I J C T A, 9(41) 2016, pp. 777-782 ISSN: 0974-5572

SMART DUAL-BAND CHANNEL ALLOCATION IN THE COGNITIVE RADIO UNDER THE SECURE ENVIRONMENT

Mehakpreet Kaur and Navleen Kaur

Abstract: The proposed model simulation has been designed with the dual channel allocation model with one dedicated module for the handling of the migratory users and the new users. The proposed model has been simulated with the 5 channels for the new users, which are allocated in the one user one channel fashion and facilitates the users to gain the maximum bandwidth to give the best performance to the local users, whereas the cell migrations are handled over the 5 reserve channels, with N sub-channels over each of the available channel for the handling of the migratory users. The channel allocation model verifies the availability of the channels before allocating the channel to user requested for the service. The migratory channel allocation plays the vital role, as there is the capability of allocating the full channel. When all of the sub-channels are available, the full bandwidth is allocated to the user requested for service, whereas shrinks the overall bandwidth between the N number of users over the sub-channels, when the number of users is higher than 1. The proposed model has undergone the in-depth performance analysis, which has been performed on the basis of the probability of dropping the handoff/migration calls, probability of blocking the new calls, throughput and percentage of successful in-cell finished calls. The proposed model has been found better than the existing model on the basis of the probability of dropping the handoff/migration calls and probability of blocking the new calls. The proposed has been recorded with the 1.0E-11 over probability of dropping in scenario A and B against the 1.0E-05 and 1.0E-06 in the existing model, which shows the significant improvement in the proposed model.

Key Words: *Cognitive Radio, Cellular cognitive radio networks, CGRN, intelligent radio networks, dual-band allocation.*

I. INTRODUCTION

The main objective of cognitive radio networks is to determine the utilization of the radio spectrum in a proper manner and to deliver communication which is reliable for all the users of that network. A cognitive radio networks is a network which is composed of different types of network as well as the communication systems thus can be known as heterogeneous in nature. Rather than focusing on spectral efficiency, architecture of cognitive radio is towards the improvement of the entire network utilization. Network utilization viewed from two perspectives that are user and operator-

From user's point of view the demand of services should be fulfilled on the given time at any place,
From operator's point of view the allocation of recourses like network and radio to deliver required packets/unit bandwidth should be in an effective manner. Components, which participate to build the cognitive radio network, are core network, base station (BSs) and mobile station (MS). The architecture is proposed by chen et al. (2008), which basically uses these components to make three different architectures in the network-

A. Infrastructure Architecture
In this architecture, a base station is accessed by a mobile station. Mobile station shall communicate with other mobile station under the transmission range of the same base station. Core network is responsible for the different cells. Mobile stations' demand can be fulfilled by the base station by executing the one or

Department of Information Technology, Chandigarh Engineering College , Landran, Punjab, India
Emails: mehakarora154@gmail.com, cecm.infotect.navleen@gmail.com

multiple communication protocol.

B. Ad-hoc Architecture

The ad-hoc network is created when a mobile station sense the another mobile station nearby which are connected via communication protocol.

C. Mesh Architecture

The Mesh architecture is composed of infrastructure and ad-hoc architecture via communication between base stations. The base stations which are having the cognitive radio capabilities can use the spectrum holes for the communication purpose. Below figure 1 shows the functions for cognitive radio where the Spectrum sensing, sense the unused available spectrum and share it without an interference, Spectrum Management determines the best available spectrum, Spectrum Mobility maintains the communication at the time of spectrum transition means vacating the channel if the primary user id detected and Spectrum Sharing provides spectrum scheduling methods between the existing user.

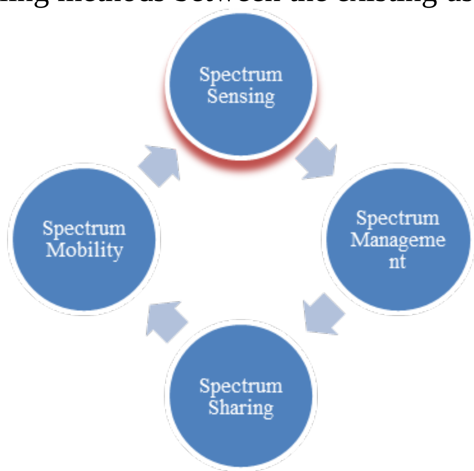

Figure 1. Acyclic Process

1.1. SPECTRUM SENSING

In cognitive radio the unlicensed users' are allowed to use the licensed band when it is not being used by the primary user so the determination of whether the primary user is using the licensed band or not is done by the spectrum sensing which sense the presence or absence of the primary user in the radio environment therefore Spectrum sensing consists an important role. Spectrum sensing can be classified into some categories namedas transmitter detection, cooperative detection, and interference-based detection which comes under the Non-Cooperative spectrum sensing, as shown in Figure 2.

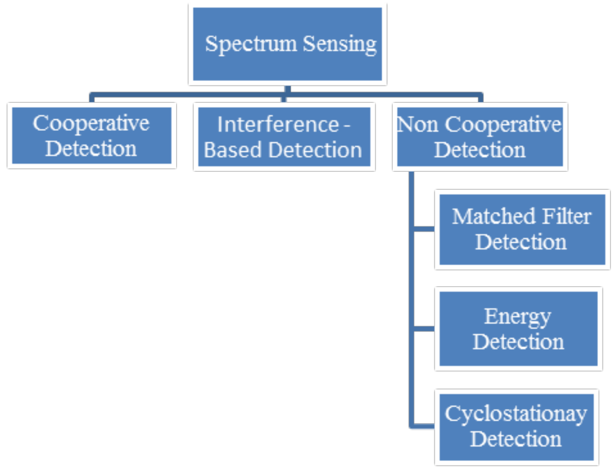

Figure 2. Spectrum Sesing Techniques

Spectrum sensing is basically divided into two parts cooperative and non-cooperative spectrum sensing and both have their advantages and disadvantages. Non- cooperative spectrum sensing has a limitation that if a problem like shadowing or fading comes in the networks, user feel difficulty to distinguish between unused part or the deep fade. Cooperative spectrum sensing technique overcomes this interference problem.

II. LITERATURE REVIEW

Wang Weifang in 2012 focusing on the security issues arising on the cognitive radio networks discuss the DoS attack at various layers. DoS attack is vulnerable, as the attacker continuously send the frequency or the signal to the authentic user which results in blocking or disabling the authentic user. ShabnamSodagari et.al. in 2010 proposed a Channel Eviction Triggering defense scheme. This paper discussed a special kind of DoS attack which is basically invoked by the Channel Eviction Triggering (CET). In this kind of attack the rival nodes suspiciously invoke mechanisms to protect the licensed users and thus interrupt secondary access which leads to the manifestation of CET attacks. This type of attack is a kind of cheating to the cognitive radios. The simulation results validates the effectiveness of the introduced CET defense scheme. Chao Chen et. al. in 2011 consider the cooperative spectrum sensing in the existence of Primary User Emulation Attack (PUEA). In the introduced scheme, at the fusion center all the sensing information of various secondary users is joint. For increasing the probability of detection the optimization of combined weights are done.

Yi Tan et. al. in 2011 consider two cases named one-stage and multi-stage case to mitigate the DoS attack in the cognitive radio networks. One-stage case, formulation of cooperative game between the malicious nodes are done and develop the effective decision strategy. In the case of multi-stage, to determine the behavior of malicious user and secondary user, the Markov chain model was proposed. Simulation results states that in the one-stage case, the coordinated attack attains was on 10-15% improvement and, in the multistage case, the existence of malicious nodes was notified which was maximizing the net payoff. Sukanya Chatterjeet. al. in 2015 focused on a different kind of attack in Cognitive Wireless Sensor Networks that is SSDF (Spectrum Sensing Data Falsification) attack. And the SSDF is the kind of DoS attack. In the SSDF attack a modification is done on the sensing report. With the help of this false information the secondary user takes the wrong decision about the spectrum usage. To minimize the effect of this attack the similarity based clustering is used to sense the data or the information.

Sumit Yadavet. al in 2012 deals with SSDF attack. The previous results showed that the various techniques failed when the number of secondary user increases as compare to authentic secondary user. So the proposed technique is not dependent upon the malicious SUs. And the proposed techniques does it work with the help of primary user's Received Signal Strength (RSS) at an SU to determine the position and match this value with the calculated once at data fusion center. SumanBhuniaet. al. in 2014 considered the honeypot theory, in which they suggested a defense mechanism named honeynet to determine the attacker in the network. The honeynet have an advantage to determine the strategy of the attacker with the past information of that attack Z. Jin et. al. in 2012 simulates the result to show the reduced number of call dropped in the network at the time of communication. The secondary networks contains the real time and non-real time traffic. PUEA basically in the radio environment increases the call drop rate and delay in the secondary network .With the help of simulated results it can be state that with the increment in the malicious traffic load, a performance improvement on the delay by up to 54% was noticed.

III. EXPERIMENTAL DESIGN

The call handling phase is responsible for tracking the nodes originating from the other cells or the posting the new requests. The node or call information updated during the initial setup phase of connectivity is altered and updated at the various intervals. The new nodes and the migrating nodes are handled differently during the registration and connection setup phases, such nodes are listed as the registered ones and other los nodes are considered as the error points. Such error points are actively tracked and the appropriate channels are allocated immediately as the query is received from the lost node, which was lost during the cell migration. The following algorithm defines the call traffic handling mechanisms in detail:

Algorithm 1: Node Information Update and Registration Model

1. Cellular nodes load the exiting node information table to the memory
2. Cellular nodes load the initial learned node information table into the memory
3. Cellular nodes verify the locations of the existing nodes obtained during the initial phase against the nodes obtained in the final phase.

   $i = \text{Linear}\ _0\int^N$

   $\text{distance}=f_x(i,{}_0\int^N j)$ if missing point found

   $\text{distance} = \infty$ if missing doesn't reply till wait period

   $f_x(i,j) = \sqrt{(x_i - x_i')^2 - (y_i - y_i')^2}$
4. Cellular nodes query to migrating cellular user nodes to the other cellular circles
5. Non reporting cellular user nodes are marked as un-located error point.
6. Cellular nodes broadcast the message for the discovery error points to minimize the chances of the connections loss from all of its neighbors
7. If nodes marked as the error points replies or queries,
   a. The new cell information is updated
   b. The node is registered under the new cell

c. Membership of the most suitable cellular node would be assigned.

8. Else

a. The error points are marked as lost nodes and they have to initiate the whole registration procedure from the beginning after coming into the coverage area

3.1. CALL ADMISSION CONTROL

The sub-rating policy has been incorporated over the occupied channel to split the data rate to half for at least two given channels for the handling of call handoffs. The call generation rate per unit area has been distributed in the uniform manner for the cellular service zone. In existing scheme the four different Markov model has been utilized for influencing and shrinking the soft handoff coverage to reduce the call dropping probability over CDMA cellular radio network. By assuming the new call generation rate per unit area small and on reserving 40 % of channels from the total available channels for handoff calls, we have shown that the handoff call dropping probability can reduce significantly for both finite capacity and finite population models. The existing system also evaluates the traffic load of new and handoff call is high, performance of the network seems to improve by reducing the soft handoff region.

IV. RESULT ANALYSIS

The proposed model simulation has been designed for the purpose of handling the new and migration calls in the cellular networks. The cellular networks are the mobile networks connected in the formation of the hexagonal cells in the indefinite connectivity based structuring. Each cell is having six number of neighboring cells, which offers the high-end connectivity and provides the ability to the users to roam around the cells. The roaming processing is handled by the handoff or migration mechanisms, where the handoff usually occurs between the cells of the similar service provider, whereas the migrations depict the users from the other service provider's cells.

Table -1 Overall Probability of dropping for handoff/migration calls based readings from Scenario-A

PARAMETER	SCENARIO	EXISTING	PROPOSED
Probability of Dropping the handoff/migration calls	**A**	**1.0E-05**	**1.0E-11**
	B	**1.0E-06**	**1.0E-11**

Table -2 Overall Probability of blocking for new calls based readings from Scenario-B

PARAMETER	SCENARIO	EXISTING	PROPOSED
Probability of Blocking the new calls	**A**	**1.0E-08**	**9.4E-10**
	B	**1.0E-12**	**8.1E-10**

The latest popular cellular model is the popular application in the 4G/LTE network, where the networks are used in the high-speed connectivity. The proposed model has been designed for the purpose of handoff and local origination call handlings. The proposed model has been defined by minimizing the probability of the connection loss while changing the coverage cell. The proposed mechanism enables the cellular users to stay connected while changing the cells in the cellular network by the means of the reserve channels and sub-channeling across the cellular networks. The cellular network nodes connect themselves with the other base station in the vital reach in order to keep itself connected while keeping all of the data or voice connections intact in the given cellular network while changing its positions from one cell to another cell. The proposed model proposes the use of reserve channel based absorption for the purpose of improvement in the handoff call handling procedure in comparison with the existing schemes. The simulation results have been obtained in the form of network performance parameters of throughput, call/finish, probability of dropping the migratory calls and probability of blocking the new calls. The experimental results have shown in the effectiveness of the proposed model in comparison with the existing models based upon the results obtained for the probability. The only odd case has been recorded in the case of scenario-B on the basis of probability of dropping or blocking.

V. CONCLUSION

For the attack prevention, the proposed model ensures the connection with the legitimate users only and does not permit to receive the data from the unauthorized users, which directly affects the cognitive radio security and does not allow any flooding attack over the secure channel. The proposed model performance has been measured using the Probability of detection and Probability of false alarm. The proposed model has been performed during the denial of service attack, which shows the effectiveness of the proposed model. In the future, the proposed model can be enhanced to secure the end-to-end channel between the cognitive radio ends. Also the proposed model can be enhanced with robust data encryption along with the key exchange scheme for the hardened security of the cognitive radio channel.

REFERENCES

[1]. Khare, Anubhuti, Manish Saxena, Roshan Singh Thakur, and KhyatiChourasia. "Attacks & preventions of cognitive radio networks survey." Int. J. Adv. Res. Comput. Eng. Technol.(IJARCET) 2, no. 3 (2013): 1002.

[2].Christo Reegan, Raj. V, Sabitha. R, Karthikha. C “An Effective Primary User Authentication Mechanism for Denial of Service Attack in Cognitive Radio Networks” (ICIIECS-2014), International Journal of Computer Applications (0975 – 8887)

[3]. Jin, Z., SanthanakrishnanAnand, and Koduvayur P. Subbalakshmi. "Impact of primary user emulation attacks on dynamic spectrum access networks." Communications, IEEE Transactions on 60, no. 9 (2012): 2635-2643.

[4]. Weifang, Wang. "Denial of service attacks in cognitive radio networks." Environmental Science and Information Application Technology (ESIAT) (2010): 530-533.

[5]. Sodagari, S., Attar, A., Leung, V. C., &Bilén, S. G. (2010, December). Denial of service attacks in cognitive radio networks through channel eviction triggering. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[6]. Chen, Chao, Hongbing Cheng, and Yu-Dong Yao. "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack." Wireless Communications, IEEE Transactions on 10, no. 7 (2011): 2135-2141.

[7]. Tan, Yi, ShamikSengupta, and K. P. Subbalakshmi. "Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks." Selected Areas in Communications, IEEE Journal on 29, no. 4 (2011): 890-902.

[8].Bhunia, Suman, ShamikSengupta, and Felisa Vazquez-Abad. "CR-Honeynet: A Learning & Decoy Based Sustenance Mechanism against Jamming Attack in CRN." In Military Communications Conference (MILCOM), 2014 IEEE, pp. 1173-1180. IEEE, 2014.