www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19539-19541

Selfish Attack detection mechanism using COOPON in Cognitive Radio

Shital.S.Patil[1], A.N.Jadhav[2], Vivek T. Patil[3]

[1] Department of ENTC, D.Y. Patil College of Engineering & Technology,
Kolhapur, Maharashtra, India
ssp.1991@rediffmail.com

[2] HOD, Department of ENTC, D.Y. Patil College of Engineering & Technology,
Kolhapur, Maharashtra, India
ajitsinhj33@gmail.com

[3] Assistant Professor, Department of Computer, D.Y. Patil College of Engineering,
Akurdi, Pune, Maharashtra, India
vvkpatil300@gmail.com

Abstract: *Cognitive radio is one of the wireless based communication technology. This technology is mainly designed to allow the unlicensed users to utilize the maximum bandwidth available in the network. An important consideration to any wireless network is secure communication. In Cognitive radio (CR), the unlicensed users use the maximum available bandwidth. When the spectrum is not used by the licensed primary user, the free channels are allocated for the unlicensed secondary users (SUs). But the problem is that some of the secondary users act selfishly to occupy all the channels. These secondary users are called as selfish attackers. Hence, to detect a selfish attacker COOPON (Cooperative neighboring cognitive radio Nodes) detection technique is used. The proposed work provides COOPON system which detects multiple selfish attacks and evaluate the detection rate by considering the parameters like selfish secondary user density, number of secondary nodes and number of neighboring nodes using MATLAB R2012a (version7.14.0.739).*

Keywords: Cognitive Radio, Primary user, Secondary user, Selfish Attacks, COOPON, MATLAB.

1. Introduction

Cognitive radio is a form of wireless communication where a transceiver can intelligently detect the channels for communication which are in use and which are not in use. An un-licensed user can use an empty channel in a spectrum band of licensed user without interference. Generally licensed users are known as primary users and un-licensed users are secondary users. When information is send through a primary user, only some channel of band is used, others are empty. These empty channels are used by un-licensed user called secondary user. Secondary users always watch the activities of primary user, and detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are active, the secondary user should either avoid using the channel. An Empty channel also known as spectrum holes.

CR attacks are a serious security problem because they significantly degrade the performance of cognitive radio network. In PUE attack, attacker transmits an emulated primary signal during a spectrum sensing interval. This PUE attacker is called 'selfish attacker' if it performs the attack for its selfish own purpose. Some SUs are selfish, and try to occupy all or part of available channels. Usually selfish CR attacks are carried out by sending fake signals or fake channel information. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels.

To detect the selfish cognitive radio attack called cooperative neighboring cognitive radio nodes (COOPON) detection techniques is used. COOPON is designed for CR ad-hoc networks with multiple channels and is designed for the case that channel allocation information is broadcast for transmission. The common control channel (CCC) is used to broadcast and exchange managing information and parameters to manage the CR network among secondary ad-hoc users. We focus on selfish attacks of SUs toward multiple channel access in cognitive radio ad-hoc networks. We assume that an individual SU use multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring SU's. They will send a larger number of channels in current use than real in order to reserve available channels for later use. The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighboring SUs.

1.1 Selfish Attacks:

In cognitive radio network, Secondary users are of two types namely Legitimate Secondary User (LSU) or neighboring secondary user and Selfish Secondary User (SSU). All secondary Nodes complete to sense available channels. But some SUs are selfish, and try to occupy all or part of available channels. Usually selfish CR attacks are carried out by sending fake signals. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels. Actually this fake signal is send by the selfish SU. Thus, these selfish attacks degrade the performance of a CR network.

In Channel pre-occupation attack system, the attackers are broadcast the current available channel information to neighboring nodes. It is carried out through a common control channel (CCC). Common control channel dedicated only to exchanging management information. A selfish SU will broadcast fake free (or available) channel lists to its neighboring SU's. The selfish SU will send a larger number of channels in current use than real in order to reserve available channels for later use. Even though a selfish SU only uses three channels, it will send a list of all five occupied. Thus, a legitimate SU (LSU) is prohibited from using the two available channels.

DOI: 10.18535/ijecs/v5i12.49

1.2 Detection Mechanism: COOPON

Cooperative neighboring cognitive radio Nodes (COOPON) is applied among a group of neighboring users to detect selfish nodes who broadcast fake channel lists. Consequently, neighboring users can detect the selfish users by comparing the transmitted channel list of the target user with their lists. This COOPON detection technique is applicable only channel pre-occupation attack system. In this system selfish secondary user (SSU) broadcasts separate channel allocation information lists through individual CCC to the LSU. A SSU attacks by sending fake current channel allocation information to its neighboring SUs. When the attackers try to pre-occupy available channels, they will broadcast larger number of channels in current use than real to reserve available channels for later use. In this case, the legitimate SU will be completely prohibited from accessing available channels.

The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighboring SUs. All neighboring SUs exchange the channel allocation information both received from and sent to the target SU. The target SU and its neighboring SUs are 1-hop neighbors. Then, each individual SU will compare the total number of channels reported to be currently used by the target node to the total number of channels reported to be currently used by all of the neighboring SUs. If there is any discrepancy between the two figures, all of the legitimate SUs will recognize a selfish attacker. Then COOPON will check the next neighboring node. It selects one of the unchecked neighboring secondary nodes as a target node. This detection procedure will continue until the last SU in a CR network is validated. Our proposed detection mechanism in COOPON is designed for an ad-hoc communication network.

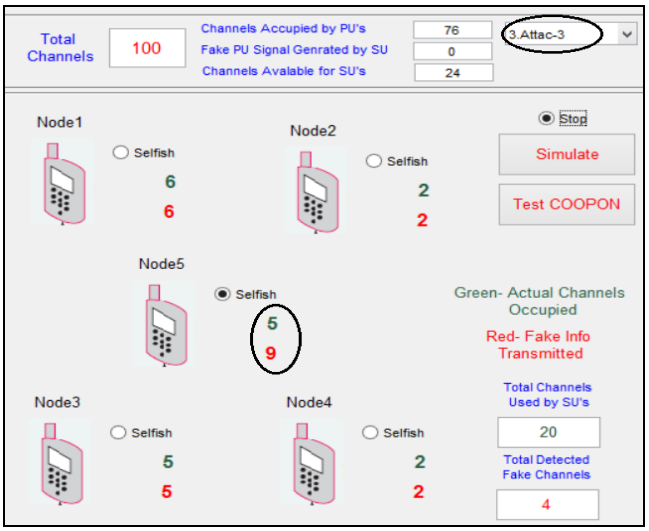

Figure 1

Selfish attack type 3 is channel pre-occupation attack system shown in above figure 1. Total channels are taken 100. Channels occupied by PU'S are 76, Channels available for SU'S are 24 and Fake PU signal generated by SU are 0. All nodes are secondary users. Select node 5 is as a selfish node and node 1, node 2, node 3, nodes 4 are neighboring secondary users. Node 1, node 2, node 3 and node 4 are actual occupied channel are six, two, five, and two respectively. They send to the information of channel to target node is same that is occupied channels and number of send channel to the target node is same. But node 5 is actually occupied channels are five, and it broadcast fake channel lists to its neighboring SU's is nine. Remaining four channels are reserved for future use. So, total detected fake channels are four.

2. Simulation

The conducted the simulation using MATLAB to verify the efficiency of COOPON. The efficiency is measured by a detection rate, which is the proportion of the number of selfish SUs detected by COOPON to the total number of actual selfish SUs in a CR network. The efficiency is measured by a detection rate as follows,

$$\text{Detection Rate} = \frac{\text{Number of detected SSUs}}{\text{Number of actual SSUs}}$$

In simulation, one SU can have two to five one-hop neighboring SUs. The experiment was performed under various selfish SU densities in a CR network.

3. Results

The simulation with a cognitive radio network with total 100 nodes, select selfish nodes are 15 denoted by N_selfsh_nodes. The COOPON detection technique is applied for three neighboring nodes denoted by Ng, shown in figure 2. The previous neighboring nodes consider as one denoted as Ng_prev and the next neighboring nodes are consider as two denoted as Ng_next.

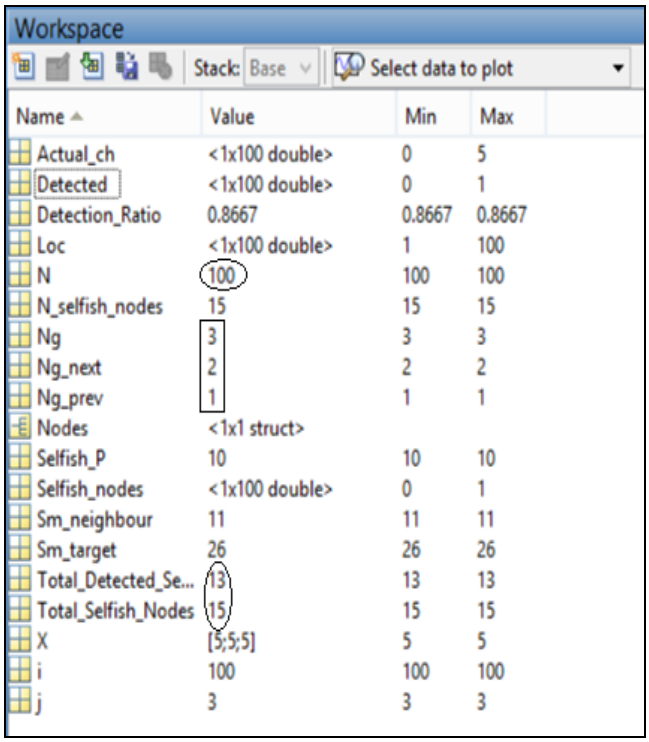

Figure 2

Shown in below table 1, taken nodes for simulation are N1 to N100. Nodes N1, N2, N3, N5, and N6 … N100, all send the information to its neighboring three nodes. Nodes N1, N2, N3, N4, and N6 are actual occupied channels and send the information to neighboring nodes (LSU) are same. Node N5 is actually used channels are 6 and it send the information to LSU is also 6. But N4 is actually used number of channels are 7, and send the fake information to neighboring users (LSU) are 9(Ng-Prev), 11(Ng-Next) and 8(Ng-Next). The detected selfish nodes are denoted by 1 and others are 0, shown in last row of table. Hence, we can say that the N5 is selfish attacker.

Table 1

nodes	N1	N2	N3	N4	N5	N6	…	N100
actual	3	5	2	7	6	4		9
Send info to LSU	3	5	2	9	6	4		9
	3	5	2	11	6	4		9
	3	5	2	8	6	4		9
From LSU	-	3	5	2	7	6		-
	5	2	7	6	4	-		-
	2	9	6	4	-	-		-
detected	0	0	0	1	0	0		0

Detection rate is evaluated shown in figure 3. Detected selfish nodes are 13 but actual selfish nodes are 15. So, the value of detection rate is 0.8667 (86.67%) shown in figure 4 denoted by black dot.

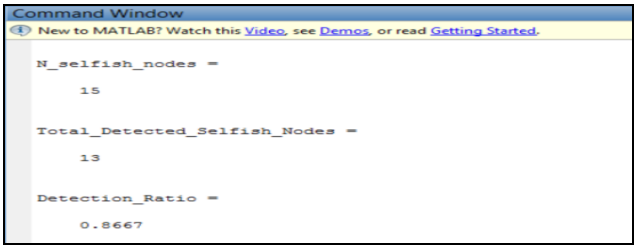

Figure 3

In Figure 4 see that the number of SUs (SU density) taken on X-axis has an effect on detection rate taken on Y-axis. However, the detection rate is very sensitive to selfish SU density. When the density of selfish SUs in the CR network increases, the detection accuracy decreases rapidly. Shown in figure selfish density 10 to16, detection rate decreases rapidly. This problem occurs due to, it is a higher possibility that more than one selfish SU exists in a neighbor with higher selfish node density. They can exchange wrong channel allocation information. Obviously it is a higher possibility that a wrong decision can be made with more faked exchanged information.

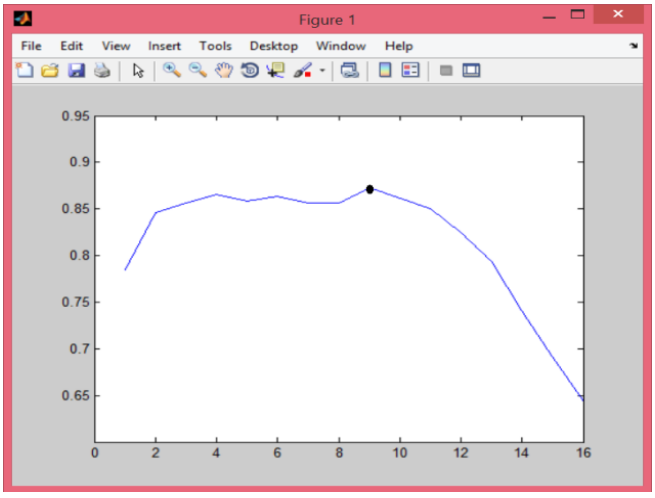

Figure 4

4. Conclusion

The result shows that, the selfish detection rate is totally depending on secondary user density and number of neighboring nodes taken in COOPON system. There is three neighboring nodes are used then detection rate is 86%. Selfish user density is affected on detection rate. It is inversely proportional to the detection rate accuracy. In COOPON system number of neighboring nodes are increases, it may be increase detection rate accuracy.

References

[1] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University, "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks", IEEE Network, 0890-8044, May 2013

[2] Zhou Yuan, DusitNiyato, Husheng Li, Ju Bin Song, and Zhu Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks", IEEE Journal on selected areas in communications, Vol. 30, NO. 10,November 2012.

[3] R. Chen, J.-M. Park, and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE JSAC, vol. 26, no. 1, Jan. 2008, pp. 25–36.

[4] Manman Dang, Zhifeng Zhao, and Honggang Zhang, "Optimal Cooperative Detection of Primary User Emulation Attacks in Distributed Cognitive Radio Network ", IEEE 8th International Conference on Communications and Networking in China (CHINACOM), 2013.

[5] TarunBansal, Bo Chen and PrasunSinha, "FastProbe: Malicious User Detection in Cognitive Radio Networks Through Active Transmissions", IEEE Network, 2014

[6] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks," in Proc. Performance Computing and Communications Conference (IPCCC), Scottsdale, AZ, Dec. 2009.

[7] S. Umanayaki1, M. Sabari Devi2, S. Regina3, " Finding an emulation attack in cognitive radio",International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.03, Special Issue No. 02, February 2015 ISSN (online): 2348 – 7550