CHAPTER 4

SECURITY MECHANISM WITH DYNAMIC TRUST

4.1 INTRODUCTION

In pervasive environment, DDoS attack is the main problem in all ad-hoc scenario i.e., in MANET and in wireless sensor networks. Due to this dynamic nature, combating or tracing of DDoS attacks is difficult. In today’s internet, to protect victims from large scale bandwidth and target machines from heavy traffic and to avoid clogging all the routes to the victim are also difficult to implement (GeethaMariappan & Manjula Dhanabalachandran 2014). So, the relevant information required by the victim is not possible to receive.

During the design of a privacy-sensitive pervasive monitoring system, issues like Information misuse, leakage, information eavesdropping, social implications, designing privacy settings and lack of support in designing privacy-sensitive applications creep into the network layer and transport layer (Anup Amber & Satyendra 2012). Also, the application layer may be affected by internal or external system attackers if they do not follow the system protocols as per the proposal of Rongxing Lu and others. So, a secure and privacy-preserving opportunistic computing (SPOC) framework form-Healthcare emergency is essential.

We focus on DDoS attacks and the mechanisms which will address the problems of those attacks that occur in pervasive environment at different
layers like network layer, transport layer and application layer. Defense mechanisms deal with the problems of an actual attack that occur before, during and after the transmission (Saman Taghavi Zargar et al 2014). So, it is important to develop a new enhanced defense mechanism for handling issues related to information security for cross layers (Saman Taghavi Zargar et al 2014).

4.2 DDOS UNCERTAINTIES

A distributed denial-of-service attack occurs if the service is denied by sending a stream of packets to trusted user after he receives request that is either consumed by some botnet resources, thus reflecting its unavailability to legitimate requested users, or provides the attacker with unlimited access to the victim’s machines, preventing him from being able to responding to the users within a time (Shishira et al 2012).

In hacker’s society, an attacker or hacker continuously sends his attack program on insecure machines in a pervasive environment (Dhakal & Gautham 2012). This results in the compromising of the insecure machine by the attack program. So, this machine is called the Master/Hacker or Zombie. Collections of these machines are called bots and the corresponding network is called botnet. Through the master, the attacker can run their attack program on the insecure machines to launch their attacks. DDoS flooding attacks and Vulnerability attacks are two major categories of DDoS attacks (Dhakal & Gautham 2012).

We focus on DDoS flooding attacks and their types in this thesis work. Based on the protocol level, it is further categorized as the following:
a. Network/Transport-level DDoS flooding attacks: These types of attacks are launched by the protocols which are used by wired, wireless and MANETs.

i. Prominent Attribute linkage attack: Attackers use trial and error method to find out their victim’s resources by the distinguished feature of that particular scenario.

ii. Service Identity Linkage attack: Attackers usually send forged requests instead of directly requesting them for the service; hence, those attackers can get access to the victim’s resources.

iii. Untrusted service provider attack: Attackers can get the details of victim’s resources providing by an untrusted service provider, knowingly or unknowingly.

iv. Service Attribute linkage attack: Using attributes of particular service’s Identity, Attackers can get the details of the original identity of the service first and can then send forged requests to the resources next.

v. Service Status availability attack: After knowing the details of services which are either available or not, the attackers may forge an attack.

b. Application-level DDoS attacks:

vi. High rate Request Attacks: Attackers send high rates of legitimate application layer requests to a server in order to get the details of its session resources.

vii. Service degrades attack: Instead of high rate requests to the server, it sends normal request to the server for
getting high-workload response. For example, a client sends a single request to consume large amounts of server resources in order to degrade the service or completely damaged it.

viii. Collaborated request attack: Attackers send huge volumes of requests to the server for getting high-workload responses in order to spoil the entire control of the application.

4.3 DYNAMIC TRUST MANAGEMENT FRAMEWORK

We propose a dynamic trust management framework, for pervasive environment which provides the feature of defense environment and the protection against attackers as shown in the Figure 4.1. As per the proposal, intrusion detection systems use parameters throughput, packet delivery fraction, end-to-end delay, normalized routing load, packet reception rate and inter arrival time to detect and avoid anomalies in MANET. These parameters are not sufficient to produce a good result in Pervasive environments.

If other parameters are added with these, more accurate results can be produced. So, in our work we incorporate different parameters in pervasive environments. We assume that our framework consists of wired network with two or more nodes, MANET with two or more nodes and wireless network with two or more nodes that communicate with each other. According to the network, a routing protocol is used and result is compared with three different cases like, normal Communication, Communication with attack, and Communication with attack detection.
4.4 PREVENTIVE, DETECTIVE, RESPONSE MECHANISM

Mobile Networks are considered in pervasive environment for route discovery and maintenance; three types of protocols are followed for communication. One type consists of Proactive protocols such as Wireless routing protocol (WRP), Destination sequence distance vector (DSDV) protocol, Fisheye State Routing (FSR) while the second type consists of Reactive protocols like Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector routing protocols (AODV). Finally hybrid protocols such as Zone Routing Protocols (ZRP), Zone-based Hierarchical Link State routing protocols (ZHLS) and Hybrid Ad-hoc Routing protocol (HARP) are used.

In order to improve the network’s operational lifetime, it is necessary that the routing protocols must use multiple paths rather than a single path. To enhance the network performance, when the primary path fails an alternative path is assumed to exist between a source and a destination. This can be increased by maintaining multiple paths between the source and the destination, at the expense of increased energy consumption and traffic generation. By doing so, the network reliability can be increased (Dependra dhakal & Kiran gautham 2013).

4.5 OVERVIEW OF AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

AODV is a reactive protocol which mixes properties of DSR and DSDV for route discovery and route maintenance as per the on-demand request from the sender (Basu Dev Shivahare et al 2012). As long as routes are required, the same can be maintained after the discovery. AODV also uses the following control messages like Route Request (RREQ), Route Reply
(RREP), Route Error (RERR) when a source sends packets to a destination (Basu Dev Shivahare et al 2012).

Route discovery process of AODV protocol can be initiated by the source to communicate with the destination, link failures or broken links. To find the destination node, route discovery process floods the RREQ messages to its neighbour. An intermediate node receives request, immediately it wants to setup reverse path to the source node with sequence number and Broadcast ID for loop free routing (Siddique et al 2012).

When Destination receives this request, it can be replied with RREP message containing number of hops and latest sequence number. RREP is routed back to the source using reverse path and forward path from the destination (Twinkle Vyas & Dhaval Rana 2014). For each reverse route entry, a concept of time to live(TTL) is associated and if no packets are sent with in this time limit, the particular route will be removed from the routing table of concerned nodes.

In route maintenance process, all nodes send a hello message to the neighbours to confirm their links. If any of the links fail, the particular node has to generate RERR message to its up streaming neighbours to update their routing table (Navjot Kaur et al 2011). After the error message is received by the source, it restarts the process of route discovery.

4.6 OVERVIEW OF DYNAMIC SOURCE ROUTING (DSR)

It is a simple and efficient proactive protocol, based on the theory of source based routing. The route discovery process is initiated by the source node if the route doesn’t know to the source. After discovery, it is maintained and stored at each node’s cache. During the process of maintenance, if any
link failure occurs, this process finds an alternate path to the destination when source sends packets to the destination.

**Figure 4.1 Overview of Security Mechanism**

### 4.7 RELIABILITY - SINGLE PATH : ALGORITHM

The single path routing reliability algorithm is described below

**Step 1:** The source node broadcasts the packet to its neighbors in the reliable path.

**Step 2:** The receiving node checks to see whether the packet’s sequence number is already in its received list of sequence numbers.

- a. If so, it drops the packet.

- b. Else, it stores the sequence number of the packet it receives and sets its id, grid id, and node type in the packet.
**Step 3:** If it has received from a node in the same grid, it compares its neighbour list with the node list in the packet.

a. If there are nodes in the neighbour list but not present in the node list, it adds those nodes to the node list and broadcasts the packet to its neighbors.

b. Else, it drops the packet.

**Step 4:** If it has received from a node in a different grid, it strips off the node list, adds all its neighbors to the node list and broadcasts the packet.

**Reliability -Single Path: Pseudo Code**

The single path routing reliability pseudo code is described below

1. Set

   tabP: Hash table of packets
   tabN: Hash table of neighbours
   tabNL: Hash table receive node list

2. Input: Packet[

   sID: source ID, gID: grid ID, seq: Sequence Number
   nT: Node Type, rNL: Receiver Node List

   If(seq) sequence number presents in tabP

   Return

   Create new entry packet(sID,seq,rNL,gID,nT)
3. If(gID==neighbour node gID)

   If(!neighbour node) neighbour node not present in rNL
   add the neighbour node into rNL and broadcast the packet to its neighbour
   else

   Drop the packet

4. If(gID!= neighbour node gID)

   Search in rNL and add the all neighbour to the node list and broadcast the packet

4.8 RELIABILITY -MULTIPATH: ALGORITHM

The multi-path reliability algorithm is briefed below:

Step 1. The source node broadcasts the packet to its neighbors.

Step 2. The receiving node checks to see whether the packet’s sequence number is already in its received list of sequence numbers.

   a. If so, it drops the packet.

   b. Else, it stores the sequence number of the packet it receives and sets its id, grid id, and node type in the packet.

Step 3. If it has received from a node in the same grid, it compares its neighbour list with the node list in the packet.

   a. If there are nodes in the neighbour list not present in the node list, it adds those nodes to the node list and broadcasts the packet to its neighbors.
b. Else, it drops the packet.

**Step 4.** If it has received from a node in a different grid, it strips off the node list, adds all its neighbours to the node list and broadcasts the packet.

**Step 5.** For each packet it checks the packet’s sequence number, and repeats the same for all the paths that come either from the same grid or from a different grid.

**Reliability- Multipath: Pseudo Code**

The multi-path reliability DALAF algorithm is briefed below

1. Set

   tabP: Hash table of packets

   tabN: Hash table of neighbours

   tabNL: Hash table receives node list

2. Input: Packet[

   sID: source ID, seq: Sequence Number, rNL: Receiver Node List,

   gID: grid ID, nT: Node Type.

3. For each ( Process the packet in all path)

   If(seq) sequence number present in tabP

   Return
4. Create new entry packet(sID,seq,rNL,gID,nT)

   If(gID==neighbour node gID)

   If(!neighbour node) neighbour node not present in rNL
   add the neighbour node into rNL and broadcast the packet to its neighbour

   else

   Drop the packet

5. If(gID!= neighbour node gID)

   Search in rNL and add all the neighbours to the node list and
   broadcast the packet

6. End

4.9 CASE STUDY

The simulation is implemented in a NS2 network simulator with the specification listed in Table 4.1. The network setup parameter for mobile ad-hoc networks in pervasive environment. We implemented a model for checking the reliability with single path routing and multipath routing techniques using proposed algorithm. The implementation result shows that when the number of nodes increases the number of reliable paths also increases according to the result as shown in the following Table 4.2. It also describes the parameters of time taken to deliver packets and packet delivery ratio from the source to destination with one way and multi way communication. It shows that the result of after applying prevention algorithm, the number of reliable paths increases while the number of nodes increases in both single and multi-path communication. Hence the nodes can be able to send or receive the packets without loss because of reduction of malicious attacks and also traffic. Also result is compared with an existing of Vanaja et al (2013) using AODV with
single and multi path communication in Mobile ad-hoc networks as shown in Figure 4.2 and Figure 4.3.

Table 4.1 NS2 Simulation set up parameters

<table>
<thead>
<tr>
<th>Specification</th>
<th>Setup parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes (N)</td>
<td>100</td>
</tr>
<tr>
<td>Area Size</td>
<td>50 X 50 meter</td>
</tr>
<tr>
<td>Mac</td>
<td>IEEE 802.15.4</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>25 sec</td>
</tr>
<tr>
<td>Transmission Range(r)</td>
<td>100m</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>Exponential</td>
</tr>
<tr>
<td>Packet Size</td>
<td>250 bytes</td>
</tr>
<tr>
<td>Transmission Rate</td>
<td>50, 75,100,125 and 150 kb.</td>
</tr>
<tr>
<td>Node ratio</td>
<td>50%, 100%</td>
</tr>
</tbody>
</table>

Table 4.2 Reliable paths in Single, Multipath Communication

<table>
<thead>
<tr>
<th>Distance between source and Destination (Mobility Nodes)</th>
<th>Time taken to deliver packets in single Path(Sec)</th>
<th>Delivery Ratio % in Single Path</th>
<th>Time taken to deliver packets in Multi Path(Sec)</th>
<th>Delivery Ratio % in Multi Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>456</td>
<td>91</td>
<td>810</td>
<td>95</td>
</tr>
<tr>
<td>2</td>
<td>624</td>
<td>92</td>
<td>870</td>
<td>94</td>
</tr>
<tr>
<td>3</td>
<td>648</td>
<td>90</td>
<td>876</td>
<td>91</td>
</tr>
<tr>
<td>4</td>
<td>660</td>
<td>95</td>
<td>942</td>
<td>92</td>
</tr>
<tr>
<td>5</td>
<td>780</td>
<td>94</td>
<td>1014</td>
<td>95</td>
</tr>
<tr>
<td>6</td>
<td>840</td>
<td>95</td>
<td>1098</td>
<td>92</td>
</tr>
<tr>
<td>7</td>
<td>900</td>
<td>92</td>
<td>1158</td>
<td>94</td>
</tr>
<tr>
<td>8</td>
<td>1020</td>
<td>94</td>
<td>1248</td>
<td>94</td>
</tr>
<tr>
<td>9</td>
<td>1200</td>
<td>94</td>
<td>1392</td>
<td>93</td>
</tr>
<tr>
<td>10</td>
<td>1260</td>
<td>93</td>
<td>1572</td>
<td>92</td>
</tr>
</tbody>
</table>
Figure 4.2  Packet Delivery Ratio - Proposed Vs AODV (Using Single Path)

Figure 4.3  Packet Delivery Ratio - Proposed Vs AODV (Using Multi Path)
4.10 SUMMARY

The dynamic trust and security mechanism scheme presented in this chapter showed an improvement in the scenario use of single path and multipath assuming that the particular path is reliable. Link-level retransmission and blacklisting routing use a metric to reflect and improve path reliability. Duplicate packets are not forwarded. This is achieved by maintaining a cache for each node, which stores the signatures of recently forwarded packets and also provides the security and privacy among the transmission.