Performance Analysis of Primary user Emulation Attacks in Cognitive Radio Networks

Devika Sampath1 and Vydeki Dharmar2,
1 Easwari Engineering college, ECE, Chennai, India.
Email: devikasampath90@yahoo.com
2 Easwari Engineering college, ECE, Chennai, India.
Email: dvydeki@rediffmail.com

Abstract— Primary user emulation (PUE) attacks, where attackers mimic the signals of primary users (PUs), can cause significant performance degradation in cognitive radio (CR) systems. It results in false alarms during the spectrum sensing phase at well-behaving secondary user (SUs) even though the PUs are actually not present.

Index Terms— cognitive radio, primary user emulation attack, primary user, secondary user.

I. INTRODUCTION

The recent development in wireless communication has led to the problem of growing spectrum scarcity. Due to increasing spectrum demand for new wireless applications the available radio frequency spectrum has become scarcer. A significant amount of allocated radio frequency spectrum is used sporadically, causing underutilization of spectrum.

Cognitive radio (CR) 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. In this dissertation we also provide a brief explanation of most of the attacks that make use of one of the inherent properties of cognitive radio.

This paper is organized as follows. In Section II, related work is investigated. The simulation of cognitive networks is described in Section III. In Section IV, the performance analysis of primary user emulation attack is done. The conclusion is described in Section V.

© Elsevier, 2014
II. RELATED WORK

Several approaches have been investigated in literature to perform analysis of primary user emulation attacks in cognitive radio systems. In [1] Shan studies on the communication analysis of SUs for CRN under PUEA. He has proposed a FDMC analysis model, which has considered four parameters, i.e., PU amount, SU amount, MMU amount and SMU amount. The results depicted that the SMU test is of very importance for PUEA detection, which can decrease blocking and dropping rates greatly.

In [2] Deepa explains that CR has also opened the door for lots of threats, especially in security because of the presence of malicious nodes, who want to vandalize the entire communication networks. The physical layer is more efficient in terms of detection of this MU, because this is the primary layer whose information is to pass to the upper layers.

In [4] Anand proposed an analytical model and a practical mechanism using WSPRT to detect PUEA in cognitive radio networks. The detection mechanism allows the user to set thresholds on probability of missing the primary user and the probability of successful PUEA and hence can accommodate a range of sensitivities.

III. SIMULATION OF COGNITIVE RADIO NETWORKS

Primary user emulation (PUE) attack is considered to be one of the severe threats to cognitive radio systems. It poses a great threat to spectrum sensing. In this attack, a malicious node transmits signals whose characteristics emulate those of incumbent signals. There are two types of behaviour associated with the primary user emulation attack, which are discussed in [3] as follows.

1) Selfish PUE attacks: The main objective is to maximize attacker’s bandwidth. For an instance, when malicious node identifies vacant band, it will prevent other secondary users from using that band by transmitting signals that resemble the incumbent signals.

2) Malicious PUE attack: The main objective is to obstruct the secondary users from identifying and using vacant spectrum bands. Malicious attacker does not necessarily use vacant bands for its own communication purposes. It is important to note that in PUE attacks, malicious nodes only transmit in vacant bands.

A. Methodology

The presence of primary user emulation attack will degrade the performance of the network which includes delay, throughput and packet delivery ratio of the network. In order to improve the performance of the network, the presence of these attacks in the network should be detected.

The methodology used to study the primary user emulation attacks in cognitive radio network is

1) Cognitive Radio networks including primary & secondary users will be simulated with 15 nodes, 25 nodes and 50 nodes with varying number of channels.
2) Numbers of attackers are varied in the above network.
3) The performance parameters such as average end to end delay, energy consumption, packet delivery ratio and residual energy will be measured for the above simulated networks.
4) Similar networks without attacks are simulated and performance parameters are computed.
5) The results of various networks with and without primary user emulation attacks are compared and analyzed.

B. Parameters

The parameters required for the analysis of primary user emulation attacks are end to end delay, packet delivery ratio, energy consumption and residual energy.

1) End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination.
2) Packet delivery ratio is defined as the ratio of the number of delivered data packet to the destination.
3) Energy consumption is defined as the amount of energy consumed by the node in order to transmit the packets from source to destination.
4) Residual energy is defined as the amount of energy left in the node after transmitting the packet from source to destination.

C. Tools Required

The environment required to simulate and analyze the performance of the network from [5] is

Operating system: Linux
Developments tools required: TCL, C++.
Tools: NS 2.31
Patch: CRCN Simulator

IV. PERFORMANCE ANALYSIS
The performance analysis of cognitive radio networks is done by measuring the parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy.

A. Networks Without Primary User Emulation Attacks
The network is created without primary user emulation attacks with 15 nodes, 25 nodes and 50 nodes.

From the Fig. 1 it is clear that when there is no attacker all the packets are sent from the source to destination. So the packet delivery ratio is higher in this network. The time taken to deliver packets from source to destination is minimal.

From Fig. 2, when the network size increases the delay in the network also increases even though there is no attacker and the packet delivery ratio starts dropping.
From Fig. 3, when the network size increases the delay in the network also increases even though there is no attacker and the packet delivery ratio starts dropping.

B. Networks With Primary User Emulation Attacks

The network with varying number of nodes and varying number of attackers are created in order to measure the performance of networks under attacks.

15 nodes with one attacker

The network with 15 nodes specifying the source node and the destination node is created with one attacker node. The animation of the network is shown in Fig. 4.

Analysis Of Parameters For 15 Nodes With One Attacker: The network parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy are calculated for different simulation time is shown in Fig. 5, 6, 7 and 8.
Figure 5. Packet delivery ratio

Figure 6. End to end delay

Figure 7. Energy consumption
Figure 8 Residual energy

15 Nodes with Two Attackers

Figure 9. Creation of 15 nodes network with 2 attackers

The network with 15 nodes specifying the source node and the destination node is created with two attacker node. The animation of the network is shown in Fig. 9.

Analysis Of Parameters For 15 Nodes With 2 Attacker: The network parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy are calculated for different simulation time for 2 attackers node is shown in fig. 10, 11, 12 and 13.

Figure 10 End to end Delay
Figure 11 Packet delivery ratio

Figure 12 Energy consumption

Figure 13 Residual energy
25 Nodes with Three Attackers

The network with 25 nodes specifying the source node and the destination node is created with three attacker node. The animation of the network is shown in Fig. 14.

Analysis Of Parameters For 25 Nodes With 3 Attacker: The network parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy are calculated for different simulation time for 3 attackers node is shown in fig. 15,16,17and 18.

Figure 14. Creation of 25 nodes network with 3 attackers

Figure 15 packet delivery ratio
Figure 16. End to end delay

Figure 17. Energy consumption

Figure 18. Residual energy
The network with 25 nodes specifying the source node and the destination node is created with five attacker node. The animation of the network is shown in Fig. 19.

**Analysis Of Parameters For 25 Nodes With 5 Attacker:** The network parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy are calculated for different simulation time for 5 attackers node is shown in fig. 20, 21, 22 and 23.
Figure 21 end to end delay

Figure 22 energy consumption

Figure 23 residual energy
50 Nodes with 7 attackers: The network with 50 nodes specifying the source node and the destination node is created with seven attacker node. The animations of the network is shown in Fig.24.

Analysis Of Parameters For 50 Nodes With 7 Attacker: The network parameters such as end to end delay, packet delivery ratio, energy consumption and residual energy are calculated for different simulation time for 7 attackers node is shown in fig.25, 26, 27 and 28.
C. Comparison of Parameter Values

The parameter values with and without primary user emulation attacks for different network scenarios is summarized in Table 1.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Packet delivery ratio</th>
<th>End to end delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 nodes without attacker</td>
<td>1.00</td>
<td>83.1026 ms</td>
</tr>
<tr>
<td>15 nodes with 1 attacker</td>
<td>0.0880</td>
<td>210.935 ms</td>
</tr>
<tr>
<td>15 nodes with 2 attacker</td>
<td>0.0782</td>
<td>212.196 ms</td>
</tr>
<tr>
<td>25 nodes without attacker</td>
<td>0.9082</td>
<td>1348.57 ms</td>
</tr>
<tr>
<td>25 nodes with 3 attacker</td>
<td>0.4043</td>
<td>2988.1 ms</td>
</tr>
<tr>
<td>25 nodes with 5 attacker</td>
<td>0.3630</td>
<td>2951.61 ms</td>
</tr>
<tr>
<td>50 nodes without attacker</td>
<td>0.0663</td>
<td>654.636 ms</td>
</tr>
<tr>
<td>50 nodes with 7 attacker</td>
<td>0.4931</td>
<td>1605.11 ms</td>
</tr>
</tbody>
</table>

V. CONCLUSION

Simulations were carried out to determine the performance of the network for PUE attack in terms of energy, average end to end delay and packet delivery ratio. The results are simulations of 15 nodes, 25 nodes and 50 nodes with one attacker and two attackers. The comparative analysis clearly indicates that the presence of primary user emulation attackers degrade the performance of the networks.

REFERENCES