CHAPTER V

5. REPUTATION BASED ON-DEMAND ROUTING PROTOCOL

This chapter explains another contribution of the thesis-reputation based on-demand routing protocol. This is also used for controlling selfishness in MANETs.

5.1 REPUTATION

Reputation is one node’s opinion about another node. For Mobile ad-hoc networks, reputation means participation of a node in routing and forwarding as seen by others. This reputation system can be used to make decisions about which nodes to include and which nodes to exclude from the network. This system can be used with any misbehaviour identifying schemes.

5.2 THE APPROACH

The proposed approach is implemented over the existing on-demand routing protocol like DSR, which is explained in chapter 3. Reputation value of node is used to classify a node as well behaving or misbehaving. Each node uses a monitoring mechanism like “watchdog” to monitor their neighbours. Monitoring the neighbours helps each node to calculate the reputation value of each of its neighbour. Reputation value is calculated using equation (5.1).
Suppose there are ‘N’ nodes in the mobile ad-hoc network. Each node ‘ni’ i=1,2,…,N, calculates the reputation (R_{i,j})_t for each of its neighbour ‘j’ at time t.

For each node,

\[ R_{(i,j),t} = \frac{\sum_{S_{\text{pkts}} = 0}^{\infty} F_{\text{pkts}}}{\sum_{S_{\text{pkts}} = 0}^{\infty} S_{\text{pkts}}} \]  \hspace{1cm} (5.1)

Where R_{(i,j),t} is the reputation value calculated by monitoring the neighbour ‘j’ directly at time ‘t’ and F_{pkts} is the number of packets forwarded by node ‘j’ and S_{pkts} is the number of packets sent by node ‘j’. This formula is used to calculate the reputation value of a node by directly monitoring the neighbouring node’s past behaviour for some amount of time. It is also possible to pass this reputation value that is calculated directly by monitoring the neighbours, to the 1 or 2 hop neighbours. But the most reliable and quickest reputation values are those which are directly derived from personal experience. Hence more importance is given to the direct observations and next to the messages from the 1st hop neighbours. This approach is called as localized access control, because only the nodes in the neighbourhood can decide whether a node is allowed to access the network or not.

Based on this calculated reputation value, a node creates and maintains some lists. There are three lists. 1. White list, 2. Black list and 3. Gray list. White list consists of nodes with high reputation value (e.g. greater than 0.8), Black list consists of nodes with lower reputation values (e.g. less than 0.8). Gray list consists of nodes which are under suspect.
Normally a node includes a node in the gray list if it receives an alert message from any one of its neighbour about misbehaviour of that node.

Thus classifying a node into well behaving or misbehaving is done based on their reputation value calculated by direct observations. If a node receives an alert message about misbehaviour of another node, it can be termed suspicious and kept in the gray list. A node in the gray list will be moved to black list if a node is found to be misbehaving by direct monitoring.

In the first part of the protocol, a node (source node) which wants to communicate with another node (destination node) would search its cache to see whether route is available. If so it will use that route. Otherwise, the source node sends a Route Request to its neighbours. In normal DSR, Route Request (Route Request) packet will be sent as a broadcast to all the neighbours of the source node. But here, the source node checks the reputation table of its own and sends the Route Request packet to only those nodes with a higher reputation value i.e. to the nodes in white list.

Fig 5.1 Example Scenario Source= 1, Destination = 9
In fig 5.1, node 1 wants to send packets to node 9. In route discovery phase, node 1 sends Route Request to node 3 and 2. Instead of sending Route Request as a broadcast, our approach sends the Route Request packet only to the neighbours with high reputation value. This reduces overhead in the network. On receiving Route Request from node 1, node 3 and 4 will check their corresponding reputation tables and send the Route Request to the next neighbour only if its reputation value is high. Thus finally the Route Request reaches node 9. As in DSR, the destination will give the RREP (Route Reply) packet to the source. This route will be a secure route since it avoids nodes with lower reputation. Reputation value decides how trustworthy a node is. Thus the route becomes trustworthy route.

A node with greater than 0.8 reputation value will be classified as high reputation and kept in white list and below that as low reputation and will be kept in black list. The source node while the process of discovering the route sends the Route Request only to those neighbours with greater than 0.8 reputation value. If there is no such node in the table, then the source node will look for other options like sending the Route Request to nodes with greater than 0.6 and so on. Anyhow by sending the Route Request to only those nodes with high reputation value we can ensure that the Route Requests are not dropped or do not reach the misbehaving nodes.

5.3 SIMULATION RESULTS

This section explains the simulation study of the proposed scheme in NS2.
5.3.1 Simulation Setup

The simulated network consists of 50 wireless nodes deployed in a field of 1200 x 1200 square meters. The random waypoint is chosen as a mobility model. Each node is first randomly placed in the field, waits for the pause time (10 second in our simulation), then moves to another random position with a speed chosen between 1 to 15 m/s. Every 10 seconds during the simulation, ten new source and destination pairs are randomly selected, therefore, every node has chances to be both a source and a destination. The Constant Bit Rate (CBR) traffic is selected as the traffic model. Each simulation is run for 900 seconds.

5.3.2 The Network Model

Following are the assumptions and network model used in this approach.

1. Each node is identified by a unique, persistent ID.
2. Each node runs a "Watchdog" mechanism to monitor other nodes
3. Network is dense enough to establish communications.
4. Links are bidirectional, i.e. If communication between A to B is possible, then communication between B to A is also possible.
5. Nodes are selfish, not malicious.
6. A node which agrees to forward in routing packets will not drop data packets. This ensures that if a trust worthy route is established between source and destination, then chances of intermediate nodes dropping the packets is less.
The reputation based DSR (R-DSR) is compared with Dynamic Source Routing protocol. The parameters used for performance analysis are 1. Overhead in the network when number of Route Requests increases 2. Reliability of the route in a network with misbehaving nodes.

Figure 5.2 gives the overhead in the network when the number of Route Requests increases. As the traffic increases, the overhead increases in DSR protocol. But in reputation based DSR, it manages to be less compared to DSR. This is because, DSR send the Route Request packets to all nodes in the network, where as R-DSR transmits Route Request packets only to the nodes with higher reputation value.
Figure 5.3 Throughput Vs. Number of misbehaving nodes.

Figure 5.3 shows, that even when the number of selfish nodes are increased, the R-DSR is able to provide reliable communication. This is because R-DSR selects the best route based on the reputation value. But, normal DSR collapses when number of selfish nodes is increased. Thus from the results it is proved that R-DSR provides better performance compared to DSR.

5.3.3 Isolating misbehaving nodes

This approach not only identifies misbehaving nodes but also isolates them from enjoying network services. When a node tries to identify a route, its Route Request will be forwarded by the neighbouring nodes only if its reputation value is higher than the threshold value. i.e. This node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no
chance of rejoining the network until the entire network is reformed. This makes sure that the misbehaving nodes are punished for their behaviour, and once punished it is very difficult for them to re-associate themselves with the network. Hence all the nodes are supposed to cooperate.

5.4 ANALYSIS OF THE APPROACH

The approach used here is very simple. It makes a little modification to the Route Discovery process of DSR protocol. But it achieves good performance compared to normal DSR. Reputation value is calculated using a simple formula. Unlike other approaches which uses counters for incrementing and decrementing the reputation values. Here we consider ratio of forwarded packets to sent packets. A sent packet means packets originated by this node. Forwarded packets mean packets forwarded by this node which was originated by some other node in the network. This ratio will give a better picture about the participation of a node in the network. But ‘when’ to calculate the reputation value is a factor to decide.

Following cases are considered for a detailed analysis of the approach.

Case 1: A node may build reputation and start misbehaving.

This case is possible, but it can enjoy network services only for a less amount of time. Reputation value is updated periodically, thus older reputation values will become obsolete.

Case 2: There is a chance that the Route Request packet is forwarded in a direction may not lead to destination. Source will not find a route to destination.
This case is partially true. Route Request packet may go in some other direction, because it is transmitted only in the direction where highly reputed nodes are available. But this will not lead to any problem in finding the route to the destination. The assumption is that the network is dense enough so anyhow the source will find a route to the destination. It may be longer path since it goes only through trustworthy nodes.

Case 3: A node may agree to forward the packets while discovering the route, but fail to forward data packets.

This case cannot happen. Again the assumption is that, if a node agrees in routing, it will not misbehave in packet forwarding.

Case 4: False positives- A well behaving node is misunderstood as misbehaving.

A node may give a false advertisement about another node that it was misbehaving. But a node will include another node only in a gray list based on the alarms from neighbours. It will move it to black list only if the node understands other node’s misbehaviour by direct monitoring.

Case 5: A node may create false packets as if it was generated by some other node in order to increase their reputation value.

Impossible case, because we are dealing with selfish nodes which does not waste its energy unnecessarily, and also address cannot be spoofed as per our assumption.
This approach has several advantages.

1. The path used for data communication is trustworthy.
2. Communication overhead is less.
3. Increases throughput in the network.
4. Implementation is simple since it needs only a little change in DSR algorithm.

The disadvantages of this approach are;

1. Need of a monitoring mechanism for calculating reputation values.
2. Malicious nodes are not considered.
3. A route with well behaving nodes is overloaded.

5.4.1 The Reputation Mechanism

Each reputation mechanism has its own characteristics. Following set of options differentiates one reputation mechanism from the other.

1. How reputation value is calculated?
2. Does the calculation make use of direct monitoring information alone? Or is it using second hand information (from neighbours) also?
3. If it uses second hand information from neighbours about any node, how often this second hand information is passed in the network? How often it is broadcasted?
4. If reputation information about another node is broadcasted by any node to all the nodes in the network, what sort of information is broadcasted? Is it about nodes-with-good-reputation or about nodes-with-bad-reputation or both?

This approach calculates the reputation value based on the number of forwarded packets and number of sent packets by a node. This calculation is done based on direct monitoring. First-hand information is used for taking decision about a node. A node is added to black list or white list based on the reputation value. Second hand information from neighbours is used for adding a node in gray list. A node is moved to black list only when a node identifies that it is misbehaving by direct monitoring. Thus this approach is not affected by false advertisements of one node about another node. An alert message is generated by a node only when a node with low reputation is trying to use the network services. Thus this approach is not introducing more communication overhead. The information about a low reputation node alone is passed. Thus this approach is not affected by collaborative misbehaviour by two or more nodes which would generate false advertisements showing high reputation values of friend nodes.

5.5 FACTORS TO DECIDE

There are many factors to be decided while implementing this protocol.

5.5.1 Threshold value.

The simulation has used 0.8 as the threshold value for deciding whether a node is well behaving or misbehaving. This value is decided based on the real world examples. If a node is 80% good, then we can believe it. Otherwise we may doubt it. But this can be decided based on some other
factors like dynamicity of the network, number of nodes in the network, traffic in the network etc. If there is less traffic in the network, then the threshold value can be still reduced.

Following table 5.1 gives an idea of setting the threshold value.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Factors</th>
<th>Values</th>
<th>Threshold Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Traffic</td>
<td>High</td>
<td>0.8</td>
</tr>
<tr>
<td>2</td>
<td>Traffic</td>
<td>Low</td>
<td>0.5</td>
</tr>
<tr>
<td>3</td>
<td>Traffic</td>
<td>Medium</td>
<td>0.7</td>
</tr>
<tr>
<td>4</td>
<td>Number of nodes</td>
<td>High</td>
<td>0.8</td>
</tr>
<tr>
<td>5</td>
<td>Number of nodes</td>
<td>Low</td>
<td>0.5</td>
</tr>
<tr>
<td>6</td>
<td>Number of nodes</td>
<td>Medium</td>
<td>0.7</td>
</tr>
</tbody>
</table>

The values high, low and medium can be quantified according to the past history of the network.

5.5.2 Periodicity of calculating the reputation value

There are two ways to determine the periodicity of calculating reputation value. 1. On-demand 2. Periodic intervals

Reputation value can be calculated on-demand. (i.e.) only when a node wants to transmit a packet or only when a node receives a route discovery packet. The node monitors the neighbours promiscuously. When it
wants to transmit a packet, it calculates the reputation value by using the equation (5.1) by considering the number of forwarded packets and number of sent packets for a time period ‘T’.

In the on-demand approach for calculating reputation value, ‘T’ value has to be decided. We can find the ratio for past one hour, or past half an hour etc. This method gives a more reliable reputation value and overhead is also less. But there are chances that a node may build reputation and start misbehave. For example if reputation value is calculated for every one hour, a node can well behave for past half an hour and misbehave for next half an hour.

Reputation value can also be updated periodically. The simulation is done by updating the reputation value periodically for every 10s. Thus for every 10s, the ratio of how many packets are forwarded, and how many packets are sent is calculated. \( T = 10s \). The advantage of this method is, a consistent reputation value is obtained by regular updating, but it involves more overhead.

5.5.3 When to re-associate an isolated node

The reputation based approach proposed in this thesis isolates a selfish node which is not cooperating in the network. This is done by not forwarding the data or routing packets of a node whose reputation value is below the threshold level. Such nodes cannot receive service until their reputation value is increased. In order to increase the reputation value, a node has to forward the packets of other nodes. Thus only a well behaving node or a cooperating node will get network services. An isolated node is not isolated forever. It can be allowed to use the network services once its reputation value reaches the threshold level.
Allowing the isolated node to rejoin the network has both advantage and disadvantage. The advantage is, if a node is mistakenly isolated, there is a chance for rejoining. The disadvantage is, a node can try to build reputation and use the network services, and then go for selfish behaviour. But anyway, the reputation value will classify the node as either well behaving or misbehaving. Periodic updates of this reputation value will help to avoid problems like sited above.

5.6 SUMMARY OF ACTIVITIES AT EACH NODE

Each source node:

Step 1: When there is a need for transmitting a packet, check the cache for possibly recent routes.

Step 2: If available use it.

Step 3: Otherwise, send the Route Request packet only to the nodes in the white list.

Step 4: If there is no node in the white list, consider nodes in the gray list. (worst case).

Step 5: Wait for a Route Reply.

Step 6: Use the route for communication.

Each intermediate node:

Step 1: When a Route Request arrives, check whether it is a duplicate, if so discard.
Step 2: Otherwise, check the reputation value of the source which has sent the Route Request packet.

Step 3: If the reputation value is greater than the threshold. (i.e. if the node is in white list), help the node either by providing a Route Reply which is available in the cache, or forward the Route Request to the neighbours in the white list.

Step 4: Otherwise drop the packet and generate alarm message about the misbehaving node.

Note that the alarm message is generated only when a misbehaving node is trying to access the network. This reduces unwanted broadcasts in the network.

Each destination node:

Step 1: Receive the Route Request, check the reputation value, and send a Route Reply.

Step 2: Wait for data and process data on reception.

5.7 SUMMARY

Thus this chapter of the thesis explained about the on-demand routing protocol using reputation mechanism. Our approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive network services. Only by forwarding other nodes' packets a node can maintain a high reputation value. Thus behaving selfish will not help them. This encourages nodes to be cooperative. Here no node is malicious. The aim of misbehaving nodes is just
to conserve energy. But conserving energy for the sake of self transmission is not possible due to the implementation of reputation mechanism over the routing protocol. This approach has the clear advantage of simplicity, ability to get a trustworthy route etc. But this approach does not consider the malicious nodes. Malicious nodes may disturb the communication by redirecting the Route Requests or simply dropping the Route Requests, or dropping or misdirecting the data packets etc. Since the main concentration of the thesis is on the selfish nodes, malicious nodes are not considered. The same reputation mechanism can be improved to handle malicious nodes by using mobile agents which is explained in next chapter.