Punishment Mechanism for Cognitive Radio Networks in Advanced Wireless Communication Systems

Himanshu Sharma [1], K. Kishore Kumar [2], G. Nithya [3], V. Ravi Kumar [4], Shashi Kant Dargar [5], and Amit Gupta [6,*]

[1] Department of Electronics and Communication Engineering, J. B. Institute of Engineering and Technology, Hyderabad, India
[2] Department of Electronics and Communication Engineering, The ICFAI University, Raipur, Chhattisgarh, India
[3] Department of Electronics and Communication Engineering, Joginpally B.R. Engineering College, Hyderabad, India
[4] Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, India
[5] Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India
[6] Department of AI and ML, J. B. Institute of Engineering and Technology, Hyderabad, India
Email: himanshu.zte@gmail.com (H.S.); kishorekamarajugadda@gmail.com (K.K.K.); dr.g.nithya.ece@jbrec.edu.in (G.N.); dr.ravikumar@klh.edu.in (V.R.K.); drshashikant.dargar@gmail.com (S.K.D.); dramitguptacv@gmail.com (A.G.)
*Corresponding author

***Abstract*—Cognitive radios are characterized as intelligent radios that can detect, learn, and adapt; they perceive their operational environment and gather information via experience. Future wireless networks are anticipated to establish a dispersed, intelligent platform for wireless communication, sensing, and computation, necessitating the complex integration of the physical and digital realms in a smooth and sustainable fashion. This research is based on the analysis and the optimal solution of security attacks related to the cognitive radio network. The risks associated with both infrastructure-less and infrastructure-based cognitive radio networks are also covered. We address the frequently disregarded longer-term behavioral changes that are imposed by such attacks through the learning capabilities of cognitive radio network in addition to the short-term consequences of attacks on cognitive radio network performance. However, a few of them considered the punishment of attackers and ignored the effective measures to punish them. In this paper, a new sanction mechanism based on cognitive trust value is proposed. To deal with this issue, a hierarchical architecture cluster heads and data fusion center, the trust value of cognitively engaged users was managed. Fusion Center would punish bad users because they would decline their confidence; it is, therefore, essential to guarantee the safety of the network through a distinction between attack users. A simulation setup based on MATLAB is built for each step of the proposed system. The simulation results show the effectiveness of the proposed architecture in detecting attacks with a detection rate of over 80%.**

***Keywords*—security, Cognitive Radio Network (CRN), attack detection, punishment, optimize, cluster heads**

I. Introduction

Cognitive technologies mainly focus on the opportunistic use by Secondary Users of the licensed band with licensed users called Primary Users. In spectrum sensing, the performance of Secondary Users. Primary Users detection can consequently be reduced by a few factors like shadows and multipath. Cooperative sensing increases the overall performance of detection by adding sensing results of the different spatially located Secondary Users. The combined sensors are more accurate due to spatial diversity than the perceptive outcome of a single Secondary Users.

The cognitive radio networks have lately gained prominence for their capacity to reconcile the disparity between restricted spectrum availability and spectrum demand. The cognitive radio network has recently become a leading provider of wireless technology networks to solve conflict between the restricted spectrum supply and spectrum demand of growing wireless applications and services, identified as the wireless networks that allow them to learn about their geographic and operational conditions, policies, and internal status. The cognitive radio networks are therefore a free, random networking environment where unlicensed secondary users can operate channels not currently operating with spectrum sensing technology for licensed Primary Users. Because of their unique cognitive characteristics, they are therefore vulnerable to new threats in addition to all of the safety risks associated with conventional wireless networks, such as User Emulation Primary Attacks. Attackers can

Manuscript received September 30, 2024; revised December 7, 2024; accepted February 25, 2025; published October 21, 2025.

successfully broadcast and duplicate the primary user within prohibited time slots, leading a protocol-compliant SU to believe that this attack is the primary user. Falsification attacks on spectrum ensign data intentional or unintended assailants give the Fusion Centre false observation details, causing the FC to make incorrect determinations.

Cognitive radio networks are facing an inevitable challenge with security problems, and how to solve them has become an area of research. The main focus of the current research is the detection of signals based on defense attacks, but it was unable to punish them. We are unlikely to punish the offender, even if the person violates morality or civil law; we can only prove it to the law enforcement office. Before our proposed one, we will analyze the existing security mechanisms. The rest of the sections of this paper are sorted out as follows. Section II analyzes previous literature that focused on research on security issues on cognitive radio networks. Section III proposes the cognitive trust value-based mechanism for the punishment of attackers and effective measures to punish them. The simulation results of this proposed approach are explored in Section IV. Finally, the conclusion of this research work is described in Section V.

II. Literature Review

Sohu *et al.* [1] proposed that that Malicious nodes are a well-known source of security threats in cognitive Radio Wireless Sensor Networks (CRWSN). This study focuses on security challenges linked to CRWSN, such as Fusion methods, Cooperative Spectrum sensing, and two severe CR attacks: Spectrum Sensing Data Falsification and Primary User Emulation (PUE).

Wang *et al.* [2] proposed an algorithm to detect fake nodes within the network. The trust and consistency factor can be calculated for every user and nodes whose values of confidence and coherence are below the threshold value and can be considered for detecting malicious nodes. The downside is that only one attacker is activated once.

Noon and Li [3] studied a new type of attack, named the hit and run attack, in which the attacker can produce a sensor report honestly or falsify sensor reports in two modes. The author also found a way to alleviate the attack. Wang *et al.* [4] suggested a soft decision scheme to detect several faux nodes of a system, in which the attacker is assumed to have a policy, and the base station knows where each user is located. The heuristic method was used to detect false nodes. Also, a posterior likelihood was used to detect each node's suspicion level. The calculated probability was then compared to the determined threshold, and if the value exceeds the determined threshold value, the node is regarded as a malicious node. This approach is also referred to as "onion peeling".

The signal generation from PUs detected nodes that sent a false signal to detect data falsification attackers provided by Bansal *et al.* [5] The authors also assessed the attack strength, in which the attack force was seen as the relationship between the number of fake nodes and the total available nodes present in the network. Huang *et al.* considered in Ref. [6] the weight factor that shows the user's contribution. Each user has a reputation, and the decline negatively impacts this reputation factor. Matsui *et al.* [7] proposed an algorithm like the proposed method of Huang et al. that would consider only the difference between the two nodes where it was assumed that the base station where SUs were located.

Chen *et al.* [8] and Clancy *et al.* [9] suggested a trusted and reputable mathematical model. Kar *et al.* [10] used four parameters for the calculation of confidentiality in their work. The active factors, consistency factors, incentive factors, and trust factors were the factors. The nodes are declared to be fake based on calculated trustworthiness. However, to apply the confidence factor, the SUs must be successfully detected [11]. Meng *et al.* [12] demonstrated that SUs might benefit from the multi-user benefit in every time frame for the installed TDMA technology.

Aishwarya *et al.* [13] uses a memetic algorithm to choose the best routing routes that maximize the data delivery ratio and minimize energy usage. When compared to conventional routing techniques, preliminary findings show a notable improvement in the network's overall performance parameters, such as a longer lifespan and improved data dependability. Saranya and Natarajan [14] proposed that, prompted by the growing need for effective spectrum use in wireless communications, to improve EE in CRNs without sacrificing PU protection. The ELSTM-RPO model, the first of its kind in s, is one of the study's main achievements. It offers systematic optimization of essential parameters and outperforms state-of-the-art techniques in terms of EE and spectrum utilization. With its exceptional performance and resilience across a range of network circumstances, this work establishes a new standard for energy-efficient CRNs. This study looks at a number of situations in which SUs may transmit data after asserting that spectrum sensing prevented the PU from being present, has been proposed by Ali *et al.* [15].

In some circumstances, SU's transmission should disrupt PU's communication, leading to wasteful spectrum use. The optimization problem in this connection is to maximize the SUE while meeting the requirements of a low likelihood of PU interference and a high target identification probability. In this approach, several SUs and PUs coexist in a realistic, overlapping clustered structure [16].

In order to gather energy from both SUs and PU transmissions for improved active probability, Sensing Reputation (SR), a revolutionary trust management technique that assesses each node's trustworthiness in the CSS system, is what we presented. SR calculation incorporates a number of choice elements, including the history-based trust factor, active factor, incentive factor, and consistency factor, in order to reflect the complexity. This SR value is used to identify suspicious individuals and filter out harmful users from the CSS scheme's decision-making process [17].

We also propose the idea of a reputation chain sensing system to document and monitor the future actions of the identified problematic people. With greater accuracy and a reduced false alarm rate, theoretical analysis and

simulation results show the effectiveness of suggested malicious user detection approach.

Wang *et al.* [18] reported a centralized data fusion center is used for decision-making. Next, we extend it to the scenario where autonomous and dispersed decision-making results are obtained from the absence of the data fusion center. Mechanism design theory serves as the foundation for our trust-based data fusion systems, which encourage users to submit real sensing data in order to increase the success rate. Amit et al. reported that one of the hardest problems in Mobile Ad-hoc Networks (MANET) is IP address auto reconfiguration, which guarantees the best routing [19].

There are two types of reconfiguration protocols: stateful and stateless. Address conflicts must be avoided, and each address must be distinct. Furthermore, we prevent needless penalties for good users by separating fraudulent reports from erroneous sensing reports caused by assaults and limited sensing capabilities. In order to determine the ideal parameter settings for our trust-based data fusion methods to beat current non-trust-based cooperative spectrum sensing data fusion systems, we conduct a theoretical study that is confirmed by extensive simulation. In order to combat data fabrication attacks, we suggested and examined trust-based data fusion techniques for cooperative spectrum sensing in cognitive radio networks. Amit et al. investigated that determine the specifications of the aerial that depend on its different geometrical parameters, a sequential parametric analysis has been conducted.

The aerial's many geometrical parameters, which include the matrix material's dielectric constant, are up to the patch and horizontal foundation planes' extended qualities and their segregation. An etched symmetrical or non-symmetrical amalgamation of organization in the horizontal foundation plane of MPA is known as a "defective ground structure." The suggested antenna is the recessed ground plane parasitic patch antenna, which is based on the existing parasitic rectangular patch antenna on a FR4-epoxy substrate material with permittivity. The substrate's dimensions are 20 × 20 × 0.5 mm. Antenna characteristics including gain, VSW R, S-parameters, and bandwidth are enhanced and contrasted by Amit et al.

To differentiate false reports resulting from hostile assaults from those caused by limited sensing capabilities, we created data fusion rules. Our architecture successfully compels malevolent nodes to disclose their actual sensing capabilities and results, enabling a high success rate. SUs must first become winning, that is, reduce their own miss detection probability below the upper limit set by PUs in order to obtain the communication chances. A proposed method for enhancing SU detection performance is Collaborative Spectrum Sensing (CSS), in which many SUs bands together and exchange sensing data. Additionally, the likelihood that successful SUs accurately identifies the idle state of PUs' spectrum will influence their communication prospects.

III. Methodology

A reputable architecture was introduced to identify cognitive users in cooperative spectrum detection algorithms by Zeng *et al.* [20]. The algorithm begins by choosing certain cognizant users as credible and categorizes each user's reputation in three states as discharged, pending and reliable. Even when their reputation is accumulated through uniform tests between local and global sensing results, an algorithm gives pending status to every cognitive user other than trustworthy. Cognitive users who exceed a trusted threshold are categorized as trustworthy, while those who do not are placed in a discarded category.

Mapunya *et al.* [21] have introduced the trust-based TCRN architecture for supporting network functions, including Dynamic Spectrum Access (DSA) and routing. As per authors, the CRN trust model should include two main components: confident association and algorithms of learning. The confident partnership involves a cognitive user's initial decision to either accept or reject the application for a neighboring partnership. Learning algorithms helps make better decisions on package transmission, routing, and confidence measures.

Sensors that raise awareness of the surroundings, actuators that allow interaction with the environment, a model of the environment that incorporates the state or memory of events that have been observed, a learning capability that aids in choosing particular actions or adaptations to achieve a performance goal, and a certain amount of autonomy in action are all features of cognitive radio. Geolocation, spectrum awareness/frequency occupancy, biometrics, time, spatial awareness or situational awareness, and software technology are the technologies that power CR. Given the variety of uses that could arise from a radio knowing its current location, as well as its intended path and destination, geolocation is a crucial CR-enabling technology.

This study aims to improve the penalty mechanism model and how to improve the effectiveness of the penalty, optimize the cognitive radio network and achieve the Nash balance among the cluster heads and the network scale. This research concerns the extension, in this regard, to the SMTD protocol proposed by Li *et al.* [22] (trust determination-based security management). The authors suggested in their work an active mechanism to detect attacks based on building trust in the clustered cognitive network. A new compensation scheme is being proposed to Implement a new spectrum sensing algorithm and a central cognitive radio network. Resources Ensure physical layer security assessment and reward and penalty allocation of confidence-built resources to trusted users but do not take data transmission protection into account. The Secret Capacity Enhancement Scheme was implemented to enhance physical layer safety in cognitive radio networks in the hybrid co-operative Spectrum Sensing Algorithm (SMTD), approach. The following is given to the network model and the flow mechanism:

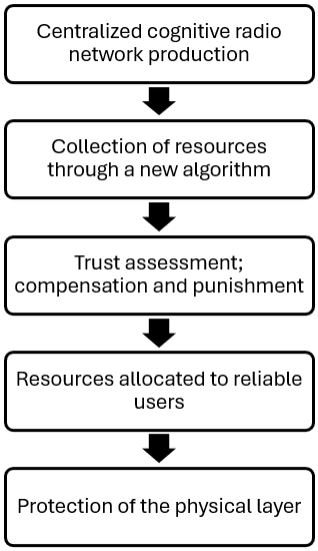

Fig. 1. Proposed paper flow work.

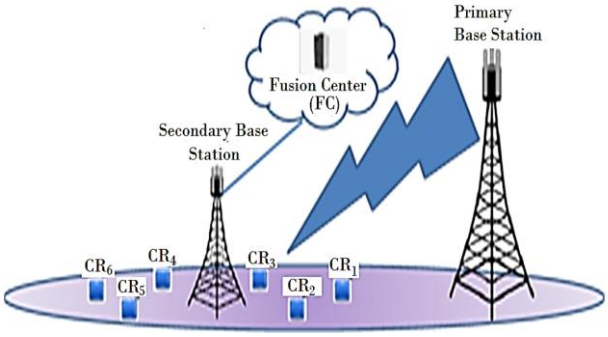

Fig. 2. Cognitive network scenario.

Consider a centralized CN scenario shown in Fig. 1, in which there are multiple CNs with the primary network. Each network is divided into different subnetworks, each of which is centralized as the cluster header [23]. A centralized Fusion Center (FC) for the assembly of open radios to primary users via cognitive users sensing know-how connects various subnets. Fig. 2 illustrates the Cognitive Network Scenario. The first step in hierarchical clustering is to regard every observation as a distinct cluster. Then, it does the next two actions repeatedly: First, determine which two clusters are closest to one another, and then combine the two clusters that are most similar. Until all of the clusters are combined, this iterative process keeps going. A cluster's reelection message is initially broadcast by the cluster leader. Each sensor node in the cluster then uploads two candidates, and all the sensor nodes vote for a new cluster. The current cluster head uses the majority rule to determine the winner after tallying the votes. If a candidate energy is sufficient, a confirmation message is sent to the sensor node once it has been chosen as a contender. However, if the applicant's energy is insufficient, the current cluster head will have to choose another candidate until someone with sufficient energy is chosen and appointed as the new cluster leader.

- Computation and storage of all cognitive users' confidence values in the cognitive network.
- Implement discipline for misbehavior users, update trust value assessments, collect confidence values from cognitive users via Cluster heads, and monitor FC experiences.
- Reporting misbehavior of user information to the FC promptly when an attack is identified.

A. Network Configuration

Consider that N cognitive users are randomly distributed over a square meter area. At the center of the field, a fusion center is deployed. Each cognitive user is preloaded with public and private key pair based on RSA and initialized with a random trust value between {0, 2}. It highlights important elements, including dynamic spectrum management, channel-state estimation, and radio scene analysis. Common uses for CRNs include spectrum trading, automatic interoperability, intelligent beamforming, opportunistic spectrum usage, and emergency services communication. CRNs are one of the main facilitators of contemporary networks due to their growing popularity in both industry and academics [24]. The radio spectrum is now divided among many wireless technologies. There are frequencies that are rarely used, leading to spectral inefficiency, even while the frequency spectrum in some mobile communications network frequency bands is becoming congested.

Latency can be increased, and data transmission can be slowed down by an abrupt spike in the number of users or an increase in the volume of data being transmitted over the network. Secondary Users (SUs) can sense licensed spectrum using a Cognitive Radio Network (CRN) and transmit if an idle band is identified. As a result, SUs must make quick use of the spectrum band as soon as it becomes accessible. In order to investigate how scalability affects a single node of the CRN and how SUs on cloud computing platforms may effectively optimize an idle band, this research suggests a novel Generalized Stochastic Petri Net (GSPN) model with intrusion detection. In this case, more resources are dynamically released to make extensive use of the spectrum space before the return of Primary Users (PUs) as soon as the band becomes unoccupied and there are SU requests awaiting encryption and transmission.

The clustering algorithm is used to meet the aforementioned criteria. In comparison to earlier clustering algorithms, this algorithm's cluster head selection necessitates resolving uneven clustering and increased communication costs. A model for optimum Cluster Head Selection (CHS) is created in relation to energy-conscious and safe routing in Wireless Sensor Networks (WSNs). Based on factors including distance, energy, security (risk likelihood), delay, trust assessment (direct and indirect trust), and Received Signal Strength Indicator (RSSI), the best CH is chosen in this case.

An SN functions as an active sensor during the data broadcast between BS and CH, and the WSN comprises a variety of SNs denoted by ZS. The WSN is often associated with data sensing, radio communication, sensor allocation, topological features, and energy consumption. In manual mode, the sensor is dispersed randomly over each application area. The CH is favored, and the number

of CHs is inferred by ZC, and the SNs are connected to create clusters. The cluster's SN must be within a small radius of the CH. Correlated data is collected by all the SNs from the predicted region and sent to the CH. The BS receives the information from the associated CH. A uniform distribution serves as the basis for each sink node's transmission pattern, which disperses data throughout the range's maximum radio frequency. Sensor nodes comprise this cluster, which resembles a network. For each cluster, the sentence identifies the appropriate cluster head. Cluster head-based routing is the collective term for this technique of spreading decrease from the cluster to the BS. Cluster head-based routing is the collective term for this technique of spreading decrease from the cluster to the BS. The distance between the cluster head and the base station is what the network model calls the distance between other nodes and the cluster head. The cluster head is selected for ease of transmission. The cluster head in the suggested model is selected according to RSSI, energy, latency, distance, security, and trust. It is intriguing to select a cluster head in order to get much more energy efficiency, power consumption, and energy load balancing during each cycle of the sensor nodes.

The authentication information of each cognitive user is stored in the fusion center. The entire initialization process of the network is divided into five phases as follows:

Step 1: Enable all cognitive trust values of the memorizer and set the FC coverage radius, the selected cluster head threshold, and the permitted maximum number of cluster heads L.

Step 2: Cognitive users report their position (xm, ym) and their initial trust value v to FC.

Step 3: FC picks up users whose trust values are higher than the threshold and records the total number as N.

Step 4: If N > L, FC should apply the following additional selection criteria:

- Cluster heads are expected to be above the FC.
- Any two selected cluster heads should be far enough away from each other.

Step 5: The L cognitive users are selected as cluster heads, and the trust value is stored as matrix V in the FC.

B. Phase-2: Resource Collection

The Fusion Center gathers knowledge about the primary user's available radio tools through a two-stage hybrid cooperative spectrum sensing algorithm. Various sensing methods encompass the following:

- Measurement of energy
- Matched filtration (MF)
- Cyclo-stationary identification

The most critical and fundamental technique is energy detection. In contrast to other methods, the detected signal is not previously aware of and resilient to unexplained fading multipath. The detection of energy depends on signal noise, but the exact noise power of the signal is almost impossible to determine. Energy detection has a huge disadvantage. To address this disadvantage, a technique based on statistical covariance or automatic correlation of the received signal was proposed. Two stages of decision-making on each continuum are carried out with regard to cluster-based architecture. The first point involves assigning cognitive users to a given spectrum in any sub-network. If n is the available number of radio resources and L is the number of cognitive subnetworks, then the sensed radio resource is assigned to each sub-network. If K is the number of cognitive users in any subset, K observations shall always be sent to the cluster head node. A data fusion based on the rules governing AND, OR, and majoritarian fusion is the clustered node. In order to compare sensing information, the fused information is sent to the melting station, where the final decision is made regarding any existing spectrum. The suggested algorithmic spectrum sensing phases are:

Step 1: The $x(n)$ represents the signal received and the sample number is Ns, and the covariance matrix of the signal received can be measured as Ns.

$$R_x(N_s) = \frac{1}{N_s}\sum_{n=L-1}^{L-2+n} x(n)x\dagger(n) \quad (1)$$

where, † Hermitian operation.

Step 2: The covariance matrix $R_x(N_s)$ determines the minimum and maximum self-values.

Step 3: To decide on signal detection by comparing the ratio $\frac{\lambda max}{\lambda min}$ with the threshold γ. If $\frac{\lambda max}{\lambda min} > \gamma$, then there is a signal; otherwise, it does not exist. The γ threshold can be calculated using the formula as follows:

$$\gamma = \left(\frac{\left(\sqrt{N_s}+\sqrt{ML}\right)^2}{\left(\sqrt{N_s}-\sqrt{ML}\right)^2}\right)\left[1+\frac{\left(\sqrt{N_s}+\sqrt{ML}\right)^{-2/3}}{(N_s\ ML)^{1/6}}\times F_1^{-1}(1-P_{fa})\right] \quad (2)$$

And the probability of false alarm is given as follows:

$$P_{fa} = 1 - F_1\left[\frac{\gamma\left(\sqrt{N_s}-\sqrt{ML}\right)^2-\mu}{\upsilon}\right] \quad (3)$$

Ns is the number of samples; *M* is the factor of oversampling and L is the factor of smoothing. The probability of detection can be measured using the formula provided, depending on the false alarm probability and threshold:

$$P_d = 1 - F_1\left[\frac{\gamma N_s+\frac{N_s(\gamma\rho ML-\rho)}{\sigma_n^2}-\mu}{\upsilon}\right] \quad (4)$$

where $F_1(t)$ is the Tracy-Widom distribution function.

C. Phase-3: Calculation of Trust – Penalty and Reward

Trust may be measured on the basis of further contact with other users and is responsible for further activity on the network by the user. The reputation of a cognitive user can be described as an evaluation by other users or a description of the past behavior of a cognitive user. The trust model should have the following characteristics:

- The ability to detect and withstand security threats such as hacking, checking fraudulently, etc. Attack resistance.
- The measured trust should be based on the outcomes of the continuous learning process and will deteriorate over time.
- The trust scheme must have provision for remuneration and penalties.
- The Trust Determination Scheme must ensure that the new consumer is authenticated.

In addition to the attributes listed above, the trust model must include a trust management mechanism involving the creation, presentation, measurement, punishment, and updating of trust facilities.

1) Generation of trust

Mechanisms to generate trust involve building trust based on sharing and communication of resources, driven by demand. An authentication header is provided for all trust reports by the fusion center.

2) Characterization of trust

The structure of the three layers for the trust given as:

$$Trust = \mathrm{V} \times \mathrm{R} \times A \quad (5)$$

V indicates an honest or malicious group of cognitive users. *R* represents the cognitive area of the radio network and *A* is the fusion center attribute that could be defined as the interaction quality (TQ), service quality (SQ), cost of CM, time for processing (PT). By changing the weight of the attribute as follows, interactive confidence for different cognitive users can be determined.

$$\mathrm{U} = a \cdot RQ + b \cdot TQ + c \cdot PT + \mathrm{d}.\, CM \quad (6)$$

The attribute weight elements here a, b, c and d fulfil the condition + $b + c + d = 1$.

The cluster leader collects and reports on the importance of trust for the uniting core in this network architecture. Each cognitive user interacts in any subnetwork with the cluster header so as to generate a trust value. The confidence value is stored with the cluster header in the trust vector $ei = [ei1, ei2, ..., ein]$, where the number of cognitive users in each sub-network is *n*. Each head cluster report collects confidence value at the fusion center or through a trust poll where each user's confidence is measured in a certain time called polling time. The fusion center collects trust value through trust reports (Tpoll). In both cases, the data is stored as follows in the fusion center's confidence matrix:

$$\mathrm{E} = \begin{bmatrix} e_{11}\ e_{12}\ldots\ldots e_{1k1} \\ e_{21}\ \ e_{22}\ldots\ldots e_{2k2} \\ e_{n1}\ e_{n2}\ldots . e_{nkt} \end{bmatrix} \quad (7)$$

where *n* = Number of network cluster header

The number of cognitive users within each head of the cluster is *ki* = 1, 2, ..., *n*).

Suppose that there are m cognitive users in *SRi*. The network initially verifies the direct interaction experience between user SUi and the cluster header SUh when a new cognitive user SUi wishes to connect.

The general confidence assessment between user *i* and user *j* is:

$$Trij = \Phi.\, DiTrij + \delta.\, InTrij + \mu.\, HisTri + rew \quad (8)$$

where,

Φ = Standardized factor of weight equal to DiTrij direct confidence

δ = *Standardized* indirect confidence equivalent weight factor In *Trij*

μ= *Standardized* weight factor comparable to historical trust $HisTri$

Also, $\Phi + \delta + \mu = 1$

rew = Rewarding trust.

The basic trust matrices for users can be given as: based on the above discussion:

3) Trust value (Direct)

Direct trust is the product of the interaction between the cluster head and the cognitive consumer. By reducing the influence that nodes with more uncertainty may have on the measurement, the NUT model seeks to reduce the measurement's total uncertainty at the network level. The notions of reputation, trust, and uncertainty are applied to the network of measuring nodes.

$$\mathrm{DirTrih} = \frac{1}{n}\sum_{l=1}^{n} \mathrm{A}(\mathrm{s}, t_1) \times \mathrm{Attr}_{ik} \times DS_{ih}^{l} \quad (9)$$

l = Interaction Frequency

$DSih$= SUh to S satisfaction assessment,

$DSih = \{SQ, TQ, PT, CM\}$

$Attrih$ = [ ] is the matrix coefficient of the weight of $DSih$.

The attenuation function is expressed as:

$$\mathrm{A}(\mathrm{s}, t_1) = \upsilon.\, e^{-s.L(t_l)} \quad (10)$$

where, *d* =decay rate ($0 < s \leq 1$)

I(tl)= Interactive Time Function

$\mathrm{I}(tl) = Round((tl - t0)/T)$

sp= Duration of scanning.

4) Trust value (Indirect)

Similarly, for interactions between user I and other $m-2$ users in the subnetwork the indirect trust value is determined as follows:

$$\mathrm{INDirTrih} = \frac{1}{n(m-2)}\sum_{k=1}^{m-2}\sum_{l=1}^{n} \mathrm{A}(\mathrm{s}, t_1) \times \mathrm{Attr}_{ik} \times DS_{ik}^{l} \quad (11)$$

5) Historical trust

The trust value (HistTr) in the past round of observation is the absolute value of the approximate trust. During the observation time, the trust value HistTi—a deterministic value but not a vector—between the user, cluster header, and FC will be recorded by cognitive users who have previously visited the network but have since departed or whose trust value license has expired.

6) Reward

Based on its reliability, the reward value of trust applies to the overall confidence of a cognitive consumer. It is used by cognitive users to promote honest behavior and the following:

$$r(t) = \lambda.\, k\left(\frac{Act_i(t).A(s,t)}{Dev(t)}\right) \quad (12)$$

Here, λ is the reward factor, $k(.)$ is the standard function and the trust differences in user value, Acti(t), A(s, t), Dev(t) is the operation material matrix. The Activity Matrix reflects the user-to-user interaction in the network and is given by:

$$Act_i(t) = \left(\frac{\sum j \epsilon C\ IndTrij}{\sum k, j \epsilon C\ IndTrkj}\right) \quad (13)$$

The attenuation function is used to restrict trust value in the predefined range and let v be the initial trust value, ¨is the attenuation factor, s is the attenuation rate and t is the scanning time.

$$A(s,t) = \sigma.round(10.\upsilon.e^{-st}) \quad (14)$$

The User Evaluation Trust Difference is a measure of the transformation of the trust value of any user in a given time and is given by:

$$Dev(t) = Var(Tr_i(t)) \quad (15)$$

The values of Eqs. (13−15) are used to determine the incentive value for each consumer.

7) Punishment mechanism

The Fusion Center is responsible not only for storing and distributing award confidence but also for penalizing misconduct and malicious users. The network's cognitive features make it vulnerable to various attacks. In essence, there are two types of online attackers: a malicious attacker and a gullible attacker. The altered trust value curves for three different user assault types. Users' trust values are initially equal to one another. After the user initiates, the value of its trust will shift. Because they have caused the network to be destroyed, the malevolent users are harshly punished. They are, therefore, relevant to example 1, and their trust levels drop to less than −1 right away. However, the recovery of trust value is a progressive process and is intended to allow re-access to the network following a penalty time, which is consistent with attenuation [25].

Both a data channel and a common control channel employed the punishment mechanism. The outcomes of the simulations demonstrate that the suggested punishment mechanism enhances the self-giving cooperation between nodes in the networks and raises the cognitive radio networks' fairness index. We examine the traits of selfish behavior and the ways in which it may be identified. This research developed a strict punishment mechanism based on network traffic to enhance the self-giving cooperation among nodes in cognitive radio networks and raise the fairness index of the entire network. Both a data channel and a common control channel employed the punishment mechanism. The outcomes of the simulations demonstrate that the suggested punishment mechanism enhances the self-giving cooperation between nodes in the networks and raises the cognitive radio networks' fairness index. When both are detected, depending on the intensity of the attack, they are treated differently. This can lead to malicious users causing SSDF, PUEA, and Denial of Service (DoS) attacks when detected; users of that kind should be punished quickly and released slowly. For malicious users, the penalty feature is as follows:

$$pen_1(t) = -\beta.e^{-\zeta t} + £ \quad (16)$$

where, $\beta \in (0, 3)$ penalty factor. $\zeta > 0$ recovery factor $£$ = regulation factor.

We demonstrate the variation rule of honest users who do not attack or engage in misbehavior, where the X-axis indicates the time of interaction and the Y-axis represents the trust level, which spans from −2 to 2. The normalized weight factors of $\alpha = 0.85$, $\beta = 0.1$, and $\gamma = 0.05$ were used to provide a range of direct trust ratings that gradually increase and mostly stay constant.

Greedy users frequently inform that the main user dominates a certain spectrum that leaves the spectrum band for all the other users. Thus, a greedy user obtains the exclusive use of a particular spectrum. Gullible users should be sanctioned and published gradually as they are not distracting. The following can be stated:

$$pen_2(t) = -\beta.e^{-\zeta t^2} + £ \quad (17)$$

a) Phase-4: Resource allocation

The Fusion Center has the right, according to the trust of any user, to grant or deny any user access to a particular resource. Therefore, a resource allocation scheme based on the threshold is taken into account. If FC provides services to SUs whose trust value exceeds that resource's access threshold ($vij \geq \lambda i$).

b) Phase-5: Information security at the physical layer

The hostile intruder in this assault mimics primary user transmissions in order to stop them from communicating and disclosing their original data. It gives the impression that the channel is busy with the secondary users. Furthermore, this assault uses a lot more energy than traditional communication since the hacker continuously scans the channel for transmission chances. The malevolent SU impersonating a PU in order to exploit the spectrum selfishly and without disclosing it to other users is known as the PU Emulation Attack. The SUs is unable to use the white space because of the false identification. In fact, the licensed PU's existence is detected wrongly by the SUs. On the other hand, the malicious emulator greedily takes use of the resource while the channel remains idle. In order to determine which unlawful route, the self-centered PUEA attackers.

The idea of a cognitive network contends that CNs are a way to handle the intricacy of the wireless medium, network parameters, and end-to-end goal needs. Specifically, we contend that the local and reactive approach of networking protocols is unable to address or comprehend the complexity of wireless networks. Due to their commonalities, we show how CNs relate to two other techniques for handling these complexities: CRs and cross-layer design. Their advantages and disadvantages in a networking setting are demonstrated, showing how many of the features that are missing from their feature list are present in a CN, altering the user's successful transmission rate standards for different types of attacks. We take into account the FC's incentive and penalty programs, the attenuation of cognitive users' trust values, etc. We Suppose that the initial successful transmission rate for each user is 0.9. The successful transmission rate of honest cognitive users increases continuously as the interactional time increases and gradually approaches 1 that complies with the reward scheme, even in the absence of attackers.

On the other hand, when attacks take place, the successful transmission rate steadily decreases because FC controls all users and has the ability to punish misbehavior to lower the trust value in order to accomplish the goal of preventing access to cognitive networks.

The time it takes for trust values to recover from the three types of frequent attacks. The graph indicates that the value of the restored trust is somewhat less than the value prior to punishment. If users repeatedly attack, they will be

barred from accessing the network as part of this punishment plan designed to restrain attackers.

The utilization of deep learning techniques in cognitive radio networks can significantly enhance the network's capability to adapt to changing environments and improve the overall system's efficiency and reliability. As the demand for higher data rates and connectivity increases, B5G/6G wireless networks are expected to enable new services and applications significantly. Therefore, the significance of deep learning in addressing cognitive radio network challenges cannot be overstated.

Denial of Service (DoS) and network degradation are possible outcomes of this type of assault. It also entails making use of unclaimed frequency bands. The attackers can jam a range of frequencies in one stretch (barrage jamming), sweep over the frequency range (sweep jamming), or target a single frequency (spot jamming). A single jammer or a group of jammers working together may also carry out the assaults, lowering user throughput by extracting more information from the channel.

Additionally, the attackers might cycle between attacking and resting modes or broadcast jamming signals continually.

Because Cognitive Radio Networks (CRNs) offer and share resources, they are exposed to several safety risks, such as eavesdropping. Both the main and secondary networks can simultaneously use the same spectrum band in the current situation. In order for eavesdroppers to be completely safe, the basic idea behind eavesdropper data security is to strengthen the main channel of the legitimate receiver. Consider the situation of contact when a Secondary User (SU-1) shares a Primary User'S (PU) spectrum in the presence of an eavesdropper to relay data to a Secondary User (SU-2). This research concentrates on the cognitive radio architecture of clusters so that the eavesdropper may be a secondary malicious user in the same subnetwork of an infected cluster header.

Single and Identically Distributed (I.I.D) Rayleigh fading both the primary Channel (SU1 to SU2) and the secondary Channel (SU1 to Eavesdropper). The coefficient for the channel is *hM*, which implies that the channel is almost static, i.e., for all channel operators the channel coefficients are constant, therefore $h(i) = hM$ total. Let *nM* indicate zero-mean Gaussian noise that is circularly symmetrically complex.

Let SU-1 want to send a message block to SU-2 encoded with:

$$x(n) = [x(1), x(2) \dots \dots \dots, x(n)] \tag{18}$$

The signal received by the SU-2 will be:

$$Y_M(i) = h_M(i)X(i) + n_M(i) \tag{19}$$

And the channel output to the eavesdropper:

$$Y_E(i) = h_E(i)X(i) + n_E(i) \tag{20}$$

where h_E and n_E have the same characteristics as the main channel, and the eavesdroppers' noise. Also, the power of the channel is believed to be constrained:

$$\frac{1}{n}\sum_{i-1}^{n} \mathrm{E}[|X(i)^2|] < P \tag{21}$$

Allow N_M and N_E to reflect on the channel main and eavesdropper. Then the SNR in SU-2 is instant:

$$\gamma_M(i) = \frac{\mathrm{P}|H_M(\mathrm{i})|^2}{N_M} = \frac{\mathrm{P}|H_M|^2}{N_M} = \gamma_M \tag{22}$$

Average SNR:

$$\bar{\gamma_M}(i) = \frac{\mathrm{PE}|H_M(\mathrm{i})|^2}{N_M} = \frac{\mathrm{PE}|H_M|^2}{N_M} = \bar{\gamma_M} \tag{23}$$

Eavesdropped instantaneous SNR:

$$\gamma E\ (i) = \frac{\mathrm{P}|H_E(\mathrm{i})|^2}{N_E} = \frac{\mathrm{P}|H_E|\,2}{N_E} = \gamma E \tag{24}$$

Average SNR:

$$\bar{\gamma E}\ (i) = \frac{\mathrm{PE}|H_E(\mathrm{i})|^2\,]}{N_E} = \frac{\mathrm{PE}[|H_E|\,2\,]}{N_E} = \bar{\gamma E} \tag{25}$$

Assuming that the SU-1 and SU-2 interact through the normal AWGN channel with N_M noise, the observation of the Eavesdropper is also distorted by Gaussian noise with Noise power $\mathrm{N_E}$, where $N_E > N_M$. Under this condition, the capacity for confidentiality can be calculated by the formula:

$$C_s = C_M - C_E \tag{26}$$

where C_M, C_E represents both the main power channel (SU-1 to SU-2) and the channel of the eavesdropper and can be detected with this formula:

$$CM = \frac{1}{2}\log\,(1 + \frac{P}{NM}) \tag{27}$$

$$CE = \frac{1}{2}\log\,(1 + \frac{P}{NM}) \tag{28}$$

If the complex AWGN channel is two real-established AWGN channels. The confidentiality capacity of the complex wiretap channel is calculated in such a case by:

$$C_s = \log\left(1 + \frac{P}{N_M}\right) - \log\left(1 + \frac{P}{N_W}\right) \tag{29}$$

Since the main and eavesdropper channels are assumed to be quasi-static, the confidentiality capacity will be:

$$\mathrm{C}s = \begin{cases} \log(1 + \gamma\mathrm{M}) - \log(1 + \gamma\mathrm{E}) & \text{if } \gamma\mathrm{M} > \gamma E \\ 0 & \text{if } \gamma\mathrm{M} \le \gamma\mathrm{E} \end{cases} \tag{30}$$

The probability of a hidden loss, i.e. the probability that the instant confidentiality capacity is less than the Rs > 0 target confidentiality limit, can be given as:

$$P_{out}(Rs) = P(Cs < Rs) \tag{31}$$

Invoking the total probability theorem,

$$\mathcal{P}_{out}(Rs) = \mathcal{P}(Cs < Rs\,|\gamma M > \gamma E)\mathcal{P}(\gamma M > \gamma E) + \mathcal{P}(Cs < Rs\,|\gamma M \le \gamma E)\mathcal{P}(\gamma M \le \gamma E) \tag{32}$$

$$\text{Now, } (\gamma M > \ ) = \frac{\bar{\gamma}\mathrm{M}}{\bar{\gamma}\mathrm{M} + \bar{\gamma}\mathrm{E}} \tag{33}$$

Consequently, we have:

$$(\gamma M \le \gamma E) = 1 - (\gamma M > \ ) = \frac{\bar{\gamma}\mathrm{M}}{\bar{\gamma}\mathrm{M} + \bar{\gamma}\mathrm{E}} \tag{34}$$

On the other hand, $(Cs < Rs\,|\gamma M > \ ) = \mathcal{P}(\log(1 + \gamma M) - \log(1 + \gamma E) < Rs \mid \gamma M > \gamma E) = \mathcal{P}(\gamma M < 2Rs\,(1 + \gamma E) - 1|\gamma M > \gamma E)$:

$$= \int_0^{\infty} \int_{\gamma E}^{2\,Rs(1+\gamma E)-1} \mathcal{P}(\gamma M, \gamma E | \gamma M > \gamma E) d\gamma E d\gamma M$$
$$= \int_0^{\infty} \int_{\gamma E}^{2\,Rs(1+\gamma E)-1} \cdot \frac{\mathcal{P}(\gamma M)\mathcal{P}(\gamma E)}{\mathcal{P}(\gamma M > \gamma E)} d\gamma E d\gamma M$$
$$= 1 - \bar{\gamma M} + \frac{\bar{\gamma E}}{\bar{\gamma M} + 2Rs\bar{\gamma E}} \exp \frac{(-2\,Rs-1)}{\bar{\gamma M}} \quad (35)$$

Since $R_s > 0$,

$$(Cs < R_s \,|\gamma M \leq \gamma E\,) = 1 \quad (36)$$

On combining these Eqs. (33), (34), (35) and (36), the result is given as:

$$\mathcal{P}_{out}(R_s) = 1 - \frac{\bar{\gamma M}}{\bar{\gamma M} + 2Rs\bar{\gamma W}} \bar{\gamma M} \exp \frac{(-2\,Rs-1)}{\bar{\gamma M}} \quad (37)$$

IV. Results

Five primary and five secondary users were provided to reflect the cognitions process with a simulation scenario based on MATLAB. In this section, we present the numerical results for the proposed mechanism. The main parameters used for the simulations are L = 10, K = 50, λ = {1.2, 1.5, 1.8}, Rf =1,500 ms and the simulations are conducted in MATLAB R2012b environment.

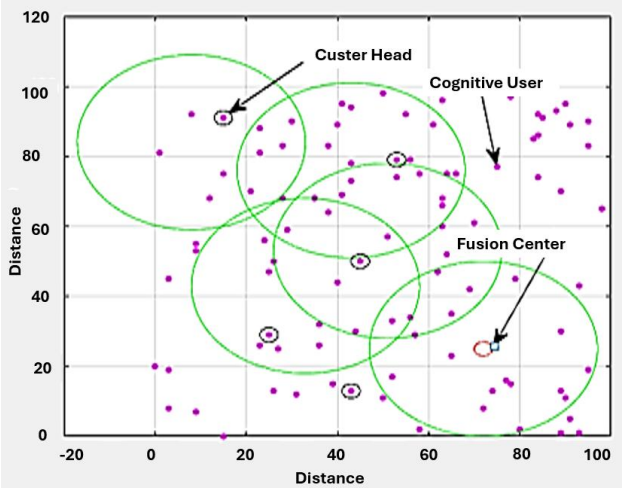

Fig. 3. Cluster head selection.

With simulation parameters, the simulation scenario is generated as given below in Fig. 3 that presents a two-level hierarchy network simulation model for the proposed cognitive radio network security system. The Fusion Center is located at the highest level of the hierarchy and is responsible for authenticating the customer who is coming in, selecting the available resources, and implementing the compensation and penalty scheme. Cluster heads are available on the second level of the hierarchy and are responsible for collecting and forwarding trust values to the fusion center. Also, the cluster head should notify the fusion core if an attack is detected. By keeping an eye on different cluster nodes, a cluster head initiates the maintenance procedure. According to the various methods, a member would be automatically removed from the neighbor list if it lost contact with the cluster leader. The main simulation objects are the variation rule of trust value, attenuation characteristics of trust value, cluster head selection scheme, penalty scheme and complexity analysis.

In Fig. 4, where the X-axis represents the contact duration and the Y-axis represents the trust level, which ranges from −2 to 2 that exhibit the variation rule of honest users who do not attack or engage in misbehavior. With

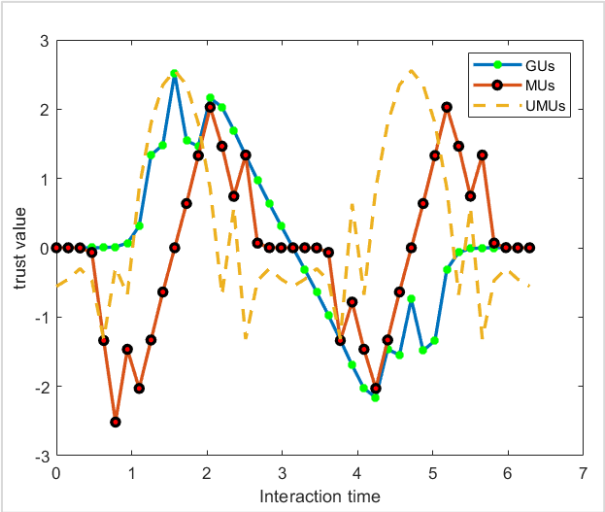

Fig. 4. Change the confidence value in three attack types.

the normalized weight factors set at α = 0.85, β = 0.1, and γ = 0.05, a series of direct trust values that progressively rise and generally remain steady were obtained. Each licensed user has a 1 kHz frequency band, which secondary users can use opportunistically. This entire process can be understood using a series of Power Spectral Density (PSD) plots.

Similarly, the cluster is deemed dead, and the cluster head will begin the neighbor-finding process if all linked members no longer have ties to the cluster head. Depending on several algorithms and security considerations, the cluster head will either approve or deny an affiliation request from a new node. In some instances, the primary cluster head uses certain metrics to choose the backup cluster head. The interaction time is represented by the Y-axis, and the trust value by the X-axis. In Cognitive Radio Networks (CRNs), a node's trustworthiness is assessed using a measure called trusted value or Trust Value (TV). The communication properties of the requesting node are used to determine the trust value. A transceiver can identify which communication channels are being used and which are not in CRNs. After that, the transceiver can enter open channels without disturbing authorized users. In Cognitive Radio Networks (CRNs), interaction time defined in the spectrum mobility management seeks to reduce spectrum handoff delay for low communication latency. Important data on the length of the spectrum handoff may be obtained using sensing techniques. Fig. 4 shows the modified trust value curves for three types of attack users

In the beginning, the user's confidence values are equal to each other. When an attack is initiated by the user, the trust value of the attack can change. By carrying out the various stages of the Cognitive Radio Network (CRN)

cycle—sensing, decision-making, sharing (accessing), and hand-off (mobility)—the CU nodes are able to access the available bands/channels. The hand-off phase is the most crucial of these as, when a PU emerges, the CU must remember all of its prior operations in order to transition its ongoing data transmissions to another accessible channel.

Additionally, from a security standpoint, a Malicious User (MU) could mimic the PU signal with the goal of preventing the CU from ever using its idle band, which eventually impairs network performance. Attacks such as the Cognitive User Emulation Attack (CUEA) and Primary User Emulation Attack (PUEA) may be encountered by the handoff procedure, which need to be resolved.

To address this issue, a secure and trusted routing and handoff mechanism is proposed specifically for the CRN environment, where malicious devices are identified at the lower layers, thus prohibiting them from being part of the communication network. Further, at the network layer, users need to secure their data that is transmitted through various intermediate nodes. To ensure a secure handoff and routing mechanism, a Trust Analyser (TA) is introduced between the CU nodes and network layer.

UMUs are the most common type of attacker. This kind of assault is simple to identify and doesn't pose any harmful subjective threats to the network. The successful transmission rate curve appears to decline as FC shows significant tolerance for this attack, resulting in a reduced penalty level. GUs are the second type of attacker that may quickly destroy the network, leading to unequal resource allocation.

As a result, FC faces harsher penalties for this kind of attack. The punishment impact is evident, and the successful transmission rate drops more sharply because of the existing punishment time and decreased trust levels. SSDF and PUEA are included in the third class of MUs. This kind of attack carries the worst punishment, and if the culprits are identified, they will face swift consequences. As a result, the successful transmission rate curve graphs show a steep decline. Under centralized management, PUEA has a higher detection probability than SSDF [26], making it easier for FC to identify them and causing their transmission rate to drop more quickly than SSDF. The findings of the simulation demonstrate that security management based on the trust value mechanism successfully protects the transmission rate of honest users while partially or completely shielding misbehaving users and validating a stronger anti-attack capability than the system possesses. Malicious users are seriously disciplined for damaging the network. Figure 5 shows that the trust value recovery time is dependent on three forms of regular attacks.

In Fig. 4, Factor μ = 0 of penalty accumulation Cycle diagram of the trust value recovery. The figure illustrates that the returned value of the trust is slightly less than the pre-penalty value. Under this penalty system, users would be barred from network access if targeted repeatedly. We determine the best channel allocation and admission control choices for cognitive overlay networks to accommodate unlicensed users' delay-sensitive communications. We solve it by converting the original formulation into a stochastic shortest path problem, which we express as a Markov decision process issue [20]. Next, we present a straightforward heuristic control strategy that consists of a largest-delay-first channel allocation scheme and a threshold-based admission control method. We also demonstrate that the latter is the most effective. Using the rollout algorithm, we also suggest an enhanced policy. The effectiveness of Cooperative Spectrum Sensing (CSS) in enhancing Cognitive Radio Networks' (CRNs') sensing capabilities has been confirmed. We examine a fundamental trade-off between the sensing, reporting, and transmission periods of CSS and assess the effect of the fusion rule with varying numbers of local sensing results, in contrast to previous works that typically consider fusion with fixed inputs and neglect the duration of the reporting period in the design. More specifically, the sensing time might be exchanged for longer transmission time or more mini slots to provide more local sensing findings for fusion. Fig. 5 illustrates the relationship between the load on the network and the user size.

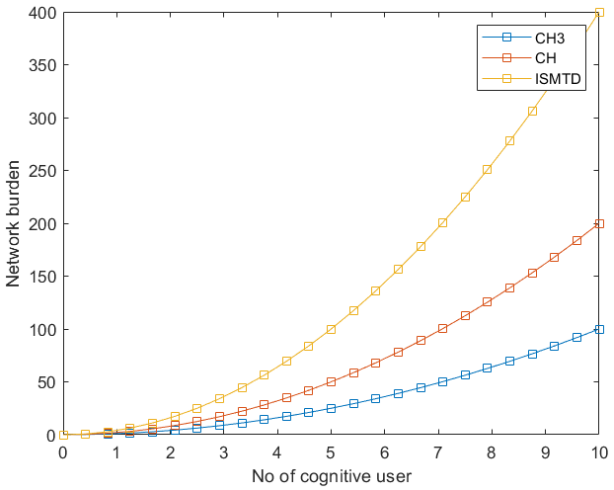

Fig. 5. The relationship between the load on the network and the user size.

A Network Load is a key index for assessing the proposed process, specifically in terms of user management complexity. We see that when the network scale is small, the network load on the proposed mechanism is comparatively higher, as the proposed mechanism has an additional burden on the added trust authentication function, the selection of cluster heads and penalty functions, etc. However, our proposed mechanism shows better results, with the increasing size of the network. The probability of detecting Signal-to-Noise Ratio (SNR) in MATLAB code uses different parameters as follows:

```
%% system model parameters
pf=.1; % target probability of false alarm
pd=.9; % target probability of detection
R=500:2:2000; % distance between PU TX and each SU TX
iter=10000;
```

```
d0=1; % reference distance
n=3; % path loss exponent
R_pu=500; % primary user transmission radius
R_su=384.9326; % secondary user transmission radius
protection_factor=.95;
p_n_dbm=-100;% noise p
pd=.9; % target probability of detection
R=500:2:2000; % distance between PU TX and each SU
TX
iter=10000;
d0=1; % reference distance
n=3; % path loss exponent
R_pu=500; % primary user transmission radius
R_su=384.9326; % secondary user transmission radius
protection_factor=.95;
p_n_dbm=-100;% noise power in dbm
p_n_db=-100-30;
p_n=10^((p_n_dbm-30)/10);% noise power in watt
snr_su_lim_db=3; % snr threshold for successful reception
      snr_su_lim=10^(snr_su_lim_db/10);
      snr_pu_lim_db=3;
snr_pu_lim=10^(snr_pu_lim_db/10);
```

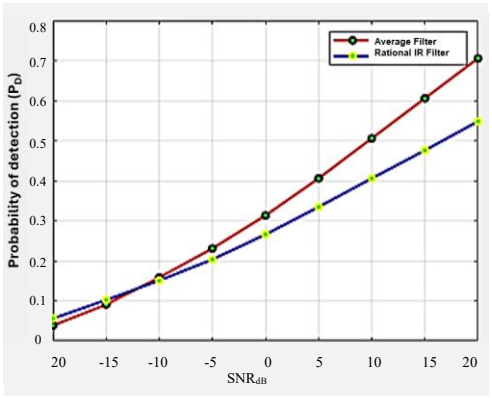

Fig. 6. Probability of detection for various SNR.

Fig. 6 illustrated that Probability of detection for various SNR. The signal-to-noise ratio is a key parameter characterizing spectrum sensing algorithm efficiency. The detection accuracy of a spectrum sensing algorithm is influenced by the Signal-to-Noise Ratio (SNR). A simulation scenario is developed to show the effect of SNR on the probabilities of detection. The suggested system establishes the threshold on the Average Received Signal Strength (RSS) of a primary signal below which feature detection is preferred and decides whether energy or feature detection incurs less sensing overhead at each SNR level. We showed that when collaborative sensing utilizes its geographic diversity, energy detection under lognormal shadowing can still perform effectively at the average SNR < SNRwall. The figure shows, for −22 dB SNR, that a probability of detection is 0.5 for PFA equivalent to 0.2, 0.75 for PFA equivalent to 0.4, and 0.9 for PFA equivalent to 0.6 for PFA.

The mass detection probability used the following parameter in for detection range in the 80%. Cognitive users N=150 and cluster head L= [3 5 10] are the parameters for network sizing. As shown in Fig. 8, there is a connection between the network effort and the number of users.

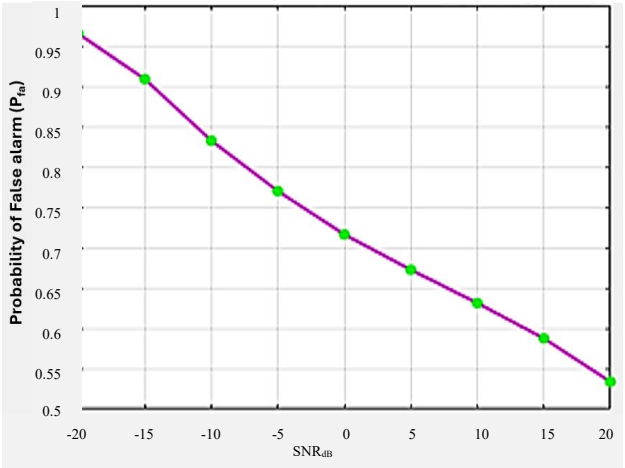

Fig. 7. False alarm probability for the model.

Fig. 8 shows the estimation for the proposed PUEA analytical model of the probability of false alarm. As can be seen, 500 iterations of PFA range from 0.2 to 0.25. Fig. 8 is the result of the proposed study's resource collection process. Change in the probability of detection is shown with SNR with a distinct probability of false alarm. The false alarm probability is also used in different parameters as follows:

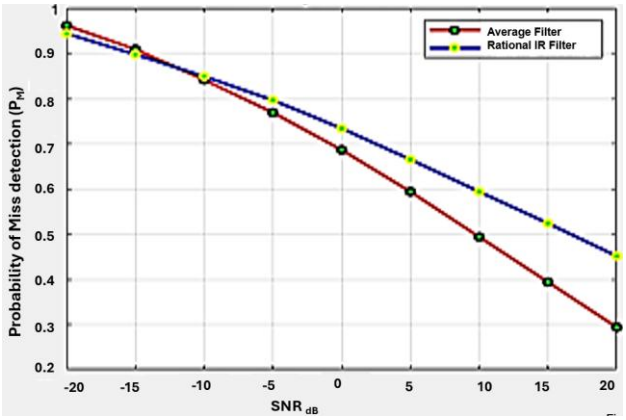

Fig. 8. Miss detection probability for the model.

Fig. 8 shows the estimated probability of not having detected the proposed PUEA detection analytical model. For 500 iterations simulation is done, and it is clear from the above figure that the chance of not detecting the proposed scenario ranges from 0.11 to 0.15. The false alarm and miss detection comparison are used in various parameters.

Fig. 9 shows the simulation result for the analysis of false alarms and the probability that they will be undetected. The simulation was conducted over 500 iterations with a threshold value of 2, considering a scenario with 10 malicious users. This simulation has confirmed the effectiveness and rationale of the mechanism discussed in this work. When compared to other mechanisms, the advantages of this approach are primarily expressed as follows:

- A trust model that aligns with the fundamental traits of human society
- To apply various penalties in accordance with the various attack kinds
- The network management complexity is successfully decreased by the FC + CH hierarchical architecture.

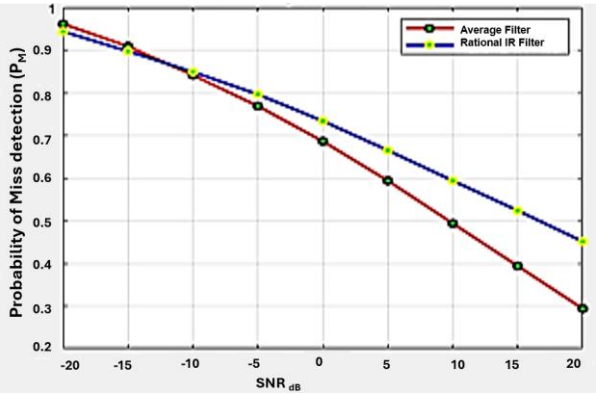

Fig. 9. False alarm and miss detection comparison for the model.

V. Conclusion

This paper discussed the challenges of fighting attacks on cognitive wireless networks. We also found that a large number of research studies focused on the detection of attackers, but also a number of important literature studies on how they can be handled while the mechanism is detected and optimised. We therefore proposed a new trust and penalty mechanism to address security concerns in the CRNs. The proposed mechanism has been confirmed to be superior to other mechanisms and to comply with current application criteria.

A survey on guarding PUEA and SSDF assaults was conducted, and the defense measures were divided into two categories: active (rapid attack detection) and passive (delayed attack detection). The cognitive radio network's defense mechanisms and a variety of assaults that target its physical layer have been examined and contrasted. The primary user emulation attack is one type of physical layer attack. The primary user signal is faked in a Primary User Emulation Attack (PUEA) to trick cognitive users into thinking the spectrum is not empty, preventing secondary users from using the channel. In reality, a number of flaws can significantly impair a CR system's performance, including noise uncertainty, channel/interference uncertainty, hardware flaws in the transceiver, signal uncertainty, and synchronization problems. For this reason, it is crucial to investigate workable ways to address different practical flaws to use cognitive technology successfully. So, in this direction, this survey report offers a summary of the enabling strategies for CR communications. The primary flaws that might arise in the most popular CR paradigms are then covered, and the current methods for fixing these flaws are reviewed.

The versions of the tools that are based on the cognitive radio network simulator are given below. Researchers may choose from a variety of tools and obtain comprehensive information about them.

Every module of the cognitive radio network has to be understood by researchers, and we provide research students with all the assistance they need to comprehend and use each module in the cognitive radio network simulator. For convenience, we have only highlighted the two main modules. Here, we have listed the study topics together with the relevant cognitive radio network simulator tools.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Himanshu Sharma and K. Kishore Kumar proposed the punishment mechanism for CRNs; G. Nithya conducted simulations and performance analysis; V. Ravi Kumar integrated trust metrics into the framework; Shashi Kant Darga carried out comparative evaluation; Amit Gupta finalized the manuscript and refined methodology; all authors reviewed and approved the final version.

References

[1] I. A. Sohu, A. A. Rahimoon, A. A. Junejo, A. A. Sohu, and S. H. Junejo, "Analogous study of security threats in cognitive radio," in *Proc. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, pp. 1–4.

[2] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. 2009 43rd Annual Conference on Information Sciences and Systems*, 2009, pp. 130–134.

[3] E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system," in *Proc. 2010 IEEE 71st Vehicular Technology Conference*, 2010, pp. 1–5.

[4] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*, 2009, pp. 1–6.

[5] T. Bansal, B. Chen, and P. Sinha, "FastProbe: Malicious user detection in cognitive radio networks through active transmissions," in *Proc. IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014, pp. 2517–2525.

[6] X. Huang, N. Han, G. Zheng, S. Sohn, and J. Kim, "Weighted-collaborative spectrum sensing in cognitive radio," in *Proc. 2007 Second International Conference on Communications and Networking in China*, 2007, pp. 110–114.

[7] M. Matsui, H. Shiba, K. Akabane, and K. Uehara, "A novel cooperative sensing technique for cognitive radio," in *Proc. 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1–5.

[8] K. C. Chen, P. Y. Chen, N. Prasad, Y. C. Liang, and S. Sun, "Trusted cognitive radio networking," *Wirel. Commun. Mob. Comput.*, vol. 10, no. 4, pp. 467–485, 2010.

[9] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008, pp. 1–8.

[10] S. Kar, S. Sethi, and R. K. Sahoo, "A multi-factor trusts management scheme for secure spectrum sensing in cognitive radio networks," *Wirel. Pers. Commun.*, vol. 97, no. 2, pp. 2523–2540, 2017.

[11] A. Gupta, M. Pavani, S. K. Dargar, A. Dargar, and A. S. Chouhan, "Improved extreme learning machine-based hunger games search for automatic IP configuration and duplicate node detection machine learning," *J. Commun.*, vol. 19, no. 3, pp. 152–160, 2024. DOI: 10.12720/jcm.19.3.152–160

[12] Z. Meng, L. Wei, and H. Yu, "Harvesting-throughput tradeoff for CDMA-based underlay cognitive radio networks with wireless energy harvesting," *Electron. Lett.*, vol. 52, no. 10, pp. 881–883, 2016.
[13] A. D. Aishwarya, S. Saranya, A. Sathiya, and J. S. Manoharan, "Optimizing wireless sensor network routing through memetic algorithms: Enhancing energy efficiency and data reliability," *Procedia Comput. Sci.*, vol. 230, pp. 150–157, 2023.
[14] S. Saranya and P. Jayarajan, "Enhanced deep learning-based optimization model for the optimal energy efficiency-oriented cognitive radio networks," *Ain Shams Eng. J.*, vol. 103051, 2024. https://doi.org/10.1016/j.asej.2024.103051
[15] M. Ali, M. N. Yasir, D. M. S. Bhatti, and H. Nam, "Optimization of spectrum utilization efficiency in cognitive radio networks," *IEEE Wirel. Commun. Lett.*, vol. 12, no. 3, pp. 426–430, 2023.
[16] A. A. Olawole and F. Takawira, "Resource allocation in multi-cluster cognitive radio networks with energy harvesting for hybrid multi-channel access," *IEEE Access*, vol. 11, pp. 38982–38998, 2023.
[17] A. Gupta, S. K. Dargar, and A. Dargar, "House prices prediction using machine learning regression models," in *Proc. 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, Tumkur, Karnataka, India, 2022, pp. 1–5.
[18] J. Wang, I.-R. Chen, J. J. P. Tsai, and D.-C. Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," *Comput. Commun.*, vol. 116, pp. 90–100, 2018.
[19] A. Gupta, S. K. Dargar, B. Raghavaiah, and A. V. N. Rao, "Recessed ground parasitic rectangular patch antenna for wireless communication," in *Proc. ICAIS 2022*, 2022.
[20] K. Zeng, P. Pawelczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 226–228, 2010.
[21] S. Mapunya and M. Velempini, "Investigating spectrum sensing security threats in cognitive radio networks," *Ad. Hoc. Networks*, pp. 60–68, 2018.
[22] 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.*, no. 1, Art. 48, 2014.
[23] 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. 1, pp. 133–140, 2019.
[24] H. Sharma and K. Kumar, "Primary user emulation attack analysis on cognitive radio," *Indian J. Sci. Technol.*, vol. 9, no. 14, pp. 1–6, 2016.
[25] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1691–1708, 2012.
[26] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 428–445, 2012.