Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2014; 2(3A):373-376 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

Detection and Prevention of a Selfish attack in Cognitive Radio Adhoc Networks

Pavan H M*, K Vijaya
EC Department, BMS College of Engineering, Bull Temple Road, Bangalore, Karnataka, 560019, India

***Corresponding author**
Pavan H M
Email: pan.hm71@gmail.com

Abstract: Cognitive radio network (CRN) is a network in which an un-licensed user is secondary user (SU) can use an empty channel in a 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.
Keywords: Cognitive radio networks, Primary user, Secondary user, selfish attack, target node.

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.

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 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.

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.

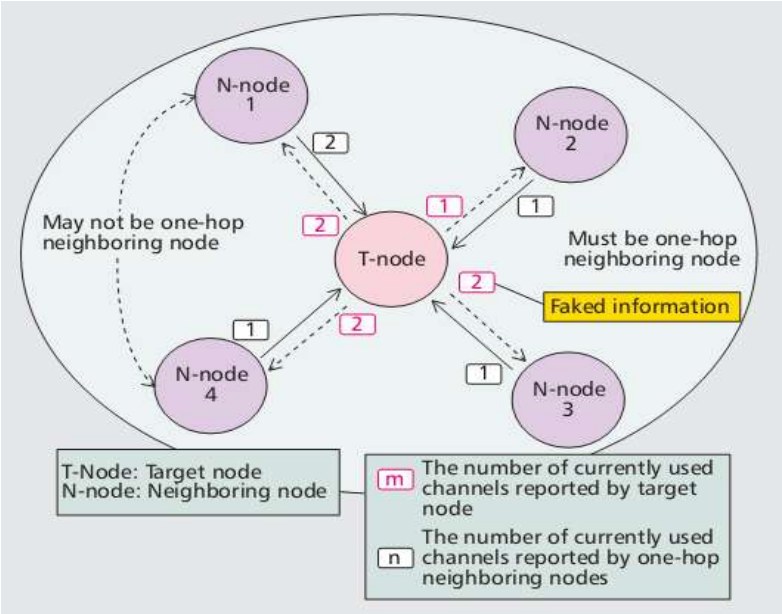


Fig. 1: Detection mechanism for selfish attack

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.

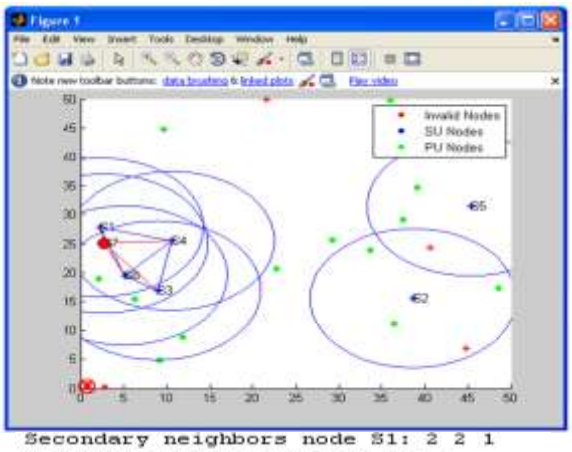
Prevention of Selfish Attack in CR ADHOC Network

After the identification of the selfish secondary user (SSU) node in the CR adhoc network, we block that SSU node, we check for the availability of free channels in the primary user (PU) node in that particular CR range. After finding the free channel in the primary user node we try to make use of necessary free channels from the primary user node in that CR range. Consider a case where secondary user (SU) node is identified as selfish attacker and it may be using 2 or 3 channels. We prevent the attack by blocking the selfish node and try to make use of 2 or 3 channels from the primary user (PU) node which lies inside CR range. Thus we prevent the selfish attack of the SU.If any free channels are not available from the PU node then we prevent the attack just by blocking the selfish node.

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 S1: 2 2 1
Secondary Target node S1: 2 1 2
Secondary neighbors node S4: 2 2 1 2
Secondary Target node S4: 1 2 1 1
Secondary neighbors node S6: 2 2 1 1
Secondary Target node S6: 2 1 1 2
Secondary neighbors node S7: 1 1 1 2
Secondary Target node S7: 2 1 2 1
```

Fig. 2: Detection of selfish secondary user node

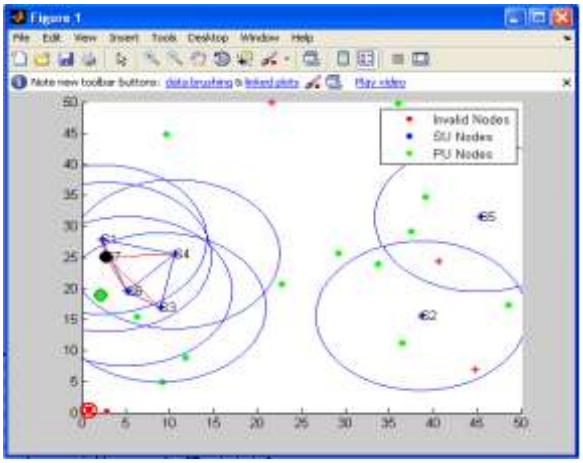


Fig. 3: Prevention of Selfish attack by blocking secondary user node

According to the simulation results secondary user node S7 is the selfish user as it broadcasts fake channel information to the neighboring node. After that we blocked the selfish node S7.

The selfish node S7 needs only one channel but he occupy two channels so we had blocked that node and we try to make use of one free channel from two primary user node (PU) that lies in that CR range. Result show that six free channels are available from both the PU's so we make use of one free channel from any one of the PU and 5 channels are still available in that range.

```
SU node channels
     1

Selfish node channels
     1

Name of the selfish node
S7
Total PU nodes in the range
     2

No.of PU node channels in the range
     6

SU node channels
     0

Selfish node channels
     0

Name of the selfish node
S7
Total PU nodes in the range
     2

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

Fig. 4: Simulation result showing free channels available in PU node

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. Mitola J III; Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD Thesis, Royal Institute of Technology (KTH), Sweden, 8 May, 2000.
2. Singh A; Study on cognitive radio and cognitive radio network. International Journal of Emerging Trends in Engineering and Development, 2012; 5(2): 238-245.
3. Haykin S; Cognitive Radio: Brain-Empowered Wireless Communications. IEEE Journal on Selected Areas in Communications, 2005; 23(2): 201-220.
4. Gao Z, Zhu H, Li S, Du S, Li X; Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks. IEEE Wireless Commun., 2012;19(6): 106–112.
5. Dai Z, Liu J, Long K; Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access. KSII Trans. Internet and Information Systems, 2012; 6(10): 2455–2472.
6. Chen R, Park JM, Reed JH; Defense against Primary User Emulation Attacks in Cognitive Radio Networks. IEEE JSAC, 2008; 26(1): 25–36.
7. Mi Y; Liang D; Lianfen H; Liang X, Jianbin T; Game-Theoretic Approach against Selfish Attacks in Cognitive Radio Networks. IEEE/ACIS 10th International Conference, Computer and Information Science (ICIS), 2011, 16-18 May: 58–61.
8. Howa KC, Maa M, Qin Y; An Altruistic Differentiated Ser-vice Protocol in Dynamic Cognitive Radio Networks against Selfish Behaviors. Computer Networks, 2012; 56(7): 2068–2079.
9. Khare A, Saxena M, Thakur RS, Chourasia K; Attacks & Preventions of Cognitive Radio Network-A Survey. International Journal of Advanced Research in Computer Engineering & Technology, 2013; 2(3): 1002-1006.