International Journal of Future Generation Communication and Networking
Vol. 11, No. 1 (2018), pp.1-12

Self B - Adaptive Key Generation for Primary Users in Cognitive Radio Networks for Less Prone Primary User Emulation Attacks

T. Lakshmibai[1]* and C. Parthasarathy[2]

[1]*Research Scholar, Department of Electronics and Communication Engineering, Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya University, Enathur, Kanchipuram, Tamilnadu, India*
[2]*Assistant Professor, Department of Information Technology, Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya University, Enathur, Kanchipuram, Tamilnadu, India*
**lakshmibai1967@gmail.com*

Abstract

Primary user attack is the major problem in the Cognitive Radio networks. Dynamic Spectrum sharing is the major advantage of Cognitive radio networks in which primary users (PU) are prioritize and authorized for using the spectrum than the Secondary users (SU). The problem arises when the Secondary users mimic the characteristics of the Primary users and use the spectrum without any deadline and make the primary users to queue for spectrum sharing. Hence the centralized system for the detection of primary attacks has been proposed. The algorithm follows the principle of Self B-Adaptive Keys for the Primary Users and keys are forwarded to the Intelligent Learning Center which can detect the different parameters ofthe primary users such as the RSSI, Power, Distance and Channel ID optimizes and compares with the thresholds which are already in the Intelligent learning centers. Hybrid PSO is used for the optimization of characterization of the primary users and Cognitive Rule Sets has been designed for the determination of the presence of the primary users among the different users in the network. The proposed scenario has been implemented in the ARM CPU as main test bench and MATLAB for the optimization and classification.

Keywords*: Self Adaptive keys, Cognitive Rule Sets, Hybrid PSO, Power, Distance, RSSI*

1. Introduction

Primary User Emulation Attack is one of the serious threatsin Cognitive radio network. With this kind of attacks, the Secondary users follow the primary user characteristics and make uses of the spectrum completely. This leads to the authorized primaryusers may use the spectrum in an inefficient manner. Several algorithms were proposed for this prevention of the attacks but every algorithm has its own advantage and disadvantages but the major problem is the lack of intelligence in the classification of the primary users among the user.

Hence the intelligent algorithm should be imparted in the classification of the user. The proposed algorithm so called Self B-Adaptive key generation for the Primary user at the Transmitter and the Intelligent Learning Center at the receiver side for the classification of the primary users. The proposed algorithm works on the generation of the key depends on the Energy, RSSI, distance and optimized by the Hybrid PSO Methods.

Received (August 26, 2017), Review Result (November 29, 2017), Accepted (December 10, 2017)

ISSN: 2233-7857 IJFGCN

At the receiver side, intelligent learning center works on the Ontology based Rule System which is used for the identification of the primary users. The optimized keys are generated randomly for each and every iteration, whichare very difficult to mimic the characteristics of the primary users. The probability of detection, false alarm ratesare evaluated which provides the satisfactory results.

2. Related Works

XiongweiXiea proposes another system in method of coding for physical layer to identify the emulators. At the point when two sequence of signal in the receiver end, the beginning stage of crash is dictated by the separations among the transmitter and the receiver. By Utilizing the interference of the signal comes about at different receivers and the places of reference senders, can decide the position of the 'claimed' primary user. After that authors able to contrast this localization result and the known position of the primary user to identify the PUE attack. They outline a PUE recognition component for remote systems with dependable reference senders. They break down the overhead of the proposed approach and concentrate its location precision through simulation.

Ruiliang Chen and Jeffrey H. Reed distinguished the PUE attack in cognitive radio networks and illustrated its problematic impact on range detecting. To counter the attack, authors proposed a new LocDef as a scheme for transmitter verification, which can be coordinated into the range detecting process. LocDef utilizes a non-interactive localization methodto recognize and pinpoint PUE attacks. Analysis for security and simulation results shows that the proposed localization method is compelling and can be utilized in threatening situations. A localization based approach isn't the best way to guard against PUE attacks. Authors are exploring an option approach that uses the inherent qualities of RF signals to recognize and distinguish producers—i.e., RF fingerprinting. In Network environments where the essential transmitters are versatile and have low power, localization based methodologies for obstructing PUE attacks don't work. For example, a proposed approach does not work when the system condition incorporates Part 74 gadgets (e.g., remote amplifiers) as primary transmitters. These Part 74 gadgets are too authorized to work in the TV groups. In such a situation, RF fingerprinting may give an option countermeasure against PUE attacks.

Di Pu, Yuan Shi and Alexander M. Wyglinski proposed an approach for identifying primary user emulation in psychological radio systems; proposed approach is started by energy recognition to find the current clients on the frequency band. The approach utilizes a cyclostationary estimation to speak to the highlights of the client signals, which are then encouraged into a simulated neural system for arrangement. Rather than current systems for identifying primary users emulation attacks in cognitive radio environments, and the proposed approach does not require any special equipment or time synchronization calculations in the remote system. Therefore, existing frameworks can promptly utilize the proposed approach without critical basic and functional changes. The proposed approach is approved by means of PC simulations and additionally by test equipment usage utilizing USRP2 stage. The equipment analyze demonstrates that our approach can accomplish a level of accurate detection around 98% in real remote situations.

Deepa Das, Susmita Das examines the PUEA with its mitigation systems. Although, a portion of the defense mechanisms have been proposed, particularly in security in view of the nearness of malicious hubs, which need to vandalize the whole communication systems. They can't totally satisfy the need of CR systems operation on the grounds that for their future work. Main objective of the system is to give issues under security and after that it need to be examine for the PUEA combined with the current methods for the solution.

Himanshu Sharma and Kuldip Kumar discussed the utilization of the cognitive radio for the dynamic spectrum issues in the communication within short range.This paper

completely give the investigation on PUEA. This paper presents reproduction structure to assess the effect of PUEA on the system of Cognitive radio. Under PUEA, a theory test at optional client in view of measured Probability thickness capacity of energy got has been directed. For Primary User Emulation Attack examination on Cognitive radio, the reproduction shows that the probabilities of miss recognition and false caution have been appeared. Finally they conclude with the number of malicious clients inside the framework, false caution probability is increased in the system.

Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and TongtongLi considers primary user emulation attacks in cognitive radio systems working in the void areas of the digital TV (DTV) band. We propose a dependable AES-helped DTV plot, in which an AES-encoded reference signal is created at the TV transmitter and utilized as the match up bits of the DTV information outlines. By permitting a mutual secret between the transmitter and the receiver, the reference signal can be recovered at the beneficiary and used to accomplish exact recognizable proof of the approved primary clients. Also, when joined with the examination on the autocorrelation of the got flag, the nearness of the noxious client can be distinguished precisely regardless of whether the essential client is available. It is demonstrated that with the AES-helped DTV plot, the essential client, and in addition vindictive client, can be recognized with high exactness under primary user emulation attacks. It ought to be stressed that the proposed plot requires no adjustments in equipment or framework structure aside from a module AES chip. Possibly, it can be connected specifically to the present DTV framework under primary user emulation attacks for more proficient spectrum sharing.

MonirehDabaghchian, Amir Alipour-Fanid and Kai Zeng, Qingsi Wang considered the ideal PUE attacking systems with no earlier information of the primary user action attributes and auxiliary client channel access arrangements. We defined the PUE attack as a non-stochastic web based learning issue. We distinguished the uniqueness of PUE attack that a PUE attack can't watch the reward on the attacking channel, however can see no less than one other channel.

To comprehend this test, we propose an attack but observe another (ABOA) plot, in which the attacks of the attacker’s one channel in the range detecting stage, yet observes no less than one other divert in the information transmission stage. We propose two non-stochastic internet learning-based attacking algorithms, EXP3-DO and OPT-RO, which select the watching channel deterministically in view of the attacking channel and uniform arbitrarily, individually. We additionally sum up OPT-RO to multi-channel perception cases. We demonstrate consistency between reproduction and diagnostic outcomes under different framework parameters.

Yi Tan, ShamikSengupta and K.P. Subbalakshmi proposed a diversion theoretic structure to study the primary user emulation attack (PUEA) on CR radio hubs. A non-cooperative dynamic multistage diversion between the auxiliary hubs and the foes creating the PUEA is figured. The pure procedure and mixed methodology Nash equilibria for the secondary client and malicious attacker are explored. In addition, we propose a novel updating framework for the auxiliary client to take in the condition of the primary client as the game advances. results comes about exhibit that our proposed system framework accomplishes preferable execution over different models for the secondary client as far as more prominent result, lower probability of missing essential client and better power to the error estimation of the primary client's state.

Rong Yu and Mohsen Guizanishows a complete presentation for PUE attacks, using the attack on the CR systems, to defense and location services. Two level detection methodis proposed for the security goal applications opposite to the PUEA in the CR communication. Energy identification and area check are consolidated for quick and reliable recognition. An admission control-based guard approach is degradation of a Cognitive network under a PUE attacks. Their final outcomes are exhibited to show the adequacy of the proposed identification and methods of defense.

EfeOrumwense, OlutayoOyerinde, Stanley Mneneystudied the impacts of Primary emulation attacks (PUEA) in a CR system comprising solitary primary transmitter and a number of co-working optional or CR clients. The primary transmitter speaks with essential receivers inside a zone called the primary exclusive region (PER). Inside the PER, no CR clients may transmit in order to ensure a specific execution for the primary receivers in the district. Outside the PER, CR clients are consistently appropriated and permitted to transmit gave they are at a remove from the essential receiver. Authors display an investigation to compute the forces and probability density function (PDF) of both malicious clients and great auxiliary clients and contrast it and the simulated results.

3. Proposed Algorithms

The proposed algorithm consist of two important phases which are given as follows

1. Generation of Self Adaptive keys at the Transmitter Side
2. Identification and Allocation of Spectrum to the PU

I Phase

3.1. Generation of Self Adaptive Keys

The Algorithm focused on the generation of the Keys adaptive to the internal parameters of the Primary User. The primary user has been characterized by the unique identifier key which normally formed by the RSSI(Received Signal Strength).Distance, Energy and ID in which the distance, RSSI, Energy are adaptive whereas the ID remains to be the Constant depends on the users.

The formation of the unique identifier as proposed in [1] is given as follows

START	ID	RSSI	ENERGY	DISTANCE	STOP

3.1.1. RSSI and Distance Calculation

The RSSI is the received signal strength indicator which is used to find the Primary user distance and localization. The primary users are identified by measuring its distance in which is used to measure the distance. RSSI of every user is calculated by the expression which is stated in [1] isgiven below

$$RSSI(dbm) = -[10 \times n \times \log(d) + \mathrm{A}]$$

RSSI is the RSSI value received (dBm)

n is the path-loss exponent

d is the distance

A is the RSSI value at a reference distance (1m)

From the above expression, the distance can be measured by the below expression:

$$\text{Distance} = 10^{\left[(A + rssi)/(10 \times n)\right]}$$

3.1.2. Energy Calculation

To deal with PUEA, indication energy level discovery is used in adding to localization of transmitters. This move is based on the next assumption: primary transmitters are users with a known place and power. SUs are having limited broadcast power. As a result, energy level finding can positively be a robust measure to validate the genuineness of primary transmission.

Overall Energy of the Primary User is calculated by the expression given below

$E_{pu} = E_t + E_p$

Where E_{pu} is the Energy of the Primary User

E_t is the Transmitting Energy (which includes transceivers interfaced)
$E_p$is the peripheral Energy of the Users (Which includes the Sensors, Main CPU etc)

3.1.3. Self –Adaptive Algorithm

In above cases, energy,distance, RSSI are calculated by the above expressions. In this case, PU .key is generated in which depends on the principle of adaptive energy in accordance with the distance and RSSI. Moreover the Energy of the primary user randomly changes in a pre-defined manner in accordance with the distance and RSSI. The energy ,distance , RSSI along with the ID of the user are considered to be the variables from which the key is formed based on the optimized variables obtained after the Hybrid PSO methods.

3.1.4. Self BestAdaptive Algorithms

After forming the relationship between the Energy and Distance with RSSI, optimized key is produced by the usage of Hybrid PSO principle. The Hybrid PSO works on the principle of the combination of genetic algorithm along with the PSO to produce the best adaptive energy in accordance with the distance and RSSI.

3.1.5. Genetic Algorithm based Estimation

The first generation populations of the chromosomes have been generated. Now next step is to obtain the fitness evaluation of each chromosome in the population. In this paper assumptions have been made that fitness functions are equally dependent on two parameters which are defined above.

In the above equation, the results have been taken as the major role which has been calculated on the basis of cumulative sum of individual fitness of all genes.

$$f_i = \begin{cases} \dfrac{w_j . | x_j - x_j^d |}{x_i^d} & if \mid x_j - x_i^d \mid < x_j^d \\ w_j & otherwise \end{cases} \quad (1)$$

$$F = \sum_{j=1}^{4} f_i \quad (2)$$

Second step includes the decision making process and also selects the best among the population of chromosomes and transfers to the next generation.

As the next step selection of the best chromosomes and to perform the cross-over operation.

3.1.6. Particle Swarm Optimization

The motivation behind in developing the Hybrid PSO algorithm is to incorporate the Genetic algorithms over the PSO for the finding the p-best solutions. Both the algorithm has its own weakness and strength. In GA, absence of the memory may lead to the data to be lost, while PSO has the memory. The basic idea for incorporating the social thinking in PSO using the GA.

3.1.7. Hybrid Particle Swarm Optimization

The Hybrid PSO is incorporated in the proposed algorithm to produce the bestkey based on Energy over randomly spaced distances and RSSI values. This optimization produces the pbest keys for the random RSSI over the distance. Hybrid PSO methodology for the generation of keys are as follows as

II Phase

After transmitting keys to the Intelligent Learning Center, the center works on the two methodologies. One is Identification of the Keys using Ontology Intelligent rule sets and Allocation of spectrum to the primary user.

3.2. Identification Phase

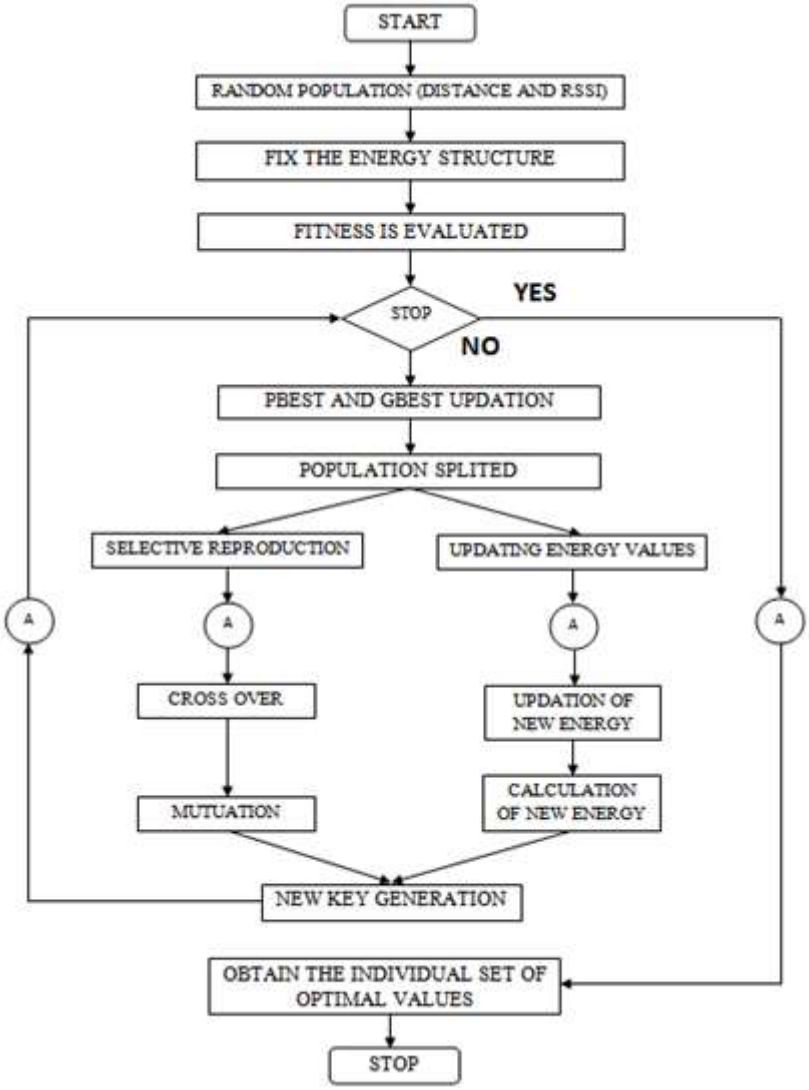

Figure 1. Overall Implementation of the Hybrid PSO Methodology for the Proposed Algorithm

The CH consists a Learned databases of the primary users s with their unique IDs, energy level and RSSI valuesThe users transmits their Self adaptive keys, which is recognised after decryption by the CH Based on the learned techniques, the keys are decrypted in which the energy and distance are extracted.

The learned databases are formed by training the best Energy with the Best distance and rule sets are formed based on the parameters. These rule sets are used for the further classification of the Primary User and Secondary users. The overall algorithm and rule sets for ILC is given below

Start:

Extract the Step by Step Process for Energy, Distance RSSI and ID

If (IDobtained $_{=}$= ID $_{\text{data base list}}$)

Then if($E_{obtained}$== $Energy_{database\_lsit}$&&$Distance_{obtained}$==$Distance_{database\_list}$)

Then

User == Primary User

/* allocation of the Spectrum to the User*/

Else

User == Secondary User

End

SL.NO	Test bench/Software Details	Specifications
01	Main CPU	ARM-7
02	Transceivers Used	Zigbee
03	Range of Distance(Minimum)	5m
04	Range of Distance(Maximum)	20m
05	API Development	Embedded C Programming
06	Software for Simulating and Hardware Interfacing	MATLAB R2012
07	No of Users tested	05/10
08	Total Range of Distance	40 m(LOS)
09	Maximum Energy Used	1mW
10	Minimum Energy Used	0.25mW
11	Data rate used	1 Mbps

3.3. Performance Evaluation

3.3.1. False Alarm Rate Detection

The false alarm rate is detected for the overall systems and it is used to evaluate the probability of the primary users for the different iterations/Users which is given by exp

False alarm Rate (FAR) = Probability of the Primary User detection/No of users

Again the False Alarm rate is evaluated for the below mentioned algorithms in the test bench and compared with the proposed algorithm .the algorithms used are as follows

Conventional Detection (Energy Detection)

Double Tier detection as proposed by [2]

Self Adaptive Keys without Intelligence

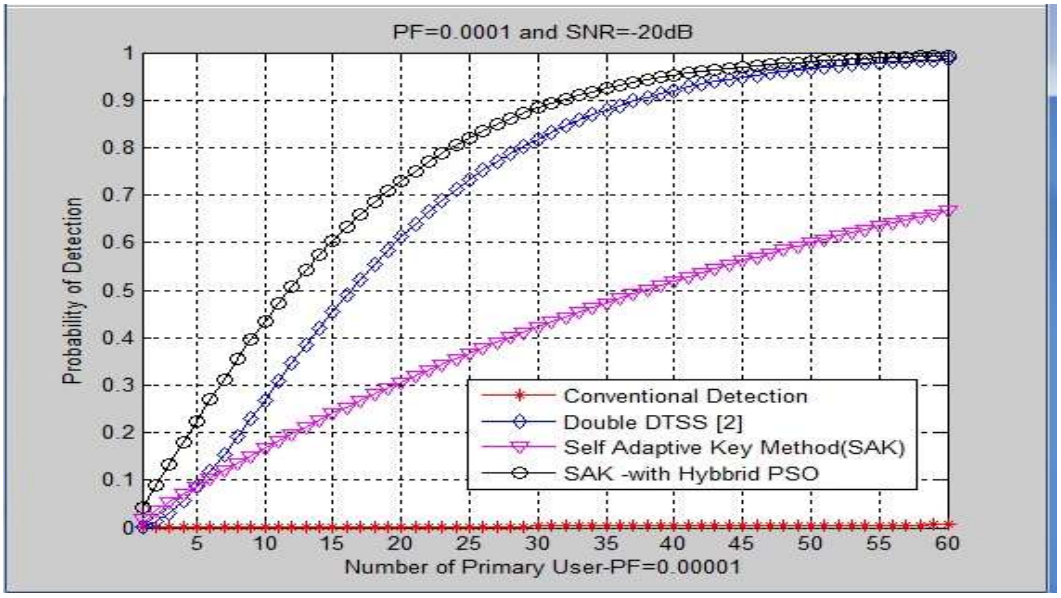

Figure 2. Comparative Analysis of the Different Algorithms Evaluated in the Test Bench

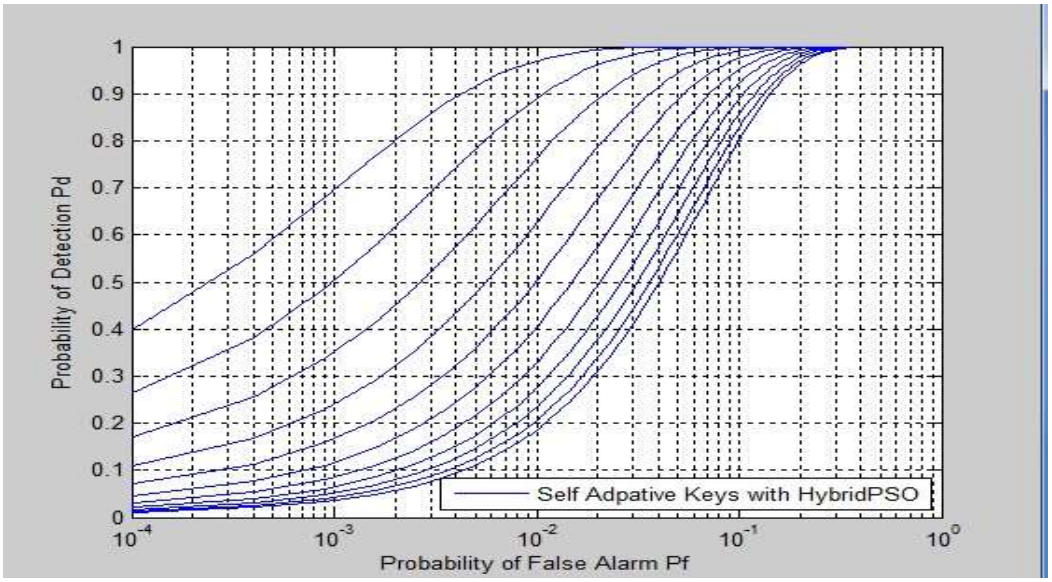

Figure 3. Analysis of the Proposed Algorithms in the Testbench at the Different Probability Rate of Detection

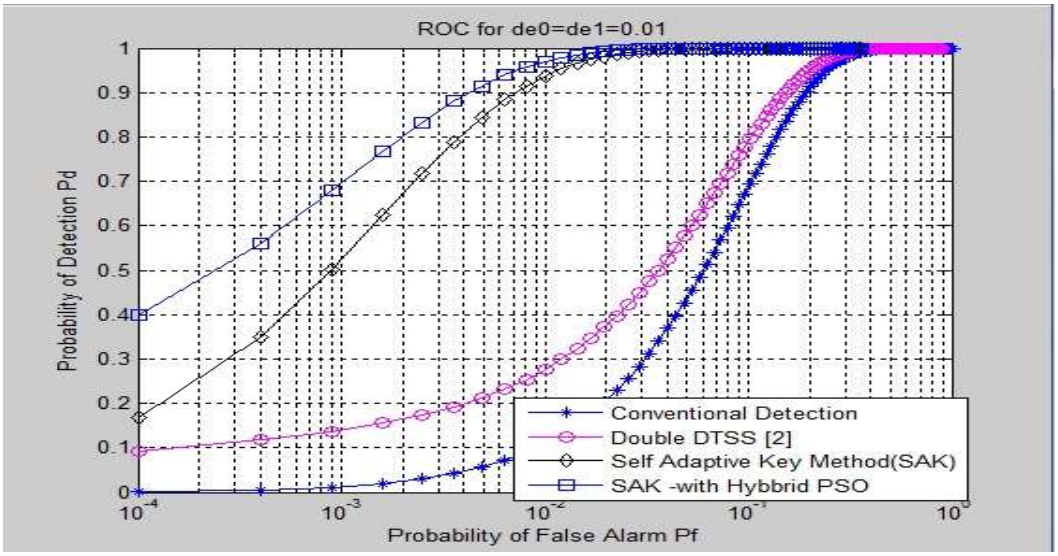

Figure 4. Analysis of the Proposed Algorithms in the Testbench at the Different Probability Rate of Detection

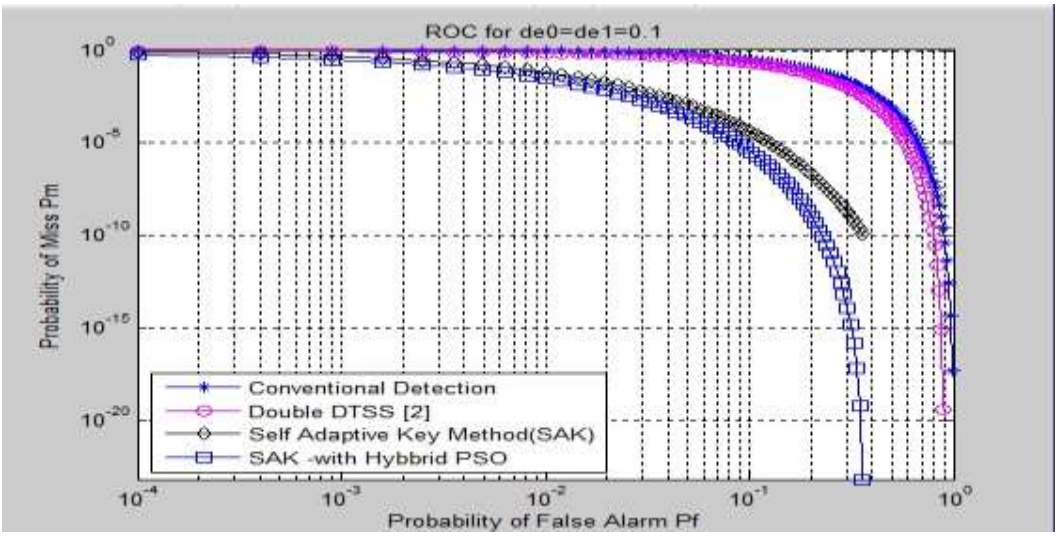

Figure 5. Analysis of the Proposed Algorithms in the Testbench at the Different Probability Rate of Detection

In the above Fig, performance of the proposed algorithm is evaluated based on the constant region of convergence in which the probability of false alarm ratio and probability of the Miss ratio is evaluated. At the different region, Proposed Algorithm has very less Miss ratio in detection of the Primary users.

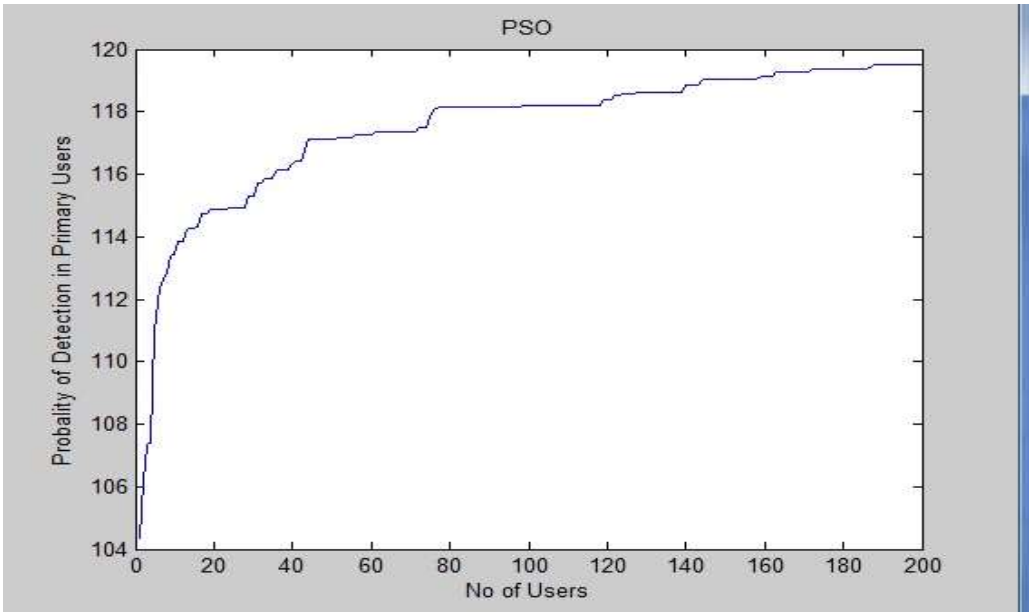

Figure 6. Analysis of the Proposed Algorithms in the Testbench at the Different Probability Rate of Detection

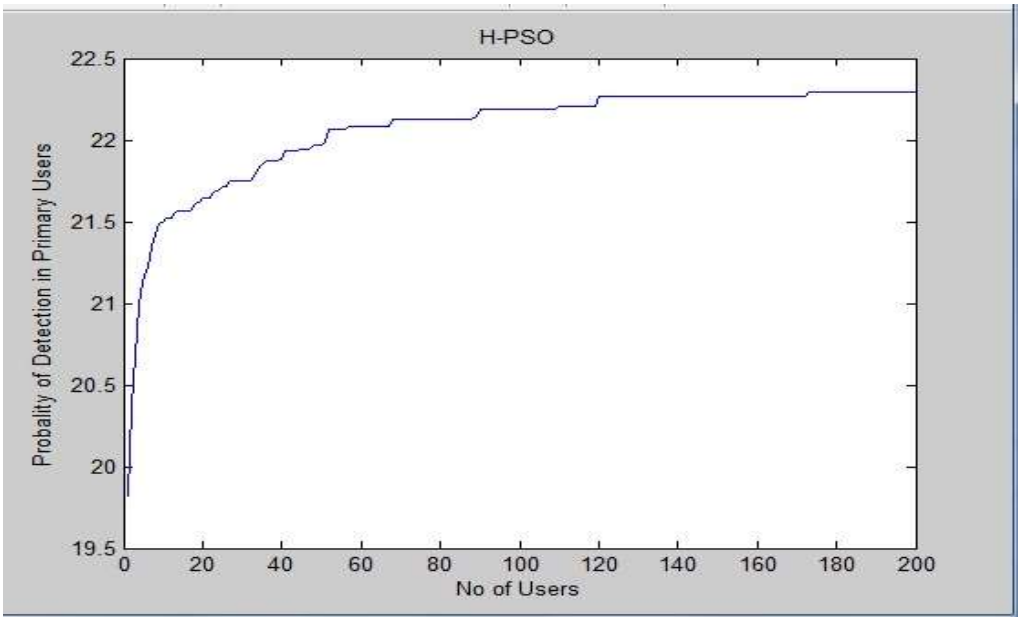

Figure 7. Analysis of the Proposed Algorithms in the Testbench at the Different Probability Rate of Detection

3.3.2. Accuracy Measurement

The accuracy has been evaluated based on the ratio of number of the primary users detected to the number of iterations. The test is conducted for the performance analysis of the overall proposed system for the classification of primary users and secondary users.

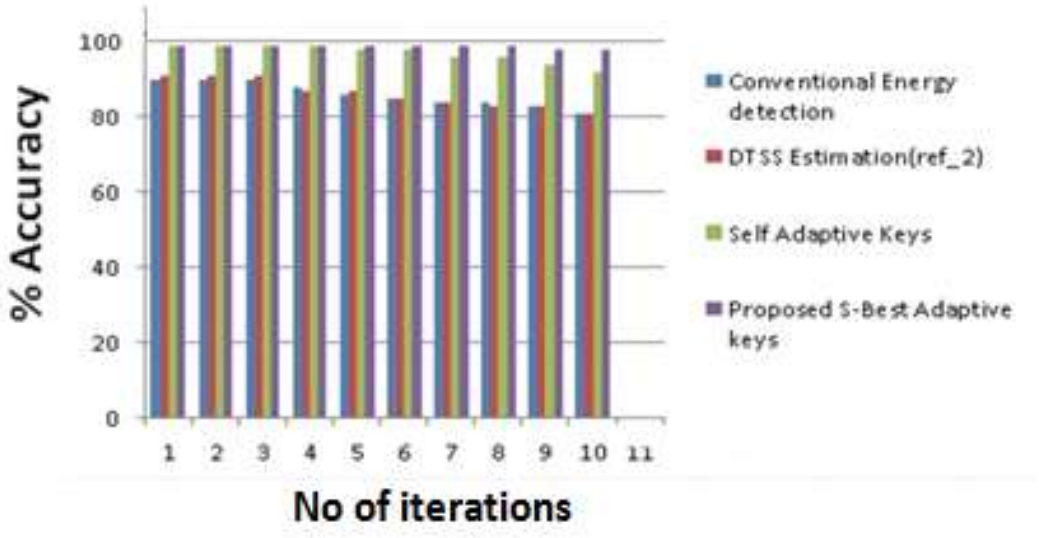

Figure 8. Accuracy Measurement for the Different Detectors used for the Classification of Primary Users

From the above fig, it clearly shows that the accuracy of the Proposed Algorithm outperforms the other algorithms as the number of iterations increases. The accuracy is maintained from 99% to 98% for every iteration whereas the other decreases gradually as the number of iteration increases.

4. Conclusion

The proposed algorithm of Self Adaptive Keys based on the Higher Security and less prone to the Primary User Emulation Attacks. The Intelligent Learning Rule Sets are integrated for the detection of the primary users among the other users. The false alarm rate and probability of detection has been taken as the two important parameters in which the adoption of Hybrid Optimizers out performs other existing algorithms. Also Even inclusion of most advanced machine learning algorithm evenimparts more accurate classification and more accuracy in the detection of the attacks.

In future we consider the intelligent attacks on the realistic channelin the network models and also convergence of the proposed work will be studied.

References

[1] T. Lakshmibai and C. Parthasarathy, "Encryption Algorithm for defending PUE Attack in Cognitive Radios", International Journal of Applied Engineering Research ISSN 0973-4562, vol. 12, no. 19, **(2017)**, pp. 8278-8285.

[2] T. Lakshmibai and C. Parthasarathy, "DTSS-Double Tier Spectrum Sensing Techniques for Cognitive Radio Communications", International Journal of Control Theory and Applications, ISSN: 0974-5572, International Science Press, vol. 10, no. 32, **(2017)**.

[3] X. Xiea and W. Wang, "Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding", International Workshop on Communications and Sensor Networks, **(2013)**.

[4] J. H. Reed, R. Chen and J.-M. Park, "Defense against Primary User Emulation Attacks in CR Networks", IEEE, Journal on Selected Areas in Communications, vol. 26, iss. 1, **(2008)**.

[5] D. Pu, Y. Shi, A. V. Ilyashenko, A. M. Wyglinski, "Detecting Primary User Emulation Attack in Cognitive Radio Networks", IEEE,Global Telecommunications Conference, **(2011)**January.

[6] D. Das, S. Das, "Primary User Emulation Attack (PUEA) in Cognitive Radio Networks: A Survey", International Journal of Computer Networks and Wireless Communications, vol.3, no. 3, **(2013)**.

[7] K. Kumar and H. Sharma, "PUEA -Primary User Emulation Attack Analysis on Cognitive Radio", Indian Journal of Science and Technology, vol. 9, **(2016)**.
[8] T. Li, A. Alahmadi, M. Abdelhakim and J. Ren, "Defense Against Primary User Emulation Attacks (PUEA) in Cognitive Radio Networks Using Advanced Encryption Standard", IEEE Transactions On Information Forensics and Security, vol. 9, no. 5, **(2014)**.
[9] M. Dabaghchian, A. Alipour-Fanid, K. Zeng, Q. Wang, "Online Learning-Based Optimal Primary User Emulation Attacks in Cognitive Radio Networks", IEEE Conference on Communications and Network Security (CNS), **(2016)**.
[10] K.P. Subbalakshmi, Y. Tan and S. Sengupta, "The Primary User Emulation Attack in Dynamic Spectrum Access Networks: A Game Theoretic Approach", IEEE, Reciprocity and Fairness in Medium Access Control Games, **(2013)**.
[11] Y. Liu, R. Yu, Y. Zhang, S. Gjessing and M. Guizani, "Securing Cognitive Radio (CR) Networks against Primary User Emulation Attacks (PUEA)", IEEE Network, vol. 29, iss. 4, **(2015)**.
[12] E. Orumwense, O. Oyerinde and S. Mneney, "Impact of Primary User Emulation Attacks on Cognitive Radio Networks", International Journal on Communications Antenna and Propagation (IJCAP), vol. 4, **(2014)**.
[13] W. Saad, "Learning Of Transfer For Device Fingerprinting With Application In Cognitive Radio Networks", International Symposium on mobile radio communications, **(2015)**.
[14] Y. S. Dabbagh, "Cyber Physical Fingerprinting for Authentication of IOT", Proceedings of the Second International Conference on IOT Design and Implementation, **(2017)**.

