CHAPTER 5

SECURED NETWORK USING PROMISCUOUS MODE AND PACKET LOSS REDUCTION METHODS

Utilization of mobility nodes nowadays has increased and the communication improvement in the system is a fundamental requirement. Ad hoc networks are commonly utilized in battle fields, defence groups, individual electronic gadget organizations and so on. The fundamental requirement in MANET is routing, which is common in wireless networks (Sivakumar et al 2011). In MANET, a node can discuss with other nodes in its limitation and to communicate with different nodes utilizing a routing technique.

One of the fundamental property of MANET is that it can be configured by itself (Yi et al 2002). Packet loss during data transmission is one of the significant constraints in MANET to be overcomed. As nodes move out of the network, the connection among the nodes will be lost and the packet droppings may occur and also due to traffic in network, packet loss occurs (Schmidt et al 2008).

Throughput is a commonly calculated parameter amongst the most critical measurements to assess the execution of a routing technique.
5.1 SECURED ROUTING

The execution in the proposed IAODV routing technique is contrasted with AODV and DSR. Although different throughput results of various networks have been acquired, the reasons for throughput selection in MANETs have not been extremely figured out.

Packet loss is one important parameter to think about throughput, since throughput is calculated based on number of lost packets (Sohail Jabbar et al 2015).

Packet loss issue is significantly more common in MANETs, since remote connections are liable to transmission errors and the network topology changes regularly (Rajamahmood et al 2007).

A packet may loss because of error during transmission, no route to the destination, broken connections, obstructions, and so on. The impacts of these causes are tightly connected with the network settings. Building a routing model to logically reduce packet loss is a challenging issue (Yi et al 2004).

In MANETs, remote connection transmission errors, portability, and congestion in network are significant causes for packet loss which has to be overcome.
A packet may be dropped if the route to destination is not available, or pending packets storage is full. It might likewise be dropped at a middle of the transmission if the connection to the destination has been lost (Soundararajan et al 2012).

The Figure 5.1 explains the packet loss in MANET. The nodes n2 and n4 drops the packets due to link errors and the nodes n3 and nk drops the nodes because of malicious actions of the nodes.
5.2 ATTACKS AND NODE AUTHORIZATION METHODS

Black Hole Attack:

AODV protocol finds a route from sender to the receiver in a MANET (SatyendraTiwari et al 2011). In AODV technique, RREQ message is transmitted by the sender to neighbor nodes, Route Reply (RREP) message is used by nodes which sends acknowledgement to source node that it has a route to destination, Route Error (RERR) message is transferred to sender if no route is available to the destination (Capkun et al 2006).

If source node S needs to transfer data to destination D which is depicted in Figure 5.2. It communicates RREQ to neighbor nodes. The nodes which receive RREQ will check the route availability to next node and if path is available it transmits RREP back. The procedure is continued till the RREQ message reaches the destination and finally the routing table is updated at source side (Sreedhar et al 2013).

In Figure 5.2 node M is considered as malicious node as it has no path to destination but sends fake routing information to source node as if it has a route to destination (Renudalal et al 2012). The sender will update the routing information and uses that path for packet forwarding in which node M misuse the sensitive information.
Figure 5.2: Dark Hole Attack

**Grey-Hole Attack**: This type of attack drops the packets even if nodes malicious action is restricted to specific conditions (Sultanuddin et al 2016). Some of the conditions are:

i) **Selected Node Attack**— in this case packets are dropped from a specific individual node which is sending or receiving data and for other nodes the data transfer operation is held normally and accurately.

ii) **Selected Time Attack**— in this case data packets are dropped only at a selected time instance and in remaining time the data packets are normally forwarded.
Figure 5.3: Gray Hole Attack.

The Figure 5.3 illustrates the gray hole attack. Detecting this kind of attack is extremely troublesome except if there exists a framework to identify, which deals with every node in the system (SoufineDjahelFarid et al 2008).

5.3 PACKET LOSS CAUSES

Packet loss can happen in MANETs because of several problems. Packet loss occurs fundamentally on account of the following issues:

A. **Congestion:** Within MANET, congestion is a primary issue for packet loss. Packet loss occurs as nodes cannot transfer the packets to the destination due to congestion in network.
**B. Path Modification:** In MANETs the path will be continuously changed because of the mobility nature. Because of this packets will be lost.

**C. Energy:** MANETs have restricted energy limitations. As the level of energy of nodes reduces the packets are dropped.

### 5.4 ROUTE DISCOVERY METHOD

The MANET is dynamic in nature and the routing method is initiated after a MANET is formed (SrdjanCapkun et al 2003). When a node in the network moves away, the packets are exchanged to neighbor nodes which have a most extreme number of neighbors.

There are three sorts of malicious nodes:

- **Malicious Nodes (MN1):** These sorts of nodes are involved in communication but after receiving data packets they deny to forward them to neighbor nodes.

- **Malicious Nodes (MN2):** These nodes do not cooperate in route identification or in data transfer.

- **Malicious Nodes (MN3):** These nodes become malicious all of a sudden.
5.5 PROPOSED SECURED NETWORK USING PROMISCUOUS MODE

For reducing different types of attacks a Secured Network using Promiscuous Mode is proposed.

5.5.1 Promiscuous Mode

Promiscuous mode is a kind of computer organizing mode where all data packets can be received and visible by means of system connectors working in this mode. This is the mode commonly utilized for packet loss that happens on a node. Promiscuous mode allows a node to catch and examine each packet behavior.

To start with, it allows all nodes in MANET to involve in communication with no extra communication overhead. Promiscuous mode deals with two sections: By utilizing the performance investigation of data transfer and the packet drops in the network.

This mechanism is Quick node repairing method that makes utilization of nodes functioning in Promiscuous mode when normal nodes drop the data packets. In Figure 5.4, the node C (malicious node) receives the data from destination as packets, drop those packets and forwards fake data to the sender that is treated as malicious node.
The algorithm for malicious node identification is explained below.

**Malicious Node Detection Algorithm**

```plaintext
if (node id is between 0 and 20)
{
    Execute malicious behavior
}
else
{
    Process the routing packet correctly
}
```

In the Proposed malicious node detection algorithm, the PKG will assign Identity (ID) for every node in the MANET which is involved in communication. Based the performance of the node, PKG allots a id to the nodes. If the node id is in between 0 and 20, then that node is
considered as malicious node and is removed from the routing table. Otherwise the data transfer will be done.

### 5.5.2 Layers Causing Packet Drop

Basically, a Medium Access Control (MAC) layer is liable for packet drops. A MAC layer is accountable for flexibility related packet drops and moreover blockage-related packet drops, though a network layer is cautious just of transmitting ability related packet drops.

Since a MANET is a particularly integral network which can be established by its own and it frequently undergoes route failure and packet loss. In the event that there is a failure of route the current route nodes remain idle and other route needs to be identified using a RREQ.

RREQ message is sent when a sender needs to transmit data and finds a route on demand, for instance, AODV method establishes the route by using route request and route reply messages. Table 5.1 shows the packet drop layers.

<table>
<thead>
<tr>
<th></th>
<th>MAC LAYER</th>
<th>NETWORK LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Related</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Congestion</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
5.6 ENHANCED 2ACK METHOD

Different ACK-based estimations are used to find malicious nodes in the framework. In the proposed 2ACK-based technique each node sends ACK to the next neighbor node before transmitting the final data and the receiver node sends ACK message to its sender in response that the node is ready to receive message. In this way 2ACK method is effectively used for reducing the packet drops which occurs due to route failure or node failure.

The proposed 2ACK method reduces the congestion control in the network, as the ACK messages are sent only to the trusted nodes involved in communication. The 2ACK method guarantees successful data transmission.

The proposed 2ACK algorithm reduces the packet droppings in the MANET by sending ACK messages before transmitting and receiving original data. If ACK message is not received from any node, then the node will wait for particular time interval and then mark the node as black list node and continue the process.

The data is transferred to the destination nodes only when the ACK is received from it. The 2ACK method effectively reduces the packet droppings caused due to route failure, node failure or because of malicious node.
2ACK Algorithm

For every node decide the drop packets
If packet dropped > edge
Include the nodes into pernicious node list
if (every node is suspected)
{
    node X checks ACK and sort them/X is the malicious node
    if ( any ACK is lost from neighbor nodes)
    {
        check the ACK from destination
        comp( ACKneighbor, ACKdestination)
        {
            if ((ACK neighbor – ACKdestination)>=7)
                Add node into malignant node list
            else
                break;
        }
    }
}

The 2ACK method checks the ACK messages of the receiver and if the message is received then only it transfers the original data to the neighbor node.