Performance study of different types of Selfish Attack in Cognitive Radio Ad-Hoc Networks

Shital.S.Patil¹, A.N.Jadhav², Vivek T. Patil³

¹Department of ENTC, D.Y. Patil College of Engineering & Technology, Kolhapur
²Department of ENTC, D.Y. Patil College of Engineering & Technology, Kolhapur
³Department of Computer, D.Y. Patil College of Engineering, Akurdi, Pune

Abstract: Cognitive radio is a wireless based communication technology which has intelligence built into it. Secure communication is a key for any wireless network. Like all other networks, cognitive radios are susceptible to various kinds of attacks like DOS attack, PUE attack, Selfish attack, tunnel attack and jamming attack. A selfish cognitive radio node can occupy all or part of the resources of multiple channels, prohibiting other cognitive radio nodes from accessing these resources. Selfish cognitive radio attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. Hence, in order to overcome this problem, a selfish attack detection technique called COOPON (Cooperative neighboring cognitive radio Nodes). The secondary user frequently broadcasts the multiple channel allocation information to all its neighboring secondary users, COOPON technique is use. In this paper identify a new selfish attack type in cognitive radio ad-hoc network. Selfish attacks are different depending on what and how they attack in order to pre-occupy CR spectrum resources.

Keyword: - Cognitive Radio, Primary user, Secondary user, Selfish Attacks, MATLAB

I. INTRODUCTION

Cognitive radio network is a network in which an un-licensed user can use an empty channel in a spectrum band of licensed user. Cognitive Radio Networks (CRN's) is an intelligent network that adapt to changes in their network to make a better use of the spectrum. 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. When information is send through alicensed spectrum band is a primary user, 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 either avoid using the channel. An Empty channel also known as spectrum holes.

However, CR wireless networks are susceptible to Primary User Emulation attack (PUE), Selfish Attack, Malicious Attack, Byzantine Attack (i.e., Spectrum Sensing Data Falsification) and cannot offer efficient security. CR attacks are a serious security problem because they significantly degrade the performance of cognitive radio network. In PUE attack, attacker transmits an emulated primary signal during a spectrum sensing interval. An attacker is called selfish attacker if it performs the PUE attack for its selfish own purpose.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.

To detect the selfish cognitive radio attack called cooperative neighboring 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.

II. ATTACK AND DETECTION MECHANISM

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.

A). Attack Mechanism:
Type 1: Single channel is occupied by attacker.

Type 1 attacks are designed to prohibit a LSU from available sensing spectrum bands by sending faked PU signals. The selfish SU (SSU) will emulate the characteristics of PU signals. When SSU send fake signal to LSU, a legitimate SU makes a decision that the PU is now active and it will immediately release the channel. This attack is usually performed when building an exclusive transmission between one selfish SU and another selfish SU. There must be at least two selfish nodes along with only a single channel.

Type 2: Multiple channels are occupied by attacker.

Types 2 attacks are carried out in dynamic multiple channel access. The selfish SU emulates the characteristics of a PU. In a dynamic signal access process, the SU's will periodically sense the current operating band. Whenever PU is not using channel, they are considered as available. SU’s will immediately switch to use available channels. In this attack type, selfish SU's continuous send fake signal on multiple channels in a round-robin fashion.

Type 3: Channel pre-occupation by attacker.

Attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring 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 neighboring SU’s. The selfish SU will send a larger number of channels in current use than real in order to reserve available channels for later use. Even though a selfish SU only uses three channels, it will send a list of all five occupied. Thus, a legitimate SU is prohibited from using the two available channels.

B). Detection Mechanism:

Cooperative neighboring cognitive radio nodes (COOPON) is designed for an ad-hoc communication network. An ad-hoc communication network based on exchanged channel allocation information among neighboring SU’s. As shown in figure (1), Target node (T-node) is taken at center and four Neighboring nodes namely N-node 1, N-node2, N-node 3 and N-node 4 are taken around the T-node.
Figure 1: Selfish attack detection mechanism

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 neighboring users will exchange the current channel allocation information list via common control channel (CCC). Each node is reported to neighboring node that how many channels are currently in use. Individual neighboring nodes will compare the summed numbers sent by all neighboring nodes to the summed numbers sent by the target node. It helps to neighboring node to check target SU is a selfish attacker or not. This detection mechanism is carried out through the cooperative behavior of neighboring nodes. Once a neighboring SU is chosen as a target node and the detection action for it is completed, another neighboring 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.

III. SIMULATION RESULTS

The simulation conducted using graphical user interface in MATLAB to identify different type of selfish attack and calculate the total channels used by SU’S and total detected fake channels.

A). Attack type 1

Figure 2. Attack type 1
As shown in figure 2, attack type 1, total channels are taken 128. Channels occupied by PU’S are 82, Channels available for SU’S are 15 and Fake PU signal generated by SU are 3. Node 1, node 2, and node 3 are the selfish nodes. Each node occupies only one single channel as shown in figure 2. So, total detected fake channels are 3.

B). Attack type 2

![Figure 3. Attack type 2](image3.png)

In selfish attack type 2 total channels are taken 128. Channels occupied by PU’S are 94, Channels available for SU’S are 28 and Fake PU signal generated by SU are 6. Node 2, node 3, and node 5 are the selfish nodes. Each node occupies multiple channels as shown in figure 2. So, the total detected fake channels are 6.

C). Attack type 3

![Figure 4. Attack type 3](image4.png)

In selfish attack type 3 total channels are taken 128. Channels occupied by PU’S are 93, Channels available for SU’S are 35 and Fake PU signal generated by SU are 0. Node 2, node 4, and
node 5 are the selfish nodes and they are actual channels occupied are 10, 8, and 7 respectively. But they are broadcast fake free (or available) channel lists to its neighboring SU's are 13, 13 and 8 respectively. Even though a selfish SU node 2 only uses ten channels, it sends a list of all thirteen occupied channels. Remaining three channels are reserved for future use. So, total detected fake channels are 9.

**IV. CONCLUSION**

In this paper studied different types of selfish attack. They are classified depending on what and how they attack in order to pre-occupy CR spectrum resources. An attack type 1, selfish SU (SSU) will emulate the characteristics of PU signals. In this type each attackers are occupy only single channel as shown. Also in Attack type 2, a selfish SU emulating the characteristics of primary user signal but they are occupy multiple channels. In attack type 3, a selfish SU is broadcast fake channel lists to its neighboring SUs. Even through the selfish SU (node 2) only uses ten channels, it send thirteen occupy channels. Thus, a legitimate SU is prohibited from using the three available channels. A selfish attack detection technique, named COOPON (cooperative neighboring cognitive radio nodes) which is designed for detecting type 3 selfish attacks.

**REFERENCES**

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