Prevention of Gray Hole Attack in Vehicular Ad-hoc Network by Enhanced Multipath Approach

Vaishali Mittal
M-Tech Student & Department of CSE & Delhi College of Technology & Management
Palwal, Haryana, India

Abstract
Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Vehicular Ad-hoc Networks (VANET). Gray hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. VANETs must have a secure way for transmission and communication which is quite challenging and vital issue.

In this paper we study the effects of Gray hole attack in VANET using both Proactive and Reactive routing protocols and then discovering a Secure Path in VANET by Avoiding Gray Holes. The measurements were taken in the light of throughput and end-to-end delay under 150 nodes. Simulation is done in Optimized Network Engineering Tool (OPNET) 16.0.

Keywords: Ad hoc Networks, AODV, Gray Hole, VANET, OLSR, OPNET.

I. INTRODUCTION

The increasing demand of wireless communication and wireless devices have tends to research on self organizing, self healing networks without the interference of any centralized or pre-established infrastructure/authority [2]. The networks with the absence of any centralized or pre-established infrastructure are known as Ad hoc networks [4]. Ad hoc Networks are the category of wireless networks that uses multi hop radio relay.

Figure 1.1: Working structure of VANET

1.1 VANET Architecture:

Vehicular Ad hoc Network (VANET) system architecture [5] consists of three different types of domains such as in-vehicle, ad hoc, and infrastructure domains and many individual components such as application unit, on-board unit, and road-side unit.
The figure 1.2[14] shows the all components and domains of VANET.

**In-Vehicle Domain:** This domain consists of one or more applications units (AUs) and a single On-Board Unit (OBU) that resides inside a vehicle [19]. Applications Units (AUs) is an in-vehicle entity, multiple AUs can be plugged in with a single OBU and share the OBU processing and wireless resources. An On-Board Unit (OBU) is used for providing the vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. An OBU is equipped with a single network device based on IEEE 802.11p radio technology; basically network device is used for sending, receiving and forwarding the safety and non-safety messages in the ad hoc domain.

**Ad hoc Domain:** This VANET domain composed of vehicles or nodes that equipped with On-Board Unit (OBUs) and road-side units (RSUs), that forming the VANET [19]. A road side unit is a physical device located at fixed positions like hospitals, shopping complexes, colleges, road highways etc. An RSU is equipped with at least a network device based on IEEE 802.11p standard [30]. The main function of RSU is to provide the internet connectivity to the OBUs. On-Board Units (OBUs) form a Vehicular ad hoc network that allows communications among vehicles without the need for a centralised coordination instance. Two vehicles directly communicate via On-Board Units (OBUs) if wireless connectivity exists among them; else multi-hop communications are used to forward data [30].

**Infrastructure Domain:** The infrastructure domain consists of Road-Side Units (RSUs) and wireless Hot-Spots (HS) that the vehicles access for safety and comfort based applications [18, 29]. These two types of infrastructure access, road-side units (RSU) and Hot-Spots (HS). In case that neither road-side units (RSUs) nor Hot-Spots (HS) provide internet access, OBUs can also utilise communication abilities of several radio networks or technologies such as GPRS, GSM, WiMax, if they are integrated in the On-Board Unit (OBU), in particular for non-safety applications.

**Application Units (AUs):** An Applications Units (AUs) is an in-vehicle entity, multiple AUs can be plugged in with a single OBU and share the OBU processing and wireless resources [29]. Examples of Application Units (AUs) are I) safety applications devices like hazard-warning, or ii) a navigation system with communication capabilities. Multiple Application Units can be plugged in with a single On-Board Unit (OBU) simultaneously and share the On-Board Units (OBUs) processing and wireless resources. An Application Unit (AU) communicates solely via the On-Board Unit (OBU), which handles all mobility and networking functions on the...
Application Unit (AU) behalf. The distinction between an Application Unit (AU) and an On-Board Unit (OBU) is only logical and an Application Unit (AU) can be physically co-located with an OBU [29].

On-Board Units (OBUs): The On-Board Unit (OBU) used for vehicle to vehicle (V2V) communications and vehicle to infrastructure or roadside unit (V2I) communications [29]. It also provides communication services to the application units and also forwards data on behalf of other On-Board Units (OBUs) in the ad hoc domain. An On-Board Unit (OBU) is equipped with at least a single network device f IEEE 802.11p standard. This network device is responsible for sending, receiving and forwarding safety and non safety messages in the ad-hoc domain. The main functions and procedures of On-Board Unit (OBU) includes wireless radio access, geographical ad hoc routing, network congestion control, reliable message transfer, data security, IP mobility support, and others.

Road-Side Units (RSUs): A Road-Side Unit (RSU) is a physical device situated at fixed positions along roads and highways, or at dedicated locations such as colleges, petrol pumps, parking places, hospitals, shopping complexes, restaurants etc [19, 29]. A Road-Side Unit (RSU) is equipped with at least a network device based on IEEE 802.11p. The main function of RSU is to provide the internet connectivity to the OBUs. An overview of the main functions performed by RSU is given below.

i. Extending the communication range of an ad hoc network by means of re-distribution of information to other OBUs and cooperating with other RSUs in forwarding or in distributing safety information (Figure 1.4).

ii. Running safety applications, such as for vehicle-to-infrastructure warning (e.g. low bridge warning, work-zone warning), and act as information source (Figure 1.5).

iii. Providing internet connectivity to all OBUs for accessing safety and non safety applications (Figure 1.6).

Figure 1.3: RSU extends communication range

Figure 1.4: RSU acts as information source

Figure 1.5: RSU providing internet access

II Gray hole Attack in VANET

In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against Gray hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node. [4]The Gray Hole attack has two
phases. Initially, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. Next, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the Gray Hole attack where the malicious node drops the received data packets with certainty. A Gray Hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. A Gray Hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

![GRAYHOLE ATTACK](image)

### III RELATED WORKS

Research related to MANETs covers many topics such as routing, security, and defence strategies against threats like black hole attacks. This section gives a brief discussion of some of the research that is closely related to the topic of this paper.

Marti et al. [2] presented a method that uses Watchdog and Pathrater to detect black hole attacks. The Watchdog enables neighbour nodes to overhear and detect malicious nodes. Watchdog makes it possible to detect malicious nodes by finding nodes that are deliberately discarding packets. Pathrater assigns a default value to each node and then observes the transmitting behaviour of each node. The value for each node changes based on the transmitting behaviour of that node. After a period of time, if the value for a node is below a certain threshold, the node will be added to the list of black hole nodes. These methods have the same detection to find malicious node, when the neighbour reply wrong observing message. In other words, this method cannot handle collaborative attacks. If the neighbor nodes collude with each other, they may be able to avoid detection.

Lu et al. [3] proposed the SAODV black hole detection scheme for MANETs that is designed to address some of the security weaknesses of AODV and withstand black hole attacks.

Deswal and Singh [4] created an enhanced version of the SAODV protocol that includes password security for each of the routing nodes and routing tables that are updated based on timeliness.

Ramaswamy et al. [5] proposed a method for identifying multiple black hole nodes. They were the first to propose a solution for cooperative black hole attacks. They modified the AODV protocol slightly by introducing a Data Routing Information (DRI) table and a cross checking mechanism. Each entry of the node is maintained by the table. This method uses the reliable nodes to transfer the packets.

Hongmei Deng et al. [6] proposed a methodology that asks every intermediate node to return next hop information along with the RREPs once a route to a destination has been determined. The source node does not transmit data packets to an intermediate node immediately. Instead, the source node waits for the RREPs and the next hop information and then sends Further Request to the next hop in order to determine if there is a route between it and the intermediate node and also to determine if there is a route to the destination. The source node receives Further Reply from the next hop. If the answers are yes for both questions, then the route is built. If the answer to either of the questions is no, then the source node will send an alarm packet to alert other nodes on the network. This methodology has an obvious drawback though. It only can address a single black hole. It cannot prevent cooperative black hole attacks if the next hop colludes with the former. In a situation like this, the source gets the wrong message. Most of the research papers above discussed methods for avoiding black hole attacks against MANETs that are based on the AODV protocol and other protocols. However, our proposed mechanism is a new solution that provides high performance and prevents black hole attacks on the AODV protocol.
IV Simulation Environment

OPNET: Optimized Network Engineering Tool (OPNET) is a commercial network simulator environment used for simulations of both wired and wireless networks. It allows the user to design and study the network communication devices, protocols, individual applications and also simulate the performance of routing protocol.

V Simulation Parameters

<table>
<thead>
<tr>
<th>Examined Protocols Cases</th>
<th>AODV with and without Gray Hole Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>100 and 150</td>
</tr>
<tr>
<td>Types of Nodes</td>
<td>Vehicular</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>55*55 km</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>1800 seconds</td>
</tr>
<tr>
<td>Mobility</td>
<td>Uniform(50-100) m/s</td>
</tr>
<tr>
<td>Pause Time</td>
<td>100 seconds</td>
</tr>
<tr>
<td>Performance Parameters</td>
<td>Throughput, Delay, Network load</td>
</tr>
<tr>
<td>No. of Gray Hole Node</td>
<td>10</td>
</tr>
<tr>
<td>Trajectory</td>
<td>VECTOR</td>
</tr>
<tr>
<td>Data Type</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td>Packet Size</td>
<td>1024 bytes</td>
</tr>
<tr>
<td>Traffic type</td>
<td>FTP, Http</td>
</tr>
<tr>
<td>Active Route Timeout(sec)</td>
<td>3</td>
</tr>
<tr>
<td>Hello interval(sec)</td>
<td>1,2</td>
</tr>
<tr>
<td>Hello Loss</td>
<td>3</td>
</tr>
<tr>
<td>Timeout Buffer</td>
<td>2</td>
</tr>
<tr>
<td>Physical Characteristics</td>
<td>Extended rate IEEE 802.11g (OFDM)</td>
</tr>
<tr>
<td>Data Rates(bps)</td>
<td>54 Mbps</td>
</tr>
<tr>
<td>Transmit Power</td>
<td>0.005</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>1024</td>
</tr>
<tr>
<td>Packet-Reception Threshold</td>
<td>-95</td>
</tr>
<tr>
<td>Performance Parameters</td>
<td>Throughput, Delay, Network load</td>
</tr>
<tr>
<td>Trajectory</td>
<td>VECTOR</td>
</tr>
<tr>
<td>Long Retry Limit</td>
<td>4</td>
</tr>
<tr>
<td>Max Receive Lifetime (seconds)</td>
<td>0.5</td>
</tr>
<tr>
<td>Buffer Size(bits)</td>
<td>25600</td>
</tr>
</tbody>
</table>

V I Proposed Algorithm

To avoid the gray hole attack, proposed algorithm has been implemented in scenario affected by gray hole attacks and this tried to normalize the scenario to its original state. Proposed algorithm, randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as gray hole attack is done by transmitter and receiver so have to decide the transmitter and receiver. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count.hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm checked the delay of all previous routes which involve any on node of the suspicious route. The node not encounter previously should be malicious. Now to find out exact malicious node, there is need to repeat the whole algorithm if more than one node is misbehaving and that will take time and resources. So to avoid this condition, transmitter will be seeking help from directly connected neighbours. Neighbours can tell the history of particular node under suspect. The node which is not involved in any of the previous activity considered to be the malicious node. Malicious nodes have been blacklisted by the nodes and hence they are not involved in future routes.

SN: Source Node
DN: Destination Node
IN: Intermediate Node
TH: Threshold
D_Seq : Destination Sequence Number
Seq: Sequence Number
1. SN broadcasts RREQ to all Nodes
2. IN receives RREQ and forwards until reach DN
3. DN receives RREQ from SN or IN
4. DN gets Seq from RREQ and verifies with Seq in its routing table
5. If Seq of RREQ is greater than Seq of its routing table
6. DN selects Seq of RREQ and plus one
7. Else
8. DN selects Seq of its routing table and plus one
9. If number of packet drop is large then start discovery of malfunctioning nodes.
10. Source and destination will be decided. Randomly Generate a Number in between 0 to maximum number of nodes. Initiate a source by making transmitter node same selected.
11. Generate the Route from selected transmitting node to any destination node with specified average route length.
12. Send packet to destination
13. Start timer (Record (Hop Count, Delay))
14. Counter (Threshold (Hop Count, Delay))
15. Store (Route, Hop Count, Delay)
16. Gray hole Detection
17. Hop count < Threshold Then Check Delay
18. Malicious Node Selection N is the number of nodes.
19. If N = 1 Then it is the attacker Else Send Route Query to neighbours
20. If neighbour detect similar malfunctioning Then mark it malicious.
21. Else
22. Repeat process
23. Send gray_ announcement message to all nodes. Any node receives gray_ announcement message it removes gray hole node id from its neighbour table and Routing Table.
24. If any forwarding node receives gray_ announcement message it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without gray hole node.
25. End.

Fig 6.1: Proposed Algorithm Overview

VII Results

Throughput:
Throughput can be defined as the ratio of the total amount of data reaches a destination from the source. The time it takes by the destination to receive the last
message is called as throughput. It can express as bytes or bits per seconds (byte/sec or bit/sec). There are some factors that affect the throughput such as; changes in topology, availability of limited bandwidth, unreliable communication between nodes and limited energy. A high throughput is absolute choice in every network.

End to End Delay:
The packet end to end delay is the average time that packets take to traverse in the network. This is the time from the generation of the packet by the sender node up to their reception at the destination and is expressed in seconds. Hence all the delays in the network are called packet end-to-end delay. It includes all the delays in the network such as propagation delay (PD), processing delay (PD), transmission delay (TD), queuing delay (QD).

VIII Conclusion
With the importance of VANET comparative to its vast potential it has still many challenges left in order to overcome. Security of VANET is one of the important features for its deployment. In our research work we proposed a feasible solution for the AODV protocol. The main concern of this work to show the performance of AODV under normal surroundings, under gray hole attack and performance after elimination of gray hole attack in term of delay, throughput and traffic received. The network performance with gray hole attack in term of throughput decreases around bits per second. By our proposed approach, we have recovered around in throughput. The network performance with gray hole attack in term of end to end delay increases around % and with our proposed approach, we have recovered around % in delay. Concept has shown improved results after elimination of the gray-hole attack in the simulation. Elimination of malicious nodes takes place on Network layer by broadcasting the
information of malicious nodes. Overall, elimination of gray hole attack has been done so that ad-hoc communication can be normalized as normal communication. It will be very useful in saving a lot of resources for mobile ad-hoc communication as we have used unicasting process instead of broadcasting which saves resources as malicious nodes are only detected through partial multicasting process. In nutshell, elimination of gray hole attack has been done so that ad-hoc communication can be normalized as normal communication.

IX References


