International Journal of Engineering Research and Technology. ISSN 0974-3154 Volume 10, Number 1 (2017)

Evaluation of Detection rate of Selfish Attack using COOPON Mechanism

Shital.S.Patil
Department of ENTC, D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India

Prof. (Dr.) Ajitsinh N. Jadhav
Department of ENTC, D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India

Prof. Sanjay B. Patil
Department of ENTC, D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India

Abstract: Cognitive radio is one of the wireless basedcommunication technology. This technology is mainly designed to allowthe unlicensed users to utilize the maximum bandwidthavailable in the network. An important consideration to anywireless network is secure communication. In Cognitive radio, 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. But the problem is that some of the secondary users are selfish to occupy all or part of the channels and prohibiting other cognitive radio nodes from accessing these resources, these secondary users is called as selfish attackers. These are a serious security problem because they significantly degrade the performance of a cognitive radio network. Hence, to detect a selfish attacker COOPON (Cooperative neighbouring cognitive radio Nodes) detection technique is used.

COOPON detection technique is designed only for multiple channels with number of neighbouring node and selfish node. It is used to detect selfish attack in cognitive radio ad-hoc network. These paper works focused on achieve very highly reliable selfish attack detection system. Simulation is carried for evaluation of detection rate by varying the parameters are selfish secondary user density, neighbouring nodes, secondary nodes and channels using MATLAB R2012a (version7.14.0.739).

Keywords: Cognitive Radio, Selfish Attacks, COOPON, MATLAB

INTRODUCTION

Cognitive radio (CR) is an opportunistic communication technology. It is designed to utilize the maximum available licensed bandwidth for unlicensed users. Today, we have faced excessive spectrum demands and the need to better utilize the available spectrum. In spectrum management, most of the spectrum is allocated to licensed users for use. CR technology is carried out in two steps. First, it searches for available spectrum bands by a spectrum sensing technology for unlicensed secondary users (SU's)[1]. When the licensed primary user (PU) is not using the spectrum bands, they are considered as available. Second, available channels will be allocated to unlicensed SU's by dynamic signal access behaviour. Whenever the PU is present in the CR network, the SU will immediately release the licensed bands.

CR wireless networks are susceptible to different types of attacks and cannot offer efficient security. Primary user emulation (PUE) is one of the most serious attacks for CR networks, which can significantly increase the spectrum access failure probability. In this dissertation work we focused on the selfish PUE attack. CR nodes complete to sense available channels. But selfish attack are try to occupy all or part of available channels. Usually CR attacks are carried out by sending fake signals and fake channel information. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU do not use the licensed channels.

Selfish attack is carried out when SU's share the sensed available channels. Usually each SU periodically informs its neighbouring SU's of current available channels by broadcasting channel allocation information such as the number of available channels and channels in use [1,2]. In this case, a selfish SU broadcasts faked channel allocation information to other neighbouring SU's in order to occupy all or a part of the available channels. Thus, these selfish attacks degrade the performance of a CR network significantly.

The COOPON will detect the attacks of selfish SU's by the cooperation of other legitimate neighbouring SU's. All neighbouring SU's exchange the channel allocation information to both received from and sent to the target SU. The target SU and its neighbouring SU's are 1-hop

neighbours. 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 neighbouring SU's. Then legitimate SU's will recognize the 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 [1].

COOPON selfish attack detection method is very reliable since it is based on deterministic information. However, COOPON has a drawback. When there is more than one neighbouring selfish node, COOPON may be less reliable for detection, because two neighbouring nodes can possibly exchange fake channel allocation information. But if there are more legitimate neighbouring nodes in a neighbour, a better detection accuracy rate can be expected, because more accurate information can be gathered from more legitimate SU's.

SELFISH PUE ATTACKS

[Primary User Emulation Attack (PUEA)]:

One of the major technical challenges associated with spectrum sensing is the problem of exactly distinguishing primary user signals from secondary user signals. In CR network, primary users possess the priority to access the channel. If a primary user be- gins to transmit across a frequency band occupied by a secondary user, it is required to leave that particular specific spectrum band immediately. Conversely, when there is no primary user activity present within a frequency range, all the secondary users possess equal rights to the unoccupied frequency channel. Based on these paradigms, there exists the potential for malicious secondary users to mimic the spectral characteristics of the primary users in order to gain priority access to the wireless channels occupied by other secondary users. This scenario is referred as Primary User Emulation, which is carried out by a malicious secondary user emulating a primary user or masquerading itself as a primary user. As a result the attacker is able to have the bands of a spectrum. In the presence of energy detection, 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, it is assumed that the signal is that of a secondary user only; otherwise it concludes that the signal is of a primary user. Depending on the motivation of the attacker, PUE attack can be a selfish PUE attack or a malicious PUE attack.

A selfish PUE attack tries to maximize its own spectrum usage. When a selfish PUE attacker detects a free spectrum band, they prevent other secondary users from using that band by emulating the signal characteristics of the primary user.

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 send 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).

DETECTION MECHANISM: COOPON

To detect the selfish cognitive radio attack called 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 to broadcast and exchange managing information and parameters to 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. 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 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 neighbouring SUs.

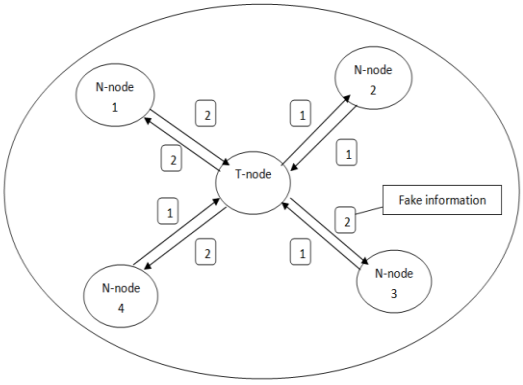

Fig1: Selfish attack detection mechanism

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 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.

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. Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals. COOPON selfish attack detection method is very reliable since it is based on deterministic information. However, COOPON has a drawback. When there is more than one neighbouring selfish node, COOPON may be less reliable for detection, because two neighbouring nodes can possibly exchange fake channel allocation information. But if there are more legitimate neighbouring nodes in a neighbour, a better detection accuracy rate can be expected, because more accurate information can be gathered from more legitimate SUs.

DETECTION ALGORITHM:

Figure 2 shows the proposed selfish attack detection algorithm flow chart of COOPON. All currently used channels in the target node and neighbouring nodes are summed up in two steps Channel target node and Channel neigbouring node. Then Channel target node will be compared to Channel neigbouring node. According to the example in Fig. 2, Channel target node is 7 (2+1+2+2) and Channel neigbouring node is 5 (2+1+1+1). Because 7 > 5, the target secondary node is identified as a selfish attacker. The checked target node inflates its currently used channels number. Then COOPON will check the next neighbouring node after it selects one of the unchecked neighbouring secondary nodes as a target node.

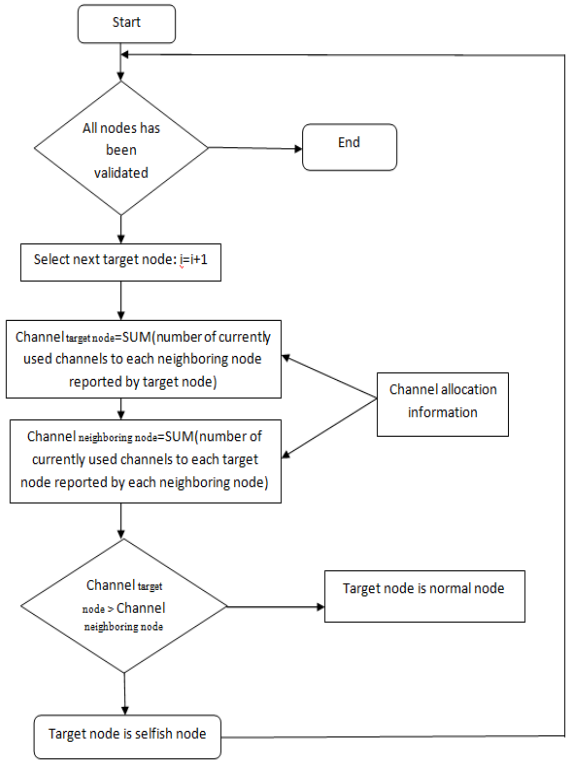

Fig. 2: Selfish attack detection algorithm

The flow chart shown in figure 2 shows the proposed selfish attack detection algorithm of COOPON. All currently used channels in the target node and neighbouring nodes are summed up in two steps Channel target_node and Channel neigboring_node. Then Channel target_ node will be compared to Channel neigboring_node. 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 neighbouring SUs. Then legitimate SU's will recognize the target SU is a selfish attacker or not.

SIMULATION ENVIRONMENT

The simulation is conducted 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.

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,

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

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

RESULT AND ANALYSIS

To detect selfish attacker COOPON detection technique is used. The proposed work provides COOPON system which detects multiple selfish attacks using MATLAB R2012a (version7.14.0.739) software on windows 8.1 operating system.

PART I: Performance analysed when number of Neighbouring Nodes (Ng) are changed.

The performance shows that, how the number of neighbouring nodes are affected on efficiency of cognitive radio network.The simulation is carried out by varying number of neighbouring nodes with keeping constant number of secondary nodes and number of channels.

Case I:
i) Number of neighbouring nodes 3, 5, 7, 9, 11.
ii) Number of secondary nodes are 100
iii) Number of channels are 100

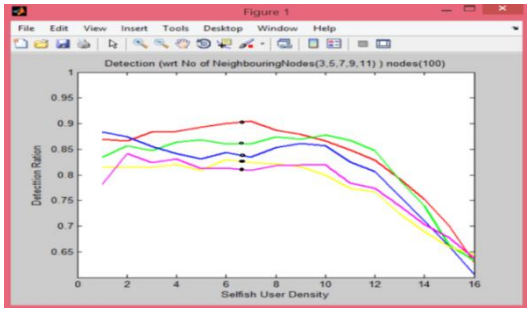

Fig 3: Ng. nodes 3,5,7,9,11. Ch:100

As shown in above figure 3, the performance is analysed by varying number of neighbouring nodes are 3, 5, 7, 9 and 11 respectively and number of secondary nodes and the number of channels are kept constant. It is seen that the selfish user density has an effect on COOPON's detection rate. As shown in table 1, AS the number neighbouring nodes are increases, detection ratio is increases. When the neighbouring nodes are 3 in CR network, achieve 81% detection ratio. However the number of neighbouring nodes are 11, they achieve 90% detection ratio that provides high accuracy

No of Ng nodes	Detection Ratio	Colour
03	0.77	
05	0.83	
06	0.85	
09	0.87	
11	0.89	

Table 1: Ng. nodes (3,5,7,9,11), Ch:100

Case II:

i) Number of neighbouring nodes 3, 5, 7, 9, 11. ii) Number of secondary nodes are 100
iii) Number of channels are 200

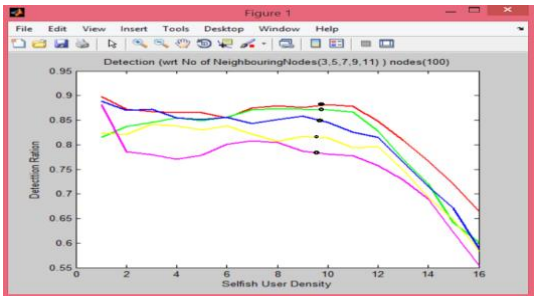

Fig 4: Ng. nodes(3,5,7,9,11), Ch:200

No of Ng nodes	Detection Ratio	Colour
03	0.81	
05	0.83	
07	0.84	
09	0.86	
11	0.90	

Table 2: Ng. nodes(3,5,7,9,11), Ch:200

Number of channels are used in this simulation are 200. As shown in table 2, the number of neighbouring nodes are 3 in CR network achieve 77% detection ratio. However the number of neighbouring nodes are 11 achieve 89% detection ratio. It is observe that, accuracy of system is increases by increasing neighbouring nodes in cognitive network.Thus, more secondary users in neighbour of a CR ad-hoc network are recommended in order to avoid selfish CR attack.

PART II: Performance analysed when number of Secondary Users are changed

The simulation is carried out with number of secondary nodes are 50,100, 150, 200 and 250.

This part is classified on the basis of number of channels which are used in simulation.

Case I:

i) Number of Secondary nodes are 50,100,150,200 and 250

ii) Number of neighbouring nodes are 3

iii) Number of Channels are 100

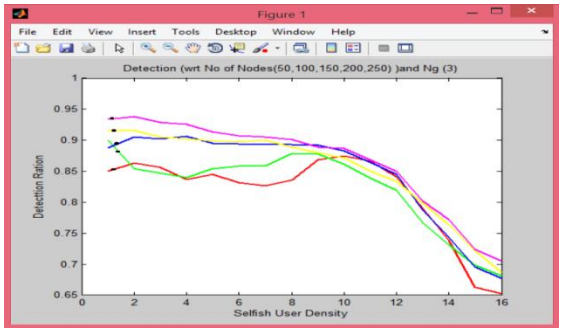

Figure 5: SUs 50,100,150.200,250,Ch:100

No of (SU's)	Detection Ratio	Colour
50	0.93	
100	0.92	
150	0.89	
200	0.87	
250	0.85	

Table 3: SUs 50,100,150,200,150,Ch:100

As shown in figure 5, 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. As shown in table 3, the number of secondary nodes are 50 provides detection ratio is 93% whereas for 250 secondary nodes provides detection ratio is 85%.

Case II :

i) Number of Secondary nodes are 50,100,150,200 and 250

ii) Number of neighbouring nodes are 3

iii) Number of Channels are 200

In this case, for simulation here the number of secondary nodes used are 50,100, 150, 200 and 250 respectively, number of neighbouring nodes are 3 and number of channels are 200 shown in figure 6. The number of secondary node are 50 provides detection ratio is 90% and the number of secondary nodes are 250 provides detection ratio is 81% as shown in table 4. The numbers of secondary nodes are increases, the detection rate decreases.This is because the possibility of more selfish SU exists in a neighbour.

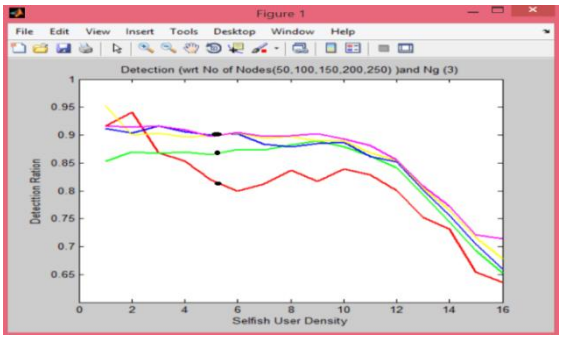

Figure 6: SUs 50,100,150,200,250, Ch:200

No of SU's	Detection Ratio	Colour
50	0.90	
100	0.90	
150	0.90	
200	0.86	
250	0.81	

Table 4: SU 50,100,150,200,250, Ch:200

PART III: Performance analysed when both number of Neighbouring Nodes & Secondary Nodes are proportionally changed

The simulation is carried out with secondary users and neighbouring nodes both are changed in proportionally. The following three cases are classified by changing the number of channels in order.

Case I:

i) Number of secondary nodes are 100, 200, 300, 400 and 500

ii) Number of neighbouring nodes are 3, 6, 9, 12 and 15

iii) Number of Channels are 100.

As shown in figure 7, these simulation used the secondary users are 100, 200, 300, 400 and 500 whereas the neighbouring nodes considered as 3, 6, 9, 12 and 15 respectively. The numbers of channel are used 100. From result it is observed that, the all graphs of respective number of neighbouring nodes are overlap to each other, therefore detection ratio almost same. The detection ratio is achieved in all cases is nearly about 87% shown in table 5

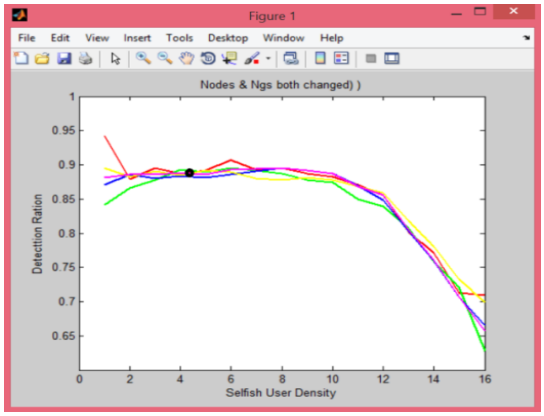

Fig. 7: SU and Ng changed ,Ch:100

No of SU's	No of Ng nodes	Detection Ratio	Colour
100	03	Nearly 0.87 all waves are overlap	
200	06		
300	09		
400	12		
500	15		

Table 5: SU and Ng both changed,Ch:100

.

Case II:

i) Number of secondary nodes are 100, 200, 300, 400 and 500

ii) Number of neighbouring nodes are 3, 6, 9, 12 and 15

iii) Number of Channels are 200.

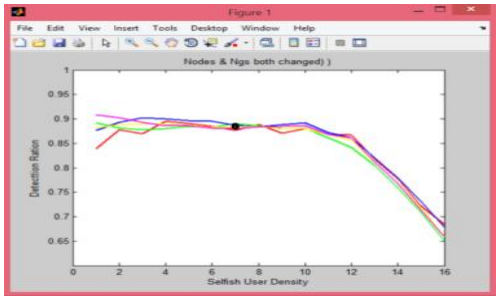

Fig. 8: SU and Ng changed,Ch:200

The numbers of channel are used in simulation 200 as shown in figure 8. This simulation provides detection ratio almost same, it is nearly 87% shown in table 6.

No of SU's	No of Ng nodes	Detection Ratio	Colour
100	03	Nearly 0.87 all waves are overlap	
200	06		
300	09		
400	12		
500	15		

Table 6: SU and Ng changed,Ch:200

The simulation of all cases is carried by changing proportionally number of secondary nodes and numbers of neighbouring nodes. It uses different number of channels are 100 and 200 which classify the case I and case II. As shown in figure 7 and 8 the all waveforms of secondary nodes and neighbouring nodes are overlap. Therefore it is conclude that when secondary nodes and neighbouring nodes are change proportionally, then detection rate get nearly same shown in table 5 and 6.It is found that variations in numbers of channels are not affected on the detection rate of cognitive radio network. Because detection rate is related to detected selfish node and actual selfish secondary nodes. However there is no relation between detection rate and variation in number of channels used.

CONCLUSION

COOPON detection technique is designed only for multiple channels with number of neighbouring node and selfish node. It is used to detect selfish attack in cognitive radio ad-hoc network.

During simulation, the performance is analysed when neighbouring nodes are changed. As numbers of neighbouring nodes are increases in order, detection rate is increases. Therefore to achieve better detection rate, it is necessary to use more neighbouring nodes. Because of there is a possibility to receive more correct channel allocation information from more neighbouring nodes.

The simulation is carried out by varying the secondary nodes, from the results observed that when numbers of secondary nodes are increases, the detection rate is decreases. This is because the possibility of more selfish SU exists in a neighbour. They can exchange wrong channel allocation information; hence the higher possibility of wrong decision can be made with more fake exchanged information. Therefore, it will be more difficult to detect selfish attacks. Thus the capabilities of detecting attacks will decreases when more selfish nodes exist in a neighbour.

The performance is analysed when both number of Neighbouring Nodes & Secondary nodes are proportionally changed. However, during this simulation, detection rate get nearly constant. Because increase in neighbouring nodes provides better detection rate while increase in secondary nodes provides weak detection rate. That is, detection rate is directly proportional to number of neighbouring nodes and inversely proportional to secondary nodes. Therefore, when both are changes proportionally, detection rate remains constant.

The performance is analysed by varying the number of channels, results shows that the number of channels are does not affected on the detection rate. From all results is observe, detection rate is depends on the detected selfish nodes and actual selfish node. There is not any interlinking of detection rate with number of channel.

REFERECNCE

[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, Dusit Niyato, 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] Tarun Bansal, Bo Chen and Prasun Sinha, "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