Indian Journal of Radio & Space Physics
Vol.50, June 2021, pp. 90-94

Fuzzy based clustering in CWPSN using machine learning model

Bhuvaneswari M[a*], Sasi Priya S[b] & Arun Chakravarthy R[c]

[a] Department of Mechatronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu 641 008, India

[b] Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu 641 008, India

[c] Department of Information Technology, KGiSL Institute of Technology, Coimbatore, Tamil Nadu 641 035, India

Received: 12 February 2021; Accepted: 5 March 2021

Cognitive wireless power sensor network (CWPSN) technology, widely used in almost all fields, has addressed various issues. The researchers have addressed the problems in the lack of radio spectrum availability and enabled the allocation of dynamic spectrum access in specific fields. The main challenge has been to support the radio spectrum allocation using intelligent adaptive learning and decision-making techniques so that various requirements of 5G wireless networks can be encountered. Machine learning (ML) is one of the most promising artificial intelligence tools conceived to support cognitive wireless networks. This paper aims to provide energy optimization and enhance security to cognitive wireless power sensor networks using a novel protocol during resource allocation. In addition to the existing methods, a novel protocol, fuzzy cluster-based greedy algorithms for attack prediction and energy harvesting using a machine-language model based on neural network techniques have been introduced. The simulation has been done using MATLAB software tools which gives efficient results.

Keywords: Energy harvesting, Greedy algorithm, CNN, Primary user, Machine learning, Artificial intelligence

1 Introduction

Cognitive wireless network and dynamic spectrum access have been the major paired approaches that cater to cognitive wireless power sensor network communication needs. A Cognitive Wireless Radio (CRN) network is a transceiver that automatically detects available wireless spectrum channels and changes its transmission or reception parameters accordingly with the support of a hybrid access point. The goal of CRN is to gain the best available range through cognitive abilities and reconfiguration. The network operator moves to another spectrum hole or remains in the same band if this band has been further used by a licensed user, altering its transmission power level or modulation scheme to avoid interference.

The use of ML-based detection methods in the 5G network has a greater advantage in almost all the research areas. Narrowband sensing investigates the available bandwidth at a time, whereas a number of frequency bands at a time are investigated by wideband sensing[1]. Energy detection, cyclo-stationary function detection, matched filter detection, covariance-based detection, and machine learning-based sensing are examples of the narrowband[2]. The supervised learning methods are based on known models and labels that can support the prediction of parameters that are unknown[3]. Massive MIMO communication channels are being used to detect data, frequency band sensing, and detection of white space in cognitive radio too, in the processing of Communications with 5G. In applications of higher layers, say inferring mobile users' locations and behaviour patterns help network operators enhance the quality of services. Input data needs to be focused on unsupervised learning in a probabilistic method. It can be implemented for cell segmentation in hyper-dense tiny-cell cooperative communications, instabilities/fault/attack detection, and behaviour patterns classification of users.

Reinforcement learning is based on a complex iterative process of learning and decision-making. The state of channel availability has been unidentified in spectrum access for distributed allocation of resources quality in cell networks and association of base stations in energy harvesting channels[4]. Table 1, illustrates the detailed survey of ML techniques in 5G[5].

The various performance improvement schemes for MIMO have been useful to achieve efficient energy management during wireless power transfer and information transfer in cognitive wireless sensor networks[19]. Network anomaly detection within consumer networks using hybrid technology has been

*Corresponding author (E-mail: bhuvaneswarim@skcet.ac.in)

Table 1 — Machine Learning techniques in 5G[5]

Type	Techniques	Features	Application	Technologies used
Supervised machine learning algorithms.	Regression models	• Evaluate the parameters and • the relationship • Linear and logistic regression	Energy training[6]	• MU- MIMO channel estimation & detection • user location behaviour learning classification • spectrum sensing and detection • learning in CR
	KNN	• Maximum vote of neighbours	Energy training[7]	
	Support vector machines (SVM)	• Non-linear mapping of a high dimension • Designation of the independent hyperplane	MIMO channel learning[8]	
	Bayesian learning	• A posteriori distribution estimate • Gaussians combination Model (GM) • Expectation maximization (EM), and hidden Markov models (HMM)	• Massive MIMO / Cognitive spectrum[9-11]	
Unsupervised machine learning algorithms	K-means clustering	• Partition clustering • Iterative • Algorithm	Heterogeneous networks[12]	• Cell cluster • User of Wi-Fi • D2D network clustering
	Principal component analysis (PCA)	• Orthogonal transformation	Smart grid[13]	• Het-Net clustering • Spectrum sensing • Intrusion detection • Signals reduction factor
	Independent component analysis (ICA)	• Reveal hidden independent factors	Spectrum learning in Cognitive Radio (CR)[14]	• Classification of the • Smart grid operator
Reinforcement machine learning algorithms	Markov decision Method processes (MDP)/ Partially observable Markov decision process (POMDP)	• Bellman equation maximization	• Iteration algorithm • Energy harvesting[15]	• Strategic thinking on an undefined network • Resource competition in selection of channels. • spectrum sharing for IoT network • Energy management during energy harvesting in CR • Het-Net organization
	Q-learning	• Unknown Model of device transformation • Maximization of the function	Small low power access point cells [16,17]	
	Multi-armed bandit	• Exploration vs.Service • Multi-armed bandit play	Device-to- Device(D2D) Communication [18]	

surveyed for various attacks using a ML approach, and Deep Cooperative Sensing (DCS) have been described[20].

Instead of the explicit mathematical modelling of Channel State Sensing (CSS), it is not easy to compute the model in Distributed Channel State. This strategy has been learned with a Convolution Neural Network (CNN) to incorporate the individual sensing results of the Secondary Users (SU) using training samples[21]. An environment-specific CSS, which the considers spectral and spatial correlation of individual sensing outcomes, is found in an adaptive, regardless of whether the individual sensing results have been quantified or not. The aim is to maximize the secondary user performance, providing sufficient protection to the primary user under the co-operative sensing scenario[22]. An iterative learning algorithm has been proposed for getting the optimum values for their parameters. Simulation results show that a wireless information transfer process, thus reducing the incidence of interference.

The method that deals with deep neural networks in data-driven sampling distribution have been intelligently proposed and analyze[23]. A DNN-based detection mechanism based on probability ratio test and extracted data ensure optimum performance. The proposed design of the primary receiver has fitted with a time-splitting energy harvesting system. The primary system will share its spectrum with the secondary system and receive the radiation for charging from the secondary base station in return. The primary information rate of the device and the energy harvested are guaranteed in the proposed fuzzy cluster based greedy algorithm in CPWRN.

2 Materials and Methods

The system model was developed for the primary user (PU) and secondary users (SUs) with the parameters such as frequency, sampling, channel number, channel status data, etc. In the wireless power transfer and wireless information phases, a model was proposed for secondary user energy recovery. Simultaneous transmission was achieved during the Wireless Power and Information Transfer (WPIT) process, thus reducing interference occurrences. The energy consumed was minimized by ML mechanism, proposed to detect various attacks. This essentially achieved the network's energy status by having an objective role in the different membership functions. The attack was then detected with a flippant, fuzzy cluster based greedy algorithm based on a cluster. Detected attacks were referred to as doctrine attacks, middle-class attacks or phishing.

Primary User would transmit information within a licensed channel to some intended recipient. Following the cease transmission of the data by the PU, the SU would initiate the energy processing of the ambient signal and use energy storage to save energy for the corresponding time frame on behalf of the data transmitted by the PU. Earlier on the primary timeline, the PU energy storage unit should be charged. In addition, the PU uses the energy collected during the final timeframe for subsequent timeframes. The SU cannot use an approved spectrum to transmit its own data to avoid a crash between the PU and SU, when the licensed channel was used as a matter of priority by the PU. Furthermore, until the licensed band was used, SU initially absorbed energy from the ambient radio signal. This saved the SU transmitters and then conveys an energy restriction process of half duplex. After the SU used the licensed inactive channel, and when the PU ended its contact at the PU time slot, the SU transmitted its own data via idle licensed SU time slot.

The SU would continue to use the energy from environmental sources and then use the energy collected from PU. The initial limitation showed that the energy used for relay transmission must be below the energy harvested from SU. SU must take the energy extracted in the current time slot, on behalf of PU. PU is greedy and requires cooperative SUs to lower the likelihood of PU secrecy outage with perfect channel state information available at the SUs. The next limitation refers to the length of a supportive broadcast which should be less than the duration of a non-cooperative broadcast.

An ML technique is a type of data analytics in which computers are trained to perform specific tasks. It is used to calculate the impact of computational learning techniques. As a result, ML models are used during the classification process. Convolution neural networks are used to investigate the CWPSN. In this case, it was critical to sensitize the network. The classifier effectively classifies the types of attacks by reaching the CWPSN's energy state and evaluating the objective function of the membership function. Finally, the attacks would be classified as Dos, man-in-the-middle, or phishing attacks. Figure 1 shows the proposed system architecture model.

Fuzzy cluster based greedy algorithm would reduce PU probability of security interruption which was the main purposes. The secondary user harvested energy from the hybrid access point during power transfer among nodes. Secondary user gained transmitter opportunity and interface with attack at the same time. The proposed algorithm was used to improve primary user security performance and also gained secondary user unlicensed band transmission opportunity during spectrum allocation. Resource allocation for secure communication could be done in different ways. In cooperative wireless network which provide more accurate information about the primary user but it lagged in identifying location of the primary user receiver.

In a centralized wireless network, the base station gathered information from other cognitive radio network to detect primary user information. While in distributive wireless network, cognitive radio network exchanged message among each other to get the desired objective.

In the CWPSN model, the fuzzy clusters based greedy algorithm was used to analyse effective resource allocation with the machine learning based membership function. The following is the proposed model algorithm:

Step 1: Assume system parameters for energy harvesting such as PU, SU, clustering, and so on.

Step 2: Determine the total number of sensing attempts per time frame, the total number of duplicate sensed spectrum holes, and the ratio of spectrum opportunity discovery.

Step 3: Divide the base station into clusters for secondary uses and proceed with the power adjustment algorithm.

Step 4: To determine the attack, set the total PU and SU condition for a normal attack and assign conditions if anyone has chosen DoS/ MIM/ Phishing.

Step 5: Examine the network's secrecy performance with the randomly assigned PUs and SUs.

Step 6: Consider user data features and the attack label when predicting labels in DNN Classification.

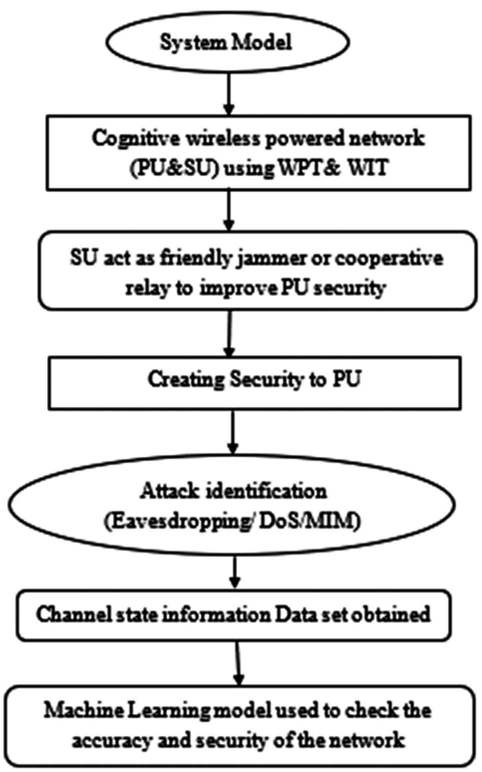

Fig. 1 — Proposed system architecture.

3 Results and Discussion

For simulation, the number of samples per symbol period were 100, the number of subchannels Np=20, PU=20, and SU=15 were distributed at random in a region. At this point, the Rayleigh channel scenario for all PUs, and the received signal power was influenced by path loss. In the proposed method, SUs were having high degree of certainty in detecting each PU's transmission at a random distance. The proposed model was compared to three different policies say cluster-CMSS, genie-aided location-aware and greedy non-cooperative spectrum sensing. The base station was known to its previous channel state information's in SUs similar to the genic aided sensing method. In a geographically dispersed and mobile network it is not practical to implement the genie assisted policy. When PU channels are underused, due to the abundance of spectrum holes, all policies have a high chance of being discovered. When it is close to one (high PU utilization), however, our proposed policy outperforms the greedy non-cooperative policy.

The review of the success of the proposed regime is available at this session. Table 2 shows average opportunity discovery versus PU channel utilization results and Table 3 shows average opportunity discovery ratio for PU. Table 2 illustrates the detailed results of proposed model with Primary user channel utilization in the scale of 0 to 1 it shows fine solution.

Table 2 — Average[3] opportunity discovery vs PU channel utilization

	Techniques	PU channel utilization										
		0	.1	.2	.3	.4	.5	.6	.7	.8	.9	1
Average opportunity discovery	Cluster CMSS policy	0.97	0.96	0.95	0.93	0.90	0.85	0.77	0.72	0.65	0.6	0.57
	Greedy Non-cooperative policy	0.87	0.86	0.86	0.86	0.85	0.83	0.77	0.73	0.65	0.58	0.51
	Genie aided location aware policy	1	1	1	0.97	0.96	0.94	0.90	0.84	0.79	0.70	0.70
	Proposed system	1	1	1	1	1	1	1	1	1	1	.08

Table 3 — Average opportunity discovery ratio for PU

Techniques	0	5	10	15	20	25
Cluster CMSS policy	0.8700	0.8650	0.8600	0.8550	0.8400	0.8350
Greedy Non-cooperative policy	0.8100	0.7800	0.7800	0.7780	0.7750	0.7700
Genie aided location aware policy	0.9600	0.9400	0.9350	0.9350	09340	0.9300
Proposed system	1	1	1	0.912	0.897	0.8824

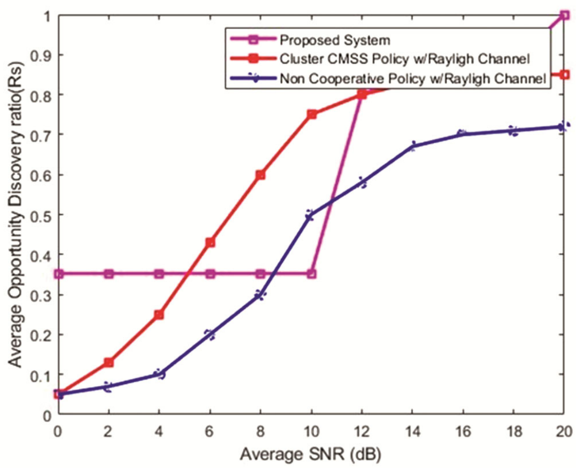

Fig. 2 — Average opportunity discovery ratio Vs average SNR (dB)

Figure 2 shows average opportunity discovery ratio Vs Average SNR (dB). The study showed that the suggested fuzzy cluster based greedy algorithm technique showed more average discovery of opportunities for the random selected nodes. The proposed technique, according to the study's findings, provides better average opportunity discovery.

The PU and SU used parameters like sampling frequency, packet data, error rate etc., were randomly declared and simulated using MATLAB inbuilt tool functions. Power adjustment functions and network-based algorithms which was fuzzy cluster based greedy algorithm, used to provide channel state information collected at the hybrid access point and wireless power transfer phase details were evaluated using deep neural network which is effective for network classification. Thus, the proposed scheme provides secure data transfer using optimum power consumption among cognitive wireless power sensor network.

4 Conclusion

A new protocol for wirelessly powered SU with PU collaboration has been proposed. During the wireless power transfer stage, the hybrid access point carried and broadcasted the SU's first energy harvest. A Fuzzy-based cluster greedy algorithm has been used to reduce PU secrecy prospect outage and provide the best optimal values. The proposed fuzzy cluster based greedy algorithm method results effective solutions as compared to other methods with accuracy, power optimization during resource distribution, security enhancement of the cognitive wireless sensor network and machine-based learning model.

In addition, this work is proposed to expand in IoT application. IoT provides direct connection and control to sensor nodes when using as MIMO IoT framework. In order to ensure the next generation of IoT products, the combination of other models and various trades-offs provides a possible path for future study.

References

1 Alnwaimi G, Vahid S, & Moessner K, *IEEE Trans Wireless Commun*, 14 (2015) 2294.
2 Aprem A, Murthy CR, & Mehta NB, *IEEE J Sel Topics Signal Process*, 7 (2013) 895.
3 Assra A, Yang J, & Champagne B, *IEEE Trans Veh Technol, 65* (2015) 1229.
4 Bhuvaneswari M, & Sasipriya S, *ICICT*, (2020) 283.
5 Choi K W, & Hossain E, *IEEE Trans Signal Process*, 61 (2013) 782.
6 Chunxiao J, Haijun Z, Yong R, Zhu H, Kwang-Cheng C, & Lajos H, *IEEE Wireless Communications*, 98 (2016).
7 Darsh P, Kathiravan S, Chuan-Yu C, Takshi G, & Aman K, *Electronics*, 9 (2020) 923.
8 Donohoo B H, *IEEE Trans Mobile Comput*, 13 (2014) 1720.
9 Hsieh K, Tseng F, & Ku M, *IEEE Wirel Commun Lett*, 5 (2016) 252.
10 Liu C, Wang J, Liu X, & Ying-Chang L, *IEEE J Sel Areas Commun*, 37 (2019) 2306.
11 Maghsudi S, & Stanczak S, *IEEE Trans Wireless Commun*, 14 (2015) 1309.
12 Nguyen H, *IEEE Trans Wireless Commun*, 12 (2013) 1532.
13 Onireti O, *IEEE Trans Veh Technol*, 65 (2016) 2097.
14 Peh EC, Liang YC, Guan YL, & Zeng Y, *IEEE Trans Veh Technol*, 58 (2009) 5294.
15 Qiu RC, *IEEE Trans Smart Grid*, 2 (2011) 724.
16 Shresthaand A P, & Yoo S J, *IEEE Trans Veh Technol*, 67(2018) 8525.
17 Wen CK, *IEEE Trans Wireless Commun,* 14 (2015) 1356.
18 Woongsup L, Minhoe K, & Dong-Ho C, *arXiv*, (2017) 1.
19 Xia M, *OSA/IEEE J Opt Commun Netw*, 4 (2012) 749.
20 Youness A, & Naima K, *Sensors*, 19 (2019) 1.
21 Yu K, Chen C, & Cheng SM, *IEEE Trans Veh Technol*, 59 (2010) 1980.
22 Zeng Y, Ying C L, Anh TH, & Zhang R, *Eurasip J Adv Signal Process*, 1 (2010)
23 Zhou P, Chang Y, & Copeland J A, *IEEE Trans Parallel Distrib Syst*, 23 (2012) 505.