Detecting Multiple Selfish Attack Nodes Using Replica Allocation in Cognitive Radio Ad-Hoc Networks

Kiruthiga S
PG student, Coimbatore Institute of Engineering and Technology
Anna University, Chennai, India

Leeban Moses M
Assistant professor, Coimbatore Institute of Engineering and Technology
Anna University, Chennai, India

Abstract - **Cognitive radio is a promising wireless technology which is helpful for the unlicensed users to utilize the free spectrum resources of licensed users. In cognitive radio ad-hic networks, some nodes may be selfish nodes i.e unlicensed users in order to occupy fully or partially available free spectrum resources. There has been done some research on selfish attack detection in CR networks. One of the selfish attacks is the channel pre-occupation selfish which broadcast the fake information among the secondary users (SU). There may be a number of selfish nodes in this type of attack which significantly degrade the network performance. In this paper, we identify a more than one selfish attack nodes in the channel pre-occupation selfish attack using a detection method based on credit risk score. We propose a technique to overcome these selfish nodes called replica allocation technique which improves the network security.**

***Keywords*-Cognitive radio networks, Secondary users, Selfish nodes, Replica allocation.**

I. INTRODUCTION

In Cognitive Radio terminology primary users also called as licensed users and secondary users are called as unlicensed users or cognitive users. The unoccupied frequency band by the primary users called as available spectrum resources or white space .The fundamental task of CR network is to detect the licensed users, if they are present then identify the available spectrum. This process is called spectrum sensing. The objective of spectrum sensing is secondary users should not cause harmful interference to primary users. Secondary users should efficiently identify the spectrum holes for required throughput. For accessing the spectrum in adaptive manner, SUs must constantly monitor the local spectrum and sense spectrum reliability to detect spectrum holes so as to avoid harmful interference to the PUs.

Cognitive radio technology provides a promising solution for the spectrum scarcity issues in wireless networks. It allows the efficient use of the finite usable radio frequency spectrum. In cognitive radio terminology, Licensed users/Primary users are defined as users who have right to use the spectrum band whereas unlicensed users/Secondary users are defined as users who can use the spectrum which is temporarily not used by licensed users, without causing interference to them. At the same time, the security concerns of cognitive radio have received more attentions as the inherent properties of CR networks would pose new challenges to wireless communications. In cognitive radio network, an attack can be defined as an activity that can cause interference to the primary users or licensed users[7].

There are three types of selfish attacks in the cognitive radio networks. They are signal fake selfish attack, signal fake selfish attack in dynamic access behavior and channel pre-occupation selfish attack. In this paper, we identify a multiple number of selfish nodes in the channel pre-occupation selfish attack. In this attack, a selfish cognitive radio nodes try to occupy fully or partially available primary users spectrum resources. The selfish nodes will significantly degrade the network performance.

The channel preoccupation selfish attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission. We 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. Detection of existing selfish technologies is unable to detect more than one selfish nodes and is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals[10].

A. Cognitive radio network architecture

This section provides a detailed description of the CR network architecture. According to the architecture, cognitive radio networks can be classified as Centralized or Distributed networks

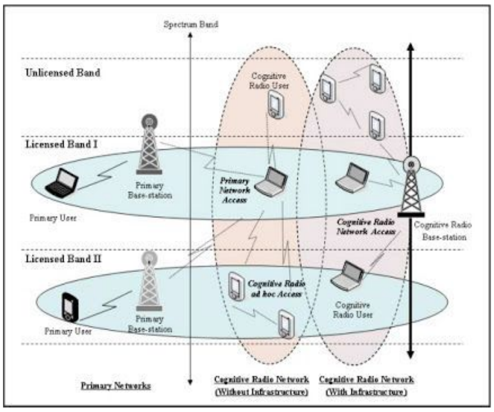

Fig.1. Cognitive Radio Network Architecture

According to operations point of view, cognitive radio networks can be classified as licensed band operation and unlicensed band operation. According to Access type, cognitive radio network can be classified as CR network access, CR ad-hoc access, and primary network access.

B. Centralized cognitive network

As shown in Fig.1, the network is infrastructure oriented. A base station is used to manage each CR user in the network. The base station communicates directly with each user and controls the medium access and the secondary users in the network.

C. Distributed cognitive network

As shown in Fig.1, the CR users communicate with each other in an ad-hoc manner. Information is shared directly between the secondary users who fall within the communication range; otherwise information is shared over multiple hops.

D. Licensed band operation

This band is dedicated for the primary users in the network. It can be used by the unlicensed user if not occupied by the primary user.CR user must vacate the licensed band if the primary user reappears then and move to another vacant spectrum band.

E. Unlicensed band operation

The unlicensed users have the same right to use the unlicensed band. There is no need to vacate the spectrum for the licensed users.

F. Cognitive radio network access

As shown in Fig.1, the cognitive users can share information with their base station on the licensed as well as the unlicensed spectrum band.

G. Cognitive radio ad-hoc access

As shown in Fig.1, the cognitive users in the network can share information with each other in ad-hoc manner on both the licensed and unlicensed spectrum band.

H. Primary network access

As shown in Fig.1, the CR users can also communicate with the primary base station on the licensed spectrum band with an adaptive medium access control protocol.

II. EXISTING METHOD

Cognitive radio has recently attracted a lot of research interest. 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. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won’t use the licensed channels and sending faked PU signals, a selfish SU prohibits other competing SUs from accessing the channels.

Another type of selfish attack is carried out when SUs share the sensed available channels. Usually each SU periodically informs its neighboring SUs of current available channels by broadcasting channel allocation information such as the number of available channels and channels in use. A selfish SU broadcasts faked channel allocation information to other neighboring SUs in order to occupy all or a part of the available channels. For example, even though a selfish SU uses only two out of five channels, it will broadcast that all five channels are in use and then pre-occupy the three extra channels. Thus, these selfish attacks degrade the performance of a CR network significantly. There has been some research on selfish attack detection in conventional wireless communications. It identify a new selfish attack type and introduce a selfish attack detection technique, COOPON (called Cooperative neighboring cognitive radio Nodes), for the attack type[10].

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, which will be investigated by all of its neighboring SUs. 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.

However, COOPON has a drawback. When there is more than one neighboring selfish node, COOPON may be less reliable for detection, because two neighboring nodes can possibly exchange fake channel allocation information. But if there are more legitimate neighboring nodes in a neighbor, a better detection accuracy rate can be expected, because more accurate information can be gathered from more legitimate SUs.

III. PROPOSED METHOD

The proposed method is used to compute the multiple selfish nodes in cognitive radio ad-hoc network and to overcome those selfish nodes using replica allocation. There are three parts to overcome the existing problems. They are

- Detecting multiple selfish nodes in the channel pre-occupation selfish attack.
- Build a SCF tree to achieve a high data accessibility in the presence of selfish nodes.
- Allocating replica to overcome the selfish nodes.

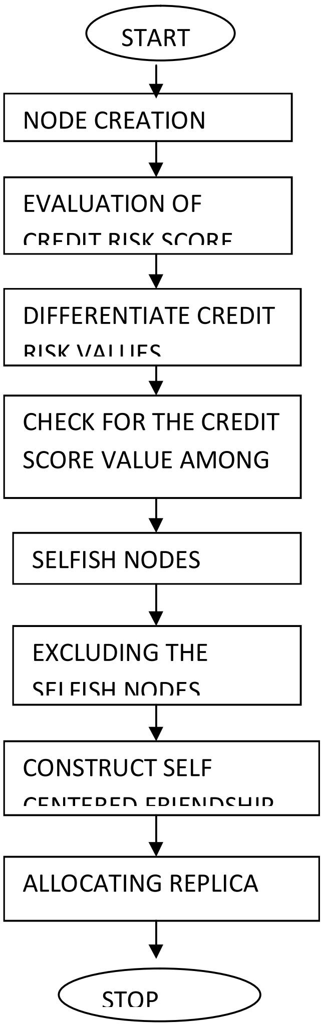

Fig.2. Flow chart of detecting selfish nodes

A. Detecting selfish nodes

The selfish nodes in cognitive radio ad-hoc will try to occupy fully or partially available spectrum resources. These selfish nodes are detected based on credit risk score. To detect the selfish node, first we have to find the shortest path to transmit the packet. To find path in CRN, first all nodes will collect the data about the neighbor nodes. The routing technique used to find paths from source node to destination node for transmitting packets. All possible paths are found by these technique in network but packet transmission done through only shortest path in a network.

Route request (RREQ) and route reply (RREP) are forwarded in between nodes to communicate. Intermediate nodes also used RREQ RREP to communicate with source and destination nodes.

Packet transmission from S node to D node which route is shortest among all possible routes. If any node behaves like selfish node in CRN, then it is not ready to transmit packets to other node. This cause may fail the communication. So in network selfish node detection is needed for efficient communication by applying "degree of selfishness" formula for each node. . Each node should calculate the credit risk score of each node which is connected to it to estimate the degree of selfishness of all its connected node based on the score.

Credit Score=Expected risk/Expected Value

To estimate the degree of selfishness, first describe the features of the selfish node that may lead the selfish replica allocation problem to determine both expected risk and expected value[11].

B. Building Scf-Tree

The SCF-tree based replica allocation techniques are inspired by human friendship management in the real world, where each person makes his/her own friends forming a web and manages friendship by himself/herself. He/she does not have to discuss these with others to maintain the friendship. The main objective of our novel replica allocation techniques is to reduce traffic overhead, to achieve the high data accessibility. If the novel replica allocation techniques can allocate replica without discussion with other nodes then the traffic overhead will decrease.

C. Allocating replica

After building the SCF-tree, a node allocates replica at every relocation period. Each node asks non selfish nodes within its SCF-tree to hold replica when it cannot hold replica in its local memory space. Since the SCF-tree based replica allocation is performed in a fully distributed manner, each node determines replica allocation individually without any communication with other nodes. Since every node has its own SCF tree, it can perform replica allocation at its discretion. It will overcome the selfish nodes to send the information among the secondary users in cognitive radio ad-hoc networks[11].

IV. PERFORMANCE ANALYSIS

The graph shows the efficient NS2 simulation result. The proposed system is mainly used to detect more than one selfish nodes in CRN. In existing COOPON technology is unable to detect numerous selfish nodes in the CRN. Here, the detection of selfish nodes is compared with the existing detection technology COOPON in Cognitive radio network. And also various graph results shown the comparison of packet drop, packet delivery, throughput, routing overhead, end to end delay COOPON technology which is less reliable for detection. In the graph we denoted the proposed technique as enhanced COOPON (ENC-COOPON) or Improved COOPON (ICOOPON)

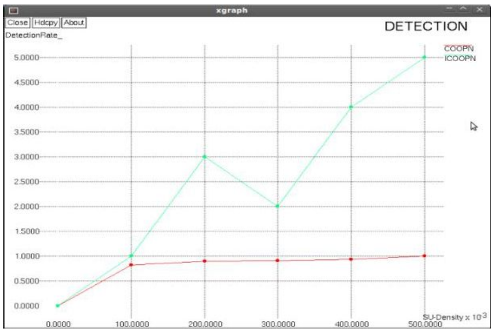

Fig.3. Performance level of selfish node detection

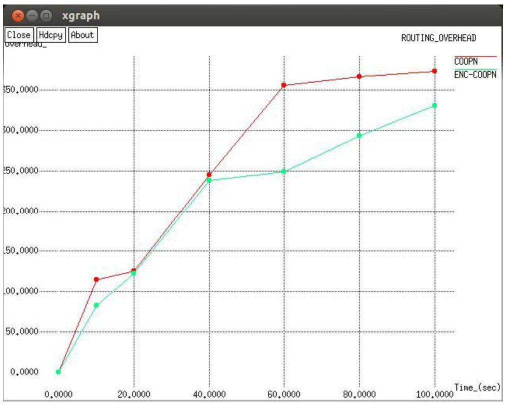

Fig.4. Performance level of routing overhead

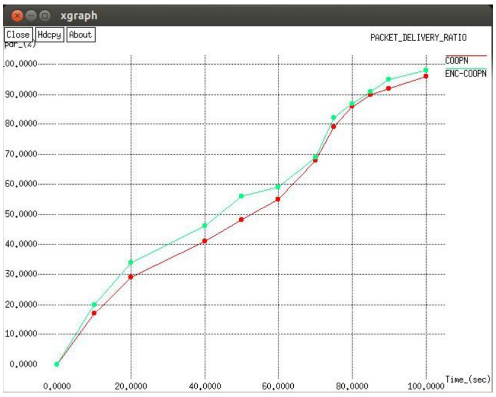

Fig.5. Performance analysis of packet delivery ratio

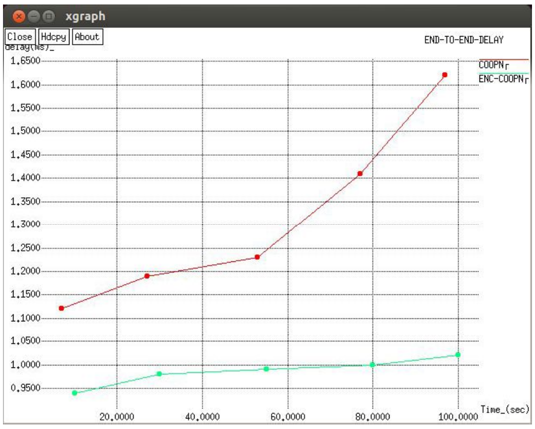

Fig.6. Performance analysis of end to end delay

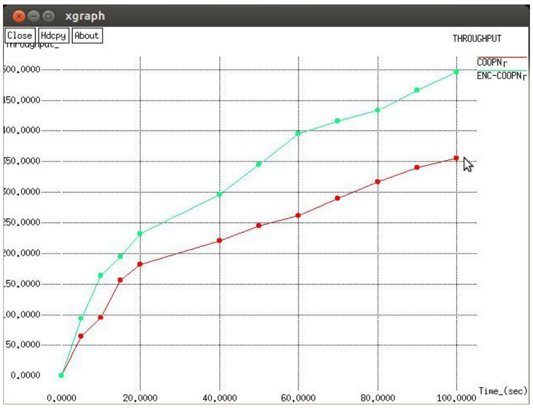

Fig.7. Performance level of throughput

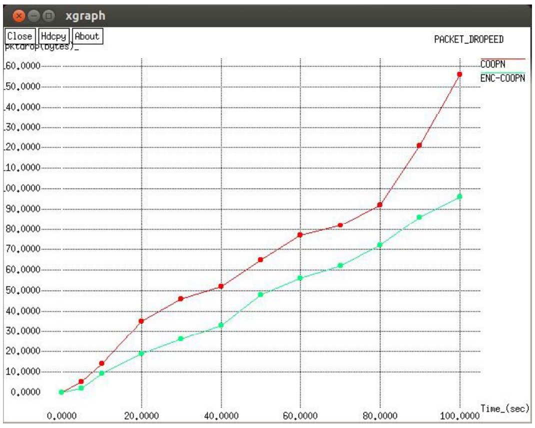

Fig.8. Performance analysis of packet dropped

V.CONCLUSION

The problem in the existing COOPON detection technology in CRN is able to detect to only single selfish node but there is possible of two or more neighboring nodes to be a selfish node in CRN. In this paper, we have identified the multiple selfish node attacks and overcome these selfish nodes using replica allocation technique. The proposed method detects multiple selfish nodes in the channel pre-occupation attack using credit risk score.

This technique is mainly implemented in this paper is for cognitive radio ad-hoc networks. This detection method is very reliable and shown a better detection accuracy rate with comparison of the existing detection technology COOPON as well as the packet drop, packet delivery, throughput, end to end delay, routing overhead also compared with the COOPON technology which results shown better than the existing technology.

REFERENCES

[1] X. Tan and H. Zhang, "A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 9, Sept. 2012, pp. 1998–2016.

[2] C.-H. Chin, J. G. Kim, and D. Lee, "Stability of Slotted Aloha with Selfish Users under Delay Constraint," *KSII Trans. Internet and Info. Systems*, vol. 5, no. 3, Mar. 2011, pp. 542–59.

[3] S. Li *et al.*, "Location Privacy Preservation in Collaborative Spectrum Sensing," *IEEE INFOCOM'12*, 2012, pp. 729–37.

[4] Z. Gao *et al.*, "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] H. Hu *et al.*, "Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 12, Dec. 2012, pp. 3061–80.

[7] 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.

[8] 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.

[9] K. Cheng Howa, M. Maa, and Y. Qin, "An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks Against Selfish Behaviors," *Computer Networks*, vol. 56, no. 7, 2012, pp. 2068–79.

[10] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University, "Selfish Attacks and Detection in Cognitive Radio Ad-hoc Networks," IEEE Network, vol. 27, no. 3, 2013, pp. 46-50.

[11] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, Fellow," Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network," IEEE Transactions on Mobile Computing, Vol. 11, No. 2, February 2012.

[12] Tarun Bansal, Dong Li, and Prasun Sinha, "Opportunistic Channel Sharing in Cognitive Radio Networks," IEEE Transactions on Mobile Computing, Vol. 13, No. 4, April 2014.