CHAPTER 5

BENIGN CLONE NODE RECOVERY PROTOCOL

5.1 INTRODUCTION

Recovery involves identification and fixing of vulnerabilities used by the attacker to enter the systems. One form of recovery is to stop an attack and to assess and repair any damage caused by that attack. In another form of recovery the system continues to function correctly while an attack is underway. This type of recovery is quite difficult to implement because of the complexity of computer systems.

This chapter discusses the algorithm of recovery protocol for the node replication attack mitigation by detecting legitimate clone among the clones and compares the performance of the protocol.

5.2 LEGITIMATE (BENIGN) CLONE NODE DETECTION

The node clone attack is detected using the proposed RTRAPD or Modified RTRAPD attack detection protocol. This protocol’s output is witnesses who have the evidence of the attack, used to recover original clone. Those witnesses detect the attack event which having different locations and same ID in their MEM. Using the RTRAPD or Modified RTRAPD algorithm to detect the clones at different locations with various trusted witnesses who detects the attack. For example, a witness has details after clone detection ([ID, l1],[ID, l2],[ID, l3]...[ID, ln]). Two methods of recovery based on where that algorithm executes are centralized and distributed approach. The first method of recovery is a centralized approach solution that executes recovery protocol at the place who initiates the detection process. The second method is distributed approach solution that executes recovery protocol at the place who witnesses the attack. These proposed recovery protocols will be discussed in the following subsections.

5.2.1 Benign Clone Detection at Initiator (BCDI) Side

In the centralized approach, all the witnesses report to the initiator with necessary evidence pertaining to clone. The initiator collects trustworthiness of each clone from their neighbours with their locations [l1, l2, l3, ..., ln]. Compares the trust value and declare highly trusted node as a benign clone.

5.2.2 Benign Clone Detection at Initiator (BCDI) Algorithm

Input: Set of location claims where replicas available from all the witnesses of detection protocols (RTRAPD, Modified RTRAPD)

Output: Benign clone location and ID

Step 1: Collect trust factor of each clone from their neighbours with their locations L= [l1, l2, l3, ..., ln]

Step 2: Compare trust factor of all Clones

Step 3: Find (Max (Trusted_Clone (L))

Step 4: Declare as legitimate clone as ID with location l, and recover data

Step 5: Alert the network

Probability of Attack detection (P0) is Success rate of node replication attack detection and Probability of Legitimate detection (P2) is the success rate of legitimate node detection.

The simulation setup for recovery protocols are: 4000 nodes are randomly deployed within a 1000m x 1000m square. The transmission range is set to 50m. Assume the All of the forwarding nodes before the witnesses are honest; since the malicious nodes can prevent replica detection if they are in the path before the witness. With this setup 5 replicas considered with different percentage of malicious witness and with the TrustLevel = 75%.

Assume, weightage of Consistency factor (C1), Communication factor (C2) and Battery value are 0.35, 0.35 and 0.30 respectively. Also the cheating neighbour is avoided by choosing highly trusted neighbour with a threshold of 85 %.

In the benign clone detection, first step is to randomly insert a replica into the network and then start the attack detection protocol either RTRAPD or Modified RTRAPD, then invoke legitimate node detection protocol. The success rate of node replication attack detection (P0) and success rate legitimate clone detection (P2) are calculated using Equations 5.1 and 5.2. The probability of legitimate clone detection purely depends on the number of successful attack detection.

\[
P_0 = \frac{\#\text{Successful Attack Detections}}{\#\text{Iterations}}
\]  
\[
P_2 = \frac{\#\text{Successful Legitimate Detections}}{\#\text{Successful Attack Detection}}
\]

Figure 5.1 shows the success rate of attack detection of RTRAPD and the success rate of legitimate clone node detection against No. of protocol runs with two clones. And also shows non-detection of attack due to Non-common witness, dishonest witness and malicious neighbour. P0 is 90% and P2 is 100%.
5.2.5.1 Security analysis

In these benign clone detection algorithms, considers as Benign \( \rightarrow \) Benign (TP), Benign \( \rightarrow \) malicious (FP), Malicious \( \rightarrow \) Benign (FN), Malicious \( \rightarrow \) Malicious (TN). The sensitivity or true positive rate will be calculated by Equation 5.3:

\[
\text{Sensitivity} = \frac{TP}{TP + FN}
\]

In general, Positive = identified and negative = rejected. Therefore:

- True Positive = correctly identified
- False Positive = incorrectly identified
- True Negative = correctly rejected
- False Negative = incorrectly rejected

5.2.5.2 Performance of benign (legitimate) clone detection at initiator (BCD1)

Figure 5.2 shows that the average detection rate of the various proposed methods of attack detection such as RTRADP, Modified RTRADP, BCD1 with RTRADP and BCD1 with Modified RTRADP. The successful legitimate clone detection rate depends on the node replication attack detection protocols RTRADP and Modified RTRADP. In the initiator approach, 100% successful detections of legitimate clone against proposed RTRADP and Modified RTRADP. Success in attack detection will result in benign detection, since initiator has all the details of clones evidenced by the witnesses. Highly trusted clone have been chosen as legitimate in BCD1.

The average detection rate of legitimate (benign) clone detection is 100% and sensitivity 100% for both initiator-origin recovery as well as witness-origin recovery when two clone in the network. Because the witness finds event of an attack with two claims of benign and malicious clones only. The witness could not detect the event of an attack when either one of its claim is not received. When there is more than one clone in the attack, the attack detection is easy, but legitimate clone detection is tough, since the witness may not have legitimate clone’s claim. Legitimate clone’s claim may be dropped by an adversary or the witness may not be common witness between legitimate observer or malicious observer due to randomness.
shows better performance in detecting clones over BCDW with RTRADP protocol.

Table 5.1 Sensitivity comparison of BCDW with RTRADP and Modified RTRADP

<table>
<thead>
<tr>
<th>Category</th>
<th>Malicious Neighbour</th>
<th>TP</th>
<th>FN</th>
<th>Sensitivity of BCDW with RTRADP</th>
<th>TP</th>
<th>FN</th>
<th>Sensitivity of BCDW with Modified RTRADP</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>0.6</td>
<td>0.40</td>
<td>0.6</td>
<td>0.6</td>
<td>0.40</td>
<td>0.6</td>
</tr>
<tr>
<td>Rare</td>
<td>20</td>
<td>0.60</td>
<td>0.40</td>
<td>0.6</td>
<td>0.6</td>
<td>0.40</td>
<td>0.6</td>
</tr>
<tr>
<td>Medium</td>
<td>40-60</td>
<td>0.35</td>
<td>0.65</td>
<td>0.6</td>
<td>0.35</td>
<td>0.59</td>
<td>0.41</td>
</tr>
<tr>
<td>High</td>
<td>80</td>
<td>0.20</td>
<td>0.80</td>
<td>0</td>
<td>0.57</td>
<td>0.43</td>
<td>0.25</td>
</tr>
<tr>
<td>Very High</td>
<td>100</td>
<td>0.00</td>
<td>1.00</td>
<td>0</td>
<td>0.25</td>
<td>0.75</td>
<td>0.2</td>
</tr>
</tbody>
</table>

Figure 5.3 shows the graph between categories in malicious neighbour and Sensitivity in percentage. The malicious neighbour categorized into None, Rare, Medium, High and Very High depend on the percentage of malicious neighbours. These malicious neighbours affect the sensitivity of BCDW with RTRADP protocol. But the sensitivity of BCDW with Modified RTRADP is improved by trusted neighbours which avoids malicious neighbours. Sensitivity of BCDW with RTRADP decreases, when increase in malicious neighbours involvement drops the claims. But BCDW with Modified RTRADP shows remarkable increase in sensitivity by 23% compared to BCDW with RTRADP even when very high malicious neighbour. But in High and Very High percentage of malicious neighbours, the malicious neighbours drop the legitimate clone’s claim which highly affects in sensitivity to zero in BCDW with RTRADP.

5.3 SUMMARY

This chapter has discussed about recovery protocols for node replication attack mitigation by detecting legitimate clone among clones using trust factor. The performance of proposed approaches called Benign Clone Detection at Initiator (BCDI) and Benign Clone Detection at Witness (BCDW) along with RTRADP and Modified RTRADP have been compared.

BCDI shows better sensitivity in detecting benign clone over the BCDW when the initiator is not compromised by an adversary. But in this BCDI approach, there is chance of single point failure due to either failure or compromise of initiator. Hence, BCDW has been proposed and its performance also compared. In addition, BCDI with Modified RTRADP depicts better sensitivity than BCDI with RTRADP. Similarly, BCDW with Modified RTRADP has better sensitivity over BCDW with RTRADP. The next chapter will discuss prevention protocol for node replication attack.