Indian Journal of Science and Technology, *Vol 9(16), DOI: 10.17485/ijst/2016/v9i16/92200, April 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Cumulative Cooperative Spectrum Sensing Scheme to Defend Against Selfish Users

K. Elangovan* and S. Subashini

VIT University, Chennai - 632014, Tamil Nadu, India; elangovan.k2013@vit.ac.in, subasundararajan@gmail.com

Abstract

Background/Objectives: This paper considers combatting the jamming and selfish attacks in Cognitive Radio (CR) networks operating at the white (unused) and grey (underused) spaces in the RF spectrum. CR facilitates effective utilization of RF spectrum resources but still vulnerable to various network attacks. **Methods/Statistical Analysis**: This study considered the jamming and selfish type of attack detection and to defend against them because of its severity. An Intrusion Detection System (IDS) is formed to combat the against jamming and selfish type of attacks in CR. **Findings:** In this system cumulative-sum algorithm is used, which incorpates the control centre information over the channel. The cumulative-sum based algorithm shows improved performance in provisioning better packet delivery ratio, throughput and minimum energy and packet drop. Further, this algorithms works better for more number of Secondary Users (SU), and the Unlicensed Users. **Applications/Improvements:** This work can be enhanced further by simulating under various network attacks and in the presence of numerous SU.

Keywords: Cognitive Radio, Jamming Attacks, Network Security, Secure Spectrum Sensing, Selfish Attacks

1. Introduction

Emerging concept in wireless access, aimed at improving the way by which the radio is utilized. The primary user is the licensed user of the spectrum. The secondary users who are the unlicensed users share the spectrum opportunistically when it is not accessed by the primary user. The drastical utility and tremendous improvement in wireless network made the scarcity in spectrum. Hence, the spectrum has to be utilized effectively. For this, in the CR networks, the transmission or reception parameters are changed to communicate efficiently without interfering with licensed users.

Each channel consists of several nodes, among these nodes one or multiple nodes may behave selfishly and try to pre-occupy the channel. This degrades the performance of the CR network. This is detected by means of an efficient and easy to implement algorithm called the IDS. If a SU user recognizes the presence of Primary User (PU) it will send fake information to the remaining nodes and prohibits other SU from utilizing the channel. There is another type of selfish attack whereby the channel allocation information such as number of available channels and the channel in use. In this case, a selfish SU[1,2] will broadcast fake details about the channel and try to preoccupy the channel even if it doesn't require all the channels. For e.g. it requires only 5 out of 7 channels it will broadcast that all 7 nodes are in use and pre-occupy those channels. In conventional system only less research has been done on CR. This is because of the dynamic nature of the cognitive radio. The selfish attack problem dealt so far is also in fewer amount.

This paper concentrates on the selfish SU attack over multiple channel access in cognitive ad-hoc radio networks. This study is considering the selfish SU occupies more number of channels than it is utilizing. Every secondary user is regularly transmitting to the other SUs in the node about the channel allocation information such as number of channels available and number of currently ulitilsed channels. The selfish SU will send to the remaining SUs that more number of channels are in use than actually used currently. This IDS algorithm will detect the selfish secondary user by cooperative working of other legitimate SUs[3,4].

**Author for correspondence*

Every channel allocation information which is being sent and received will be exchanged between the secondary users. The channel information sent by target SU to neighbor secondary SUs is based on the the difference between the legitimate secondary users and selfish attacker. This proposed algorithm is simple yet reliable as it is based on the channel allocation information shared cooperatively by the secondary users. This is proved by simulation.

2. Nature of Cognitive Radio

The dynamic nature of the cognitive radio network made it hard to detect the selfish attack in conventional wireless networks. Chen et al. is the first to identify a selfish attack threat called PU attack. In this attack the characteristics of PU is emulated transmitted by the selfish node. Signal energy level and source signal location are combined and the legitimate source signal is found in this transmitter verification process which are applied a game theory approach called nash equilibrium approach to overcome this PUE attack[5,6]. The selfish attack by an SU increases the access probability of the node by reducing the back-off window size in CSMA- based CR network. The selfish attack is a type of denial-of-service attack[7]. A cross-layer Altruistic Differentiated Service Protocol (ADSP) is proposed for dynamic cognitive radio networks which aims at providing quality of service for selfish nodes. Types of attacked in CR netwprk includes: Primary User Emulation (PUE) attack, Sybil attack, wormhole attack, node impersonation attack, Timing attack, Illusion attack, Sinkhole attack etc[9].

3. Attack and Detection Mechanism

The CCC is used to broadcast the parameters and managing information to the secondary users of CR network. The present channel allocation information is listed and broadcasted to all neighboring SUs. The channel allocation information is broadcasted by the SSU separately to the left side and right side LSU through individual CCC. If a list is broadcasted it should contain channel allocation[10] information of all neighboring nodes. This information list which is broadcasted by SU to access the channels. This CCC is used by the SSU for sending fake current channel information to its neighboring SUs. During the attack, the SSU will broadcast large number of channels used than the actual numbers. Due to this the other LSU will be prohibited from utilizing the channel. The SSU may also broadcast a list of partially pre-occupied channel list though it uses only fewer channels. For example, the SSU uses five out of seven channels but broadcasts as utilizing six out of seven channels. Hence, the LSU will use one channel but will loose the chance of utilizing one more channel.

This study considers a cognitive radio network which has autonomous and distributed power management characteristics. This study propose a detection mechanism called IDS for ad-hoc network. The autonomous decision capability of ad–hoc communication is used to exchange the channel allocation information. The current channel location information is exchanged between a specified SU and its 1-hop neighbor through dedicated channel. From the comparison of information received by all the nodes the selfish SU is identified.

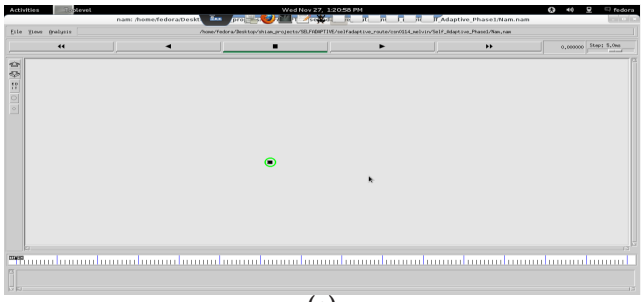
4. Simulation Environment

The efficiency of IDS is evaluated from the simulation results using network simulator[11,12]. This is calculated from the detection rate, which is the ratio between Number of detected selfish secondary users and Number of actual selfish secondary users. A secondary user may possess maximum of 8 channels and a CCC. The data rate of the channel is 11 Mb/s this experiment is done under various densities of secondary user.

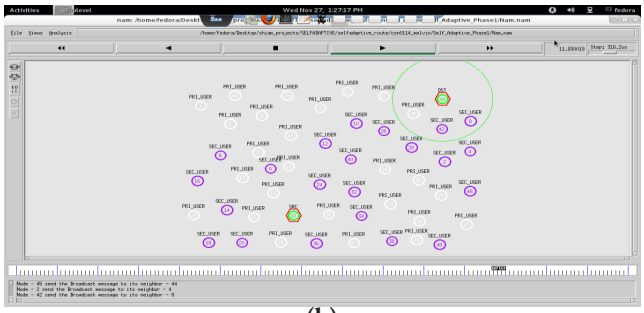
5. Results and Discussion

Figure 1 shows the PU and SU node formation. Figure 2 indciates the communication establishment. Figure 3 shows the message broadcast from source to destination through neighbors. Figure 4 shows the IDS Formation. Figures from 5 to 8 show the reliable performance of proposed IDS system for various network parameters.

An experiment carried out with 50,100 and 150 SUs to detect how the SU density affects the accuracy from that the number of SUs will have an trivial effect on IDS algorithm for detection of SSU shown in Figure 1 and 2. The SSU density is a sensitive issue for detection rate. With the increase in the detection of selfish SU in CR node the accuracy decreases rapidly shown in Figure 3. The main reason for the problem is that more than 1 SSU will be found in the neighboring node with a high selfish node density. There is high range of possibility that a



(a)



(b)

Figure 1. Primary and secondary node formation.

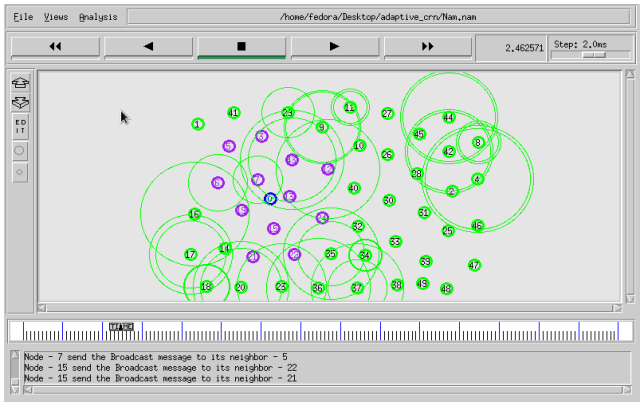
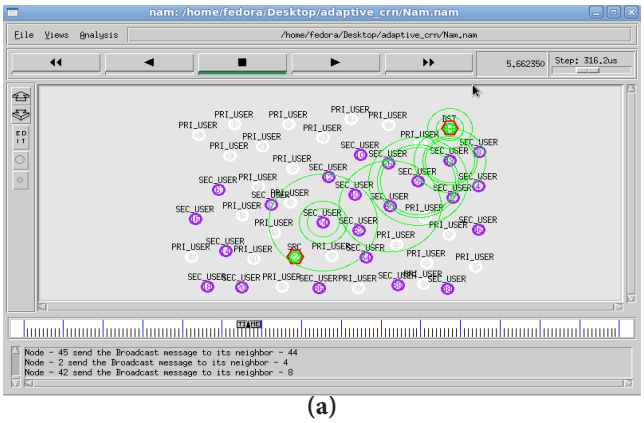
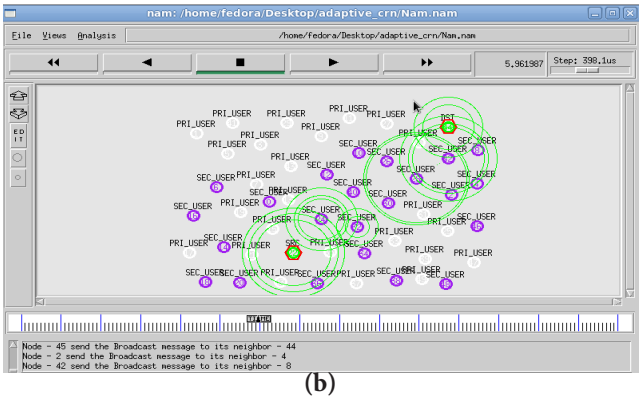


Figure 2. Communication establishment.



(a)



(b)

Figure 3. Message broadcast from source to destination through neighbors.

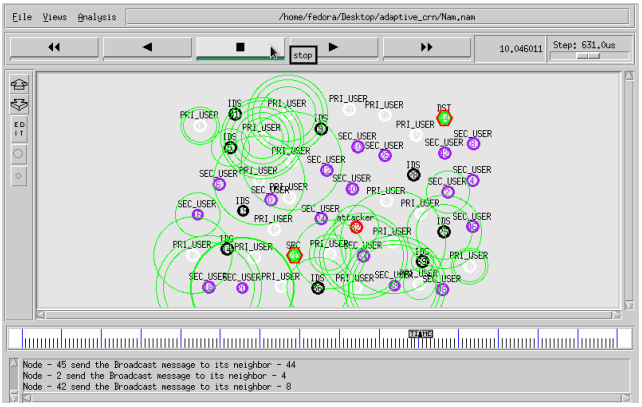


Figure 4. IDS formation.

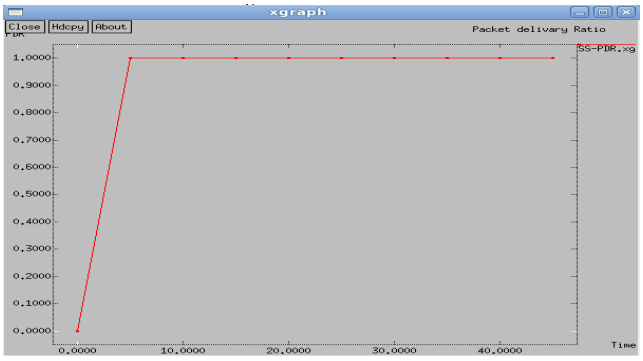


Figure 5. Packet delivery ratio.

wrong decision can be made due to faked channel information. It is hard to detect the selfish attack when both nodes exchange fake information shown in Figure 4. The density of SSU in reality is 3-4; the detection accuracy for detection of selfish attack using IDS is more than 97 shown in Figure 5-8.

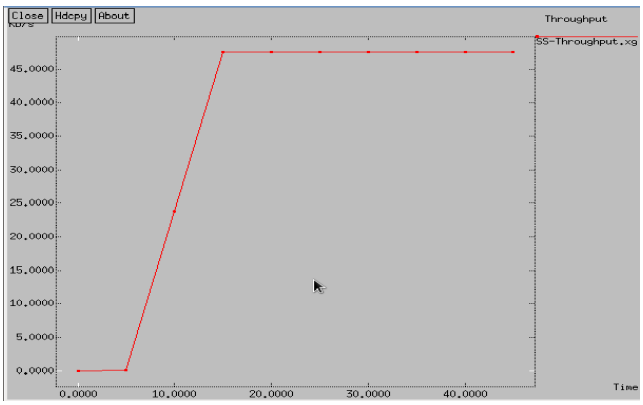


Figure 6. Throughput

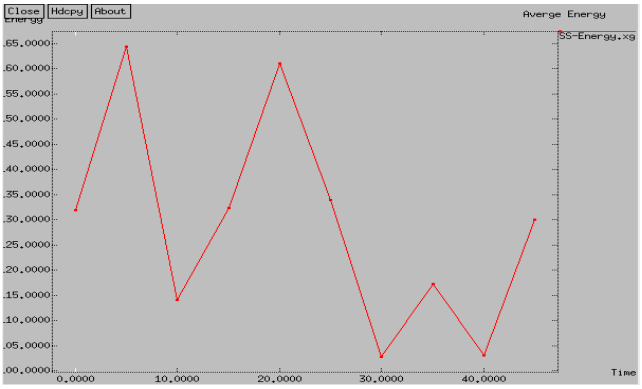


Figure 7. Average energy.

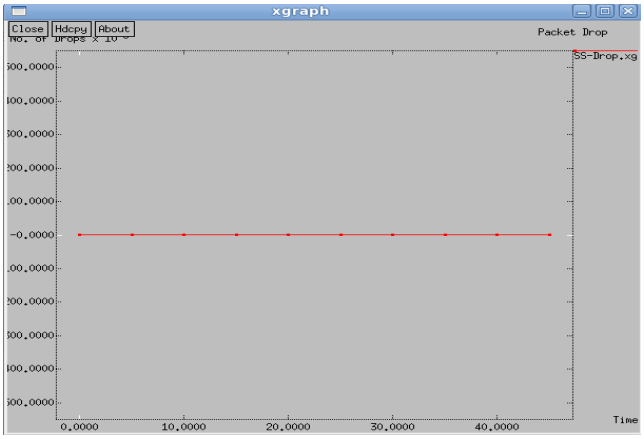


Figure 8. Packet drop.

6. Conclusion

This study proposed effective IDS, which can be easily implemented in the secondary users' cognitive radio software. The proposed IDS uses a non-parametric cusum algorithm, which offers anomaly detection. By learning the normal mode of operations and system parameters of a CRN, the proposed IDS detects suspicious (i.e. anomalous or abnormal) behavior arising from an attack. Using a jamming attack as example against a CRN secondary user, we demonstrated how the proposed IDS detected the attack with low detection latency. The future work will focus on how to enhance the detection sensitivity of the IDS under more number of selfish and secondary users.

7. References

1. Fadlullah ZM, Nishiyama H, Kato N, Fouda MM. Intrusion Detection System (IDS) for combating attacks against cognitive radio networks. IEEE Networks. 2013; 27(3):51–6.
2. Suchita SP, Mallikarjun K. Selfish attacks and detection in cognitive radio ad-hoc networks using markov chain and game. IJSR. 2014; 3(8):1999–2003.
3. Kaligineedi P, Khabbazian M, Bhargava VK. Malicious userdetection in a cognitiveradio cooperative sensing system. IEEE Transactions on Wireless Communications. 2010; 9(8):2488–97.
4. Akyildiz IF, Lo BF, Balakrishnan R. Cooperative spectrum sensingin cognitive radio networks: a survey. Physical Communications. 2011; 4(1):40–62.
5. Chen R, Park JM, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal of Selected Areas Communications. 2008; 26(1):25–37.
6. Li H, Han Z. Combating primary user emulation attacks in cognitive radio systems, Part I: Known channel statistics. IEEE Transactions on Wireless Communications. 2010; 9(11):3566–77.
7. Chen X. Distributed denial of service attack and defense. IEEE International Conference on Educational and Information Technology (ICEIT); 2010. p. 318–20.
8. Chong CY, Kumar SP. Sensor networks: Evolution, opportunities and challenges. Proceedings of the IEEE. 2003; 91(8):1247–56.
9. Lo BF. A survey of common control channel design in cognitive radio networks. Physical Communication. 2011; 4(1):26–39.
10. Roos T, Myllymaki P, Tirri H. A statistical modeling approachto location estimation. IEEE Transactions on Mobile Computing. 2002; 1(1):59–69.
11. Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network. Indian Journal of Science and Technology. 2013 Feb; 6(2):4045–57.
12. Renjit JA, Shunmuganathan KL. Network based anomaly intrusion detection system using SVM. Indian Journal of Science and Technology. 2011; 4(9):1105–8.