International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

A Proposed Algorithm to Enhance Security in CRN

Kriti, Dr. Ajay Kaul
Department of Computer Science and Engineering SMVD University, Jammu & Kashmir, India

ABSTRACT

With the growing demand of the wireless spectrum leading to its scarcity, motivated the use of Cognitive Radio as the successful way to deal with this problem. The efficient exploitation of the spectrum is done by the Cognitive Radio that allows the licensed spectrum to be utilized by the unlicensed users effectively. This paper illustrates an algorithm which enhances the security in CRN irrespective of the security threat or the attack done by the malicious users. It uses the concept of cluster head generated through random numbers and the formation of slots for the free spectrum based on the round robin algorithm. The efficient management of the spectrum is done so that each user utilizes the spectrum in an effective way without causing harm to the primary users.

Keywords : primary user (PU); secondary user (SU), cognitive radio network (CRN), primary user emulation (PUE)).

I. INTRODUCTION

With the passage of time, tremendous advances have been shown by the wireless communication that includes the network which is being complemented by the systems that are not only self- organizing but also heterogeneous with the infrastructure being hybrid adding the communication nodes of peer-to-peer. The researchers are attracted towards the cognitive radio in these days, where the frequency band, the sharing of frequency is realized for the assignment to the primary system [1]. The secondary cognitive terminal senses the frequency band being assigned to the primary systems, by transmitting the signals without causing any interference between the two. But the situation of interference is fluctuated, in the cognitive networks, in terms of time, frequency and location. Therefore for the ad-hoc cognitive network, the basic techniques for routing are not effective [2].

NEED FOR CRN- the motivation

To establish and manage, a wireless networks for cognitive radio, a new model is proposed using the trainable and the adaptive radio. A number of intelligent tasks are implied in cognitive radio in the motion of cognition and hence robust knowledge is required to represent the facility of sharing and knowledge reuse. The capability of reconfiguring the infrastructure defines the cognitive network, which adapts itself to the continuously changing environment in the network, for machine learning techniques. To support the decision making, the learning engines have been proposed for the services and applications which are context-aware. In turning these models of learning, are the challenges, into viable commercial products [8].

II. BACKGROUND AND HISTORY OF COGNITIVE RADIO

Spectrum is a very limited product and due to the spectrum insufficiency facing by the wireless based

service providers lead to high overcrowding stages. The main reason that leads to useless utilization of the radio spectrum is the licensing system itself. If the allocated radio spectrum is not used by primary users then it also cannot be utilized by SUs. As a result, wireless systems are intended to work only on a devoted band of spectrum for fixed and rigid allocations. It cannot change the band as changing the surroundings. As illustration if one channel of spectrum band is greatly used, the wireless system cannot alter to work on any other more lightly used band.

The authorized access of spectrum is usually defined by owner of spectrum; transmit power, frequency, space and the license duration. In general, a license is allocated to one licensee and the use of band by this owner must have the requirement e.g. highest power of transmit, base station location. In present spectrum licensing system, the license cannot vary the application or giving the access to another licensee. This restriction causes in low consumption of the frequency spectrum. Spectrum hole is defined as a group of frequencies given to a licensee, except that user is not using the band at exact time and exact geographic location [10].

The allocation of radio band is in power of the central government. Federal Communications Commission (FCC) printed a statement in beginning of 20th century which was ready by the spectrum plan mission force that was intended to improving this expensive source. The allotment of the unlicensed frequency bands leads to the congestion of these bands.

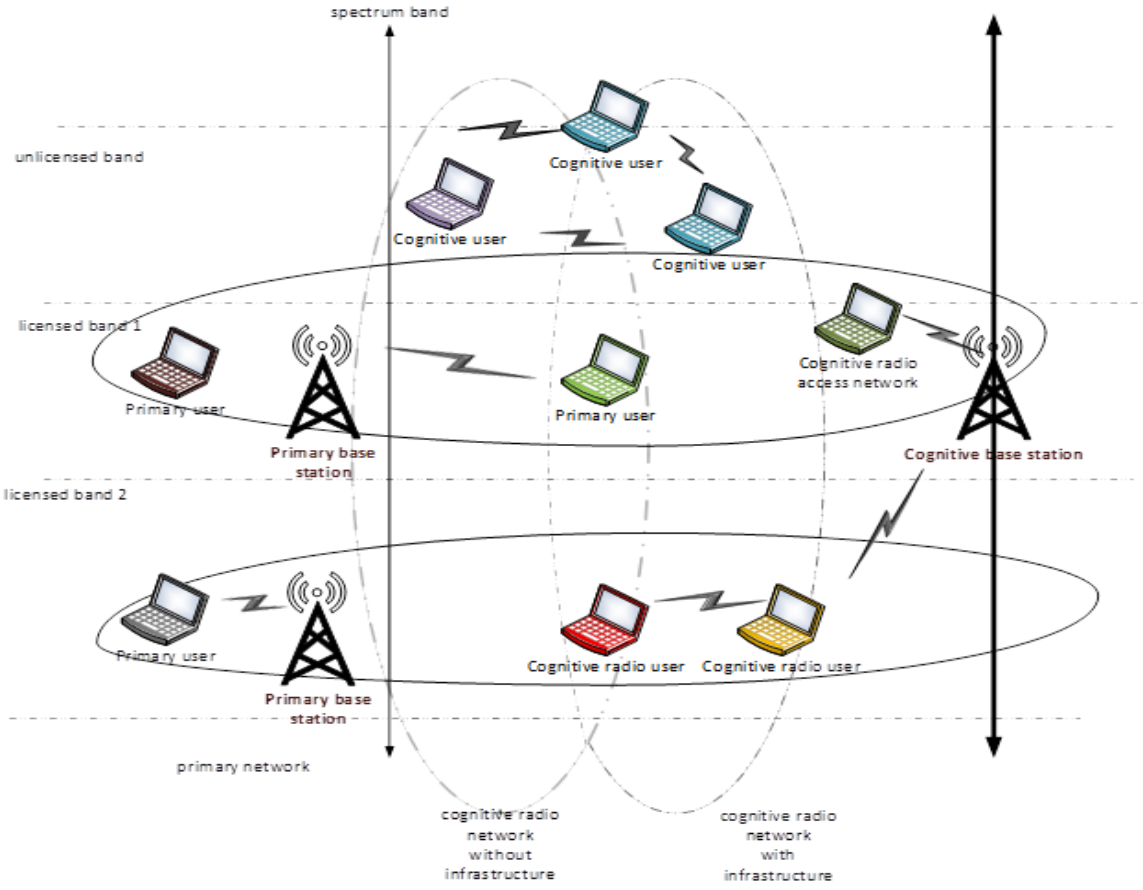

Figure 1. Cognitive Radio Network

A. Cognitive Radio Network: an introduction

The ability to sense the spectrum by software radio intellectuality and to seek the spectrum hole by automatic sensation of electromagnetic environment, cognitive radio is used which adjust the optimum condition by bi-lateral signal parameter of the communication protocol and the algorithms.

Cognitive Radio (CR) is the category of wireless system in which either an entire network or a single node varies its communication or response parameter to correspond effectively. It avoids obstruction with primary user (PU) and secondary user (SU). It is considered to be an intelligent communication system which is sensitive of surrounding atmosphere and uses the techniques to gain knowledge from the surroundings and adjust its internal conditions to arithmetic changes in the arriving RF by creating consequent variation in definite working factors.

A CR is intended to be alert and responsive to that alters in its neighboring that makes spectrum sensing an imperative necessity for the understanding of secondary networks. Spectrum sensing method allows SUs to use the vacant spectrum segment adaptively to the radio atmosphere [12].

B. Fundamentals of CRN

1. **CR characteristics:** The two fundamental resources for communication which are energy and bandwidth are scarce which in turn limits the service quality and channel capacity. The new communication and network paradigm fetched the attention of the researchers to utilize the scarce resources efficiently and intelligently.

2. **CR function:** The various functions performed by CR include spectrum sensing, analysis, management and handoff etc. Spectrum sensing and analysis includes detection of white space in the spectrum and then utilize it. And in order to avoid harmful interference to PU when they again start using the spectrum, CR does sensing. The spectrum management and handoff function enable the choice of best frequency band available.
3. **Network Architecture and application:** The secondary network and the primary network are the major components in CR network architecture, where the SU are the unauthorized user that utilizes the unused unlicensed band temporarily owned by PU. Also CR functionality is present in both SU and secondary base station. The spectrum broker is a central network that coordinates spectrum usage if one common spectrum band is being used by several secondary networks. Cognitive communication increases spectrum efficiency and also supports services that require high bandwidth by sensing, detecting and monitoring the RI environment surrounding it.

C. The Classification Based on Network Architecture

One is centralized in which the central unity is held responsible for controlling and coordinating the spectrum allocation and access of SU. The other classification is based on the access behaviour of SU. One is cooperative in which all SU focuses towards a common goal. The other is non cooperative where they no longer cooperate to achieve common objective [13].

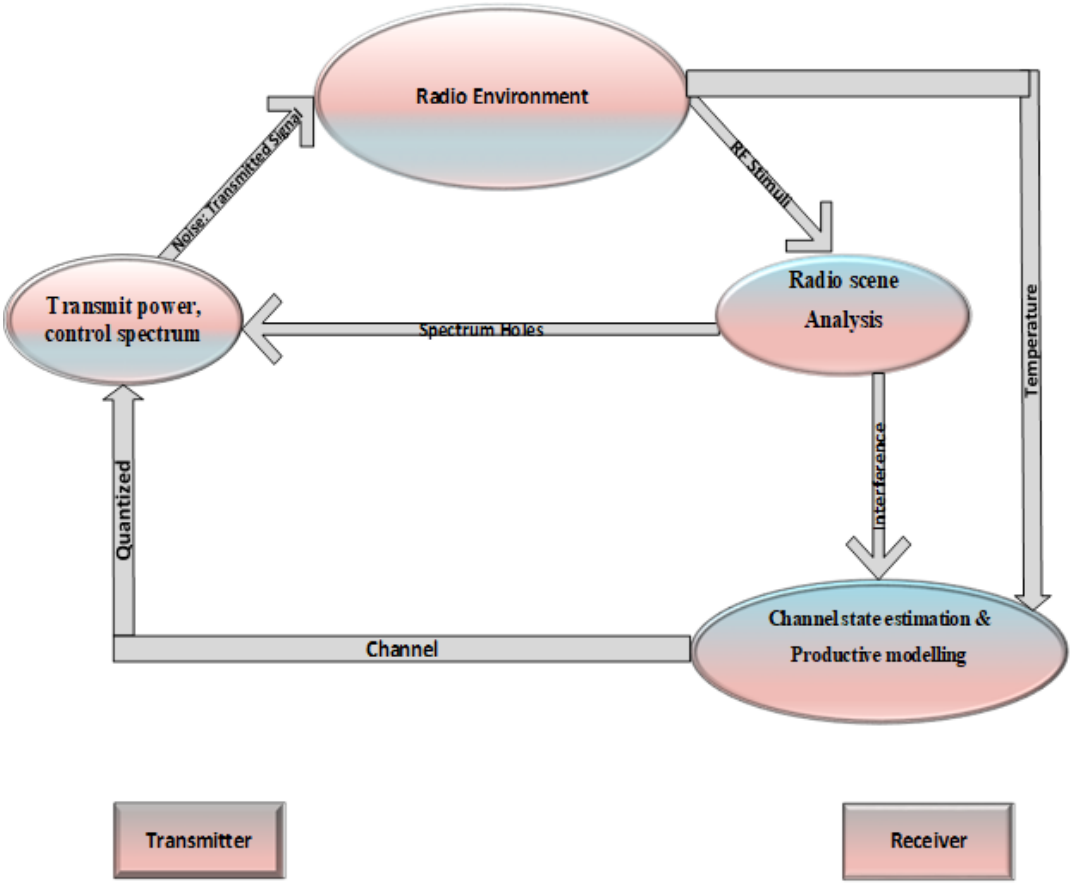

Figure 2. Cognitive cycle model

A. Security Threats in CRN and the PUE Attack

The PUE attack is further classified into two types:

1) Selfish PUE Attacks: To maximize the spectrum usage for itself is the objective of the attacker. When a fallow spectrum band is detected by the attacker, this prevents the SU from competing against particular band.

2) Selfish PUE Attacks: When the DSA process obstructed, the prime objective of the attack is fulfilled to harm the legitimate secondary user. This attack leads to denial of service. The fallow spectrum band is not necessarily used by the malicious attacker to serve its communication purpose unlike the selfish attacker [18].

III. METHODS TO DETECT MALICIOUS USERS

The performance of the system for cooperative sensing is significantly affected by the presence of the nodes which are malicious. Due to the malfunctioning of the device or some selfish reason the node acts maliciously. For example if the absence of signal is detected by the node but it might generate false positive, and the wrong decision is taken by the access point considering the presence of the primary signal and hence the malicious node can transmit its own signal selfishly over the free channel available.

Different type of malicious node has been considered 'Always Yes' node or 'Always No' nodes are simple malicious nodes. In case of 'Always Yes' the value given all the time is above the threshold and in case of 'Always No' the value given is below the threshold. With 'Always Yes', the probability of false alarm Pf is increased whereas with 'Always no' the probability of detection decreases.

B. PRE-FILTERING OF THE SENSING DATA

To identify and then remove the node which is malicious, pre-filtering of the data sensed is essential which in turn affect the final decision significantly at the access point hence giving values that are extremely false.

C. TRUST FACTORS:

To give the reliable measure, the trust factor is used for a particular user. While the calculation of the mean for the values of energy which are obtained for the various users, the trust factor are hence used as the weighing factor.

D. QUANTIZATION:

The need to quantize the energy value before sending to the access point is essential since limited bandwidth is offered by the control channels. Hence leads to the extensive studies of the schemes for optimal quantization for the distributed detection. However, it is highly complex and moreover the problem of optimization is non-linear to find the optimal threshold value [20].

Hence in many of the frequency bands, there is low usage of spectrum due to the conventional fixed spectrum allocation policy. And to exploit this under-utilized spectrum the promising technology proposed is CRN [21].

IV. PROPOSED ALGORITHM

As mentioned in [22], a trust- based system in be defined to prevent the PU and SU from various attacks. The author in the paper has built a trust model for CRN. Basically after checking trustworthiness which depends on a trust value it assigns free spectrum to the SU. The communication activity of the SU depends on the availability of the free spectrum. Hence using stochastic approach the author proposed Markov model showing the availability of spectrum for SUs and addressing the corresponding SU as authenticated user. The cognitive nodes are all included to calculate the trust level for all its surrounding nodes and which in turn are stored for later use. Also based on the new interactions, these values will be updated.

Table 1

Existing Method Drawbacks	Proposed Method Advantage
Defining the correct threshold for trust level.	It does not involves defining any threshold.
To set up a trust value it involves each cognitive node.	The cognitive node involved can be malicious node, hence it can be easily detected using methodology given below.
PU has to check the trustworthiness of SU on the demand to the available free spectrum.	PU has no role to be played in spectrum assignment hence reducing its overhead.
Assignment of free spectrum by PU.	The SU searches for free spectrum.

Each cognitive node will calculate trust for all its surrounding nodes and store these values for later use; these values should be updated in a specific time period based on new interactions. Hence in the proposed algorithm the secondary users are the in charge for allocating the free spectrum to them. One of the SU is selected as the cluster head for the region of availability of spectrum for particular primary user. The selection of the SU as cluster head is primarily done on the basis of random number generation. Then following the round robin pattern the available spectrum is divided into equal slots depending upon the SU demanding for that free spectrum. This pattern does not involve either defining trust value or the overhead caused to the PU to allot the free spectrum. Moreover it will help

detecting the malicious user in the vicinity as uneven slots of spectrum will otherwise be created due to its intervention in the spectrum assignment.

Proposed Methodology:

Steps to be followed are:

- Step 1:

Creation of CRN.

A network that consist of:

1) **Various primary users and the secondary users.**
2) **The primary base station and the secondary base station.**

- Step 2:

SU searches for free spectrum

For free spectrum of PU

Select one of the SU as the cluster head using random number generator.

Selected SU form slots for each SU demanding the free spectrum based on Round Robin algorithm.

Allocate the spectrum

If any unevenness in allotment detected for particular SU report it as malicious node.

ELSE

REPEAT UNTIL

Spectrum is available and demand is still not fulfilled

End

V. OPEN ISSUES AND FUTURE RESERCH DIRECTION

The issue of security fragility is one issue that cannot be resolved easily. The requirement of fundamental security is violated by the SU because of sensing where the legitimate analysis of the traffic is performed for the utilization of the spectrum, it is compromise in security.

In the wireless communication, the security and reliability trade-off is an important consideration in the presence of eavesdropping attack. Also various security algorithms thus that are efficient from the energy point of view as well as the low in complexity.one desirable in making CR technology viable solution in the wireless communication for the future generation.

VI. CONCLUSION

In cognitive radio networks, some malicious secondary users may create interference by accessing the primary user's available spectrum band. Such malicious SUs can seriously break down the whole network performance. To tackle this problem, we want to redefine a trust based model to check the trustworthiness of the secondary user who wants to use primary user's free spectrum band. After allowing the SU to form a cluster head to other SU in a PU vicinity, that SU allocate the spectrum forming slots to each SU in demand of the spectrum. Also the malicious activity can be easily detected. Hence the proposed algorithm not only reduces the overhead of the PU to spectrum allocation but also detect malicious node in an efficient way.

VII. REFERENCES

[1]. FCC, "Spectrum Policy Task Force Report," Vol. ET Docket Issue 02-155, November 2002.

[2]. Danijela Cabric, Shridhar Mubaraq Mishra, Robert W. Brodersen, " Implementation Issues in Spectrum Sensing for Cognitive Radios," Signals, systems and computers, 2004. Conference record of the thirty-eighth Asilomar conference on, Vol. 1, pp. 772-776. IEEE, 2004.

[3]. MacKenzie, Allen B. and Stephen B. Wicker. "Game theory in communications: Motivation, explanation, and application to power control." In Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE, vol. 2, pp. 821-826. IEEE, Year 2001.

[4]. Zhu, Xiaorong, Lianfeng Shen and T-SP Yum. "Analysis of cognitive radio spectrum access with optimal channel reservation."

Communications Letters, no. 4 pp. 304-306.IEEE, Year 2007.

[5]. Ji, Zhu and KJ Ray Liu. "Cognitive radios for dynamic spectrum access-dynamic spectrum sharing: A game theoretical overview." Communications Magazine, IEEE 45.5 pp. 88-94, Year 2007.

[6]. Cheng, Shilun and Zhen Yang. "Energy-efficient power control game for cognitive radio systems." In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, vol. 1, pp. 526-530. IEEE, Year 2007.

[7]. Liu, Jishun, Lianfeng Shen, Tiecheng Song and Xiaoxia Wang. "Demand-matching spectrum sharing game for non-cooperative cognitive radio network." In Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference on, pp. 1-5. IEEE, 2009.

[8]. P. Rostaing,T. Pitarque, E. Thierry, " PERFORMANCE ANALYSIS OF A STATISTICAL TEST FOR PRESENCE OF CYCLOSTATIONARITY IN A NOISY OBSERVATION," In Acoustics, Speech, and Signal Processing, 1996. ICASSP-96. Conference Proceedings., 1996 IEEE International Conference on, Vol. 5, pp. 2932-2935, 1996.

[9]. V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," Communications Magazine, IEEE, Vol. 43, Issue 12, pp. 112-119, December 2005.

[10]. Mishra, Shridhar Mubaraq, Danijela Cabric, Chen Chang, Daniel Willkomm, Barbara Van Schewick, Adam Wolisz, and Robert W. Brodersen, "A real time cognitive radio testbed for physical and link layer experiments," New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on, pp. 562-567. IEEE, 2005.

[11]. Danijela Čabrić and Robert W. Brodersen, "Physical Layer Design Issues Unique to Cognitive Radio Systems,"Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on, Vol. 2, pp. 759-763. IEEE, 2005.

[12]. Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "Next generation/ dynamic spectrum access/cognitive Radio Wireless Networks: A Survey," COMPUTER NETWORKS JOURNAL ELSEVIER," Vol. 50, pp. 2127-2159, 2006.

[13]. William A. Gardner, Antonio Napolitano, and Luigi Paura, "Cyclostationarity: Half a century of research," Signal Processing, Vol. 86, Issue 4, pp. 639-697, 2006.

[14]. Kyouwoong Kim, Ihsan A. Akbar, Kyung K. Bae, Jung-sun Um, Chad M. Spooner, and Jeffrey H. Reed, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," New frontiers in dynamic spectrum access networks, 2007, pp. 212-215,2007.

[15]. Alex Chia-Chun Hsu, David S. L. Wei† and C.-C. Jay Kuo, "A Cognitive MAC Protocol Using Statistical Channel Allocation for Wireless Ad-hoc Networks," Wireless Communications and Networking Conference, pp. 105-110. IEEE, 2007.

[16]. Lundén, Jarmo, Visa Koivunen, Anu Huttunen, and H. Vincent Poor. "Spectrum sensing in cognitive radios based on multiple cyclic frequencies."Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 2nd International Conference on, pp. 37-43. IEEE, 2007.

[17]. Qing Zhao and B.M. Sadler, "A Survey of Dynamic Spectrum Access," Signal Processing Magazine, IEEE, Vol. 24, Issue 3, pp. 79-89, may 2007.

[18]. ShiyuXu, Zhijin Zhao, Junna Shang, “Spectrum Sensing Based on Cyclostationarity,” Power Electronics and Intelligent Transportation System, 2008. PEITS'08. Workshop on, pp. 171-174. IEEE, 2008

[19]. Jun Ma, Guodong Zhao and Ye (Geoffrey) Li, "Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, pp. 4502-4507, Vol. 7, no 11, November 2008.

[20]. Kim, Hyoil, and Kang G. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection" in Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 14-25. ACM, 2008.

[21]. Zayen, Bassem, A. M. Hayar, and Dominique Nussbaum, "Blind spectrum sensing for cognitive radio based on model selection," in Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, pp. 1-4. IEEE, 2008

[22]. Parvin, Sazia, Farookh Khadeer Hussain, Omar Khadeer Hussain, and Abdullah Al Faruque. "Trust-based Throughput in Cognitive Radio Networks." Procedia Computer Science 10 (2012): 713-720.