

# **PERFORMANCE ANALYSIS FOR SELFISH ATTACK DETECTION USING COOPON TECHNIQUE**

Shital. S. Patil<sup>1</sup> and Prof. A. N. Jadhav<sup>2</sup>

**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 neighbouring 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 neighbouring nodes using MATLAB R2012a (version7.14.0.739).

**Keywords –** Cognitive Radio, Selfish Attacks, COOPON, MATLAB

## **I. INTRODION**

Cognitive Radio Networks (CRN's) is an intelligent network. To make a better spectrum utilisation cognitive radio adapt to changes in their network. CRN's solve the spectrum shortage problem. It is allowing unlicensed users to use spectrum band of licensed user without interference. Licensed users are known as primary users and un-licensed users are secondary users. Primary user send information through a licensed spectrum band, it mostly 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. They detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are active, the secondary user should release the channel. An Empty channel also known as spectrum holes.

IN CR wireless networks numbers of attacks are present namely Primary User Emulation attack (PUE), Selfish Attack, Malicious Attack, Byzantine Attack (i.e., Spectrum Sensing Data Falsification). They cannot offer efficient security. CR attacks are a serious security problem. They significantly degrade the performance of cognitive radio network. In PUE attack, attacker transmits an emulated primary signal during a spectrum sensing interval. If some attackers are performs the PUE attack for its selfish own purpose, called as selfish attacker. CR nodes compete 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 channel information to the neighbouring secondary user. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels.

CR technology is works in two steps. First, for unlicensed secondary users (SU's), it searches for available spectrum bands by a spectrum sensing technology. If the licensed primary user (PU) is not using the spectrum bands then they are considered as available. Second, available channels will be allocated to unlicensed SU's by dynamic signal access behaviour. Whenever the SU is recognise that the PU is present in the CR network, and then they will

<sup>1</sup> *Department of ENTCT, D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India*

<sup>2</sup> *Department of ENTCT, D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India*

immediately release the licensed bands. Selfish attack is carried out when SU's share the sensed available channels to neighbouring secondary users. Each SU periodically informs its neighbouring SU's of current available channels by broadcasting channel allocation information. They are sent the information about the number of available channels and channels in use. In this case, a selfish SU broadcasts faked channel allocation information to other neighbouring SU's. They occupy all or a part of the available channels. Thus, these selfish attacks degrade the performance of a CR network significantly.

To detect the selfish cognitive radio attack cooperative neighbouring 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 for detection method to broadcast and exchange managing information and parameters to manage the CR network among secondary ad-hoc users. By the cooperation of other legitimate neighbouring SU's the COOPON will detect the attacks of selfish SU's. All neighbouring SU's exchange the channel allocation information to the one hop neighbouring secondary nodes. First select the any one target node. The neighbouring user is both received from and sent to the target SU's. Then, each individual SU will compare the total number of channels reported by the target node to the total number of channels reported by all of the neighbouring SU's. Then legitimate SU's will recognize the target SU is a selfish attacker or not.

## II. ATTACKS IN CRN

For design and analysis of secure distribution system, trust is an important feature. Trust and security in Cognitive Radio Networks are always interlinked; both are complementary and mutually inclusive to each other. The attacks on CRN classify based on the layers in which the attack can occur. At the Physical layer, Primary User Emulation attack (PUE), Objective Function Attacks, Jamming, etc. At the Link layer include Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DOS Attack (CCSD), etc. At the Network layer, Hello Flood Attack and Sinkhole Attack are discussed. At the Transport layer, Lion attack is well known. Some of these attacks might work on different layers. Such as, jamming, this can be launched at physical or MAC layers.

CR attacks are a serious security problem because they significantly degrade the performance of cognitive radio network. During a spectrum sensing interval the PUE attacker transmits an emulated primary signal. Some attacker is called selfish attacker, reason is that it performs the PUE attack for its selfish own purpose. CR nodes compete to sense available channels. Some SUs are selfish; they are tried to occupy one or more available channels.

They send the fake information to neighbouring users is that they occupy more channels than they are actually occupied. Usually selfish CR attacks are carried out by sending fake signals or fake channel information to legitimate SU. If a SU recognizes the presence of a PU by sensing the signals of the PU, then SU is immediately release the licensed channel.

### A). Primary User Emulation Attack (PUEA)

The major technical challenges associate with spectrum sensing. In spectrum sensing the mostly problems are related to the exactly distinguishing primary user signals from secondary user signals. Primary user emulation (PUE) is one of the most serious attacks for CR networks. It can significantly increase the spectrum access failure probability. In CR network, primary user has higher the priority to access the channel. If a primary user begins to transmit across a frequency band occupied by a secondary user then SU is required to leave that particular specific spectrum band immediately. When there is no primary user activity present within a frequency range, all the secondary users possess equal rights to the unoccupied frequency channel. In the presence of energy detection method, a secondary user can recognize the signal of other secondary users but cannot recognize the signal of primary users. When a signal is recognized, which is detected when a secondary user is on, otherwise it concludes that the signal is of a primary user. PUE attack is classified namely a selfish PUE attack and malicious PUE attack.

**a.** Selfish PUE attacks -A selfish PUE attack is emulating the signal characteristics of the primary user. When a selfish PUE attacker detects a free spectrum band, they send fake information to other SU, and they prevent other secondary users from using that band.

**b.** Malicious PUE attacks -Malicious PUE attack is also emulating the signal characteristics of the primary user. It is similar to denial of service attack. It prevents the legitimate secondary users from detecting and using the free spectrum bands.

## III. SELFISH ATTACK

In cognitive radio network, nodes compete 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 sent by the selfish SU. Thus, these selfish attacks degrade the performance of a CR network. Selfish attacks are different depending on what and how they attack in order to pre-occupy CR spectrum resources. Secondary users are of two types namely Legitimate Secondary User (LSU) and Selfish Secondary User (SSU). There are three different types of selfish attacks. The focus is given on the study of different types of selfish attacks and their detection mechanism.

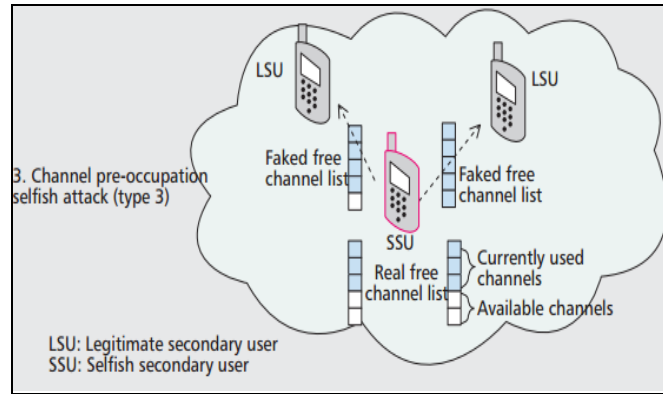


Figure 3.1 Channel Pre-occupation selfish attack

Attacks can occur in the communication environment that is used to broadcast the current available channel information to neighbouring 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 neighbouring SU's.

#### IV. DETECTION MECHANISM: COOPON

To detect the selfish attack cognitive radio cooperative neighbouring cognitive radio nodes (COOPON) detection techniques is used. COOPON is designed for CR ad-hoc networks with multiple channels. COOPON is used for only one case, and the case that channel allocation information is broadcast for transmission. To broadcast and exchange managing information and parameters in CR network, the common control channel (CCC) is used. It is manage the CR network among secondary ad-hoc users. Focus on selfish attacks of SUs toward multiple channel access in cognitive radio ad-hoc networks. In this detection mechanism assume that an individual SU use multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighbouring Sus. They will send a larger number of channels in current use than they actually occupied, to reserve available channels for later use. The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighbouring SUs.

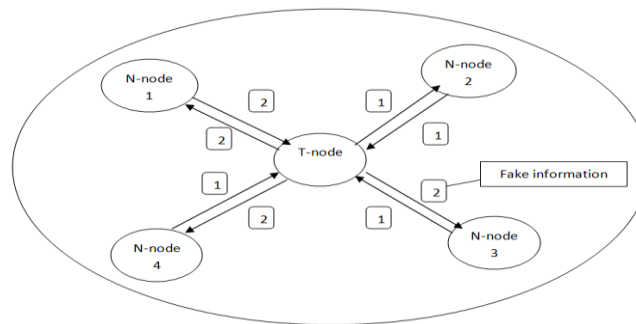


Figure 4.1: Selfish attack detection mechanism

A cooperative neighbouring cognitive radio node (COOPON) is designed for an ad-hoc communication network. An ad-hoc communication network based on exchanged channel allocation information among neighbouring SU's. As shown in figure 4.1, Target node (T-node) is taken at centre and four Neighbouring nodes namely N-node 1, N-node 2, N-node 3 and N-node 4 are taken around the T-node. T-Node is basically a SU, and the other SUs, N-Node 1, N-Node 2, N-Node 3, and N-Node 4, will scan any selfish attack of the target node (T-Node). The target SU and all of neighbouring users will exchange the current channel allocation information list via common control channel (CCC). Each node is reported to neighbouring node that how many channels are currently in use. Individual

neighbouring nodes will compare the summed numbers sent by all neighbouring nodes to the summed numbers sent by the target node. It helps to neighbouring node to check target SU is a selfish attacker or not. This detection mechanism is carried out through the cooperative behaviour of neighbouring nodes. Once a neighbouring SU is chosen as a target node and the detection action for it is completed, another neighbouring SU will be selected as a target node for the next detection action. This detection procedure will continue until the last SU in a CR network is validated.

**V. SIMULATION ENVIRONMENT**

Simulated estimation with the help of Matlab R2012a software on Windows 8.1 operating system to verify the efficiency of COOPON techniques. The efficiency is verified by using detection rate.

**A). Detection Rate**

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 neighbouring SUs. The experiment was performed under various selfish SU densities in a CR network.

**B). Parameters used for Performance Analysis**

The performance of selfish attack mechanism is analysed on the basis of following metrics:-

1. Detection Rate
2. Throughput
3. Secondary user density
4. Number of neighbouring node
5. Number of Secondary node

**VI. EVALUATION OF DETECTION RATE USING COOPON**

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 neighbouring nodes denoted by Ng, shown in figure 9.2.4. The previous neighbouring nodes consider as one denoted as Ng\_prev and the next neighbouring nodes are consider as two denoted as Ng\_next.

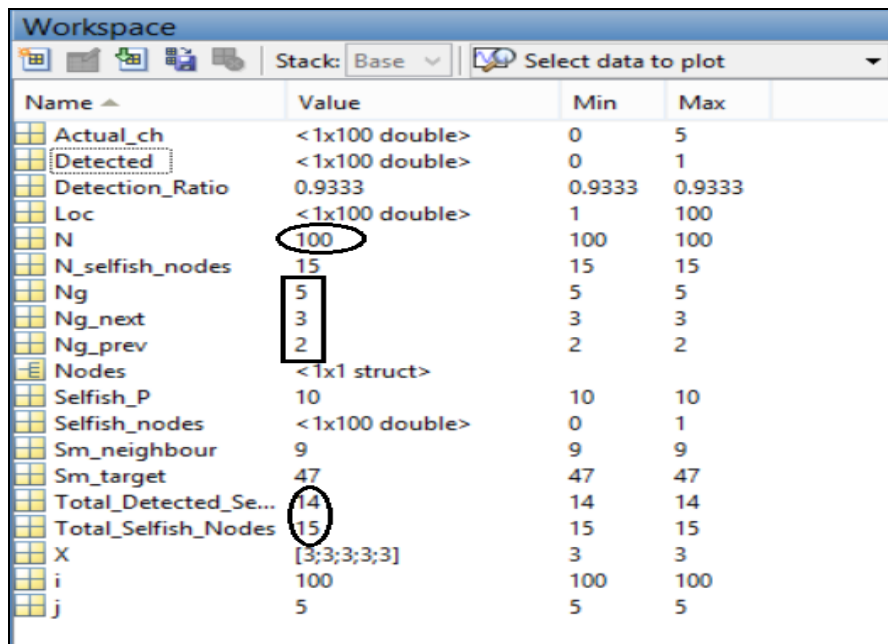


Figure 6.1:Parameter Representation using MATLAB

| Nodes            | N1 | N2 | N3 | N4 | N5 | N6 | N7 | ... | N100 |
|------------------|----|----|----|----|----|----|----|-----|------|
| Actual occupied  | 2  | 7  | 4  | 3  | 6  | 5  | 1  |     | 8    |
| Send info to LSU | 2  | 7  | 6  | 3  | 6  | 5  | 1  |     | 8    |
|                  | 2  | 7  | 9  | 3  | 6  | 5  | 1  |     | 8    |
|                  | 2  | 7  | 5  | 3  | 6  | 5  | 1  |     | 8    |
|                  | 2  | 7  | 8  | 3  | 6  | 5  | 1  |     | 8    |
|                  | 2  | 7  | 7  | 3  | 6  | 5  | 1  |     | 8    |
| From LSU         | -  | -  | 2  | 7  | 8  | 3  | 6  |     | -    |
|                  | -  | 2  | 7  | 5  | 3  | 6  | 5  |     | -    |
|                  | 7  | 9  | 3  | 6  | 5  | 1  | -  |     | -    |
|                  | 6  | 3  | 6  | 5  | 1  | -  | -  |     | -    |
|                  | 3  | 6  | 5  | 1  | -  | -  | -  |     | -    |
| Detected         | 0  | 0  | 1  | 0  | 0  | 0  | 0  |     | 0    |

Table 6.1: COOPON using 5 neighbouring nodes Figure 6.2: COOPON mechanisms with neighbouring nodes are five

In figure 6.2 shows actual COOPON mechanism with neighbouring nodes 5. We select N3 is target node and N1, N2, N4, N5 and N6 are neighbouring nodes of target node. They send the information about occupied channels through the common control channel. The all currently used channels in the target node and neighboring nodes are summed up in two steps Channel target\_node and Channelneighboring\_node. Then Channel target\_node will be compared to Channel neighboring\_node. According to the example in Figure 9.2.5. Channel target\_node is 35 (6+9+5+8+7)[which are taken in box] and Channel neighboring\_node is 23 (2+7+3+6+5). Because  $35 > 23$ , the target secondary node is identified as a selfish attacker. In other words, the checked target node inflates its currently used channels number.

**VII. RESULT AND ANALYSIS**

**A). COOPON using MATLAB**

We conducted the simulation using MATLAB to verify the efficiency of COOPON techniques. The efficiency is measured by a detection rate which is depending on number of detected selfish secondary nodes and actual selfish secondary nodes.

In MATLAB simulation we taken as total 100 secondary nodes. Figure 7.1 show nodes are N8 to N21. They are actually occupied channels are 4, 3, 1, 1, 3, 4, 0, 3, 2, 1, 4, 0, 0 and 3 respectively. Nodes N8, N9, N11, N12, N13, N14, N15, N17, N19, N20 and N21 are send the information to the neighbouring user is same as it is actually occupied channels. Nodes N10, N11 and N10 are actually occupied channels are 1, 2, and 4. But they are send fake information to the neighbouring user.

Figure 7.2 shows that, detected selfish secondary users denoted by ‘1’ and others denoted by ‘0’, that is nodes N10, N16 and N18 are the selfish attackers.

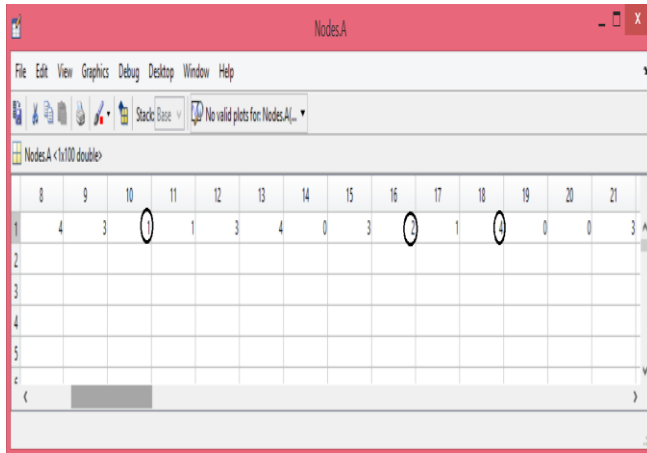


Figure 7.1: Actual no of channels occupied

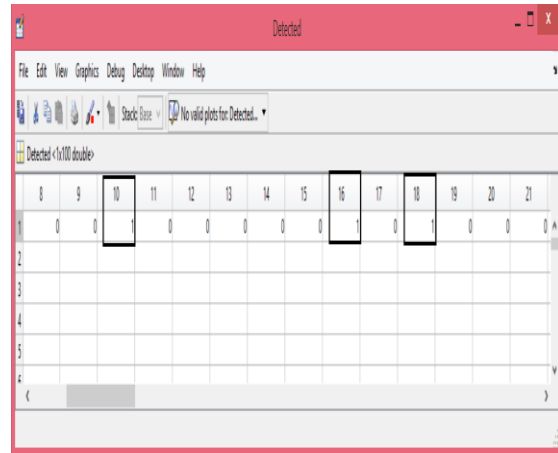


Figure 7.2: Detected Nodes



Figure 7.3: Target node send fake information to Ng Nodes.

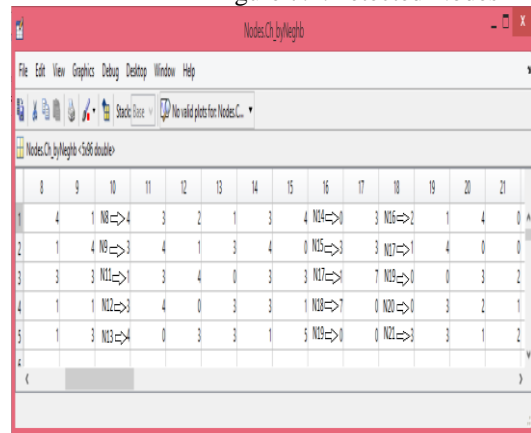


Fig. 7.4 : From Neighbouring Node to Target node

For simulation we select two previous nodes and three next nodes of target node. First select a target node N10, the channel information send from the neighbouring node N8, N9, N11, N12 and N13 is 4, 3, 1, 3 and 4 respectively. Second target node is N16, the channel information send from the neighbouring node N14, N15, N17, N18 and N19 is 0, 3, 1, 7 and 0 respectively. Third target node is N18, the channel information send from the neighbouring node N16, N17, N19, N20 and N21 is 2, 1, 0, 0 and 3 respectively, shown in figure 7.4.

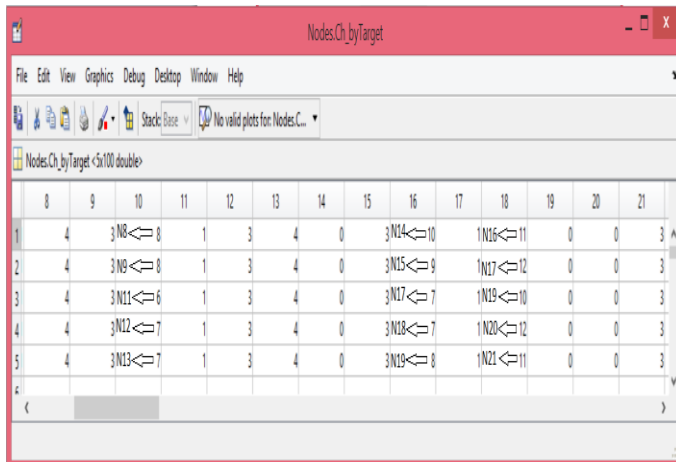


Figure 7.5 From Target node to Neighbouring Node

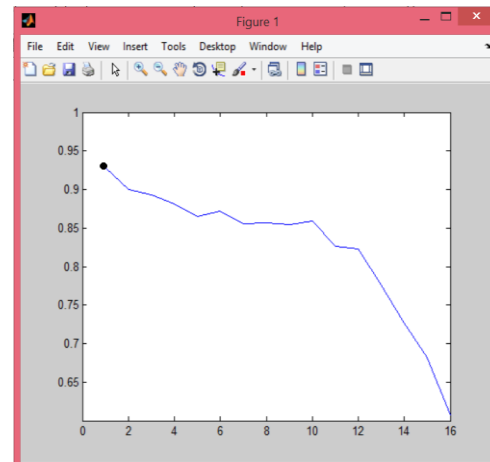


Figure 7.6: Detection Ratio vs. secondary user density

As shown in fig.7.5, target nodes are send the channel information to the neighbouring node. Actual occupied channel by N10 is only 1, but it broadcast the fake channel information (number of extra occupied channels) to the neighbouring node N8, N9, N11, N12 and N13 is 8, 8, 6, 7 and 7 respectively. Actual occupied channel by N16 is 2, but it broadcast the fake channel information to the neighbouring node N14, N15, N17, N18 and N19 is 10, 9, 7, 7 and 8 respectively. As the same way, actual occupied channel by N18 is only 4, but it broadcast the fake channel information to the neighbouring node N16, N17, N19, N20 and N21 is 11, 12, 10, 12 and 11 respectively.

In Fig. 7.6 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. Here we are taken five neighbouring nodes for COOPON detection techniques then we get detection rate is 0.93 or 93% shown in figure which is denoted by black dot.

**B). Performance analysed when number of neighbouring Nodes (Ng) are changed.**

The experiment was carried out with 3, 5, 7, 9 and 11 neighbouring SUs respectively, the number of channels taken as 100. Two hundred secondary nodes are used in this experiment. From Figure 7.7, we can see that the number of SUs has a trivial effect on COOPON’s detection rate. 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. As shown in table 7.7, the number neighbouring nodes are increases, detection ratio is proportional increases. Three neighbouring in CR network achieve 85% detection ratio. However eleven neighbouring nodes achieve 93% detection ratio that is very high accuracy. Thus, more secondary users in neighbour of a CR ad-hoc network are recommended in order to avoid selfish CR attack.

No. of Nodes=200 No. of channels=100

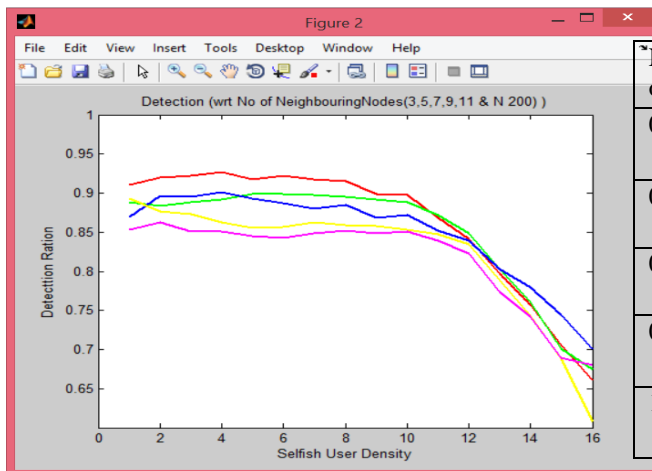


Fig. 7.7: Ng. nodes are changed

| No. Neighboring of nodes | Detection Ratio | Colour |
|--------------------------|-----------------|--------|
| 03                       | 0.85            |        |
| 05                       | 0.86            |        |
| 07                       | 0.89            |        |
| 09                       | 0.90            |        |
| 11                       | 0.93            |        |

Table 7.7: Ng. nodes are changed

**C). Performance analysed when number of Secondary Users are changed**

As shown in fig. 7.8, the detection rate is very sensitive to selfish user density. When the density of selfish SU’s in the CR network is increases, the detection ratio decreases rapidly. The experiment is carried out with 50, 100, 150, 200 and 250 SU’s respectively shown in table 7.8. When numbers of secondary users are less in CR network then we get high accuracy. The secondary users are increases in CRN then detection ratio is decreases inversely. The experiment is carried out with 50 secondary nodes, we get detection ratio 92%. If CR network with 250 secondary users, we get detection ratio is 80%. This problem is occurs is that higher possibility that more than one selfish SU exist in a neighbour with higher selfish node density.

No. of Neighbouring Nodes=03 No. of channels=100

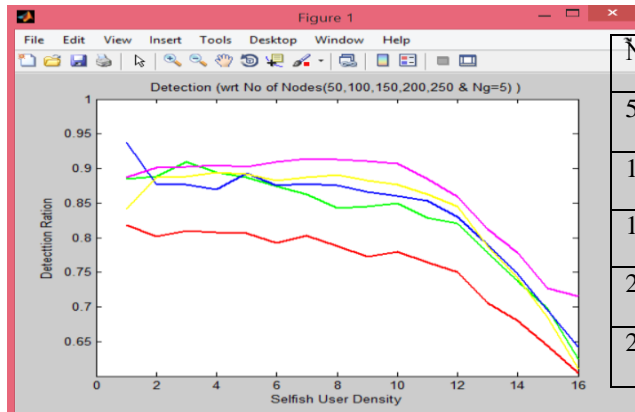


Fig.7.8: Secondary nodes are changed






| No of nodes(SU's) | Detection Ratio | Colour  |
|-------------------|-----------------|---|
| 50                | 0.92            |  |
| 100               | 0.89            |  |
| 150               | 0.87            |  |
| 200               | 0.83            |  |
| 250               | 0.80            |  |

Table 7.8: Secondary nodes are changed

They can exchange wrong channel allocation information. Obviously it is a higher possibility that a wrong decision can be made with more fake exchanged information. Selfish nodes may broadcast faked channel allocation information; it will be more difficult to detect selfish attacks when both information exchanging nodes send fake channel allocation information. Thus the capabilities of detecting attacks will decrease when more selfish nodes exist in a neighbour.

## VIII. CONCLUSION

In channel pre-occupation selfish attack Selfish SU is broadcast fake free channel lists to its one hop neighbouring SU's, show in fig. 3.1. The COOPON detection technique helps to detect selfish SU's, by using cooperation of other legitimate neighbouring SU's, as shown in fig.4.1. The efficiency of COOPON system is measured by a detection rate. The detection rate is totally depending on the available number of neighbouring nodes and secondary users in CRN. In this paper studied, how efficiency of cognitive radio depends on neighbouring nodes and SU's. Shown in fig. 7.7 the detection rate is directly proportional to neighbouring nodes which are taken in COOPON detection. This experiment maximum eleven neighbouring nodes are taken, then get higher detection rate 93%, because a possibility to receive more correct channel information from more neighbouring (legitimate) SU's. As shown in fig.7.8, the number of secondary users is increased, the detection rate is decreased. This problem occurs is that, it is higher probability that more number of selfish SU's exist in CRN. Obviously it is higher possibility that wrong decision can be made, because the more Selfish SU broadcast more faked exchanged information. So, Secondary user increases in CRN, they are reversely affected on efficiency of CR. When 50 secondary nodes exist in CRN is less, then get higher detection rate is 92%. Secondary users increase then detection ratio decreases proportional show in table 7.8.

## REFERENCES

- [1] Minh 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 PrasanSinha, "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. Umanayaki<sup>1</sup>, M. Sabari Devi<sup>2</sup>, S. Regina<sup>3</sup>, " Finding an emulation attack in cognitive radio", International Journal of Advanced Technology in Engineering and Science [www.ijates.com](http://www.ijates.com) Volume No.03, Special Issue No. 02, February 2015 ISSN (online): 2348 – 7550