CHAPTER 5

DYNAMIC ENDORSEMENT SCHEME

Pervasive Network (PN) is a network which can grant different services as of single Access point. One of the applications of these networks is appeared as VANET. Vehicular ad-hoc network is a network which contains vehicles as their participants. The vehicle to vehicle communication and the vehicle to road side based station are possible in VANET. In VANET, each and every vehicle has high mobility. Hence, the nodes in the VANET are vulnerable to several attacks like movement tracking, DoS attack. So, there is a need to provide high security in the communication between the vehicles. The VANET uses the Geographical Positioning System (GPS) to capture the geographical position of each vehicle. In this case, Each and every vehicle is free to capture the geographical location of all other vehicles in a region. To restrict the accessibility of individual information, a Dynamic Endorsement Scheme (DES) is proposed. As the VANET is used in the patrol control system, the accessibility of patrol vehicle information by culprits needs to be restricted.

5.1 MOTIVATION FOR DES DESIGN

VANETS come under the category of wireless ad-hoc network. In vehicular ad-hoc network the node may be a vehicle or the road side units. The nodes can communicate with each other by allowing the wireless connection up to a particular range. The VANET is mainly used to exchange the traffic condition to avoid accident. Nowadays VANET is widely used for entertainment. The best example is TracNet which was introduced by Microsoft. It is used to provide internet access in vehicles.

The security challenges in VANET include three major things. First, information confidentially in which the unauthenticated access to the information is denied. So, a vehicle cannot access another vehicle without getting permission.
Second, is the integrity of the exchanged information in VANET. The integrity of information refers to the prevention of malicious actions like information alteration, information removal etc. The integrity of exchanged information prevents vehicle from broadcasting the wrong traffic conditions. Third one is the vehicle authentication. Vehicle authentication plays a vital role to detect that which nodes belong to the same network or which have the privilege to access the network.

5.2 DYNAMIC ENDORSEMENT SCHEME

The VANET application in Patrol Control System is considered. The patrol control system is used for vehicle tracking and trace out the location of the culprit vehicles. In that process the RSU is also involved. In patrol control system, it is required to provide privacy for all the vehicles but at the same time the safety messages should be exchanged between the vehicles. The ultimate goal of the VANET is to provide safety to the drivers. So, the dynamic endorsement scheme is proposed to achieve privacy and the proper exchange of safety messages.

![Figure 5.1 Block diagram of Dynamic Endorsement Scheme](image-url)
Figure 5.1 is the block diagram of the proposed scheme. The road side unit stores all the vehicle information including patrol ID. The patrol vehicle has the power to control all the vehicles in its region. The vehicles exchange the traffic condition with the vehicles in its region. The nodes do not know about each other, because all the information is exchanged in the form of anonymous messages. In case, if any one of the vehicles is in need of another vehicle’s information, it has to send the authentication request to that vehicle with its vehicle Id and its location information. On receiving the authentication request, the RSU verifies the authentication request and then it checks with the vehicle ID which it has. Only by using that authenticated code it can access the private information of the vehicle. The steps involved in the proposed scheme are as follows:

**Steps Involved:**

- The road side base station stores the patrol ID information. So, the patrol vehicle has the control on all the vehicles in its region.

- All vehicles in a region can receive the message from all other vehicles in the same region. But, DES restricts to access the information of other vehicle. So that the accident alert messages and traffic status information can be received by all nodes as the anonymous message.

- If one vehicle wants to access the information of another vehicle means, it sends an authentication request to that vehicle.

- The authentication request contains the vehicle ID and current location of the vehicle information.

- If the vehicle wants to provide the authentication, it generates a authentication code by using the following equation (4).
\[ A_{\text{code}} = (m \cdot V_{\text{ID}}) + n \quad (4) \]

Where,

\( m, n \) are the randomly generated largest prime number.

\( V_{\text{ID}} \) refers to Vehicle identification number

- This authentication code is used to access the information from a secured vehicle.
- This authentication code dynamically changes as the region changes dynamically.

As the vehicles are moving with high speed, the VANET is vulnerable to several attacks. The proposed scheme uses authentication code to provide the privacy of the vehicles. If the authentication code is captured by the adversaries, it means they can easily access the private information in the unauthenticated way.

### 5.3 SIMULATION RESULTS

Simulations were performed in the Network Simulator (NS2). The results obtained from the network simulator to analyze the efficiency of the proposed system include packet delivery rate, packet loss rate and delay. The simulation parameters used for simulation of DES and Public key approach are shown in table 5.1 below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Type</td>
<td>Wireless Channel</td>
</tr>
<tr>
<td>Radio Propagation model</td>
<td>TwoRayGround</td>
</tr>
<tr>
<td>Network interface type</td>
<td>WirelessPhy</td>
</tr>
<tr>
<td>MAC Type</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>Interface Queue Type</td>
<td>PriQueue</td>
</tr>
<tr>
<td>Link Layer Type</td>
<td>LL</td>
</tr>
<tr>
<td>Antenna Model</td>
<td>Omni Antenna</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>100 ms</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>24</td>
</tr>
<tr>
<td>Packet Size</td>
<td>100 bytes</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>1500 x 1500 m</td>
</tr>
</tbody>
</table>
Packet Delivery Rate (PDR):

The performance of the proposed method is analyzed by comparing its performance with the existing public key approach technique. Packet delivery rate is obtained by plotting the number of packets delivered (Y axis) against the simulation time in ms (X axis) for both DES and public key approaches.

![Packet Delivery Rate Graph](image)

**Figure 5.2** Packet delivery rate graph of DES and Public key approach

From figure 5.2, it is obvious that, the proposed technique DES outperforms the existing public key approach in terms of packet delivery rate. The packet delivery rate is calculated by using the formula in (5):

\[
PDR = \frac{\sum \text{Number of packets received}}{\text{Time}}
\]  

(5)

The number of packets delivered successfully to the destination for the particular period is called as packet delivery rate. The packet delivery rate is also one of the QoS parameters. The packet delivery rate depends on the interface queue size and the traffic flow in the network.
**Packet Loss Rate (PLR):** The packet loss rate refers to the number of packets dropped per unit time of the simulation period. It is obtained by plotting the number of packets lost (Y axis) against the simulation time in ms (X axis).

![Packet Loss Rate Graph](image)

Figure 5.3 Packet loss rate graph of DES and Public key approach

Figure 5.3 shows that, the packet loss rate for the proposed method is very low when compared with existing method public key approach. The packet loss rate is calculated by using the following formula:

\[
PLR = \frac{Number \ of \ packets \ sent - Number \ of \ packets \ delivered}{Time}
\]  

(6)

The lower value of packet loss rate indicates the better performance of the proposed method. The packet loss rate depends on the interface queue size, the traffic flow and the malicious behavior of the network.

**End to End Delay (ETED):** The end to end delay means that the time taken by a data packet to reach the destination. Otherwise, the difference between time in which the last packet delivered and the time in which the current packet reaches the destination.
The delay (Y axis) is plotted against simulation time in ms (X axis) using the last Packet Time parameter in NS2 for both DES and Public key approaches.

Figure 5.4 shows the graph plotted for the DES delay and the existing public key approach. From that, it is observed that the proposed method outperforms than the existing public key approach. The lower value of delay indicates the better performance of the proposed method.

5.4 SUMMARY

The Dynamic Endorsement Scheme (DES) is designed and simulated to improve the security of the VANETs. Simulation results have shown that DES provides 20% greater packet delivery rate than the public key approach. Also the packet loss and delay are minimized by 50% by DES when compared to the public key approach. Hence the performance of the network is increased along with the security of the network.