Detection and Prevention of a Channel occupation selfish attack by SU in Cognitive Radio Networks

Pavan H M
EC Department
BMS College of Engineering
Email id:pan.hm71@gmail.com

Mrs. K Vijaya
Assistant professor, EC Department
BMS College of Engineering
Email id: vijaya.ece@bmsce.ac.in

***Abstract*--**Cognitive radio network (CRN) is a network in which an un-licensed user is secondary user (SU) can use an empty channel in spectrum band of licensed user known as primary user (PU). It is useful as well as harmful too. Because of this some selfish secondary user can use this empty channel through selfish attacks. In this paper we focus on selfish attack in cognitive radio (CR) adhoc network where selfish SU will occupy all or part of resources of multiple channels prohibiting other SU from accessingthe empty channels. Here an attempt is made to detect the selfish node and prevent the selfish attack in CR adhoc network.

Key words*: Cognitive radio networks, Primary user, Secondary user, selfish attack, target node.*

*****

I Introduction

Cognitive radio networks (CRN's) solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. Generally licensed users are known as primary users and un-licensed users are secondary users [1]. When information is send through a licensed spectrum band 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 avoid using the channel [2][3].

As spectrum is made available to unlicensed users, it is expected that all such users will follow the regulatory aspects and adhere to the spectrum sharing and access rules. However, the inherent design of cognitive radios exposes its configuration options to the controlling entity. Controlling entity could be the service provider that deploys the Cognitive Radios (CRs) who needs to frequently change the operation parameters- for example, the operating band, access policies, transmission power and modulation. As a consequence, configurability and adaptability features open up for manipulation as well due to software-based air interface [4][5]. Moreover, problems arise when regulatory constraints are not followed. A CR can be induced to learn false information by malicious or selfish entities, the effect of which can some-times propagate to the entire network. It is apparent that the inherent design, flexibility and openness of opportunistic spectrum usage have opened the way for selfish attacks. [6][7].

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 signals or fake channel information, it is called as channel pre-occupation selfish attack. Channel pre-occupation attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission. Consider a communication environment that broadcasting is carried out through a common control channel (CCC) which is a channel dedicated only to exchanging management information. A selfish SU will broadcast fake free (or available) channel lists to its neighboring SUs. Even though a selfish SU only uses three channels, it will send a list of all five occupied channels. Thus, a legitimate SU is prohibited from using the two available channels [8][9].

In this paper we detect the selfish attack called as channel pre occupation attack in the CRadhoc network by using the channel broadcating information through common control channel (CCC) by the nodes in the adhoc network and finally prevent the selfish attack by the selfish node.

The rest of this paper is organized as follows: Section II gives the brief idea about channel preoccupation attack. Section III introduces detection mechanism to identify the selfish SU node. Section IV presents the prevention method for selfish attack by SU. The simulation scenario and results are discussed in Section V. This paper is concluded in Section VI.

II. Brief idea about Channel Preoccupation Attack

In a cognitive radio adhoc network, 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. The CCC is a channel dedicated only to exchanging managing information and parameters. A list of current channel allocation information is broadcast to all neighboring SUs. The list contains all of other neighboring users channel allocation information. In channel preoccupation a selfish secondary user (SSU) broadcasts separate channel allocation information lists through individual CCC to its neighboring secondary user node. In reality, a list is broadcast once, and it contains the channel allocation information on all of the neighboring nodes. The SU will use the list information distributed through CCC to access channels for transmission. A selfish secondary node will use CCC for

 ISSN: 2321-8169
1252– 1254

selfish attacks by sending fake current channel allocation information to its neighboring SUs.On the other hand, other SUs are prohibited from using available channel resources or are limited in using them.

III. Detection of Selfish SU node in ADHOC Network.

We consider a cognitive radio ad-hoc network. Ad-hoc networks have distributed and autonomous management characteristics. We make use of the autonomous decision capability of an ad-hoc communication network based on exchanged channel allocation information among neighboring SUs. The target SU (T node) and all of its 1-hop neighboring users will exchange the current channel allocation information list via broadcasting on the dedicated channel.

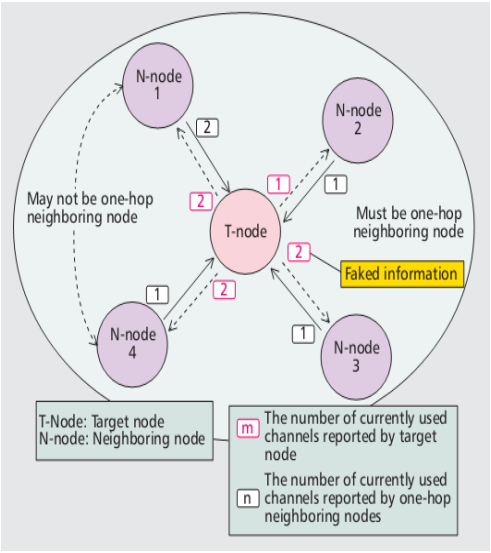

Figure 1: Detection mechanism for selfish attack

All 1-hop neighboring SUs sum the numbers of currently used cannels sent by themselves and other neighboring nodes. In addition, simultaneously all of the neighboring nodes sum the numbers of currently used cannels sent by the target node, T Node. Individual neighboring nodes will compare the summed numbers sent by all neighboring nodes to the summed numbers sent by the target node to check if the target SU is a selfish attacker.

IV. Prevention of Selfish Attack in CR ADHOC Network

After the identification of the selfish secondary user (SSU) node in the CR adhoc network. That SSU node is blocked. An assumption has been made that secondary user (SU) node is assigned three channels. After blocking the selfish node, the channels of the SSU is assigned to the primary user (PU) nodes in that cluster range. Here the availability of free channels in the PU node is checked, example if PU has four channel, it has left with one free channel, so we can make use of that free channel. Again, primary user (PU) node can have five channels, if all five channels have been occupied by it, the selfish attack is prevented just by identifying or blocking the selfish node.

V. Simulation and Results

Here an adhoc wireless network is created by considering size of 50x50 field, which consists of the primary users node and secondary users node. A channel had been created between 1 hop neighboring secondary users. A valid secondary user is treated as the target node and number of channel used by the target node is calculated. Mean while number of channel used by the neighboring node is calculated. 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 to identify the selfish node. If there is any mismatch in the channel information given by that node, then that node is treated as selfish node.

```
Secondary neighbors node S3: 2 1
Secondary Target node S3: 2 2
Secondary neighbors node S4: 1 2
Secondary Target node S4: 1 1
```

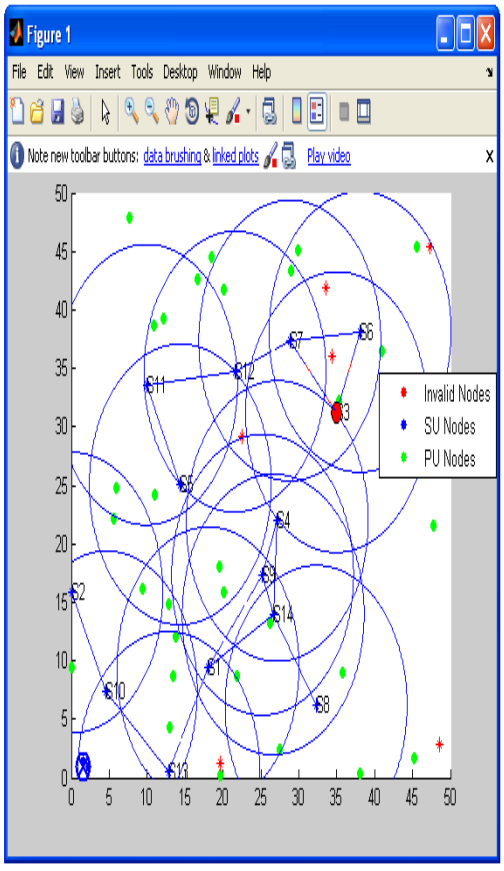

Figure 2: Detection of selfish secondary user node

According to the simulation results secondary user node S3 is the selfish user as it broadcasts fake channel information to the neighboring node.

Node S3 is detected as the selfish node. The selfish attack is prevented by blocking that node as indicated by the black color node. Now, there exist two primary nodes in that cluster range. In the result Temp indicate the number channel in the SU node and pTemp indicate number channel in the PU node, as pTemp is three in one PU node it will be having two free channel. According to the simulation result of detection of selfish node, SSU is using only 2 channels, so that two channels of SSU is assigned to PU node which is indicated by the blue color node.

```
Temp =

     3


pTemp =

     3

Name of the selfish node
S3
Total PU nodes in the range
     2

No.of PU node channels in the range
     5
```

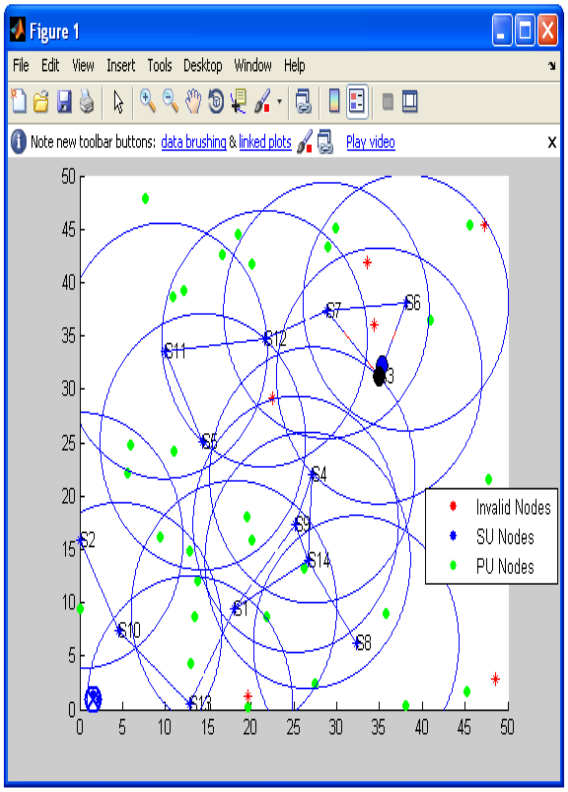

Figure 3: Prevention of Selfish attack by blocking secondary user node

VI. Conclusion

In this work, a focus on selfish attacks of SUs toward multiple channel access in CR Adhoc network is made, have assumed that individual SU accommodates multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring SUs, including the number of channels in current use and the number of available channels, respectively. The selfish SU will broadcast fake information on available channels in order to pre-occupy them. 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 mismatch in the channel allocation information then that target node is treated as the selfish attacker and we prevented the selfish attack by blocking the attacker node and make use of free channels from primary user node.

References

[1] J. Mitola III, “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio”. PhD Thesis, Royal Institute of Technology (KTH), Sweden, 8 May, 2000

[2]Amrita Singh “STUDY ON COGNITIVE RADIO AND COGNITIVE RADIO NETWORK”, international journal of emerging trends in engineering and development, ISSN 249-6149,issue 2 vol.5(july 2012).

[3] Simon Haykin. “Cognitive Radio: Brain-Empowered Wireless Communications”. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 2, FEBRUARY 2005

[4] ZHAOYU GAO, H AOJINZHU, SHUAI LI, ANDSUGUODU,, “Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks,” IEEE Wireless Commun. , vol. 19, no. 6, 2012, pp. 106–12.

[5] Z. Dai, J. Liu, and K. Long, “Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access,” KSII Trans. Internet and Information Systems, vol. 6, no. 10, Oct. 2012, pp. 2455–72.

[6] 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

[7] M. Yan et al., “Game-Theoretic Approach Against Selfish Attacks in Cognitive Radio Networks,” IEEE/ACIS 10th Int’l. Conf. Computer and Information Science (ICIS) , May 2011, pp. 58–61.

[8] K. Cheng Howa, M. Maa, and Y. Qin, “An Altruistic Differentiated Ser-vice Protocol in Dynamic Cognitive Radio Networks against Selfish Behaviors,” Computer Networks, vol. 56, no. 7, 2012, pp. 2068–79.

[9] Dr.AnubhutiKhare, Manish Saxena, Roshan Singh Thakur, KhyatiChourasia, “Attacks & Preventions of Cognitive Radio Network-A Survey”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013