Security over Wormhole Attack in VANET Network System

Shahuraje Nikam  
Research Scholar, Department of CSE, IES College of Technology, Bhopal, Madhya Pradesh, India

Anshul Sarawagi  
Assistant Professor, Department of CSE, IES College of Technology, Bhopal, Madhya Pradesh, India

DOI: 10.23956/ijarcsse/V7I6/0325

Abstract: VANET plays important role while dealing with different vehicle communication. Security threats are always rising while working with heavy and public network. In past technique different dissemination techniques were introduced which deals with the security and proper communication in between the nodes and traffic. In this paper, previous approach over the data transmission is performed which deals with the lacking of security terms. Here a presentation of secure ECC with dynamic heuristic approach is presented which exhibit proper performance parameter while communicating in VANET network.

Keywords: VANET, Heuristic algorithm, security VANET, data dissemination, Elliptic Curve Cryptography, RSU, Security in VANET, Encryption approach.

I. INTRODUCTION

Major challenge of dynamic reconfiguration is Quality of Service (QoS) assurance, which is meant to reduce application disruption to the minimum for the system’s transformation. However, this problem has not been well studied. This paper investigates the problem for component-based software systems from three points of view. First, the whole spectrum of QoS characteristics is defined. Second, the logical and physical requirements for QoS characteristics are analyzed and solutions to achieve them are proposed. Third, prior work is classified by QoS characteristics and then realized by abstract reconfiguration strategies.

Vehicular ad-hoc networks (VANETs) are intended to enable communication between vehicles, with or without fixed infrastructure. VANET (Vehicle Ad-hoc Networks) is eminent technologies that they deserve the consideration and attention of the industry and the academics organizations and institutions. The vehicular communication (VC) meet in the center point of various activities of the research that improve the security and the productivity of transportation system, providing, for example, affirmations of the encompassing conditions (snow, fire, and so on.), movement in the street conditions (emergency, construction sites, or congestion).

Congestion control is an essential research issue to ensure reliable and safe vehicle to vehicle (V2V) communication by utilizing the limited resource which are available as a part of vehicular ad-hoc networks (VANET). Every vehicle in VANET is a node which can transmit its own message and can receive messages from different vehicles [3].

It generally deals with the technical obstacles that occur in the deployment of VANET. For example:

- **Environmental Impact:** For deploying the VANET some conditions should be considered. VANET generally uses electromagnetic waves for communication. These waves sometimes effected by the environmental conditions. So environmental conditions can have a serious impact on VANET. As it can affect the reliability of vehicular networks. Environment is one of the major issue in VANET.

- **Congestion and collision Control:** The network size or the unbounded network can also create a challenge. The traffic conditions are low in rural areas and low in the night in urban areas. Due to this, the network partitions frequently occurs due to the traffic load while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network. So to maintain the vehicular network it should be kept in mind that it can be easily maintained in high density areas and low density areas. Network should not be partition in low density area and should not be congested in high density area.

- **Network Management:** Due to high mobility in the network, the network topology and channel condition change rapidly. Because of this, we can’t use structures like tree because these structures can’t be set up and maintained as rapidly as the topology changed. SO here the mobility is directly affecting the vehicular network.

- **Security:** The VANET generally provides the applications of providing the safety and security to the user on roads so the safety of these messages should also be secures and satisfied. As the wrong transmission of messages in vehicular network can also trouble people so it is important that message should be secure and satisfied.

II. LITERATURE REVIEW

Overviews over the various techniques which are used to control congestion are presented in this section.
In paper Savas Konur and Michael Fisher[6]. Vehicular ad hoc networks (VANETs), which are a class of Vehicular ad hoc networks, have recently created a standard method for correspondence among moving vehicles. Since VANETs are imperative to the wellbeing and safety of the vehicles, the people and the infrastructure, a profound analysis of their potential behavior is obviously required. In this paper they give this analysis using formal verification. In particular, they formally examine a particular congestion control protocol for VANETs utilizing a probabilistic model checking procedure, and researching its effectiveness and adequacy.

In paper Author Trishita Ghosh and Sulata Mitra [7]. The remote access in vehicular environment system is created for upgrading the driving security and comfort of car users. In any case, such framework endures from quality of service degradation for security applications brought on by the direct congestion in scenarios with high vehicle density. The work is a congestion control technique in which vehicular networks are safe from congestion. It supports the correspondence of protected and unprotected messages among vehicles and infrastructure.

III. PROBLEM IDENTIFICATION

As per observed there are different problem formulation associated which deals with the existing communication protocol. These are the following protocol identification and problems which gives the drawback of previous algorithm.

1. No efficient approach for the prevention of Wormhole attack is given, most of the algorithm work towards the wormhole attach detection only.
2. Routing approach such as DSR and other DSDV are vector driven which make use of existing computed values.
3. No efficient energy based and enhanced algorithm to select an optimized path is investigated which can further be merging in security aspects and provide a unique path for communication.
4. No Approach which make of security algorithm with complex structure to deal with the anomaly and packet security is committed. Thus an efficient security is required.
5. Algorithm with efficient packet delivery along with maximum security is nowhere introduced.
6. Previous algorithm exhibit low security with low throughput and also perform with high end to end delay.

Thus these are the problem issues arise in previous techniques which still need to overcome and solve in the further delivery.

IV. PROPOSED TECHNIQUE

In existing techniques there are various variants of AODV with security and other routing techniques are presented. But, in this technique multiple routes are considered to provide solution. Thus selection mechanism is required to select an optimized route to transmit packet. That process consumes too much time which increases the waiting time to route packets, which increases the delay which degrades the performance of the whole technique. In there are multiple links presented to connect one node to other, when an optimized route selected some other shortest route also selected with that which also increases the normalized routing ratio.

![Flow Diagram for proposed technique](image-url)
A new technique is required which resolves all the routing related issues in existing techniques. A security based technique is presented which provides an enhance mechanism to route packet from source to the destination. In this technique a one hop energizing for all the nodes is conducted. Energy is formed in a manner, each node having one link to the other node to transmit data packet. That reduces the time taken to route packet from source to the destination node. Because it takes small span of time to select optimized route to deliver packet from source to the destination.

In that technique first energy head for the energy is performed, to select energy head a hello message from one node is broadcasted, replies for that broadcasted message are counted which comes from the various nodes. Then a comparison for the last information sent by different nodes is conducted. If two nodes information matched then a check for the speed of the nodes is conducted the node having higher speed is selected as a energy head.

In the figure 1 above a flow diagram for the algorithm is given which works towards the complete flow followed in approach.

V. PROPOSED ALGORITHM

Inputs: Nodes, Input packet, Key, Security parameter, AODV protocol.
Output: Packet transfer, secure packet, optimal route, parameter computation which is PDR, delay and throughput.

Steps:
Begin- foreach(Packet i-n) {
Algorithm initialized();
Key generation ECC();
AODV setup();
findingOptimalHead();
Energyroute selection ();
Return efficient path ();
Security packet transmission();
}
Compute PDR();
Compute End to End Delay();
Compute throughput ();
Return parameter ();
Exit;
End;

VI. EXPERIMENTAL SETUP AND RESULT ANALYSIS

To actualize proposed method a NS2 network stimulator is utilized. Parameters of simulation for the proposed technique are presented in Table 1.

<table>
<thead>
<tr>
<th>Table 1: Simulation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
</tr>
<tr>
<td>Number of sources</td>
</tr>
<tr>
<td>Area</td>
</tr>
<tr>
<td>Mobility Model</td>
</tr>
<tr>
<td>Bandwidth</td>
</tr>
<tr>
<td>Velocity</td>
</tr>
<tr>
<td>Pause Time</td>
</tr>
<tr>
<td>Buffer Size</td>
</tr>
<tr>
<td>Transmission Range</td>
</tr>
<tr>
<td>Sensing Range</td>
</tr>
<tr>
<td>Packet Size</td>
</tr>
<tr>
<td>Traffic Source</td>
</tr>
<tr>
<td>MAC Protocol</td>
</tr>
</tbody>
</table>
To analysis of original VANET wormhole attack detection using effective routing, heuristic based approach and VANET efficient path with security algorithm Network Simulator (NS2) was used. The simulate are run for existing AODV and under same environment it will again be run for AODV-SEC or Modified AODV to see the comparison of performance on differences against Average Delay, Packet Delivery Ratio (PDR) and Throughput. The Modified AODV is simulated using with following scenarios given in table 1.

Packet Delivery Ratio (PDR) Vs Speed
Packet delivery ratio increases as chances of packet loss due to path breaks reduces. Clearly, modified AODV-ENC performs better than the original one.

As PDR increases, the impact is clearly on throughput that increases too. Also here Throughput is also shown.

Table 2: Throughput, PDR Vs Speed

<table>
<thead>
<tr>
<th>Speed</th>
<th>AODV Throughput</th>
<th>AODV-ENC Throughput</th>
<th>AODV PDR</th>
<th>AODV-ENC PDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>71.01</td>
<td>71.89</td>
<td>99.41</td>
<td>99.95</td>
</tr>
<tr>
<td>1</td>
<td>71.91</td>
<td>72.23</td>
<td>99.19</td>
<td>99.98</td>
</tr>
<tr>
<td>5</td>
<td>70.26</td>
<td>70.95</td>
<td>98.12</td>
<td>98.88</td>
</tr>
<tr>
<td>10</td>
<td>64.14</td>
<td>70.08</td>
<td>89.55</td>
<td>95.04</td>
</tr>
<tr>
<td>15</td>
<td>63.23</td>
<td>67.33</td>
<td>85.35</td>
<td>86.33</td>
</tr>
<tr>
<td>20</td>
<td>64.65</td>
<td>65.24</td>
<td>84.70</td>
<td>84.97</td>
</tr>
</tbody>
</table>

Table 2 above demonstrates the efficiency of our proposed algorithm using efficient parameter which is throughput and PDR.

VII. CONCLUSION
VANET and attack on its network is important while discussion with security over Vehicles. It makes use of efficient encryption approach over the packet delivery before it initiate to the network. Elliptic curve model for the security over the data packet transfer such that the packet which are being transferred are driven in given route and not be distracted. Also the efficiency is derived from the heuristic integration which gives packet transfer in particular decided path. Thus the wormhole attack is avoided using the algorithm approach followed by us. It increases the network efficiency while comparing with Computed parameter and their values shows the effectiveness of our approach.
A better communication protocol with enhancement in security along with heuristic is proposed which compute efficiency towards packet transfer and also it helps in avoid wormhole attack.

REFERENCES
