ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2020.0343

ENERGY EFFICIENT POWER ALLOCATION FOR COGNITIVE RADIO NETWORKS WITH OPTIMAL SPECTRUM UTILIZATION USING ENSEMBLE ADAPTIVE NEURO FUZZY INFERENCE SYSTEM

V. Sangeetha and A. Prakash
Department of Computer Science, Hindusthan College of Arts and Science, India

Abstract

Radio Spectrum (RS) is underutilized by primary licensed users. Though many techniques for effective use of RS exist, OSA (Opportunistic Spectrum Access) has been most feasible in optimizing spectrum utilization as they allow unlicensed users access RS opportunistically. OSA approaches use CR (Cognitive Radios) which sense unused spectrum and familiarize their operating characteristics accordingly in real time environments. A recent study proposed spectrum access control and RS use by secondary users using probabilistic neural networks. The work also introduced an enhanced IDS (Intrusion Detection System) using Improved Support Vector Machine (ISVM)to identify anomalies in network's behaviour after learning normal behaviour from network traffic flows, protocol operations and primary user access times. Energy efficiency, an important aspect of CRNs (Cognitive Radio Networks) was not catered to in this study. This paper proposes a model for optimal Spectrum Utilization of wireless systems with CRNs where antecedents are also regarded for selection of spectrum bands. Anomalous behaviours in networks are also identified. Additionally this work introduces an energy efficient framework for power allocation to secondary users.

Keywords:

Opportunistic Spectrum Access, Spectrum Utilization, Primary User Access Time, Utility Function, Power Allocation

1. INTRODUCTION

Existing WNs (Wireless Networks) are dominated by static allocation policies in spectrum usage. Licensed users are allowed spectrum access on a long term basis by Government agencies. The sudden rise in authorized users has resulted in scarcity in allocated spectrum bands. On the other hand huge portions of the spectrum is used at irregular intervals leading to underutilization of spectrum bands [1] [2]. Hence, DSA (Dynamic Spectrum Access) techniques have been proposed overcome this inefficiency. A key technology in DSAs is CRT (Cognitive Radio Technology) which has the ability to share spectrum bands in an opportunistic manner. CRNs provide higher bandwidths to mobile users using multiple wireless architectures and DSA techniques. Thus, the problem can be overcome only with dynamic and efficient spectrum management techniques [3] [4]. Game theory have been used for opportunistic spectrum shared access in CRNs. Spectrum bands were allocated using a graph coloring algorithm, but without considering secondary user accesses. Only two secondary users using the same band were tested where certain secondary users might lose while competing for spectrum access. Monitoring users conflicting spectrum band usage was a complex issue [5] – [7].

To overcome the aforesaid issues, this work proposes a novel FLS (Fuzzy Logic System) to control RS access by secondary users. The scheme called EESAC (Energy Efficient Spectrum Access Control) is an improved model for optimized utilization of wireless systems in CRNs. Spectrum access is controlled by EANFIS (Ensemble Adaptive Neuro Fuzzy Inference System). The scheme also uses antecedents for spectrum selections of secondary users. An enhanced IDS with ISVM is also suggested for judging anomalies in the network. An energy efficient power allocation framework using PSO (Particle Swarm Optimization) for secondary users is also suggested a part of the proposed work.

2. LITERATURE REVIEW

This section reviews related studies on CRN spectrum utilizations.

The study of Dai and Wang [8] used clustering for resource allocations in a multiuser OFDM (Orthogonal Frequency Division Multiplexing) based CRN. Simple clustering divided SUs into groups based on mutual interference degrees. SUs shared OFDM sub-channels for improving spectrum utilization efficiency. SUs facing heavy mutual interferences were clustered in the same group and used many sub-channels to lessen interferences. The scheme's simulations indicated improvements in SUs throughput in a stable and quick manner when compared to other methods.

HMM (hidden Markov model) was used by Jin et al. [9] in their study for a co-operative spectrum sensing to predict network statuses. Traditional predictions assume uniformity in CR nodes though their channel availability differs leading to lower prediction accuracies in complex radio environments. Their scheme learnt historical spectrum sensing results to help networks in their energy-efficient spectrum sensing. Their experimental results showed their algorithm improved energy efficiency and spectrum utilization by 13% and 15% when compared to conventional HMM-based methods.

Spectrum management was proposed by Zhao, et al. [10]. Their study considered both spectrum and user's mobility in their predictions. They combined predictions with cooperative sensing where a CR base station obtained future locations of secondary users for prearranging high quality channels in advance. Their channel selection scheme made multiple channels availability. Their extensive simulations verified that their spectrum management strategy improved system performance significantly in reducing handoff times and improving user satisfactions, connection reliability and channel utilizations.

Koushik et al. [11] managed spectrum mobility in CRNs intelligently. Their scheme included spectrum handoff condition when the user switched to a new channel or a wait condition. Optimization schemes for spectrum mobility management need to consider long time impacts on network performances like throughput and delay, instead of optimizing only short-term performance. The study used TACT (Transfer Actor-Critic Learning), a ML (Machine Learning) scheme, for managing spectrum mobility. TACT had a comprehensive reward function that considered CUF (Channel Utilization Factor), PER (Packet Error Rate), PDR (Packet Dropping Rate), and flow throughput in experimentations and found TACT's performance mean was higher when compared to myopic and Q-learning based spectrum management schemes.

Multi-user multi-channel scenarios in CRNs were investigated in the study of Huang, et al. [12]. Their scheme first applied Dirichlet Process to learn online and predict channel usage based on ACK/NACK feedbacks. The learning was then used to optimize spectrum access strategies in CRNs. This avoided frequent information exchanges between users. The prediction results were used to compute delays on user transmissions of multimedia packets on specific channels. They derived their PDR for channel usage to reflect competitions between users from predictions. They defined their QoS (Quality of Service) parameters in multimedia applications as joint delay and throughput performances. They also proposed a dynamic spectrum access scheme for optimizing QoS metrics. Their simulations demonstrated that their QoS and PSNR (Peak-Signal-to-Noise Ratio) parameters outperformed three other existing spectrum access algorithms. Their algorithm achieved more PDR enhancements of 21.8%, 5.4%, and 3.9% with PSNR gains over 3.23 dB, 0.82 dB, and 0.50 dB in transmission powers of 10, 20, and 30 units.

Fuzzy logic was proposed by Ali, et al. [13] in their FLB-DSS (Fuzzy Logic Based Decision Support System) scheme that catered to channel selection and switching for enhanced CRN throughputs. Their proposal reduced SU channel switching rates to make channel selections more adaptable. FLB-DSS, when evaluated on Matlab, showed promising results in terms of throughputs and handoffs counts, making it a suitable candidate for SUs in CRNs.

Markov model was used by El-Toukhey et al. [14] in their proposal to evaluate finite and infinite number of users using two classical channel access techniques namely random and reservation channel schemes. Impacts on changing arrival and service rates in priority-based SUs (Secondary Users) were evaluated for the probabilities of blocks, drops and hand offs in SUs. Their proposal classified SUs into two classes of priorities where their analysis demonstrated enhancements in radio system performances.

3. PROPOSED METHODOLOGY

The proposed scheme is detailed in this section. The scheme has three phases namely network anomaly detection using ISVM, power allocation using PSO and spectrum access control using EANFIS (Ensemble Adaptive Neuro Fuzzy Inference System). The overall architecture of the proposed system is depicted in Fig.1.

3.1 SYSTEM MODEL

Assuming there is N number of SUs as transmitters in a CRN with a SBS (Secondary Base Station) as the common receiver, the study considers uplink communication. Transmitters use licensed spectrum band of a PU's (Primary User) transceiver pair with a primary BS as the receiver and OFDM (Orthogonal Frequency-Division Multiplexing) technology is used in both types of transmissions. To avoid degradations in transmission quality of primary users the interferences from secondary transmitters to the primary BS has to be a below the threshold value denoted by I^{th}. OFDM divided the licensed spectrum band into K sub-channels or each wireless link on a sub-channel is allotted a fixed time slot where the slot can change in the next allotment. Each link gains different sub-channels independent of each other.

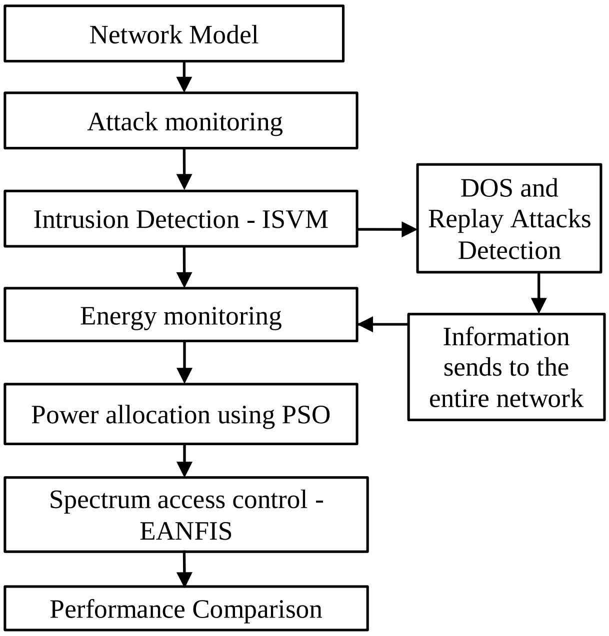

Fig.1. Overall Architecture of the proposed model

3.2 THREATS IN CRN

CRNs are elementary WNs which inherit security threats. These threats can be categorized based on layers for attack taxonomy. TCP (Transport Control Protocol) is susceptible to transport layer threats and mainly the "Lion" attack. Sinkhole and HELLO flood attacks are network layer attacks contrasting CRN attacks. Link layer attacks occur on sensing spectrums which include Byzantine attacks analogous to ad hoc networks, DoS (Denial of Service) attacks using CRN controls. Further, physical layer attacks are the most challenging to counter in CRNs and include PUE (Primary User Emulation), jamming and objective function attacks, Replay attack.

3.3 INTRUSION MONITORING AND DETECTIONS USING IMPROVED SVM

This work identifies abnormal activities in CRNs by learning through the network's regular activities. Improved SVM is used to predict protocol operation patterns and thus detect attacks. This work detect DOS and replay attacks. A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. So it can be detected by transmitted and received signal length.

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it. It can detect by calculating the delay rate of transmitted signals.

In SVM how to select kernel function depends on the distribution of sample data and the relationship between sample data and predicted variables. Since different feature space has different data distribution, the performance of SVM depends largely on the choice of kernel function. Kernel functions can be divided into local and global types, the local kernel function has good learning ability but weak generalization ability, while the global kernel function has good generalization ability but weak learning ability. Gaussian radial basis kernel function (RBF) and polynomial kernel function (Poly) are typical local and global kernel function, respectively. Thus they are often used for prediction, following are their formulas.

$$K(x,x_i) = [\gamma(x*x_i)+1]^q \tag{1}$$

$$K(x,x_i) = \exp(-\gamma\|x-x_i\|^2) \tag{2}$$

The Eq.(1) is Poly and Eq.(2) means RBF, γ is subjected to kernel function, which implicitly determines the distribution of the data after being mapped to the new feature space, q means the power parameter.

The network flow varies in complex modes. In order to adapt to the nonlinearity and randomness of network flow, as well as improving the accuracy of algorithm, set a hybrid kernel function which is formulated by combining both Eq.(1) and Eq.(2) with adaptive weights, the formula is as follow.

$$K(x,x_i) = \beta.\exp(-\gamma\|x-x_i\|^2)+(1-\beta).[\gamma(x*x_i)+1]^q \tag{3}$$

where β = [0,1] means the hybrid kernel function's weight coefficient.

To make full use of both advantages when predicting the network flow, propose the method to make the weight adjust adaptively according to the change or slope of real-time network signal, following is the formula.

$$\beta = 1-\frac{1}{e^{|k|}} \tag{4}$$

where $K = \dfrac{y_{i-1}-y_{i-2}}{x_{i-1}-x_{i-2}}$ means the slope of the previous two values of traffic volume. When the value of $|k|$ is decreasing, the curve of network flow tends to normal, and should increase the kernel function's global generalization ability, that is increasing the weight of polynomial kernel function, or decreasing the value of β. When the value of $|k|$ is increasing, the curve tends to sharp, and should increase the kernel function's local learning ability, that is increasing the weight of Gaussian kernel function, or increasing the value of β.

3.3.1 Learning Protocol Operations with Improved SVM:

The proposed design for efficiently detecting anomalies caused by attacks is based on learning traffic flows, SS (Signal Strengths), primary user access times, PDR (Packets Received / Packets Sent) and normal behaviour of protocol operations. IDS learns from normal CRN conditions to construct statistical profiles i.e. with reduced level of malicious activities. Jamming attacks on the physical layer is considered in this phase and analyzed based on secondary user's SS and PDR. IDS, in its learning phase does not restrict to this feature alone. Other aspects like CRN system specifications, wireless protocol behavior, etc., are also taken into account for learning CRN modes of operations. Thus, information acquired is used for discovering intrusions or attacks in the targeted CRN which is then learned by ISVM.

Have $\mathcal{L}$ sample sets $\{(x_i,y_i)|x_i\in R^v, y_i\in R\}$, where x_i is an input vector of dimensionality v and y_i is the output vector corresponding to xi. Then construct the optimal decision-making function in the feature space as follows:

$$f(x) = \sum_{i=1}^{L}\left(\alpha_i-\alpha_i^*\right)K(x,x_i)+b \tag{5}$$

where α_i and α_i^* are Lagrange coefficients representing the two slack variables, $b\in$R is the bias, and $K(x,x_i)$ is the kernel function

3.3.2 Change Point Detection:

Point changes in CRNs are suggested in the IDS detection phase during attacks. Assuming a jamming attack occurs on the physical layer, secondary user connections get jammed. PDR value falls below the required level while estimating SS which does not reduce implying the secondary does not receive some/all packets sent. The change point in PDRs on jamming attacks can be obtained as follows. Assuming, IDS is executed in equal time-rounds Δn for n = 1,2,3 and so on, the mean of F_n in the profiling period is m which has a value nearing 1 when the network is not attacked. Randomly chosen sequence means values have to be in the negative under normal conditions and turn positive on changes. Thus, a new sequence $G_n=b-F_n$ is acquired where b is minimum/ negative peak average values of F_n in the profiling period. In a jamming attack, G_n increases the mean's lower bounded by $h=2\beta$ where the cu sum sequence Y_n can be stated using Eq.(6) and Eq.(7)

$$Y_n = (Y_{n-1}+G_n)^+ \tag{6}$$

$$Y_0 = 0 \tag{7}$$

where $x^+=x$ if $x > 0$; otherwise, $x^+ = 0$. An anomaly can be inferred when the value of Y_n is large the detecting threshold value θ can be computed using Eq.(8)

$$\theta = (m-\beta)t_{des} \tag{8}$$

where t_{des} - required detection time and lesser value detects anomalies quicker. IDS calculations of Y_n in a time frame are zero for normal conditions and increases when a jamming attack occurs on the network. Y_n surpasses q as long as assessed SS of secondary user is high, IDS creates an attack alert and forwards it to probabilistic neural network for preventing spectrum accesses.

3.4 ENERGY EFFICIENT POWER ALLOCATION USING PSO

Power allocation of secondary transmitters in each time slot is considered in this phase. If P_k^i is transmitted power of SU i over subcarrier k (k=1,2,...,K) in a time slot and $G_k^{ii}\,(i=1,2,...,N)$ is the link gain from i to SBS, then SINR (Signal to Interference Ratio) for i's communication over k denoted as γ_k^i can be given as Eq.(9):

$$\gamma_k^i = \frac{G_k^{ii}P_k^i}{\sum_{j\neq i}G_k^{ij}P_k^j+\sigma^2} \tag{9}$$

- **Utility function:** SU communications over sub-channel k is defined as a utility function denoted by U_k^i. This function reflects service quality. This work adopts a sigmoidal utility for greater user satisfaction levels This function's value of the service provided to the user can be defined as Eq.(10).

$$U_k^i = \frac{1}{1+e^{-a_i\left(\gamma_k^i - b_i\right)}} \tag{10}$$

where a_i - slope parameter (large value means application has a soft quality in services) and b_i - shift parameter to average data rates in the application. Higher utilities with less energy consumptions is defined as an energy efficiency metric and is expressed as a ratio of utility to transmission power (utility/Joule), given as Eq.(11):

$$E = \frac{\sum_{i=1}^{N} U_k^i}{\sum_{i=1}^{N} p_k^i + P_c} \tag{11}$$

where, P_c is the static transmission power consumptions other than wireless networks (circuit power consumptions).

- **Constraints:** Interferences received by the primary BS from secondary transmissions in each sub-channel is bound by a threshold I_{th} and $G_k^{oi}\left(k=1,2,...,K\right)$ is the link gain from SU_i to primary BS. This power interference constraint is depicted as given as Eq.(12)

$$\sum_{i=1}^{N} G_k^{Oi} p_k^i \le I_{th} \tag{12}$$

The total transmission power over each sub-channel should also be bound by P_{max} and given as Eq.(13)

$$\sum_{i=1}^{N} P_k^i \le P_{\max} \tag{13}$$

In considering the maximal energy efficiency amidst power interferences in terms of power constraints and total transmit power constraints, optimization can be formulated as:

$$\text{Maximize } E = \frac{\sum_{i=1}^{N} U_k^i}{\sum_{i=1}^{N} p_k^i + P_c} \tag{14}$$

$$\text{Subjected to } \sum_{i=1}^{N} G_k^{Oi} p_k^i \le I_{th} \tag{15}$$

$$\sum_{i=1}^{N} P_k^i \le P_{\max} \tag{16}$$

$$P_k^i \ge 0 \tag{17}$$

Initial Population: SU selection is treated as problem and optimized to find an optimal subset of users [21] – [23]. The set of users F, represented as a vectors $F_i = f_{i,1}, f_{i,b},...,f_{i,j},...,f_i$ where t is the number unique users and i is the identity. Assuming FS a new subset of users $S_{Fi} = s_{i,1}, s_{i,2},...,s_{i,j},...,s_{i,m}$ generated by the selection algorithm with length m, s_{ij} is in the range {0, 1}, j = 1, 2,..., m. When s_i, j=1 it implies the j^{th} user is selected as the informational users with identity i. While $s_{i,j}$ = 0 implies j^{th} user is an uninformative user.

- **Solution representation:** PSO has a collection of positions which are binary vectors/rows and includes secondary user positions. Each particle in PSO represents a solution or denotes a subset of secondary users. Each position represents the sample's single user and j^{th} position indicates j^{th} user. PSO algorithm selections begin with random solutions and keep improving to reach global optimality, the new subset of secondary users where each unique user in the network is one search space. When j =1, j^{th} secondary user is chosen as an optimal secondary user while j = 0 implies the j^{th} secondary user is discarded and j = −1 implies the secondary user is not a part of the network.
- **Fitness function:** This work uses PSO algorithm's Energy as the fitness function for power allocation problem [24] [25]. The function evaluates ach candidate solution that is obtained by the selection algorithm. Its each generation computes fitness of all candidate solutions. The solution gets replaces when its quality increases and finally the solution with highest fitness value is treated as the optimal solution and in this work the optimal power allocation scheme for the current Network.

Thus, power is allocated only for selected optimal secondary users using the power allocation algorithm and depicted below:

Step 1: Swarm (Secondary user initialisation). Randomly initialise the position x_i, and velocity v_i of each particle

Step 2: Particle (Secondary user) Fitness (E) evaluation

Step 3: If Fitness of $x_i > p_{best}^i$

Step 4: $p_{best}^i = x_i$

Step 5: If Fitness of $p_{best}^i > g_{best}^i$

Step 6: $g_{best}^i = p_{best}^i$

Step 7: Update the velocity of particle (secondary user)

$$V_{id}^{t+1} = \omega_{id}^{t+1} = C_1 r_{ii}\left(p_{id} - x_{id}^t\right) + c_2 r_{2i}\left(p_{gd} - x_{id}^t\right)$$

Step 8: Update the position of particle

$$x_{id}^{t+1} = x_{id}^t + V_{id}^{t+1}$$

Step 9: If stopping citation is not met continue step 2 and step 3

Step 10: Return g_{best} and Fitness value (E)

3.5 SPECTRUM ACCESS CONTROL USING EANFIS

EANFIS executes an Opportunistic Spectrum Access by choosing appropriate secondary user instances to access free spectrum bands devoid of interferences from primary users. EANFIS gathers instance information using descriptors listed below [26].

- SUE (Spectrum Utilization Efficiency)
- DM (Degree of Mobility)
- Distance of the Secondary user from Primary User

- **ANFIS (Adaptive Neuro Fuzzy Inference System):** The above listed descriptor information become ANFIS network's inputs. ANFIS networks are based on Neuro fuzzy networks where their architecture implements rules.

ANFIS in this work is tested thrice for its ensemble learning operations. First layer nodes are customizable with outputs as fuzzy memberships given by Eq.(20)

$$O_i^1 = \mu_{Ai}(x) \text{ for } i=1,2 \tag{20}$$

where x,y-input nodes, A,B-linguistic labels, (x),(y)-membership functions which may assume a bell shape due to higher or lower equivalent to 1 and 0 and given in Eq.(21)

$$\mu(x) = \frac{1}{1+\left(\frac{x-c_i}{a_i}\right)2b_i} \tag{21}$$

where, a_i, b_i, c_i - parameters set in the premise.

The 2nd layer of ANFIS has fixed nodes labelled as M for indicating simple multiplications. The layer's output, firing strength of a rule, is depicted in Eq.(22)

$$O_i^2=w_i=\mu_{Ai}(x)\mu_{Bi}(y), i=1,2 \tag{22}$$

where w_i - firing strength of a rule.

Third layers nodes resulting in normalized firing strengths are also fixed and labelled as N, indicating normalization of firing strengths inputs of the previous layer and is represented as Eq.(23).

$$O_i^3 = w_i=w_1/(w_1+w_2),\ i=1,2 \tag{23}$$

4th layer has customizable nodes where each node is the product of normalized firing strengths and its output can be equated to Eq.(24)

$$O_i^4=w_if_i=w_i(p_ix+q_iy+r_i) \tag{24}$$

where w - 3rd layer output, $\{p_i,q_i,r_i\}$ - resultant parameter set.

The ultimate layer has only one single fixed node labelled as S to signify summation of incoming signals and its output is given by Eq.(25):

$$O_i^5 = \sum_{i=1} w_i f_i = \frac{\sum_i w_i f_i}{\sum_i w_i} \tag{25}$$

Ensemble Process: The main reason for using the ensemble process is to avoid errors from individual classifier outputs which have diverse features. Averaging these model outputs results in reduction of errors. Ensemble learning improves classification or prediction performances as it minimizes errors and specifically in multiclass classifications. ANFIS generates N values where each has their own initial values chosen randomly from a distribution. Thus, ANFIS is trained separately and their values are averaged.

4. RESULTS AND DISCUSSION

The proposed Improved Energy Efficient IDS is assessed by considering IEEE 802.22 WRAN topology. The Table.1 lists the associated information of the WRAN system, in which the model of WRAN CRN has taken 68 channels, where maximally 12 secondary users may concurrently access each of the channels. The deployment of proposed IDS to these users reveals its efficient function of defending the overall users from the impacts of the attack, which has depicted through the simulation process carried out under matlab. Moreover, this segment differentiates the efficient performance of the proposed EESAC strategy from the current approaches, namely MASAS, FLS and ESAC.

Table.1.IEEE 802.22 WRAN based cognitive radio network system parameters

Chosen Parameters	Value
Wireless bandwidth	54 to 806 MHz
Number of channels	68
Individual channel bandwidth	6 MHz
Band ranges	54 to 72 MHz, 76 to 88 MHz, 174 to 216 MHz and 470 to 806 MHz
Maximum number of simultaneous secondary users	12
Minimum peak downlink rate per secondary user	1.5 Mbps
Minimum peak uplink rate per secondary user	384 Kbps
Cell coverage	33 to 100 km
Spectral efficiency	3 bits/s/Hz
Total physical data rate per channel	18 Mbps
Packet size (MTU)	1518 bytes
Minimum frames per second (received per secondary user)	129.51

4.1 NETWORK FEATURES TO DETECT ATTACKS

After performing measurements on some basic features, these measurements will be served as basic reference. Features that are measured depend on the transmitted packets and connection features. The features that depend on the incoming packets are measured by

- The number of the packet sent during one sampling period (depends on network density and the sampling period),
- Network adaptability,
- The number of outgoing packets,
- The data packet rate and
- The channel rate.

The connection features are changed when using the handoff (during the handoff process some transmission parameters are changed such as the carrier frequency and the bandwidth). All of these features and measurements represent the generation feature, which sets the standard mode of this environment. So, identifying a minimal set of CRN features that to be used to identify the attacks in progress is the key task in building a successful threat detection system (any CRN attack will cause an abnormal behaviour scenario, and it is required to be able to accurately identify this anomalous behaviour).

Table.1. Performance comparison results for Throughput

Methods	Number of nodes				
	10	**20**	**30**	**40**	**50**
MASAS	40	43	48	51	55
FLS	48	50	54	58	61
ESAC	58	60	63	68	70
EESAC	60	63	65	70	76

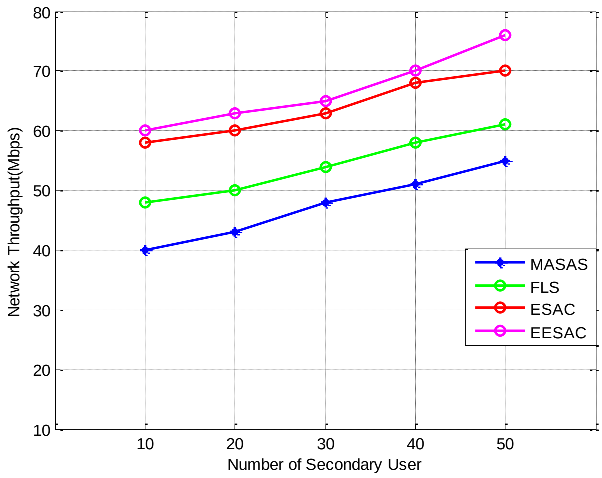

Fig.2. Throughput results vs. Number of secondary users

Table.2. Performance comparison results for system utility rate

Methods	Number of nodes				
	10	**20**	**30**	**40**	**50**
MASAS	49	52	54	57	60
FLS	50	55	58	60	64
ESAC	61	64	68	71	76
EESAC	63	68	73	72	78

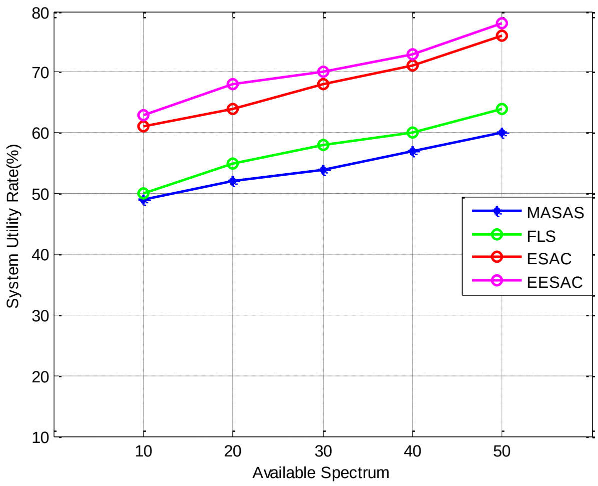

Fig.3. System utility rate vs. available spectrum range

In Fig.2, the Throughput values of proposed EESAC strategy has contrasted from the current approaches of MASAS, FLS and ESAC in which X-axis embodies total count of secondary users, whereas Y-axis implies Throughput values. During this research, the implementation of Gaussian kernel in the ISVM enhances the Throughput ratio, as it enables the optimal classification of attack. The outcomes prove that the proposed novel EESAC strategy has the ability to attain 75 Mbps Throughput, which is superior to the Throughput values of MASAS, FLS and ESAC methods, since they solely obtain 55, 61 and 76 Mbps correspondingly.

The Fig.3 compares the system utility rate between the proposed novel EESAC technique and current approaches (such as MASAS, FLS and ESAC), where the available spectrum range lies on X-axis, besides the Y-axis stands for the values of System utility rate. The involvement of fuzzy kernel in Adaptive neuro fuzzy inference system augments the system utility rate by choosing the optimal secondary user. The outcomes depict that the proposed EESAC strategy has secured higher System utility rate of 78%, whereas the MASAS solely obtains 60%, FLS method holds 64% and ESAC method hold 76%.

Table.3. Performance comparison results for Packet delivery ratio

Methods	Number of nodes				
	10	**20**	**30**	**40**	**50**
MASAS	45	47	50	52	56
FLS	47	50	54	59	62
ESAC	60	65	68	70	74
EESAC	64	68	70	73	79

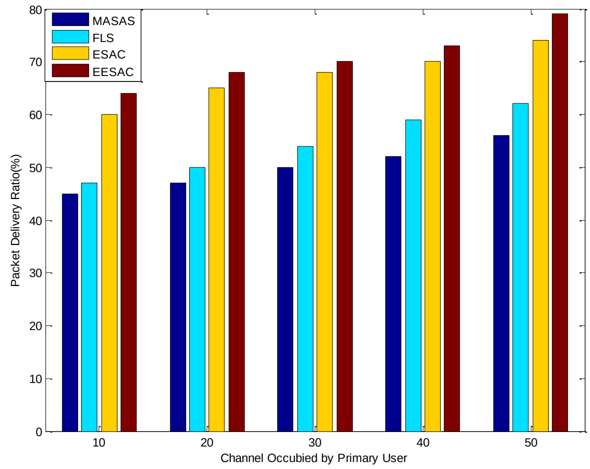

Fig.4. Packet delivery ratio vs. Channels used by the users

Table.4. Performance comparison results for Attack detection rate

Methods	Number of nodes				
	10	**20**	**30**	**40**	**50**
MASAS	44	48	52	56	58
FLS	49	54	58	62	65
ESAC	55	59	63	68	73
EESAC	59	63	65	71	75

In Fig.4, proposed EESAC strategy packet delivery ratio has contrasted from the current methods of MASAS, FLS and ESAC. In the graph, the X-axis embodies the channels used by the Secondary users, whereas the Y-axis implies the values of Packet delivery ratio, which demonstrates that the proposed novel EESAC strategy has the capacity to obtain 79% packet delivery ratio, which is higher than the current methods of MASAS, FLS and ESAC since they solely acquire 56%, 62% and 74% correspondingly.

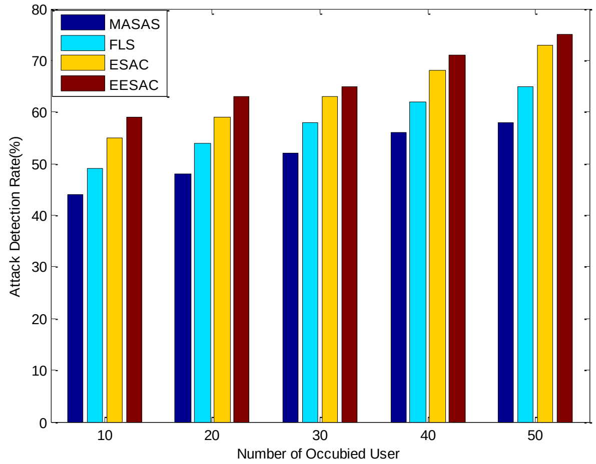

Fig.5. Attack detection rate vs. Channels used by the users

The Fig.5 compares the Attack Detection Rate acquired by the proposed EESAC strategy and current approaches (such as MASAS, FLS and ESAC), in which the utilized Channel count lies on X-axis, besides the Y-axis stands for the Attack detection rate. The results demonstrate that the proposed novel EESAC strategy has delivered the 75% of attack detection rate which is superior to the current approaches of MASAS, FLS and ESAC as they solely hold 58%, 65% and 73% correspondingly.

Table.5. Performance comparison results for Energy consumption

Methods	Number of nodes				
	10	20	30	40	50
MASAS	1.34	2.68	4.02	5.36	6.7
FLS	1.23	2.46	3.69	4.92	6.15
ESAC	1.19	2.38	3.58	4.76	5.96
EESAC	1.02	2.04	3.06	4.08	5.1

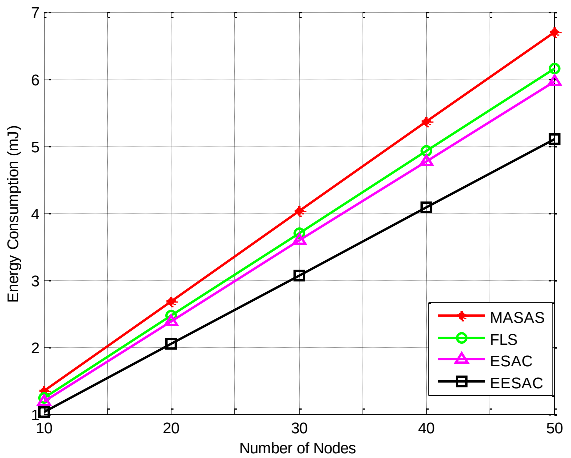

Fig.6. Energy consumption vs. Channels used by the secondary users

In Fig.6, proposed EESAC strategy Energy consumption has contrasted from the current methods of MASAS, FLS and ESAC. In the graph, the X-axis embodies the channels used by the Secondary users, whereas the Y-axis implies the values of Energy consumption, which demonstrates that the proposed novel EESAC strategy has the capacity to obtain 5.1mj Energy consumption, which is lower than the current methods of MASAS, FLS and ESAC since they solely acquire 6.7mj, 6.15mj and 5.96mj correspondingly.

5. CONCLUSION AND FUTURE WORK

Cognitive Radio is one of the key ideas introduced to overcome spectrum scarcity. This work attempted to provide an energy efficient and secure spectrum access model where secondary users are selected for spectrum access control using EANFIS. ISVM based IDS identified anomalous behaviour in CRNs. The detections were attained by assessing normal protocol operation behaviours like traffic flow and primary user access time. The study allocated power using PSO utility function for optimizing allocations to secondary users. The experimental results of the proposed methodology show that the model provides energy efficient spectrum access when compared to other existing methods. The proposed model produces a 78% packet delivery ratio. However, the proposed system may fall into a local optimum in high-dimensional spaces and can be improved in its future optimizations.

REFERENCES

[1] Z. Jin, K. Yao, B. Lee, J. Cho and L. Zhang, "Channel Status Learning for Cooperative Spectrum Sensing in Energy-Restricted Cognitive Radio Networks", *IEEE Access*, Vol. 7, pp. 64946-64954, 2019.

[2] A. Ali and W. Hamouda, "Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Applications", *IEEE Communications Surveys and Tutorials*, Vol. 19, No. 2, pp. 1277-1304, 2016.

[3] M. El Tanab and W. Hamouda, "Resource Allocation for Underlay Cognitive Radio Networks: A Survey", *IEEE Communications Surveys and Tutorials*, Vol. 19, No. 2, pp. 1249-1276, 2016.\

[4] I. Kakalou, D. Papadopoulou, T. Xifilidis, K.E. Psannis, K. Siakavara and Y. Ishibashi, "A Survey on Spectrum Sensing Algorithms for Cognitive Radio Networks", *Proceedings of 7th International Conference on Modern Circuits and Systems Technologies*, pp. 1-4, 2018.

[5] Y. Wang, Z. Ye, P. Wan and J. Zhao, "A Survey of Dynamic Spectrum Allocation based on Reinforcement Learning Algorithms in Cognitive Radio Networks", *Artificial Intelligence Review*, Vol. 51, No. 3, pp. 493-506, 2019.

[6] P. Yang, L. Li, J. Yin, H. Zhang and Z. Han, "Dynamic Spectrum Access in Cognitive Radio Networks using Deep Reinforcement Learning and Evolutionary Game", *Proceedings of IEEE/CIC International Conference on Communications in China*, pp. 405-409, 2018.

[7] S.V. Bhagate and S. Patil, "Maximizing Spectrum Utilization in Cognitive Radio Network", *Proceedings of International Conference on Big Data, IoT and Data Science*, pp. 82-90, 2017.

[8] J. Dai and S. Wang, "Clustering-Based Spectrum Sharing Strategy for Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 35, No. 1, pp. 228-237, 2016.
[9] Z. Jin, K. Yao, B. Lee and L. Zhang, "Channel Status Learning for Cooperative Spectrum Sensing in Energy-Restricted Cognitive Radio Networks", *IEEE Access*, Vol. 7, pp. 64946-64954, 2019.
[10] Y. Zhao, Z. Hong, Y. Luo, G. Wang and L. Pu, "Prediction-Based Spectrum Management in Cognitive Radio Networks", *IEEE Systems Journal*, Vol. 12, No. 4, pp. 3303-3314, 2017.
[11] A.M. Koushik, F. Hu and S. Kumar, "Intelligent Spectrum Management based on Transfer Actor-Critic Learning for Rateless Transmissions in Cognitive Radio Networks", *IEEE Transactions on Mobile Computing*, Vol. 17, No. 5, pp. 1204-1215, 2017.
[12] X.L. Huang, X.W. Tang and F. Hu, "Dynamic Spectrum Access for Multimedia Transmission Over Multi-User, Multi-Channel Cognitive Radio Networks", *IEEE Transactions on Multimedia*, Vol. 22, No. 1, pp. 201-214, 2019.
[13] A. Ali, L. Abbas, M. Shafiq, A.K. Bashir and K.S. Kwak, "Hybrid Fuzzy Logic Scheme for Efficient Channel Utilization in Cognitive Radio Networks", *IEEE Access*, Vol. 7, pp. 24463-24476, 2019.
[14] A.T. El Toukhey, A.A. Ammar, M.M. Tantawy and I.F. Tarrad, "Performance Analysis of Different Opportunistic Access based on Secondary Users Priority using Licensed Channels in Cognitive Radio Networks", *Proceedings of National Conference on Radio Science*, pp. 160-169, 2017.
[15] D. Mlakic, H.R. Baghaee and S. Nikolovski, "A Novel ANFIS-Based Islanding Detection for Inverter-Interfaced Microgrids", *IEEE Transactions on Smart Grid*, Vol. 10, No. 4, pp. 4411-4424, 2018.
[16] S.D. Nguyen, S.B. Choi and T.I. Seo, "Recurrent Mechanism and Impulse Noise Filter for Establishing ANFIS", *IEEE Transactions on Fuzzy Systems*, Vol. 26, No. 2, pp. 985-997, 2017.
[17] K.P. Vijayakumar, K.P.M. Kumar, K. Kottilingam, T. Karthick and P. Ganeshkumar, "An Adaptive Neuro-Fuzzy Logic Based Jamming Detection system in WSN", *Soft Computing*, Vol. 23, No. 8, pp. 2655-2667, 2019.
[18] A. Kumaravel and M. Chandrasekaran, "Performance Analysis of Malicious Node Detection in MANET using ANFIS Classification Approach", *Cluster Computing*, Vol. 22, No. 6, pp. 13445-13452, 2019.
[19] S. Acharya and C.R. Tripathy, "A Reliable Fault-Tolerant ANFIS Model based Data Aggregation Scheme for Wireless Sensor Networks", *Journal of King Saud University-Computer and Information Sciences*, Vol. 32, No. 6, pp. 741-753, 2017.
[20] C.L. Lim, C. Goh, A. Khan and Y. Li, "Predicting Types of Failures in Wireless Sensor Networks using an Adaptive Neuro-Fuzzy Inference System", *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 1-7, 2016.
[21] P. Parwekar, S. Rodda and S.V. Mounika, "Comparison between Genetic Algorithm and PSO for Wireless Sensor Networks", *Smart Computing and Informatics*, pp. 403-411, 2018.
[22] Z. Yan, P. Goswami, A. Mukherjee and G. Palai, "Low-Energy PSO-Based Node Positioning in Optical Wireless Sensor Networks", *Optik*, Vol. 181, pp. 378-382, 2019.
[23] S.P. Singh and S.C. Sharma, "A PSO Based Improved Localization Algorithm for Wireless Sensor Network", *Wireless Personal Communications*, Vol. 98, No. 1, pp. 487-503, 2018.
[24] D.R. Edla, M.C. Kongara and R. Cheruku, "SCE-PSO based Clustering Approach for Load Balancing of Gateways in Wireless Sensor Networks", *Wireless Networks*, Vol. 25, No. 3, pp. 1067-1081, 2019.
[25] D.R. Edla, M.C. Kongara and R. Cheruku, "A PSO Based Routing with Novel Fitness Function for Improving Lifetime of WSNs", *Wireless Personal Communications*, Vol. 104, No. 1, pp. 73-89, 2019.
[26] A. Prakash and V. Sangeetha, "Review of Opportunistic Spectrum Access Approach in Cognitive Radio Networks", *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 12, No. 7, pp. 222-229, 2020.