OT-IDS-CR: OPTIMAL TRUSTED INTRUSION DETECTION SYSTEM FOR COOPERATIVE SPECTRUM SENSING AND ALLOCATION IN COGNITIVE RADIO NETWORKS

A. Krishna Srikanth[1*] and A.Ch. Sudhir[2]

Abstract

Cognitive radio network (CRN) is the main solutions for the efficient spectrum band utilization. The rapid growth of services demand new spectrum bands which affects the effective utilization of resources ie. spectrum scarcity. Cooperative spectrum sensing (CSS) is the standard method to solve the spectrum shortage problematic to enhance the spatial diversity gain. Moreover, mischievous sensing nodes can falsify the spectrum sensing data to avoid valid nodes from applying the spectrum. It causes a serious security threat and degrades the performance of network. Therefore, wireless security has developed an significant issue in CRNs to safeguard reliable spectrum sensing and fair resource distribution and organization. For further enhancement in spectrum sensing and allocation, we proposed an optimal trusted intrusion detection system for considerate spectrum sensing and distribution in cognitive radio networks (OT-IDS-CR). The first contribution is to introduce an improved chaos butterfly optimization (ICBO) algorithm for efficient clustering which divide the sensing nodes into number of clusters. Second, we estimate the trust degree of each secondary user (SUs) based on sensing information's with the help of cooperative random learning based trust management system (CRL). Then, we utilize the multi-swarm biogeography optimization (MBO) algorithm to optimize the sensing information's to avoid the dimensionality problem to ensure the secure spectrum sensing and allocation. Finally, to evaluate the performance of our OT-IDS-CR model through different simulation scenarios and the simulation results are likened with the present state-of-art models.

Keywords: trusted intrusion detection system, clustering, cooperative spectrum sensing, cognitive radio network, trust management system, trust degree.

[1*]Research Scholar, Dept of EECE, GIT, GITAM (Deemed to be University), Visakhapatnam, A.P, India.
[1]krishnasrikant@gmail.com
[2]Asst. Professor, Dept. Of EECE, GIT, GITAM (Deemed to be University), Visakhapatnam, A.P, India.
[2]camanapu@gitam.edu

***Corresponding Author:** A. Krishna Srikanth
*****Research Scholar, Dept of EECE, GIT, GITAM (Deemed to be University), Visakhapatnam, A.P, India.
[1]krishnasrikant@gmail.com

DOI: - 10.48047/ecb/2023.12.si5a.0113

1. Introduction

Cognitive radio networks (CRNs) used to upsurge the competence of the use of incomplete radio frequency capitals. However, such a cooperative system introduces overlapping traffic for control signal and information transmission, which upsurges power consumption, particularly in multi-hop nets. Energy effective CRN includes: improving spectrum utilization; reduce primary interference; and reduce energy consumption for secondary communication [1]. The preceding the whole thing on liveliness efficient spectrum sensing absorbed on the discovery of spectrum sensing though on communication protocol. Understanding the spectrum reliably and effectively is a major challenge for cognitive radio systems [2]. However, during the spectrum sensing procedure, detection is compromised when the knowledge user experiences shadowy or ambiguous results, or when uncertain failure occurs. To reduce such effects, recent studies have shown that the discovery competence of a cognitive radio scheme can be improved in a cospectral sense if joint sensing is performed at the same node [3]. In CRNs, conduits not castoff by primary users are searched for and used by subordinate users through frequency channels initially supplied to main operators [4][5]. The CRN channel should automatically identify the potential enterprises to be transferred by the primary user of the used channel. If the primary user starts the transfer, the secondary user must stop the transfer. There are two types of spectrum sensitivity: energy sensitivity and signal-based sensitivity [6]. Energy sensitivity-based spectrum sensing methods [7] easy to implement in a short time and give sensitivity results, but they require low noise volume and perform poorly in signal-to-noise (SNR) environments [8]. CRN is seen as a revolutionary example of the use of high spectrum for wireless communication, in which spectrum can be opportunistically accessed by unlicensed secondary users (SUs) and primary workers (PU) spectrum.

The attendance of a malevolent user lowers the effectiveness of collaborative spectrum sensing detection. It is an unwanted and unlawful user who satirizes a legitimate user and spreads unture info about the primary signal position. Also, if righthand nodes are the main decision basis, the value of cooperative spectrum sensing (CSS) [9][10] is reduced. An extended hierarchical CSS arrangement was castoff in which SUs were questioned to assign their sensitivity score based on their reputation. CRN covers all layers of message network technology counting network layer, transport layer and other upper layer technologies. Present research mainly focuses on the bodily layer and MAC layer of CRNs. One-Hope offers a range of options to suit landscape systems. Though, they are not compatible with multi-hop CRNs. In CRN multihop communiqué [11], how to rapidly and precisely choice a route from a node to a terminus node is an significant research task. Trail design in CRNs requires dynamic modification of node SOPs, i.e.network layer route selection must work in conjunction with spectrum allocation on the MAC layer [12]. It is presented in the results of continuous research. Spectrum consciousness is classified as passive based and active nuclear consciousness. SU learns the existence of spectrum from outside companies through traffic lights or geographic database. SUs generate local sensitivity to spectrum compatibility define as spectrum sensing [13]. Also, when approaching the SU panel, the panel should periodically check the PU for any unexpected appearance. This naturally limits the operation of the SUVs, or reduces the quality of service (QoS) guaranteed [14][15]. Distributed network do not essential a central agency, and each node shares its material with neighbours to make a joint decision. Distributed applications are highly robust to changes in network topology and centralized applications [16], and they adapt to direct or live changes to the network. CSS is shown to improve spectrum detection accuracy. However, a compromise agreement can be compromised if the computer is attacked by malicious users [17][18]. By spreading unture sensitivity information from the fusion centre and significantly reducing the effectiveness of the sensitivity system detection, malicious users can mislead and mislead decision makers. It is therefore important to identify the consequences of misinformation by attacks and to develop mitigation technologies. Also, preferences are considered when selecting spectrum for SUs with different capabilities. An advanced intrusion detection system (IDS) [19][20] is recommended to detect net irregularity conduct, which is achieved finished normal protocol process behavior, traffic flow, and PU admission time. These issues assistance identify unusual activities to achieve security. The proposed IDS plays its key role in improving the spectrum utilization related to bandwidth, system utilization rate and packet delivery rate. Our contributions: In this study, an optimal trusted intrusion detection system (OT-IDS) for CSS and allocation in CRNs (OT-IDS-CR) which resists from the spectrum sensing data falsification (SSDF) attacks to ensure a secure CSS.

A key contributions have involved in this study is summarized as follows:

1. An improved chaos butterfly optimization (ICBO) algorithm is used to form clustering which divide the sensing nodes into number of clusters.
2. To compute the trust degree of each SU based on sensing information's with the help of cooperative random learning based trust management system (CRL).
3. Multi-swarm biogeography optimization (MBO) algorithm is utilized here for optimize the sensing information's to avoid the dimensionality problem to ensure the secure CSS and allocation.
4. To validate our OT-IDS-CR method through different simulation scenarios and compared with a existing state-of-art methods.

The break of the daily is summarized as shadows. In Segment 2, related works was depicted utilizing previous studies in terms of secure obliging spectrum sensing. Section 3 explains about the issue in existing methods and the new plan for secure cooperative spectrum sensing is given. In Segment 4, we define the overall working function of our planned OT-IDS-CR method for secure cooperative spectrum sensing in CRNs. The imitation consequences and their comparative examination are discussed in Segment 5. Lastly, the daily accomplishes in Segment 6.

2. Related Works

In this segment, we deliberate recent works related to the secure obliging spectrum sensing in CRNs. The literature summarized in various aspects and tabulated in Table 1.

Guo et al. [21] have proposed energy-based integration of spectrum perception in reasoning radio networks. Given the potential for unture alarms, the Law on Linear Matching explores how to reduce the risk of loss of detection. They proposed a new and practical linear addition law that requires only the mean and variability of local experimental figures. The effectiveness of the proposed access rule is considered in three important sequences: slow toning, volume disappears, and disappears quickly. The simulations show that the proposed strategy is as effective as the optimal probability ratio test approaches and surpasses the traditional linear addition methods. Hajihoseini et al. [22] have proposed a distribution-based system in which SUs collaborate to improve the recital of spectrum sensing. This method offers significant improvements in storage speed and reliability. The imitation results indicate that the planned algorithm achieves satisfactory efficiency and integrates twice as fast as the equivalent sensitivity spectrum algorithms recently proposed in the literature, and almost eliminates contact connection failure.

Liu et al. [23] have proposed a technique for multi-antenna CR based on transmission operation and power generation, allowing PU signal emission frequency energy at SUs output and noise to compensate for energy loss. For multi-antenna CRs, a time-split perfect and an antenna split model are planned to achieve uniformity of co-spectrum sensitivity and generation output in which the SU can perform spectrum coefficient detection, energy storage, and data transmission. The integrated resource allocation between these two models is designed to address optimization issues related to sensitivity time, yield, number of sensitive antennas, and power transmission. An integrated optimization algorithm is proposed to find appropriate solutions to optimization problems. Simulation results indicate that specific models can achieve better results compared to the business model of critical activity. Kar et al. [24] have presented secure CSS for CRN-specific security attacks are data untrue occurrence or complex bout. In which a hateful internal associate of the net declares untrue sensitivity outcomes in order to intensification sensitivity mistakes. To meet CRN safety supplies, they have planned a new trust organization system that assesses the reliability of each node active in the CSS program. To solve the problem, SR calculations include several decision-making factors such as historical confidence issue, active issue, motivation factor and sustainability issue. By this SR worth, it identifies suspicious users and filters malicious users in the CSS project decision making process. Verma et al. [25] have proposed a new standby program for CSS under rally hidden channel. In a specific weight scheme, the PU of CR nodes is determined based on the reliability of the distance of each CR, thus giving the appropriate weight to dissimilar users. The CSS procedure that uses the new weighted arrangement is better than the standard CSS algorithm. In traditional CSS, the edges of each CR are connected to an evenly weighted merge centre. Not all results are equally reliable given the different distances of each CR from the PU, so different weights should be given depending on their reliability.

Muthukumar et al. [26] have proposed priority-based two-step discovery model (PPDSTM) that used to examine SU and PU collaboration strategies. Distributed CSS conscious SUs constantly test themselves and make comprehensive decisions about the attendance or

nonappearance of PU by means of an entropy-based vigor uncovering system. The imitation consequences show that the use of this scheme significantly increases the sensitivity time sensitivity and energy efficiency sensitivity. Ezzavati et al. [27] have distributed a system of spectrum sensitivity to effectively upsurge the ethereal efficacy of the network. A modified dispersed Kalman filter is used to upsurge the rating accuracy by estimating the location, speed, and control of the main spreaders. These data are used to improve spectral opening optimization and spectral utilization likened to central methods. The results gotten are assessed through applied implementation and imitations. Presenting and using a linear model to evaluate the transmitter location in the Results of this used energy from the spectrum of visual and optical conditions, Kalman transforms the extended filter and activates the sensitivity of the distributed spectrum; the advantages of this method over other methods of spectrum sensitivity are explained. Prasad et al. [28] have investigated the problem of CRN in CSS once manifold inactive stations are obtainable. CRN-CSS This article is about pregnancy, coordination and decision making. To integrate CRN-CSS with 5G to extends network connectivity and provide greater security for users. Trinity team shares with users. Multichannel communication, including the dynamic multichannel slot assignment (DMCSA) algorithm, which effectively identifies the channel, causes the shutdown. The fusion centre is used for decision making and spectrum allocation as it creates a global end-merger centre map based on reports from second-hand users and spectrum agents.

Abdel-Sayed et al. [29] has introduced rapid matching propensity (FMP) a dissolute and precise greed retrieval procedure for short detection. We demonstration that the spectral information are low for port band and bandwidth pocket domains. FMP is used to detect wide range of cognitive radio networks. Spectral signals from our specific algorithm models repeated at around 25% of the NQ, which is quicker than other connected procedures, with a 99% detection likelihood and less than 1% on a unture alarm. Rapetswa et al. [30] have investigated the CR spectrum performance degradation problems to support high-reliability low-pass communications that are sensitive to traffic and spectrum competition. It provides a good overview of CR and explains the direction of future research in the afresh recognized 5G investigate areas in manufacturing and education. Eappen et al. [31] have solved the quality problem in CRN spectrum sensing. Explores various advanced computing techniques through detailed comparative analysis of traditional and advanced computing techniques. The challenges of CRN implementation and its requirements have been addressed. The various components and requirements of spectrum sensitivity are given and the roadmap for spectrum sensing with smooth computing techniques up to 5G is considered. In addition, this article discusses the future of spectrum realization in CRN, investigate challenges, and open-ended subjects related to soft calculation methods. Al-Kofahi et al. [32] have analyzed the problem of improving the selection of sensors needed to meet a specific need, i.e. reducing total energy consumption. The issue of spatial and temporal planning, taking into account sensor level, power level, and maximum SUs and monitoring time required. The problem is designed to be a complete linear program. The sub-optimal greed algorithm works here best with respect to optimal solutions.

Table1 Summary of research gaps

Ref.	Methodology	Algorithm	Improvement	Research gap
[21]	Secure CSS	PSO	Sensing accuracy	Optimal performance affected by huge density of SUs
[22]	CRN-CSS	Diffusion based		Network topography improves reliability from changes and connection failures
[23]	Spectrum sensing	Splitting model	FPR and FNR	Greater performance than the traditional sensitivity-performance transfer model
[24]	CSS	CSS scheme	Sensing accuracy	Decrease the belongings of SSDF assailants in CRNs
[25]	Trusted CSS	Weighted scheme	Sensing accuracy	Improvement in sensing performance
[26]	CSS	PBDSTM		Efficiency
[27]	Secure CSS	Kalmann filter	Sensing accuracy, FPR and FNR	Improvement of spectrum utilization
[28]	Spectrum allocation	DMCSA		Throughput efficiency is highly increased
[29]	Secure CSS and allocation	FMS	FPR and FNR	Fast and accurate reproduction of scattered signals
[30]	Spectrum sensing	DSA	Average trust value	Sensing uncovering verge is set at a appropriate equal
[31]	Spectrum sensing	GA, PSO	FPR & FNR	Use accessible spectrum more efficiently through opportunistic spectrum
[32]	On-demand spectrum sensing	ILP	Sensing accuracy, FPR and FNR	Cost showing better performance

3. Problem Methodology

3.1 Research Gap

A trust organization arrangement is used for multi-hop cooperative spectrum sensing to overcome SSDF outbreak [33]. This scheme discusses the reliability of electrical relay SUs and the trust worth of sensor SUs to evaluate the reliability of multihop reports. Considering the reliability of the multi-hop path and the trust of the sensor SU can decrease the negative effect of hateful operators on the role of the relay or sensor nodes, thereby improving the correctness of the spectrum sensing consequences. Assume that the trust value of the path is equivalent to the smallest trust value of the relay nodes in the path. Imitation fallouts show that the discovery correctness of spectrum holes and the performance of cooperative spectrum sensing are improved by using path confidence values. In general, CSS improves the accuracy of PU occupancy detection by collecting sensing info from SU [21]. Though, CSS also opens the way for malicious attacks that change reports by mistaking the channel used for reporting as generic. An SSDF attack, usually occurring at the data link layer, involves the modification of a sensitive account by a malicious user. The SSDF attack is always classified into five classes: in the absence or presence of the PU, the malicious user always reports the presence of the PU to evade the original SU; Never: To enable interference, the malicious user always reports the PU's nonappearance in its presence; Transformer: A malicious user always objects to the detection output of real SUs; Selfishness: Sometimes, a hateful attacker does not contribute in the sensing procedure to save energy; and random: data are chance [33].

They production smart enough to be difficult to detect. Faith is a firm confidence in dependability. The authenticity of SUs is unhurried by measuring the level of trust. Though, calculating the reliability of all SUs can upsurge the difficulty in time and interplanetary [27]-[31]. Also, collaborative sensing techniques are less susceptible to spectrum sensing data falsification (SSDF) attacks [31][33]. Malicious radios can negatively affect the final sensing result by sending incorrect spectrum sensing results to the fusion center [32]. So, to mislead other normal CR users, the hateful user sends fake sensing information to make a wrong choice on the operation of PUs. Therefore, identifying the SSDF security attack is crucial to take suitable measures for precise cooperative spectrum sensing.

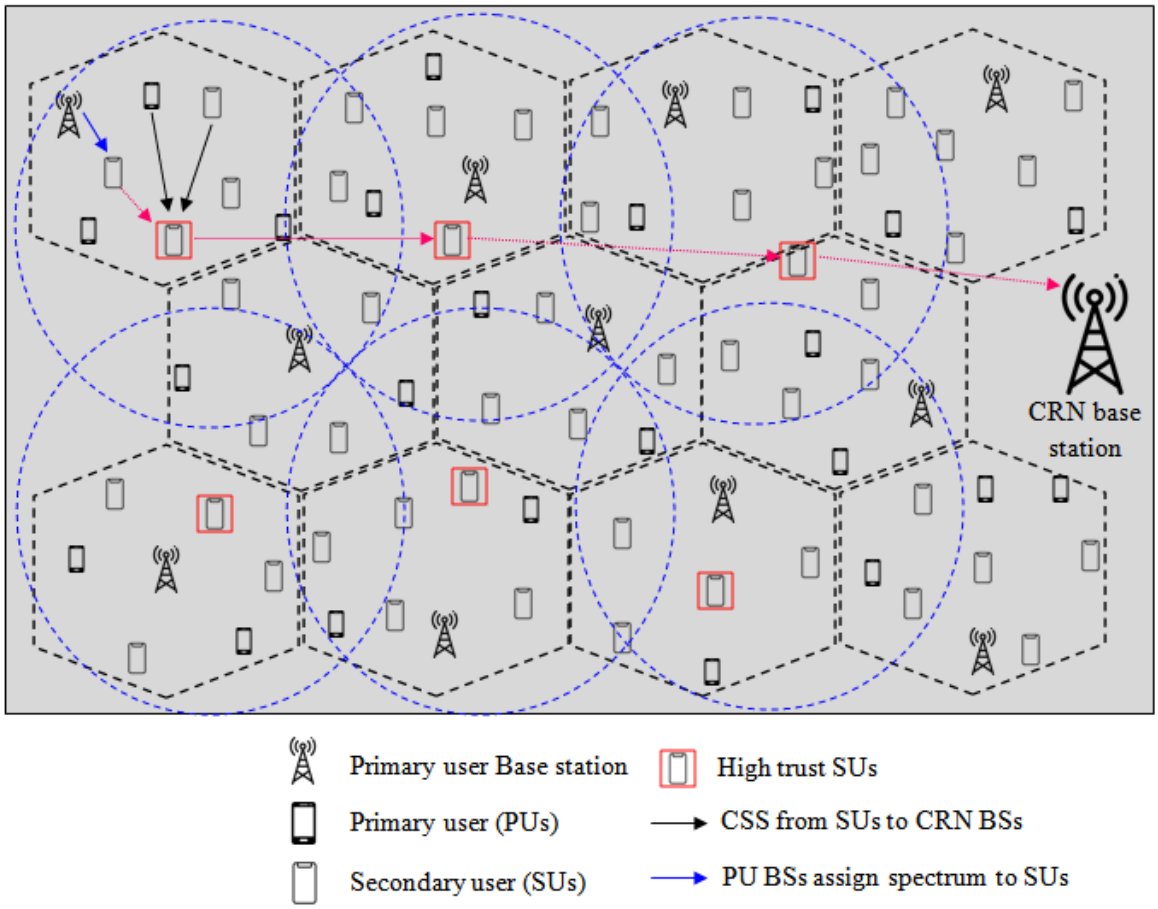

Fig. 1 Overall system architecture of our proposed OT-IDS-CR model (assumed structure)

3.2 System architecture of proposed work

The cognitive radio network in this paper has an ad-hoc construction and is distributed in the cellular network area acting as the main net. Figure 1 displays the hypothetical system architecture of CRN using the proposed OT-IDS-CR model. In this net, PUs are cellular users and SUs form an overlap ad hoc net. SUs do not have a complete view of the status of spectrum groups in the net and require CSS. It should be noted that multihop broadcast of spectrum sensing intelligences to other SUs is not ideal since it causes large collisions between SUs, mostly due to high broadcast power, which brands transmission impossible. Therefore, multipath routing is used for SSs to temporarily distribute their spectrum sensing information to each other through more reliable SSs. For example, if the associated Primary User BSs (PBSs) transmit data to the PU, the SUs located in the PBS transmission range can detect the signal, while the others do not obtain power. Therefore, multipath routing is necessary to inform an SU of its spectrum position before obtaining a temporary connection with another SU in that range.

4. Proposed Methodology

In this section, the detailed working process of our proposed OT-IDS-CR method is described with the proper mathematical models. Our proposed OT-IDS-CR method consists following set of process are SUs cluster formation, trust degree computation, secure spectrum sensing and allocation.

4.1 Clustering using improved chaos butterfly optimization (ICBO)

The motivation for cluster in CRN is to decrease network message overhead, safeguard stability finished PU meddling management, and grip dynamic changes in network network topology due to node flexibility. Cluster creation in old-style wireless networks trusts on a switch station to convey control mails throughout cluster formation. The lively countryside of channel obtainability in CRNs makes it unreasonable to use fixed channels to convey control mails amongst nodes. The event is recorded, the nodes suitable for the cluster determine the local location of the nodes between the event and the pool. Then select a hop member to increase the number of hop neighbours that single hop neighbours have access to through cluster channels to increase the connection between clusters. Clusters eliminate consumption due to unnecessary cluster formation and technical overlap. In this study, we utilized an improved chaos butterfly optimization (ICBO) algorithm for efficient cluster formation which divides the sensing nodes into number of clusters. This algorithm automatically transfers the monarch butterfly individuals to the next generation and ensures that no operator can replace them. This ensures that the action of the monarch butterfly populace will not ever decline with the growth of optimal solution generations. An ICBO algorithm consists of two main workers: the relocation worker and the butterfly regulation operative. They are the centre piece of the monarch butterfly optimization system. We describe migration operator,

$$y_{j,i}^{T+1} = y_{s_{1,i}}^{T} \quad (1)$$

$$y_{j,i}^{T+1} = y_{s_{2,i}}^{T} \quad (2)$$

where $y_{j,i}^{T+1}$ generating the T + 1 element indicating the position of the monarch butterfly. Rand is a chance number gained from a single delivery.

$$R = Rand * Peri \quad (3)$$

Then update monarch butterfly elements in subpopulation:

$$y_{j,i}^{T+1} = y_{Best,j}^{T} \quad (4)$$

where $y_{j,i}^{T+1}$ is Factor of cohort T + 1, indicating the location of the monarch butterfly j, although $y_{j,i}^{T+1}$ is the 2nd component of ybest in the T generation is the best place for king butterflies in Land 1 and 2. To apprise the rudiments of monarch butterflies in subpopulation as follows:

$$y_{j,i}^{T+1} = y_{s_{3,i}}^{T} \quad (5)$$

where $y_{j,i}^{T+1}$ is the reactive element in cohort T + 1, indicating the location of the monarch butterfly j, while $y_{s_{3,i}}^{T}$ is factor i in generation T, indicating the position of the monarch butterfly. The condition of the butterfly is further updated by the custom plane, which is a conditional fitness value.

$$y_{j,i}^{T+1} = y_{j,i}^{T+1} + \alpha \times (cy_z - 0.5) \quad (6)$$

$$cy_z = Levy(y_i^T) \quad (7)$$

$$\alpha = R_{Max`} / T^2 \quad (8)$$

The variable fitness is a butterfly configuration column. Algorithm 1 describes the working steps involved in the SUs cluster formation using ICBO.

Algorithm 1 SUs clustering using ICBO

	Input: SUs initial position, velocity, SUs ID Output: cluster formation
1	Initialise the parameters
2	Compute the migration operator using $y_{j,i}^{T+1} = y_{s_{1,i}}^{T}$
3	Generate randomness using $y_{j,i}^{T+1} = y_{s_{1,i}}^{T}$
4	Update monarch butterfly using $y_{j,i}^{T+1} = y_{Best,j}^{T}$
5	Indicate the position of the butterfly
6	Determine the fitness using $\alpha = R_{Max`} / T^2$
7	End procedure

4.2 Trust degree computation using cooperative random learning (CRL)

The reliability of a sensor node is assessed based on the closeness of its frequency state statement to the concluding decision made by the SU determining the channel state. If the SU sensitivity account is the final result, confidence in this SU sensitivity ought be augmented. Consequently, the quantity of precise sensitivity statements about the beta reputation mechanism will increase by 1. Otherwise, if the sensing report contradicts the final result, the amount of unture sensing intelligences is incremented by 1. SUs detect limited spectrum bands in their nearby setting and transmission their sensing consequences. Susceptibility consequences of SUs are stated in binary mode. “0” indicates absence and “1” indicates presence of PU. SUs sensitivity report packets contain the subsequent arenas: "Node_id" arena that classifies the sensitive SU. The "Seq_num" arena is the package classification number used to identify new packets due to routing loops from old packets. At the detection stage, request messages are sent only to malicious nodes. After path revenue, path trust is calculated based on the reliability of existing path nodes and is linked to path latency to select data sharing paths. At the identical time, rendering to the node belief, the method of recompence and sentence is followed to begin the truthful redirection of the nodes. Multi-hop CRNs should have the same channel as neighbouring communication nodes. The stations of apiece link are completely different from the basis nodes to the target nodes. Dynamic changes in node SOPs can lead to overcoming the existing path. This method, on request, a routing plan is a good excellent. At the same time, it is unavoidable that many channel shift glitches will occur in reasoning radio networks. Trail delays will be an significant indicator of steering protocol project and route optimization. In this study, we utilize the cooperative random learning (CRL) model to estimate the trust degree of each SU based on sensing information’s. Let us consider that each CRN-BS select a maximum of one highest trust degree SU node at a time.

$$\sum_{a=1}^{A} u_a^z \le \forall z \in Z \tag{9}$$

For the Z CR, let {0, 1} indicates the distribution of resources by binary rate. CRN selects only one source at a time.

$$\sum_{n=1}^{B} d_{a,z}^m \le \forall z \in Z, \forall a \in A \tag{10}$$

Interference and noise rate signal (SINR) for communication between k CRN-BS in time slot

$$\xi_{a,z}^m = \frac{e_{c,z}^m u_a^z d_{a,z}^m q_{a,z}^m}{\sigma^2 + \sum_{i \in A/\{a\}} e_{i,z}^m q_i + \sum_{v \in V} e_{v,z} q_v} \tag{11}$$

where, $e_{c,z}^m$ Indicates channel gain between CRN-BS and zth CRN in m resource over time in d resource and , $q_{a,z}^m$ Zth refers to the bandwidth used in the SU resource and related CRN-BS. Therefore, the data velocity of zth SU in t resource over time is calculated according to the Shannon formula.

$$c^z = L \log_2 \left(1 + \xi_{a,z}^m\right) \tag{12}$$

Therefore, each CRN must choose m resource, i.e. advance the presentation of the organization as a recompense. Thus, the total volume of zth CRN,

$$S^z = \sum_{m=1}^{M} c^z = \sum_{m=1}^{M} L \log_2 \left(1 + \xi_{a,z}^m\right) \tag{13}$$

The problem of resource allocation can be expressed as a problem of maximize

$$S = Max \sum_{z \in Z} S^z \tag{14}$$

The level observed by t and zth SU over time is determined

$$r_T^z = \{j, z, J_z\} \tag{15}$$

The activity performed by each SU over time d indicates the portable capacity of the resource portion

$$b_T^z \{d_{a,z}^m, q_{a,z}^m\} \tag{16}$$

Activity performed by each SU

$$s_T^z = \begin{cases} S, if\ D1 to\ D4\ are\ satisfied \\ 0, otherwise \end{cases} \tag{17}$$

The expected discount level for infinite time locations is determined as follows:

$$U^{\pi}(r) = H\left[\sum_{T=0}^{\infty} (\gamma^T) s(r_T, \pi(r_T))\right] \tag{18}$$

where H(.) represents the operator and the [0,1] discount factor. The value function is over written as follows:

$$U^{\pi}(r) = H\left[s(r,\pi(r))\right] + \gamma \sum_{r \in R} t_{r,r'}(\pi(s)) U^{\pi}(R') \quad (19)$$

The optimal action selection strategy is determined at each time point.

$$\pi_T^z(t^z, b^z) = \begin{cases} (1-\varepsilon), \arg\max_b P(r', \tilde{b}) \\ \varepsilon, Otherwise \end{cases} \quad (20)$$

In time slot T, each SU selects an action r^z in the state b^z with probability,

$$\pi_T^z(r^z, b^z) = \frac{h^{P_T^z}(r^z, b^z)/\Gamma}{\sum_{\tilde{b} \in B_z} h^{P_T^z}(r^z, b^z)/\Gamma} \quad (21)$$

where Γ represents total network size. A higher value leads to the choice of equivalent probabilities, while a lower value makes a big difference in their Q-frequency. In many agent environments the Q-value is repeated with information.

Algorithm 2 Trust degree computation using CRL method

Input: energy consumption, signal strength, and congestion rate
Output: Trust degree of each SUs

1. Initialise the parameters
2. Compute the SINR using $\xi_{a,z}^m = \dfrac{e_{c,z}^m u_a^z d_{a,z}^m q_{a,z}^m}{\sigma^2 + \sum_{i \in A/\{a\}} e_{i,z}^m q_i + \sum_{v \in V} e_{v,z} q_v}$
3. Calculate resource over time using $c^z = L \log_2\left(1 + \xi_{a,z}^m\right)$
4. Determine infinite time location using $U^{\pi}(r) = H\left[\sum_{T=0}^{\infty} (\gamma^T) s(r_T, \pi(r_T))\right]$
5. Compute the probability using $\pi_T^z(r^z, b^z) = \dfrac{h^{P_T^z}(r^z, b^z)/\Gamma}{\sum_{\tilde{b} \in B_z} h^{P_T^z}(r^z, b^z)/\Gamma}$
6. Define the system performance using $SW(r,b) = \sum_{m=1}^{M} \sum_{z \in Z} u_c^z d_{c,z}^m \log_2(1 + \zeta_{a,z}^m)$
7. End procedure

$$P_{T+1}^z(r^z, b^z) = (1-\alpha^T) P_T^z(r^z, b^z) + \left\{ \sum_{b=z \in A} \left[SL(r^z, b^z, b^{-z}) \prod_{i \in Z/\{z\}} \pi_T^i(r^i, b^i) \right] + \gamma \underset{\tilde{b} \in B_z}{Max} \right\} \quad (22)$$

The fitness value computation is performs as follows:

$$SW(r,b) = \sum_{m=1}^{M} \sum_{z \in Z} u_c^z d_{c,z}^m \log_2(1 + \zeta_{a,z}^m) \quad (23)$$

Therefore, the impact factor is calculated based on information from local agents available for a limited time.

$$\tau_T^z(r^z, b^{-z}) = \tau_{T-1}^z(r^z, b^{-z}) + \mu^z\left[\pi_T^z(r^z, b^z) - \pi_{T-1}^z(r^z, b^z)\right] \quad (24)$$

where μ indicates positive level. The working steps involved in the process of SUs trust degree computation using CRL method, described in Algorithm 2.

4.3 Secure spectrum sensing and allocation using MBO algorithm

In particular, the use of a spectral sensitivity compression model effectively reduces the sample ratio. In addition, the principle of spectrum distribution in neighboring CUs is an obstacle in the signal recovery process. Thus, this integrated program deals with spectrum sensing and spectrum distribution, exploring the vast network of the Internet, and solving the problems of many users. In fact, CIs do not need to cross the entire signal because they only want to find active users. Also, if there is a certain frequency channel, this should not be considered in the PUs or SUs spectrum distribution approach. Here we utilized the multi-swarm biogeography optimization (MBO) algorithm to optimize the sensing information's to avoid the dimensionality problem to ensure the

secure spectrum sensing and allocation. Initially, the MBO algorithm starts with the approximate number of particles in the search area. Positioning optimization refers to the solution of a problem candidate and uses speed to update the position. Each particle changes velocity according to the individual optimal state and the universal optimal state on which the total mass is found. We first define the initial fitness values for jth particles:

$$u_j(T+1) = lu_j(T) + d_1 s_1\left(qBest_j - y_j(T)\right) + d_2 s_2\left(qBest(T) - y_j(T)\right) \quad (25)$$

$$y_j(T+1) = y_j(T) + u_j(T+1) \quad (26)$$

where $u_j = u_{j1}, u_{j2}...., u_{jC}$ and $y_j = y_{j1}, y_{j2}...., y_{jC}$ are j velocity and location of atoms; the depressive loads, C1 and C2 are hastening coefficients; r1 and r2 are random numbers produced within [0, 1]. The individual best position $qBest_j = qBest_{j1}, qBest_{j2}...., qBest_{jC}$ is updated for each generation as follows:

$$qBest_j(T+1) = \begin{cases} y_j(T+1), & if\ (y_j(T+1)) < (qBest_j(T)) \\ qBest_j(T), & otherwise \end{cases} \quad (27)$$

The global best levels of the crowd are updated for each generation as follows:

$$fBest(T+1) = \begin{cases} qBest_j(T+1),\ if\ g(qBest_j(T+1)) < g(fBest(T)) \\ \forall_j = \{1,....,M\} \\ fBest(T), \quad Otherwise \end{cases} \quad (28)$$

We apprise the velocity and position of each element as follows:

$$u_j(T+1) = lu_j(T) + d_1 s_1\left(qBest_{\overline{g}}(T) - y_j(T)\right) \quad (29)$$

$$y_j(T+1) = y_j(T) + u_j(T+1) \quad (30)$$

where particle qBest in individual best positions, all particles are classified from the best to worst. Consider for a mitigating problem as follows:

$$g(qBest_{r_1}) \le ... \le g(qBest_{r_z}) \le ... \le g(qBest_{r_M}) \quad (31)$$

Second, the rating of each particle is compute as follows:

$$Rank(y_{r_z}) = M - z,\ z = 1,2,....M \quad (32)$$

The particle has a large nominal value, while a bad particle has a small nominal value. Third, the particle settlement rate is calculated as the rate and the settlement rate as the rate.

$$\begin{cases} \lambda_z = \left(1 - \dfrac{Rank(y_{r_z})}{M}\right) \\ \mu_z = \left(\dfrac{M - rank(y_{s_z})}{M}\right) \end{cases}, z = 1,2...,M \quad (33)$$

where J and H represents emigration and immigration maximum rates which equivalent to the J =H=1. Algorithm 3 describes the steps involved in the secure spectrum sensing and allocation using MBO algorithm.

Algorithm 3 Secure spectrum sensing and allocation using MBO

Input: Random j-th particles, threshold condition

Output: sensing and allocation

1 Initialise the parameters

Compute individual position using

2 $$qBest_j(T+1) = \begin{cases} y_j(T+1), & if\ (y_j(T+1)) < (qBest_j(T)) \\ qBest_j(T), & otherwise \end{cases}$$

Update each position using

3 $$fBest(T+1) = \begin{cases} qBest_j(T+1),\ if\ g(qBest_j(T+1)) < g(fBest(T)) \\ \forall_j = \{1,....,M\} \\ fBest(T), \quad Otherwise \end{cases}$$

Update velocity and position of the particle using

4 $$u_j(T+1) = lu_j(T) + d_1 s_1\left(qBest_{\overline{g}}(T) - y_j(T)\right)$$

$$y_j(T+1) = y_j(T) + u_j(T+1)$$

5 Calculate the rank using $Rank(y_{r_z}) = M - z,\ z = 1,2,....M$

6 Determine the calculate rate using $\begin{cases} \lambda_z = \left(1 - \dfrac{Rank(y_{r_z})}{M}\right) \\ \mu_z = \left(\dfrac{M - rank(y_{s_z})}{M}\right) \end{cases}, z = 1,2...,M$

5. Results and Discussion

In this segment, we validate our OT-IDS-CR model using the different simulation scenarios and their simulation results are associated with the existing state-of-art models. First, we analyzes the simulation results of the clustering process in which our proposed ICBO algorithm is associated with the existing state-of-art procedures such as weight based clustering (WCL), multi-objective cluster optimization (MOCO), cluster formation protocol (CFP), and local minimum dominating set (LMDS) [34]. Second, we analyze the simulation results of the secure CSS process in which our overall proposed OT-IDS-CR method is compared with the existing IDS method [33].

5.1 Simulation setup

The simulation was performed using a network simulator (NS-2). We solve a simulation environment of 1100×700 m^2 area with several cognitive 802.11 nodes using cellular net as PU net and SU as ad hoc network. The maximum broadcast variety of SU nodes is 250 meters, and the system propagation model is two-beam ground. Using the spatial node delivery of the random way point flexibility model, we perform simulations on different numbers of SUs where nodes are located in the same simulation region. Each node has six boundaries to implement six stations. They use a two-ray perfect of Earth's reflectivity as the surface model. Both SU and PU operate in the same transmission range and meddling range. PU functions follow an exponential delivery as an ON/OFF process. The ON state of the PU indicates that its transmission is enabled, while the OFF national is the opposite. SUs are armed with 802.11MAC protocol to avoid crashes. In this imitation, we evaluate the performance of the procedure in contradiction of various SSDF attacks such as Byzantine, brute force, and random attacks. We set the total simulation time to 160 seconds. Stand 1 summarizes the simulation limits used in this paper.

Stand 1 Simulation parameters

Parameter	Value
Simulation area	1100×700 m^2
Number of SUs	50–200
Interference range	500 m
MAC protocol	802.11
SUs mobility model	Random waypoint
Transmission range	250 m
Type of antenna	Omni-directional
Propagation model	Two ray ground
Simulation time	160 seconds

5.1 Comparative analysis on clustering algorithms

In this scenario, we vary the number of SUs as 50, 80, 120, 150 and 200 with the fixed network size as 1100×700 m^2 area. The simulation results of our planned ICBO procedure is likened with the existing algorithms, WCL, MOCO, CFP, and LMDS [34] in terms of number of clusters, execution time, message overhead, packet loss and disconnected nodes respectively. Fig. 2 demonstrations the number of cluster contrast of planned and exciting clustering algorithm. From the plot, we perceive that the number of clusters shaped in the proposed ICBO algorithm is 15.79%, 36.64%, 55.86%, and 76.64% less than that in other algorithms, WCL, MOCO, CFP, and LMDS [34] respectively. Fig. 3 shows the execution time comparison of our proposed and exciting clustering algorithm. From the plot, we observe that the execution time in the proposed ICBO algorithm is 34.211%, 56.140%, 68.354%, and 75.962% less than that in other algorithms, WCL, MOCO, CFP, and LMDS [34] respectively. Fig. 4 shows the message overhead comparison of proposed and exciting clustering algorithm. From the plot, we observe that the message overhead in the proposed ICBO algorithm is 22.964%, 38.873%, 53.97%, and 65.133% less than that in other algorithms, WCL, MOCO, CFP, and LMDS [34] respectively. Fig. 5 shows the packet loss comparison of proposed and exciting clustering algorithm. From the plot, we observe that the packet loss ratio in the proposed ICBO algorithm

is 11.504%, 20%, 27.007%, and 32.886% less than that in other algorithms, WCL, MOCO, CFP, and LMDS [34] respectively. Fig. 6 shows the disconnected nodes judgement of planned and exciting clustering algorithm. From the plot, we observe that the disconnected nodes in the proposed ICBO algorithm is 25.64%, 46.29%, 58.86%, and 69.15% less than that in other algorithms, WCL, MOCO, CFP, and LMDS [34] respectively.

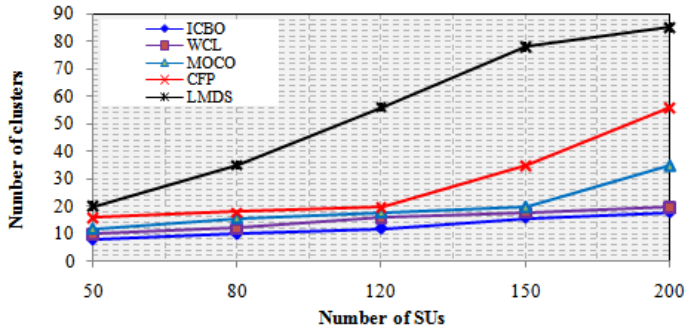

Fig. 2 Comparison of number-of-clusters

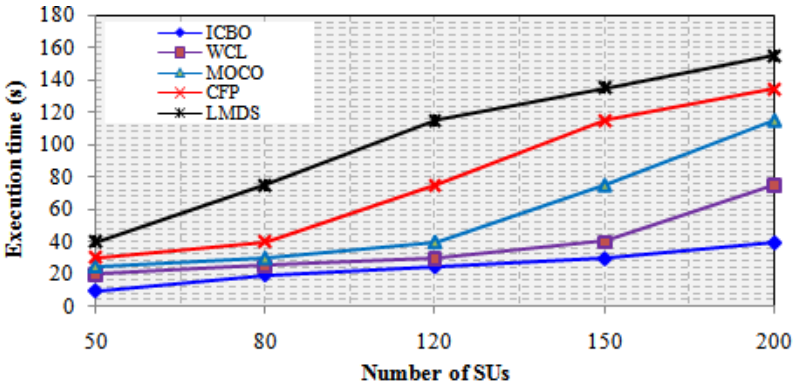

Fig. 3 Comparison of execution time

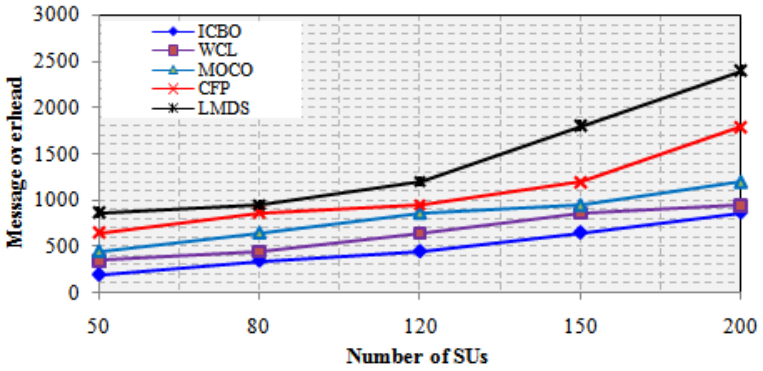

Fig. 4 Comparison of message overhead

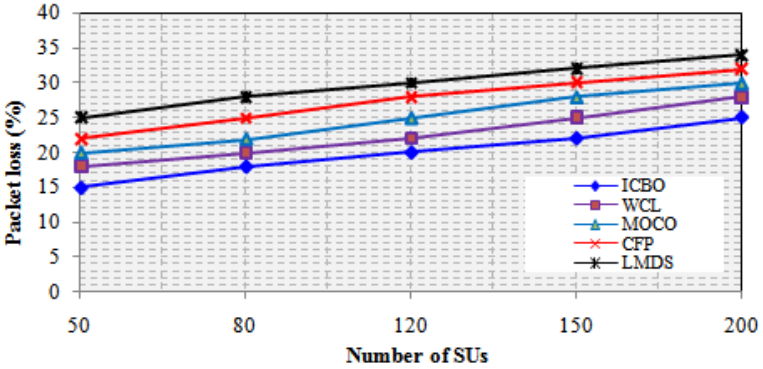

Fig. 5 Comparison of packet loss

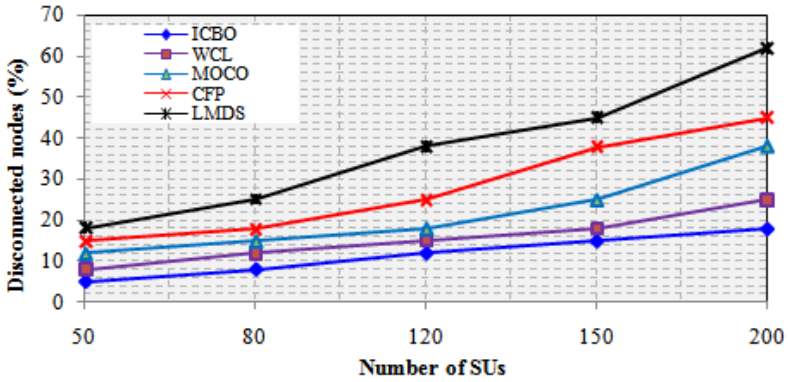

Fig. 6 Comparison of detached nodes

5.2 Comparative analysis on secure cooperative spectrum sensing and allocation

This scenario, we examine the simulation results of the secure CSS and allocation by using two different cases in which our overall performance of our OT-IDS-CR method is compared to the existing IDS method [33] with the different SSDF attacks are Byzantine, crude and random. First, we vary the number of SUs as 50, 80, 120, 150 and 200 without attacks, with the fixed network size as 1100×700 m^2 area. The simulation results of our OT-IDS-CR method is compared with the existing IDS method [33] in standings of sensing accuracy, untrue positive rate, unture negative frequency and miss detection rate. Fig. 7 shows the average sensing accuracy comparison of proposed and exciting IDS methods. From the plot, we observe that the average sensing accuracy of the proposed OT-IDS-CR method is 28.525% efficient than the exciting IDS method [33]. Fig. 8 displays the untrue positive rate comparison of proposed and exciting IDS methods. From the plot, we perceive that the unture positive rate of the planned OT-IDS-CR technique is 42.966 % efficient than the exciting IDS method [33]. Fig. 9 shows the unture negative rate comparison of planned and exciting IDS approaches. From the plot, we observe that the untrue negative rate of the planned OT-IDS-CR method is 41.401% efficient than the exciting IDS method [33]. Fig. 10 shows the miss detection rate comparison of proposed and exciting IDS methods. From the plot, we observe that the miss detection rate of the planned OT-IDS-CR method is 50.138 % efficient than the exciting IDS method [33].

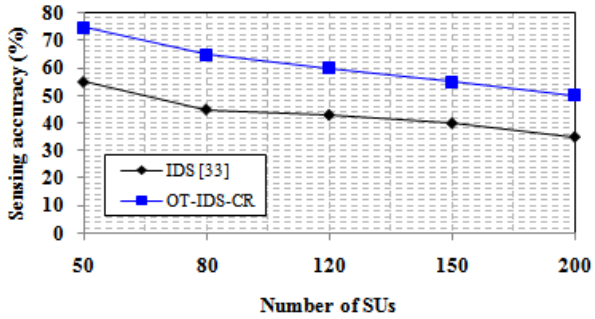

Fig. 7 Comparison of sensing accuracy without attacks

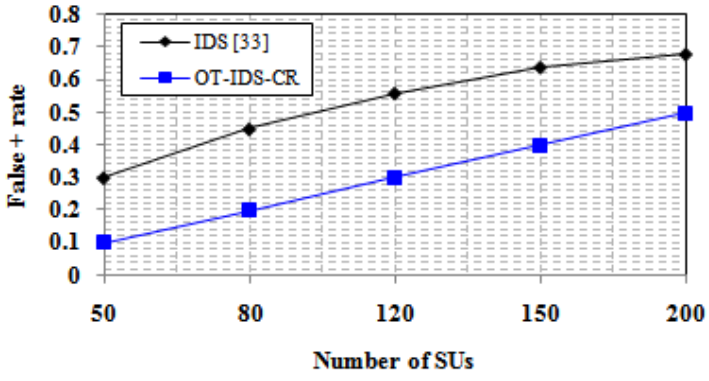

Fig. 8 Comparison of untrue positive rate without attacks

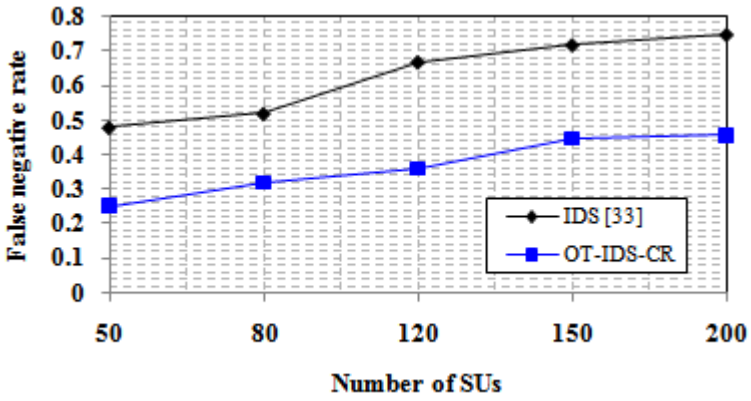

Fig. 9 Comparison of untrue negative rate without attacks

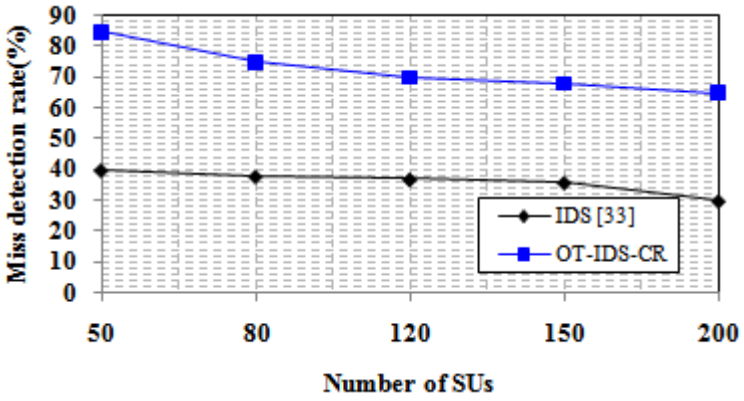

Fig. 10 Comparison of miss detection rate without attacks

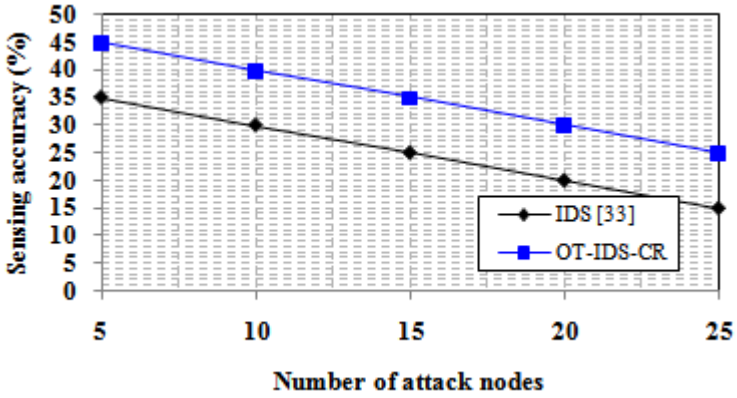

Fig. 11 Comparison of sensing accuracy with Byzantine attacks

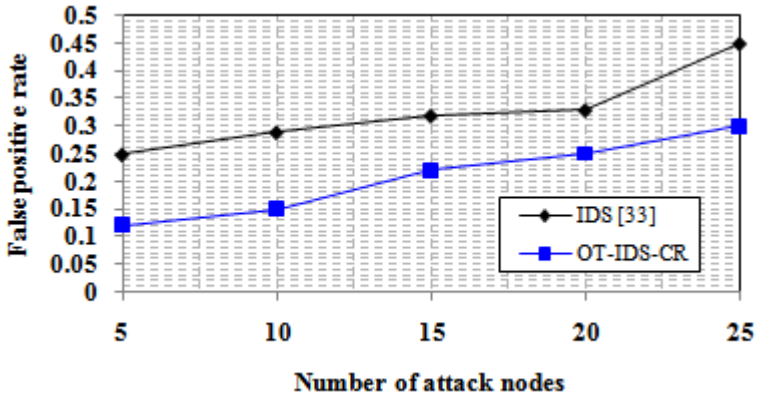

Fig. 12 Comparison of untrue positive rate with Byzantine attacks

Second, we vary the number of Byzantine attacks as 5, 10, 15, 20 and 25 with fixed SUs as 200, and the fixed network size as 1100×700 m^2 area. The simulation results of our OT-IDS-CR method is compared with the existing IDS method [33] in standings of sensing accuracy, unture positive rate, unture negative frequency and miss detection rate.

Fig. 11 shows the average sensing accuracy comparison of proposed and exciting IDS methods. From the plot, we observe that the average sensing accuracy of the proposed OT-IDS-CR method is 28.571 % efficient than the exciting IDS method [33].

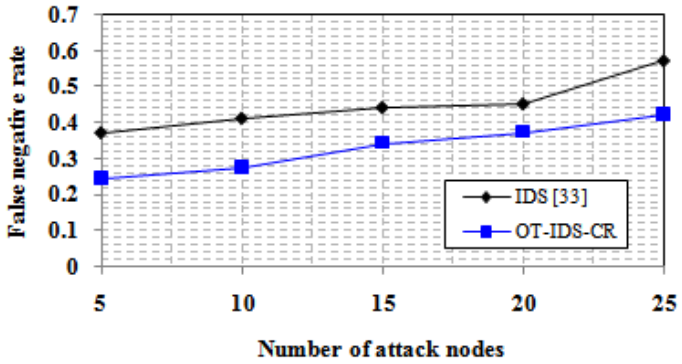

Fig. 13 Comparison of unture negative rate with Byzantine attacks

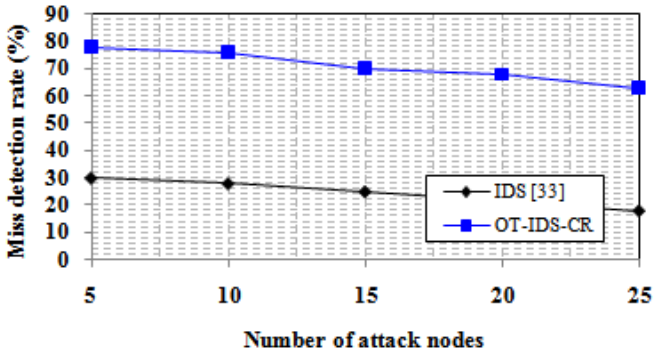

Fig. 14 Comparison of miss detection rate with Byzantine attacks

Fig. 12 shows the untrue positive rate comparison of proposed and exciting IDS methods. From the plot, we perceive that the untrue positive rate of the proposed OT-IDS-CR method is 36.585% efficient than the exciting IDS method [33]. Fig. 13 shows the untrue negative rate comparison of planned and exciting IDS systems. From the plot, we detect that the untrue negative rate of the planned OT-IDS-CR technique is 26.549% efficient than the exciting IDS method [33]. Fig. 14 shows the miss detection rate comparison of proposed and exciting IDS methods. From the plot, we observe that the miss discovery rate of the planned OT-IDS-CR method is 65.352% efficient than the exciting IDS method [33].

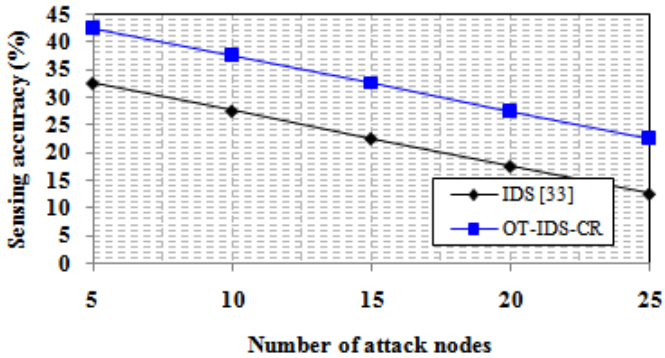

Fig. 15 Comparison of sensing accuracy with Crude attacks

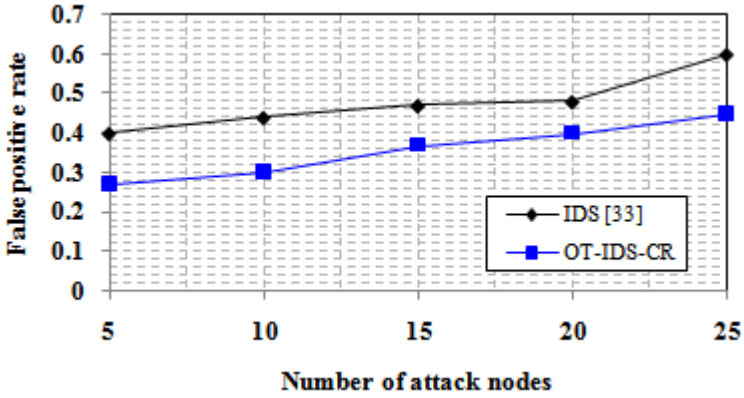

Fig. 16 Comparison of unture positive rate with Crude attacks

Third, we vary the number of Crude attacks as 5, 10, 15, 20 and 25 with fixed SUs as 200, and the fixed network size as 1100×700 m^2 area. The simulation results of our OT-IDS-CR method is compared with the existing IDS method [33] in rapports of sensing accuracy, untrue positive rate, untrue negative rate and miss detection rate. Fig. 15 shows average sensing accuracy comparison of proposed and exciting IDS methods. From the plot, we observe that the average sensing accuracy of the proposed OT-IDS-CR method is 30.628% efficient than the exciting IDS method [33]. Fig. 16 shows the unture positive rate comparison of proposed and exciting IDS methods. From the plot, we perceive that the untrue positive rate of the proposed OT-IDS-CR method is 25.105% efficient than the exciting IDS method [33]. Fig. 17 shows the untrue negative rate comparison of planned and exciting IDS systems. From the plot, we perceive that the untrue negative rate of the proposed OT-IDS-CR method is 19.934% efficient than the exciting IDS method [33]. Fig. 18 shows the miss detection rate comparison of proposed and exciting IDS methods. From the plot, we observe that the miss discovery rate of the planned OT-IDS-CR method is 68.69% efficient than the exciting IDS method [33].

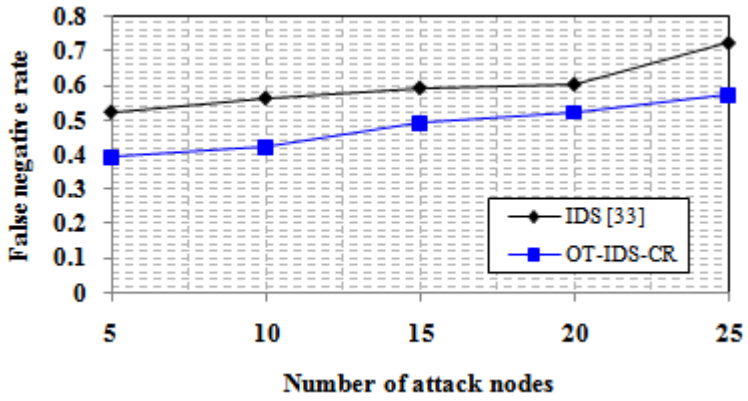

Fig. 17 Comparison of unture negative rate with Crude e attacks

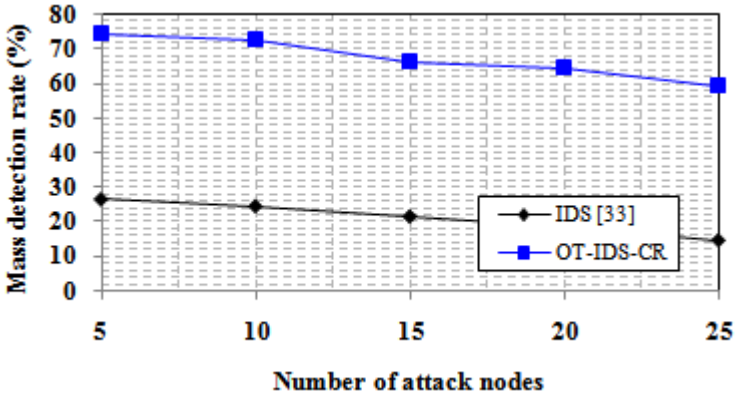

Fig. 18 Comparison of miss detection rate with Crude attacks

Finally, we vary the number of random attacks as 5, 10, 15, 20 and 25 with fixed SUs as 200, and the fixed network size as 1100×700 m^2 area. The simulation results of our OT-IDS-CR method is compared with the existing IDS method [33] in footings of sensing accuracy, unture positive rate, untrue negative rate and miss detection rate. Fig. 19 shows average sensing accuracy comparison of proposed and exciting IDS methods. From the plot, we observe that the average sensing accuracy of the proposed OT-IDS-CR method is 33.003% efficient than the exciting IDS method [33]. Fig. 20 shows the unture positive rate comparison of proposed and exciting IDS methods. From the plot, we perceive that the untrue positive frequency of the proposed OT-IDS-CR method is 70.472% efficient than the exciting IDS method [33]. Fig. 21 shows the untrue negative frequency comparison of planned and exciting IDS means. From the plot, we perceive that the untrue negative rate of the proposed OT-IDS-CR method is 56.646% efficient than the exciting IDS method [33]. Fig. 22 shows the miss detection rate comparison of proposed and exciting IDS methods. From the plot, we observe that the miss discovery rate of the planned OT-IDS-CR method is 72.387% efficient than the exciting IDS method [33].

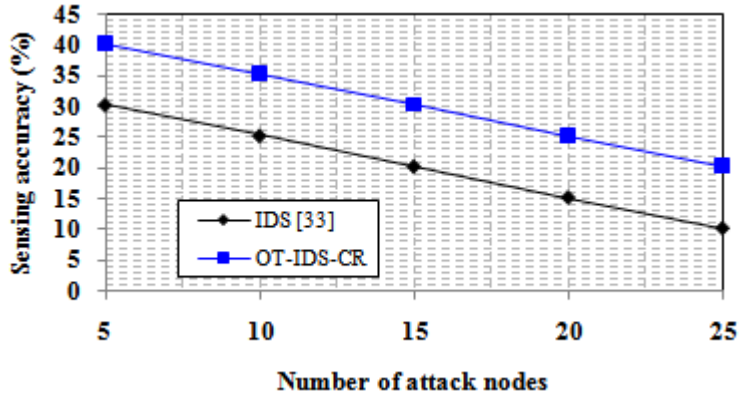

Fig. 19 Comparison of sensing accuracy with Random attacks

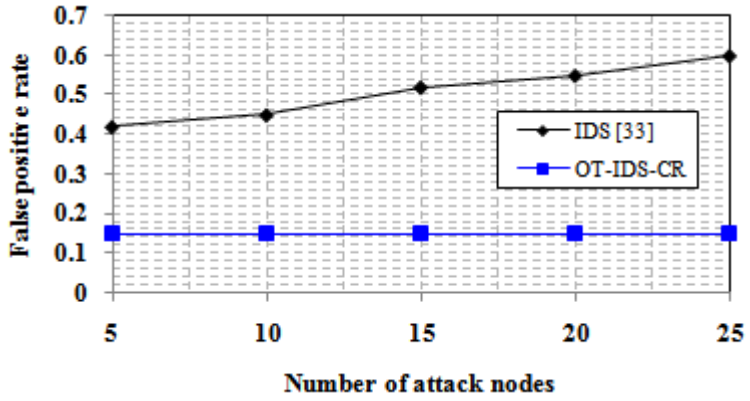

Fig. 20 Comparison of unture positive rate with Random attacks

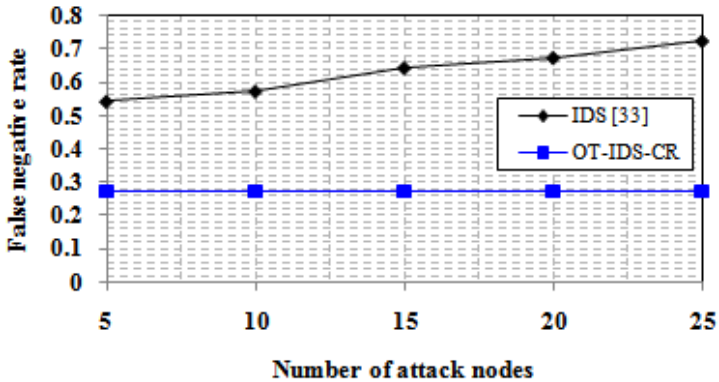

Fig. 21 Comparison of unture negative rate with Random e attacks

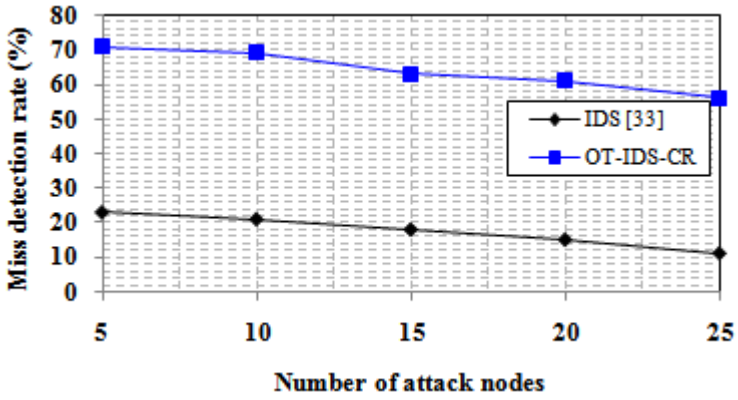

Fig. 22 Comparison of miss detection rate with Random attacks

6. Conclusion

An optimal trusted intrusion detection system is proposed for obliging spectrum sensing and allocation in CRN (OT-IDS-CR). The following contributions have involved in this work, an ICBO algorithm for efficient clustering which divide the sensing nodes into number of clusters; the trust degree of each SU is based on sensing information's with the help of CRL based trust management system; and MBO algorithm was used to optimize the sensing information's to avoid the dimensionality problem to ensure the secure spectrum sensing and allocation. From the imitation results, we experiential that the planned OT-IDS-CR model perform very effectively in terms of with and without attacks. We conclude that our proposed OT-IDS-CR model resists to the different SSDF attacks such as Byzantine, crude and random.

References

1. Lee, D.J. and Jang, M.S., 2009. Optimal spectrum sensing time considering spectrum handoff due to unture alarm in cognitive radio networks. *IEEE Communications Letters*, *13*(12), pp.899-901.
2. So, J. and Srikant, R., 2015. Improving channel utilization via cooperative spectrum sensing with opportunistic feedback in cognitive radio networks. *IEEE Communications Letters*, *19*(6), pp.1065-1068.
3. Li, S., Xiao, S., Zhang, M. and Zhang, X., 2015. Power saving and improving the throughput of spectrum sharing in wideband cognitive radio networks. *Journal of Communications and Networks*, *17*(4), pp.394-405.
4. Hattab, G. and Ibnkahla, M., 2014. Multiband spectrum access: Great promises for future cognitive radio networks. *Proceedings of the IEEE*, *102*(3), pp.282-306.
5. Düzenli, T. and Akay, O., 2016. A new spectrum sensing strategy for dynamic primary users in cognitive radio. *IEEE Communications Letters*, *20*(4), pp.752-755.
6. Wang, H., Yang, E.H., Zhao, Z. and Zhang, W., 2009. Spectrum sensing in cognitive radio using goodness of fit testing. *IEEE Transactions on Wireless Communications*, *8*(11), pp.5427-5430.
7. Van Nguyen, T., Shin, H. and Win, M.Z., 2011. Optimal sensing cardinality for cognitive radios. *IEEE communications letters*, *15*(7), pp.716-718.
8. He, H., Li, G.Y. and Li, S., 2013. Adaptive spectrum sensing for time-varying channels in cognitive radios. *IEEE Wireless Communications Letters*, *2*(2), pp.1-4.
9. Arienzo, L. and Tarchi, D., 2014. Statistical modeling of spectrum sensing energy in multi-hop cognitive radio networks. *IEEE Signal Processing Letters*, *22*(3), pp.356-360.
10. Chen, Z., Guo, N. and Qiu, R.C., 2010. Demonstration of real-time spectrum sensing for cognitive radio. *IEEE Communications Letters*, *14*(10), pp.915-917.
11. Liu, S.Q. and Hu, B.J., 2014. Analysis of sensing efficiency for cooperative spectrum sensing with malicious users in cognitive radio networks. *IEEE Communications Letters*, *18*(9), pp.1645-1648.
12. Shokri-Ghadikolaei, H. and Fallahi, R., 2012. Intelligent sensing matrix setting in cognitive radio networks. *IEEE communications letters*, *16*(11), pp.1824-1827.
13. Sun, H., Chiu, W.Y. and Nallanathan, A., 2012. Adaptive compressive spectrum sensing for wideband cognitive radios. *IEEE Communications Letters*, *16*(11), pp.1812-1815.
14. Lee, S.H., Shamaiah, M., Vikalo, H. and Vishwanath, S., 2013. Message-passing

algorithms for coordinated spectrum sensing in cognitive radio networks. *IEEE communications letters*, *17*(4), pp.812-815.
15. Tehrani, M.N. and Uysal, M., 2013. Auction based spectrum trading for cognitive radio networks. *IEEE Communications letters*, *17*(6), pp.1168-1171.
16. Mahesh, R. and Vinod, A.P., 2011. A low-complexity flexible spectrum-sensing scheme for mobile cognitive radio terminals. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *58*(6), pp.371-375.
17. You, C., Kwon, H. and Heo, J., 2011. Cooperative TV spectrum sensing in cognitive radio for Wi-Fi networks. *IEEE transactions on consumer electronics*, *57*(1), pp.62-67.
18. Huang, C.C. and Wang, L.C., 2012. Dynamic sampling rate adjustment for compressive spectrum sensing over cognitive radio network. *IEEE Wireless communications letters*, *1*(2), pp.57-60.
19. Althunibat, S. and Granelli, F., 2014. An objection-based collaborative spectrum sensing for cognitive radio networks. *IEEE Communications Letters*, *18*(8), pp.1291-1294.
20. Tadayon, N. and Aïssa, S., 2015. A multichannel spectrum sensing fusion mechanism for cognitive radio networks: design and application to IEEE 802.22 WRANs. *IEEE Transactions on Cognitive Communications and Networking*, *1*(4), pp.359-371.
21. Guo, H., Jiang, W. and Luo, W., 2017. Linear soft combination for cooperative spectrum sensing in cognitive radio networks. *IEEE Communications Letters*, *21*(7), pp.1573-1576.
22. Hajihoseini, A. and Ghorashi, S.A., 2017. Distributed spectrum sensing for cognitive radio sensor networks using diffusion adaptation. *IEEE sensors letters*, *1*(5), pp.1-4.
23. Liu, X., Li, B. and Liu, G., 2018. Simultaneous cooperative spectrum sensing and energy harvesting in multi-antenna cognitive radio. *Mobile Networks and Applications*, *23*(2), pp.263-271.
24. Kar, S., Sethi, S. and Sahoo, R.K., 2017. A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks. *Wireless Personal Communications*, *97*(2), pp.2523-2540.
25. Verma, G. and Sahu, O.P., 2018. A distance based reliable cooperative spectrum sensing algorithm in cognitive radio. *Wireless Personal Communications*, *99*(1), pp.203-212.
26. Muthukkumar, R. and Manimegalai, D., 2018. Enhancing cooperative spectrum sensing in cognitive radio ad hoc networks using priority-based two-stage detection model. *Wireless Networks*, *24*(8), pp.3295-3307.
27. Ezzati, N. and Taheri, H., 2018. Distributed spectrum sensing using radio environment maps in cognitive radio networks. *Wireless Personal Communications*, *101*(4), pp.2241-2254.
28. Prasad, R.G. and Venkatesan, P., 2019. Group based multi-channel synchronized spectrum sensing in cognitive radio network with 5G. *Mobile Networks and Applications*, *24*(2), pp.327-339.
29. Abdel-Sayed, M.M., Khattab, A. and Abu-Elyazeed, M.F., 2019. Fast matching pursuit for wideband spectrum sensing in cognitive radio networks. *Wireless Networks*, *25*(1), pp.131-143.
30. Rapetswa, K. and Cheng, L., 2020. Convergence of mobile broadband and broadcast services: A cognitive radio sensing and sharing perspective. *Intelligent and Converged Networks*, *1*(1), pp.99-114.
31. Eappen, G. and Shankar, T., 2020. A Survey on Soft Computing Techniques for Spectrum Sensing in a Cognitive Radio Network. *SN Computer Science*, *1*(6), pp.1-36.
32. Al-Kofahi, O.M., Almasaeid, H.M. and Al-Mefleh, H., 2020. Efficient on-demand spectrum sensing in cognitive radio networks. *Computer Communications*, *156*, pp.11-24.
33. Khalunezhad, A., Moghim, N. and Ghahfarokhi, B.S., 2018. Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks. Journal of information security and applications, 42, pp.29-35.
34. Kumar, S. and Singh, A.K., 2021. A localized algorithm for clustering in cognitive radio networks. Journal of King Saud University-Computer and Information Sciences, 33(5), pp.600-607.