed the method based on game theory without using any complex calculation and second methods (RSS, GPS and so on), PUEA can be detected. This method is especially proposed for MANET and can be used in any circumstance of CRNs (ad-hoc, centralized, distributed).

Bennaceur et al.[8], proposed the authentication mechanism of primary users in CRN to avoid primary user emulation attack (PUEA) and also for efficient utilization of spectrum. The authentication of PU has to be done at the physical layer only because SU and PU may not use the same protocol above the physical layer. And also, location-based authentication protocols are not suitable for mobile primary users.

Clement. [25], demonstrated the challenges in defending attacks in cognitive wireless networks. The author focused on addressing the attackers. A novel management mechanism SMTD is proposed which is based on trust and penalty to deal with security problems in CRNs.

Morales et al[26], provided a novel effective algorithm using the kernel KMC (k-means clustering) method to be answerable for attacker detection, which not only improves the attacker detection performance but also offers processing and memory savings.

2.2. Research Gaps and Challenges

- The authentication of users is needed to be effectively achieved using the machine learning concept and maintaining the database of honest and regular users.
- The behaviour analysis of the users needed to be tracked to build up a better defence mechanism against falsification attacks.
- Authentication ID allotment mechanism can be optimized for minimizing the delays in spectrum allocation to the needed users.

2.3. Problem Formulation

- The inability to make use of a free of charge CRN channel is a major concern in such networks, the challenge of the spectrum for which the researchers had to find a solution. There are a large number of studies in the literature, which effectively solve the existing problems together. On the contrary, some of the critical questions remain open in the other. This research is in addresses the conditions of its existence, cause the CRN to lose the ability to make use of the other channels that are available on the CRN.

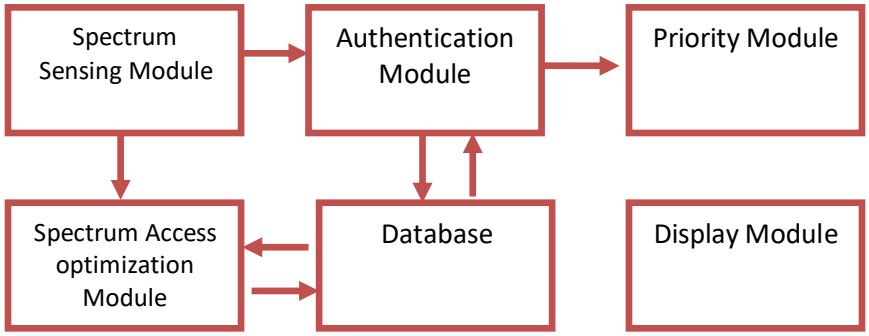

Figure 2.2 the Proposed System Block Diagram

3.1 Methodology Used

The methodology of the proposed work is based on the aim of the mitigation of the SSDF attack with the authentication mechanism of secondary users. The aim is to make secure access to the spectrum and good decision making in the process of spectrum allocation. The rule is to check the trust of the users that want the spectrum by checking the conditions and behaviours of individual users and based on the detection makes the decision. The authentication is like a key strategy to access the spectrum lock and the key is provided based on the user's performance in the authentication process.

The user's authentication approach is followed by a two-stage verification process and providing the trust value to the users as a certificate of authenticity. The authentication algorithm is applied and on the basis of the allotted trust value the malicious users are sorted from the hub and spectrum is granted to the honest secondary users. The energy and location of each user node are optimized and the reliability of search is increased. The optimization module helps in the stabilization of the network.

The defence is based on the trustworthiness of the users and allocation of spectrum done on the decision making of fusion centres. The database is maintained at each level which keeps track of the past and present work of the system.

The methodology adopted to develop the proposed system will include the following steps and module wise the steps are categorized and evaluated:

i. The primary user transmitted energy is detected.
ii. The secondary users present in the network are allowed to senses the spectrum.
iii. The secondary users generate their sensing reports.
iv. The accessing of the spectrum is checked periodically.
v. The users send the sensing report to the decision centre
vi. The spectrum sensing mechanism is optimized to improve performance and reduce randomness.
vii. The users are authenticated with the help of the verification process and allotted with the trust value.
viii. Trust evaluation is conducted for spectrum accessing for the users and malicious users are hence searched with the algorithm based on the location.

ix. The geo-location database is updated with the time stamp.
x. Previous honest users are prioritized with knowledge-based.
xi. The database is updated and the authentication mechanism utilizes the database
xii. The database-based report gets analyzed.
xiii. Authenticated ID is allocated to honest users for easy future use.
xiv. The spectrum information is displayed periodically and on-demand.

The flowchart showing the working procedure of the model is shown in Fig.3.1.

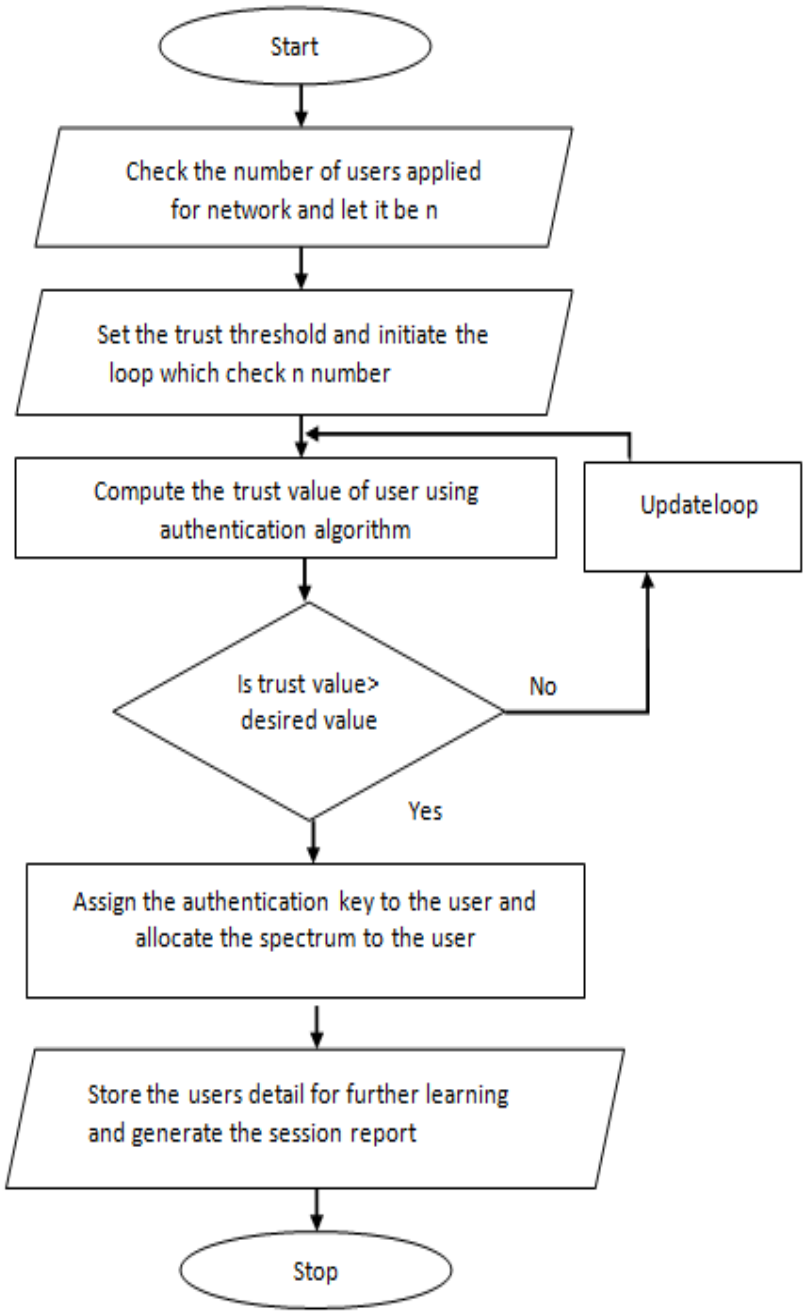

Figure.3.1. Systematic Flowchart of Proposed Model

This section gives the details of the MATLAB simulation for implementation of the proposed model of authentication mechanism to mitigate the SSDF attacks. The simulation parameters and simulation mechanism are demonstrated with simulation in MATLAB software.

Let us assume that all secondary users are area oriented and able to communicate w.r.t the cyclostationary features. The location of SU's is stored at the base station database. The transmission range of primary users and the secondary users in that range are permitted to sense the radio spectrum. The energy-based approach is utilized for RF sensing and detecting the presence of the Primary user in the proposed model. The SU's that want the allocation of spectrum firstly sense the spectrum in the particular period and give its sensing report to the fusion centre. The sensing reports are submitted at fusion centres by the secondary users. The fusion centre makes a global decision based on the combination of local sensing decisions. Here, some SUs are malicious secondary users that intentionally send false sensing information to fusion centres to change global decisions.

The authentication algorithm is applied and based on the allotted trust value the malicious users are sorted from the hub and spectrum is granted to the honest secondary users. The energy and location of each user node are optimized and the reliability of search is increased. The optimization module helps in the stabilization of the network.

Simulation

We consider randomly distributed users with primary users and secondary users. This random environment is created with Gaussian or Poisson's distribution [5]. The locations of the users are loaded in the database. The MATLAB simulation of PUs and SUs, with different distributions, is done. The primary user is detected with energy-sensing. The SU's that want the allocation of spectrum firstly sense the spectrum in the particular period and give its sensing report to the fusion centre.

The secondary users are randomly distributed and the performance of the simulated scenario is evaluated with the probability of both the positive alarm as right access by users and negative false alarm as the wrong approach of users. The sensing reports are submitted at fusion centres by the secondary users. The implementation is done and evaluated in a controlled environment.

Table I below shows the considered simulation parameters.

Table III: Simulation parameters

sr.no.	Parameter	Value
1	Area of field	100*100
2	No. of Primary Users(PU)	2
3	No. of Secondary Users(PU)	N
4	Simulation time	t sec

Every user is allowed to sense the spectrum and generate the sensing report. The energy of the primary transmitter is detected by the secondary users. The information given to the fusion centre where the threshold is compared of each user forms the basis for the fusion centre to process the decision. Here, the energy detection technique finds the spectrum holes on basis of the energy sensed at the receiver.

The secondary users are randomly distributed and the performance of the simulated scenario is evaluated with the probability of both the positive alarm as right access by users and negative false alarm as the wrong approach of users. All secondary users need to sense the energy level for a specific time duration. Let t be the spectrum sensing duration.

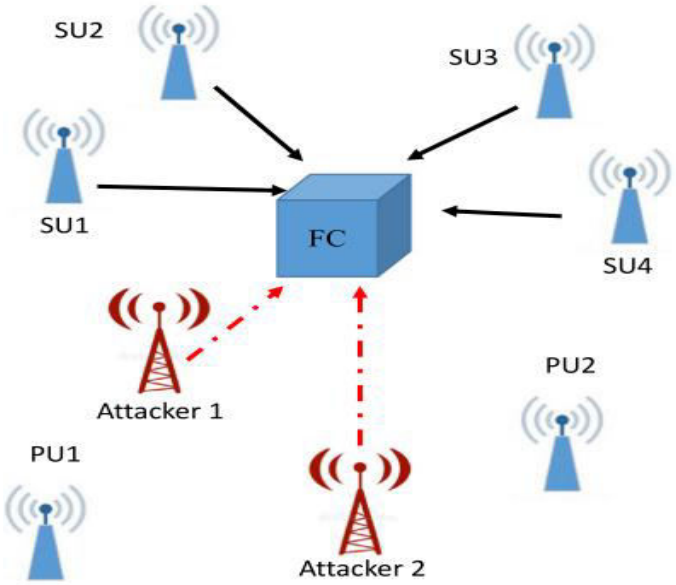

Figure 4.1 A Scenario of Simulation of Attack [1]

Let the secondary users nodes distributed in the region that want the spectrum access is represented as 4.1,

$N = \{n1, n2, n3 \ldots ni\}$, where i = 1, 2…, n	(4.1)

Let transmitted power of the Primary user is represented as in 4.2,

$P = \{P1, P2, P3 \ldots Pi\}$, where i = 1, 2…, n	(4.2)

Each user senses the spectrum and the information sent to the fusion centre represented as with equation 4.3 below,

F = {*f1, f2, f3.... fi*}, where i = 1, 2…, n	(4.3)

The fusion centre makes a global decision based on the combination of local sensing decisions. Here, some SUs are malicious secondary users that intentionally send false sensing information to the fusion centre to change global decisions.

During the instance of attacks, the CRN users as sense the spectrum with primary user transmitter power as represented with equation 4.5 below,

$Pi,n = Pt + 10\alpha \log(d0\ di,n) + ci,n + wi,n$ where, $i = 1, 2, \ldots, Nn = 1, 2, \ldots, Nc$	(4.5)

The ci, represents the change made by the CRN user during receiving of the power and in the case of honest user it does not change and in case of a malicious user, it is equal to the false value as the change added by the malicious user intentionally.

4.2 Spectrum Sensing Module

Every user is allowed to sense the spectrum and generate the sensing report. The energy of the primary transmitter is detected by the secondary users. The information given to the fusion centre where the threshold is compared of each user forms the basis for the fusion centre to process the decision. Here, the energy detection technique finds the spectrum holes on basis of the energy sensed at the receiver. The secondary users are randomly distributed and the performance of the simulated scenario is evaluated with the probability of both the positive alarm as right access by users and negative false alarm as the wrong approach of users. All secondary users need to sense the energy level for a specific time duration. Let t be the spectrum sensing duration.

Let $S_i(n)$ represents the i^{th} signal sensed by the secondary user n and $w_i(n)$ is Gaussian noise with mean 0 and variance $\sigma 2$ and σ_I is the gain

H0	$S_i(n) = w_i(n)$ where, i = 1, 2…, n: when PU is absent	(4.6)

H1	$S_i(n) = \sigma_i s_i(n) + w_i(n)$, where , i = 1, 2…, n : when PU is present,	(4.7)

Figure 4.2 below shows the energy detected of the primary transmitter.

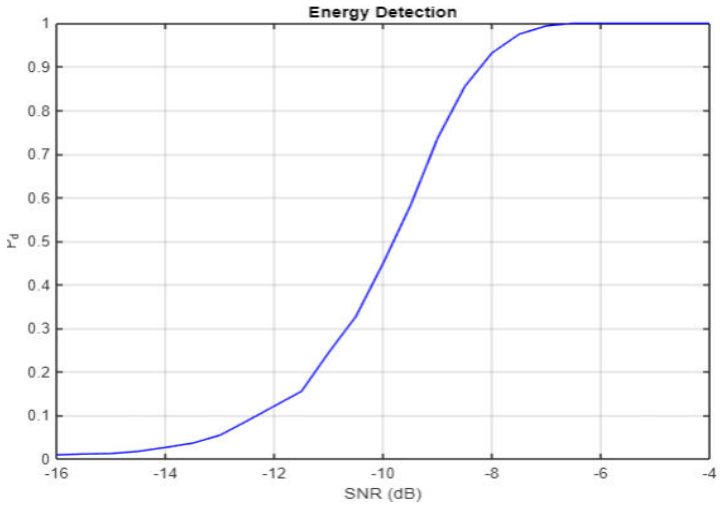

Figure 4.2. Showing the Energy Detection Graph

The secondary users are allowed to sense the spectrum and generate the sensing report. The energy of the primary transmitter is detected by the secondary users. The information given to the fusion centre where the threshold is compared of each user forms the basis for the fusion centre to process the decision. The sensing report is then sent to the fusion centre and this information is based on the various parameters that are time to time compared with the predefined thresholds. If the group of secondary users sends the information passed the threshold test, the reliability of the users is considered to be good.

The sensing time is very important and considered carefully for increments. The sensing is affected with an increase in malicious users attacks because with an increase in malicious users the falser decision sends to the fusion centre. The detection time needs to be analyzed as an important characteristic. Figure 4.3 below shows the false alarm probability versus missed detection. Based on their statistical distributions, we examine how likely false alarms and false negatives would happen. When transmissions are done the database is updated again in the appropriate trust value table based on current observations with timestamp information. SUs is allowed to communicate their observations amongst each other. The database is maintained and helps in updating the sensing report. The pre-defined threshold comparison is performed while updating automatically the trust values that help in the search of malicious users.
For the evaluation of detection performance, the probabilities of detection Pd and false-alarm

For the evaluation of detection performance, the probabilities of detection Pd and false-alarm Pf are defined as :

$Pd = P(\mathrm{dP} > \mathrm{a}\|H1), PFa = P(\mathrm{dP} > \mathrm{a}\|H0)$	(4.8)

$\mathrm{Pf} = 1 - \mathrm{Pd} = \mathrm{P}(\mathrm{dP} < a\|H1)$	(4.9)

In the SSDF attack, the attacker makes the high global false alarm probability to enlarge the output The fusion centre apply several rules to make a good global decision and it is done within a specific time frame as the binary numbers are used so rules based on logical operations are utilized such as OR, etc operations. As the sensing information is considered as the binary value so it is vulnerable and affected with attack easily and SSDF attack is done with false sensing submission of the report and thus affecting the final decision of the fusion centre. As a result, the wrong decision is made so careful majority rule strategies are suitable for it. The trust value of the malicious user's calculation helps in the detection of SSDF attackers and the strategies are observed on basis of this value. They generate false high values so that the authentication is implied to check it.
The fusion centre has the information of users and comparison its analysis finds the malicious users and Step by step the users are checked periodically and the process is continuous and periodic in nature. The sensing report is prepared with the measurement of the received power of the primary transmitter. The value of power changes with the absence or presence of the PU.

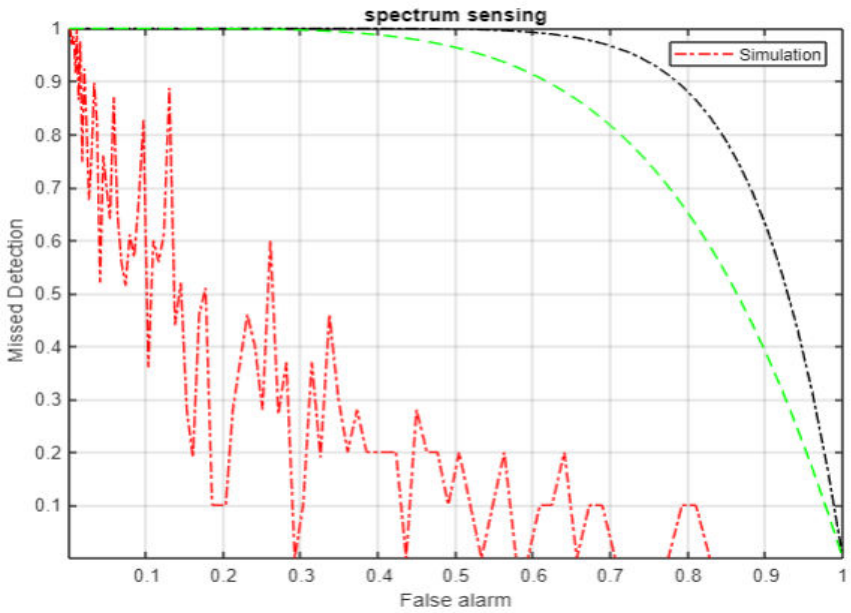

Figure 4.3. Showing graph of the false alarm probability versus missed detection

4.3 Spectrum Optimization Module

Spectrum sensing is optimized to improve the performance of the proposed model. The location of SU's is stored at the base station database. The transmission range of the primary user and the secondary users in that range are permitted to sense the radio spectrum. The energy-based approach is utilized for RF sensing and detecting the presence of the Primary user in the proposed model. The SU's that want the allocation of spectrum firstly sense the spectrum in the particular period and give its sensing report to the fusion centre. The sensing reports are submitted at the fusion centre by the secondary users.

Let us assume that all secondary users are area oriented and able to communicate on basis of the cyclostationary features. The location of SU's is stored at the base station database. The parameters are updated periodically. The transmission range of the primary user and the secondary users in that range are permitted to sense the radio spectrum. The energy-based approach is utilized for RF sensing and detecting the presence of the Primary user in the proposed model. The authentication algorithm is applied and based on the allotted trust value the malicious users are sorted from the hub and spectrum is granted to the honest secondary users. The energy and location of each user node are optimized and the reliability of search is increased. The optimization module helps in the stabilization of the network. For optimization of the sensing module, an algorithm is applied after the sensing so that make the sensing is made more focused and reliable. The randomness can be avoided efficiently with optimization mechanisms and sensing reports are made more precise. The energy and location of each user node are optimized and the reliability of search is increased. The optimization module helps in the stabilization of the network.

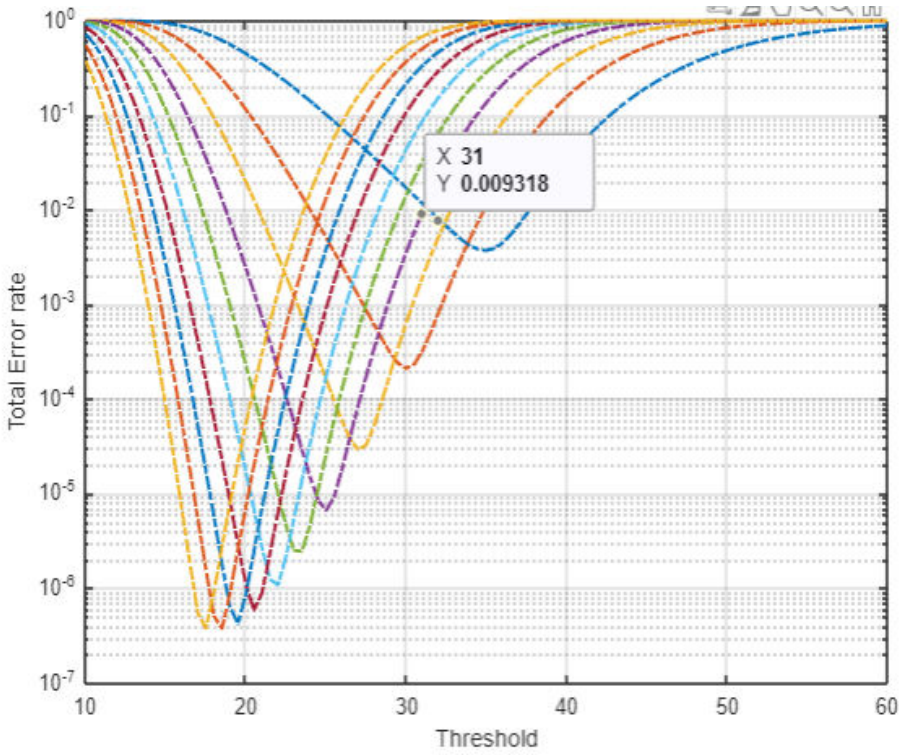

Figure.4.4. Showing Spectrum Sensing Optimization

4.4 Authentication Module

Authentication: The authenticated mechanism is meant to prevent malicious user's spectrum assessment with the identification of honest users. The user nodes are analyzed sequentially and periodically and nodes that fail to authenticate are rejected from the network. The goal of the authentication of the user is to assure secure access to the primary user spectrum and helps in the mitigation of SSDF attacks. Authentication is an essential requirement of cognitive radio networks. The authentication algorithm is applied and on the basis of the allotted trust value the malicious users are sorted from the hub and spectrum is granted to the honest secondary users.
The authentication algorithm is implemented based on the generated trust value and the malicious users are sorted from the group of users and the spectrum is granted to the honest secondary users. The energy and location of each user node are optimized and the reliability of search is increased. The main aim of authentication is to verify the authority gain of the users.

Online authentication based on login access is a good way to implement the authentication mechanism. Secondary user accesses the login. The password is allowed to give to regular secondary users and for a new user, the login access is created with their identity verification. The database is accessed and on behalf of authentication, a trust value is generated. The session key is allotted to the user and after the second stage verification decision centre will allot the spectrum. A trust mechanism is implemented to process all the necessary steps and updating of the trust value of the respective secondary user. The authentication module here is based on database correlation of users identities based on verification. This verification is sent to the fusion centre and helps in the improvement of decision making done with computation of trust value.

4.4.1 User Identification:

The database of regular secondary users is saved with passwords in tables and new users need to authenticate. The authentication algorithm solves this purpose. This first stage of verification generates the first trust value which is sending to the decision centre.

Figure 4.5. Showing the Authentication Login

The authenticated mechanism is meant to prevent malicious user's spectrum assessment with the identification of honest users.

- The user nodes are analyzed sequentially and periodically and nodes that fail to authenticate are rejected from the network.
- The database of each session is maintained and updated periodically. The database is maintained in excel and can be accessed and analyzed easily for future use as well.
- Online authentication based on login access is a good way to implement the authentication mechanism. Secondary users access the login. The password is allowed to give to regular secondary users and for a new user, the login access is created with their identity verification. The database is accessed and on behalf of authentication, a trust value is generated. Figure 4.5 shows the GUI seen by the user while authentication.
- The login is based on password access.
- The session key is allotted to the user and after the second stage verification decision centre will allot the spectrum. The honest secondary users only pass the authentication process efficiently.
- In MATLAB the database is stored in .mat format and during the algorithm application, it is accessed and updated automatically.
- The newly updated database is made to store automatically from time to time based on sensing time. The confidential strategies are applied to save the data from malicious intents.

$T1 = \{t1, t2, t3 \ldots . ti\}$,	(4.8)

4.4.2 Search Algorithm:

The search algorithm is implemented for the second step of verification. The attack is simulated probably and with the algorithm, the honest users are detected on basis of the identification and appropriate location updated in the database.

The search algorithm is based on the location features and a second trust value is generated on the user's node that is find as honest users with the algorithm. Figure 4.6 shows the algorithm search for honest users.

In the first stage of authentication, the primary user information is stored in the database and the secondary users with an honest approach are only permitted to access the primary user band and the database generated trust values from time to time while login access protects from the malicious users for the first value.

In the second stage of authentication, the users authenticated in the first stage and also have valid trust value in search algorithm that is based on cyclostationary parameters evaluation are combined. The trust value is generated before the sending of the sensing report to the fusion centre and the primary user also can access the trust value.

The followed algorithm for trust key generation is as follows:

Step 1 The input given for the key generation
Step 2 Select the random numbers.
Step 3 Calculate the final values T1 and T2 AND (U)

If the value is invalid the user is not allowed to access the spectrum. In this way, the security aspects are implemented with MATLAB.

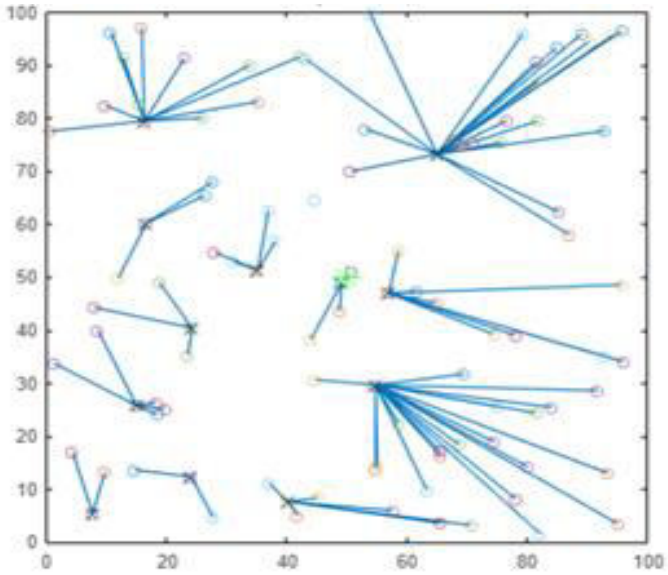

Figure 4.6. Showing Search of Honest Users

$T2 = \{t1, t2, t3 \ldots . ti\},$	(4.9)

The valid trust value comes from a two-stage verification process and comparison with threshold trust value at every stage is done that leads to better authentication of the user.

Further, the detection of honest secondary users is shown in figure.4.7.as marked in green colour circles and the location of the user is saved automatically in the database. The display module

represents the honest and malicious user with the encirclements as done with graphics in the algorithm of searching.

$T = \{T1\ U\ T2\}$,	(4.10)

Decision making: Efficient decision making is the main goal to achieve by a fusion centre that follows the following steps:

- The Fusion centre will have a trust value for each user and after comparison with the trust threshold value, the spectrum allocation is approved (T >Th) where Th, is the threshold trust value.
- The decision-making process of the fusion centre to allocate the spectrum is based on the trust value. The location and values related to users are stored and maintained in the database.
- When transmissions are done the database is updated again in the appropriate trust value table on the basis of current observations with timestamp information. SUs are allowed to communicate their observations amongst each other which helps in updating the sensing report.
- The predefined threshold comparison is performed while updating automatically the trust values that help in the search of malicious users.
- The location information is important in authentication and saving it in the database helps to make an efficient framework for authentication.
- An honest SU can access the spectrum and utilize it for data transmission when the fusion centre permits it and schedule the transmission with the assignment of the session key.
- The trust calculation is done to make a decision and allot the spectrum to provide the session key that is randomly generated only after the user authentication and sorting out the malicious users from the queue.
- The fusion centre provides the identity authentication consisting of Identity, time, free channels etc.

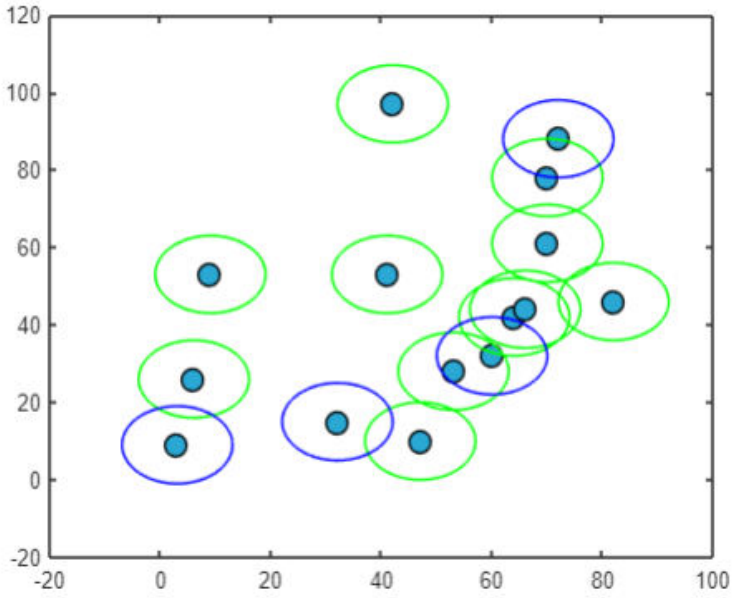

Figure 4.7 Authentications of Honest Users with Encirclement**.**

- The trust is the basis of the trustworthiness of the users and always the updated value of the particular sensing time is considered. The mechanism is well versed does not need any information regarding the surroundings and is not affected by malicious identities of surroundings.
- The fusion centre rejects the malicious user reports itself and other honest users don't need to bother it.
- The authentication mechanism to mitigate the SSDF attack based on the two-stage verification of the users is achieved. The performance of the model is improved with an optimization algorithm.

The identification and mitigation of attacks in an effective way is important for the establishment of a secure strategy for cognitive radio networks. Moreover, the security is essential for efficient functionality of the network as well as for an implemented framework optimization of the spectrum sensing mechanism and malicious users sorting efficiently on the basis of trust value predictions done in two verification stages. The honest users are authenticated with the implementation of user's identification and identification login is allotted to the honest users. The database of honest users is maintained and honest users are able to access the spectrum on basis of it. The database can be utilized effectively in excel for analyzing the network actively and report generation. The display module is effectively able to show honest users and malicious users. The optimization technique utilized as the second stage of the spectrum sensing can verify the decision and make it more efficient with spectrum mechanisms. The authentication mechanism can mitigate the SSDF attacks effectively and in less time and effort with good strategy. The various scenarios of the attack strategies are considered and a predefined threshold is utilized for comparison and decision rules implementation.

5.1 Conclusion

We have proposed a trust-based authentication mechanism for the security of the network from an SSDF attack. The proposed model is implemented in the MATLAB simulation and supports the context privacy of honest users. The research is done to mitigate the spectrum sensing data falsification attack in cognitive radio networks. The authentication mechanism to mitigate the SSDF attack based on the two-stage verification of the users is achieved. The performance of the model is improved with an optimization algorithm. The identification and mitigation of attacks in a proper way is the necessity for the establishment of a secure system for cognitive radio networks. The implemented framework is able to optimize the spectrum sensing mechanism and able to reject malicious users efficiently based on trust value predictions done in two verification stages. The honest users are authenticated with the implementation of user's identification and identification login is allotted to the honest users. The database of honest users is maintained and honest users are able to access the spectrum on basis of it. The database can be utilized effectively in excel for analyzing the network actively and report generation. The display module is effectively able to show honest users and malicious users. The optimization technique utilized as the second stage of the spectrum sensing can verify the decision and make it more efficient with spectrum mechanisms. The authentication mechanism is able to mitigate the SSDF attacks effectively and in less time and effort with good strategy. The various scenarios of the attack strategies are considered and a predefined threshold is utilized for comparison and decision rules implementation. The malicious users are successfully detected and eliminated from the region. The fusion centre allots the spectrum band to the honest users correctly. The users need to show

their authenticity to use the spectrum and after that use the spectrum without any interference and do their data transmission safely. The security of the users is improved with this approach and future use of the spectrum will be also eased. The two-stage verification and allotment of trust value differentiate efficiently the malicious users from the honest users and the performance of the network is improved.

References

[1] F. Salahdine and N. Kaabouch, "Security threats , detection , and countermeasures for physical layer in cognitive radio networks : A survey," *Phys. Commun.*, vol. 39, p. 101001, 2020, doi: 10.1016/j.phycom.2020.101001.

[2] Z. Sun, Z. Xu, M. Z. Hammad, X. Ning, Q. Wang, and L. Guo, "Defending against Massive SSDF Attacks from a Novel Perspective of Honest Secondary Users," *IEEE Commun. Lett.*, vol. 23, no. 10, pp. 1696–1699, 2019, doi: 10.1109/LCOMM.2019.2931974.

[3] J. Walko, "Cognitive radio," *IEE Rev.*, vol. 51, no. 5, pp. 34–37, 2005, doi: 10.1049/ir:20050504.

[4] J. Kelly and J. Ashdown, "Spectrum Sensing Falsification Detection in Dense Cognitive Radio Networks using a Greedy Method," *Proc. IEEE Natl. Aerosp. Electron. Conf. NAECON*, vol. 2018-July, pp. 144–151, 2018, doi: 10.1109/NAECON.2018.8556759.

[5] F. Zeng, J. Li, J. Xu, and J. Zhong, "A trust-based cooperative spectrum sensing scheme against SSDF attack in CRNs," *Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Proce*, pp. 1167–1173, 2016, doi: 10.1109/TrustCom.2016.0190.

[6] A. A. Sharifi, "Attack-Aware Defense Strategy: A Robust Cooperative Spectrum Sensing in Cognitive Radio Sensor Networks," *Iran. J. Sci. Technol. - Trans. Electr. Eng.*, vol. 43, no. 2011, pp. 133–140, 2019, doi: 10.1007/s40998-018-0133-x.

[7] H. Yu, S. Liu, A. C. Kot, C. Miao, and C. Leung, "Dynamic Witness Selection for Trustworthy Distributed Cooperative Sensing in Cognitive Radio Networks," no. September, 2011, doi: 10.1109/ICCT.2011.6157821.

[8] J. Bennaceur, S. Souihi, H. Idoudi, L. A. Saidane, and A. Mellouk, "Game-based secure sensing for the mobile cognitive radio network," *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, vol. 2017-Octob, pp. 1–7, 2018, doi: 10.1109/PIMRC.2017.8292623.

[9] S. Jain, M. Hussain, and R. M. Garimella, "Primary User Authentication in Cognitive Radio Network using Authentication Tag," pp. 1–5, 2016.

[10] R. Wan, L. Ding, N. Xiong, and X. Zhou, "Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 9, 2019, doi: 10.1177/1550147719870645.

[11] H. Kim, "Delegation Based User Authentication Framework over Cognitive Radio Networks," *J. Sens. Actuator Networks*, vol. 6, no. 29, pp. 1–16, 2017, doi: 10.3390/jsan6040029.

[12] J. Li, Z. Feng, Z. Wei, Z. Feng, and P. Zhang, "Security management based on trust determination in cognitive radio networks," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 1–16, 2014, doi: 10.1186/1687-6180-2014-48.

[13] M. Wang, B. Liu, and C. Zhang, "Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio networks," *2013 IEEE Int. Conf. Commun. Work. ICC 2013*, pp. 342–346, 2013, doi: 10.1109/ICCW.2013.6649256.

[14] X. Xie, W. Wang, and U. N. C. Charlotte, "Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding," *Procedia - Procedia Comput. Sci.*, vol. 21, pp. 430–435, 2013, doi: 10.1016/j.procs.2013.09.057.

[15] S. Xia, X. Tao, N. Li, and S. Wang, "Malicious User Detection in Non-Orthogonal Multiple Access Based on Spectrum Analysis," *IEEE Signal Process. Lett.*, vol. 27, pp. 1390–1394, 2020, doi: 10.1109/LSP.2020.3012826.

[16] R. Biswas, J. Wu, X. Du, and Y. Yang, "Mitigation of the spectrum sensing data falsifying attack in cognitive radio networks," *Cyber-Physical Syst.*, vol. 00, no. 00, pp. 1–20, 2020, doi: 10.1080/23335777.2020.1811387.

[17] D. L. Chaitanya and K. M. Chari, "Secure Channel Allocation Approach for Video Streaming in Cognitive Radio Networks," *Wirel. Pers. Commun.*, vol. 94, no. 4, pp. 2613–2631, 2017, doi: 10.1007/s11277-016-3856-x.

[18] P. Subbulakshmi, M. Prakash, and V. Ramalakshmi, "Honest Auction Based Spectrum Assignment and Exploiting Spectrum Sensing Data Falsification Attack Using Stochastic Game Theory in Wireless Cognitive Radio Network," *Wirel. Pers. Commun.*, vol. 102, no. 2, pp. 799–816, 2018, doi: 10.1007/s11277-017-5105-3.

[19] Q. Pei, R. Liang, and H. Li, "A trust management model in centralized cognitive radio networks," *Proc. - 2011 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2011*, pp. 491–496, 2011, doi: 10.1109/CyberC.2011.104.

[20] B. Wang, Y. Wu, and K. J. R. Liu, "Game theory for cognitive radio networks: An overview," *Comput. Networks*, vol. 54, no. 14, pp. 2537–2561, 2010, doi: 10.1016/j.comnet.2010.04.004.

[21] M. A. Mirza, M. Ahmad, M. A. Habib, N. Mahmood, C. M. N. Faisal, and U. Ahmad, "CDCSS: cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber attacks," *J. Supercomput.*, vol. 74, no. 10, pp. 5082–5098, 2018, doi: 10.1007/s11227-018-2378-6.

[22] Y. Jararweh, H. A. Bany Salameh, A. Alturani, L. Tawalbeh, and H. Song, "Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks," *Telecommun. Syst.*, vol. 67, no. 2, pp. 217–229, 2018, doi: 10.1007/s11235-017-0329-9.

[23] M. S. Khan, M. Faisal, S. M. Kim, S. Ahmed, M. St-Hilaire, and J. Kim, "A correlation-based sensing scheme for outlier detection in cognitive radio networks," *Appl. Sci.*, vol. 11, no. 5, pp. 1–12, 2021, doi: 10.3390/app11052362.

[24] N. Gul, I. M. Qureshi, M. S. Khan, A. Elahi, and S. Akbar, "Differential Evolution Based Reliable Cooperative Spectrum Sensing in the Presence of Malicious Users," *Wirel. Pers. Commun.*, vol. 114, no. 1, pp. 123–147, 2020, doi: 10.1007/s11277-020-07354-7.

[25] J. C. Clement, "Jettison the Defectives: A Robust Cooperative Spectrum Sensing Scheme in a Cognitive Radio Network," *Circuits, Syst. Signal Process.*, vol. 37, no. 6, pp. 2471–2491, 2018, doi: 10.1007/s00034-017-0672-9.

[26] J. A. Morales, A. Al-Bataineh, S. Xu, and R. Sandhu, "Analyzing and exploiting network behaviors of malware," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 50 LNICST, pp. 20–34, 2010, doi: 10.1007/978-3-642-16161-2_2.