Detection and Prevention of Black Hole Attacks in Vehicular Ad Hoc Networks

Lakshmi.S, Mary Anita E A, Jenefa J

Abstract: ***Vehicular networks are prone to various security attacks because of its dynamic topology. One such attack is the black hole attack which advertises itself to source vehicle as the shortest path to the destination and drops the received packets. An efficient solution to detect black hole attackers in the vehicular network is proposed in this paper. It detects as well as broadcast information about the attackers to all other vehicles through RSUs. Thereby data packets will not be transmitted in the routes with attackers and it will be isolated from the network by which the network will be prevented from the black hole attack. Both simple as well as collaborative attackers are simulated and the performance of the proposed scheme is compared with that of the other related schemes. Simulation results show that the proposed scheme has better performance in terms of PDR and throughput with acceptable delay.***

Keywords: AODV, Black Hole Attack, Hash Function, Security, VANET

I. INTRODUCTION

Recently, with the increase in the number of accidents, Vehicular Adhoc NETworks (VANET) have played an efficient role in providing safe driving experience for drivers. It is considered as a sub-type of Mobile Adhoc NETwork (MANET) where vehicles act as nodes and communications are established without any infrastructure. Due to the high mobility of the vehicles, it has dynamic topology which changes in an organized pattern and hence it is prone to various security attacks. It has various security issues due to its unique characteristics. These issues have a major impact since it transmits life critical information. Communication between vehicles last for a short duration due to the mobility of the vehicles hence researchers proposed many efficient routing protocols for establishing secure communication among vehicles. They mainly focus on the increasing Packet Delivery Ratio (PDR) and throughputs with less overheads.

Routing protocols in ad hoc networks are generally classified as proactive, reactive and hybrid protocols. Proactive protocols are fully dependant on routing tables, it updates the routing information periodically and hence any time it has updated routes to all the nodes in the network. Destination Sequence Distance Vector (DSDV) is the example of proactive protocol. Reactive protocols on the other hand, it updates the route on demand from a node. Hence periodic updating of routing tables are not needed in this protocol.

Revised Manuscript Received on May 07, 2019.

Lakshmi.S, Research Scholar, AMET University, Chennai, India
Mary Anita E A, Professor/CSE, S.A.Engineering College, Chennai, India
Jenefa J, Research Scholar, Anna University, Chennai, India

Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are some of the examples of reactive protocols. Hybrid protocols use advantage of both reactive and proactive protocols, example: Zone Routing protocol.

AODV protocol is an efficient routing protocol for ad hoc networks. Researchers proposed different schemes based on the AODV protocol to avoid routing attacks. A node which has the data to be transmitted to the destination node will broadcast Route REQuest (RREQ) packet to all its nearby nodes. Neighbor nodes will either forwards the received RREQ packet to its nearby nodes (if it is not the destination node) else it will send Route REPly (RREP) packet (if it is a destination node). Thereby route for a particular node from source will be discovered in the network. A brief overview of the AODV protocol is given in further sections.

Even though the AODV protocol is an efficient routing protocol, it is prone to some routing attacks. One among the attack is the black hole attack, it is also known as the packet drop attack. Attackers, which have no intention of transmitting the received data packets will send the RREP packet to the source node as soon as it receives RREQ packet, to notify that it has the route to the destination node. After receiving data, it just drops the data packet without forwarding it to the destination. Thereby it acquires all the data packets of the destination node and just drops it. Both single as well as cooperative black hole attacks are possible in the vehicular networks which will be explained in further. The remaining paper is arranged as follows: some of the black hole detection techniques are discussed in Section II. A brief overview about the AODV protocol and the black hole attack is given in Section III. Section IV describes about the proposed work and the performance of the proposed scheme is analyzed in Section V with the simulation results. Section VIII concludes this paper.

II. RELATED WORK

Researchers proposed different schemes to detect black hole attackers in the vehicular network. Most of the schemes detect only single black hole attacks, whereas detection of the collaborative black hole attack incurs high overheads. Some of the black hole detection techniques proposed by different authors are discussed in this section. Sanzgiri et al. [7] proposed an Authenticated Routing protocol for Ad hoc Networks (ARAN). It uses cryptographic public key certificates. It maintains the routing table and finds the route efficiently. ARAN is an efficient protocol like AODV protocol. The main drawback is it has large packets which increases overheads.

Perrig et al. [11] proposed an algorithm for black hole detection in vehicular networks. It uses secret keys which are shared between vehicles to avoid attacks. It is based on Dynamic Source Routing (DSR) protocol. Even though it provides distributed framework, it still has few drawbacks when compared with that of the standard routing protocol. Dokurer et al. [3] proposed a solution for issues based on black hole attacks. It ignores the first RREP message, since the possibility of the first RREP message is from an attacker is higher and hence it has better results. But the possibility of the second RREP message sent by an attacker is not considered in this paper.

Raj and Swadas [7] proposed an efficient model to detect black hole attackers in the network. In this model, the source node will be responsible to identify the black hole attackers. It monitors the RREP message sequence number and compares it to the predetermined threshold value, if it is higher than the threshold value then the node will be identified as the attacker. After identifying the attacker, source node will alert the nearby vehicles by using ALARM packet. It has high routing overheads which are its main drawback.

Lachdhaf et al. [8] proposed a new method based on the AODV protocol to detect and prevent black hole attackers in the vehicular network. In this method, source node will use the 32 bit checksum value in the RREQ message, instead of the destination IP address. Intermediate nodes will compare its IP address checksum value with that of the received value. If it is same then it will identify it as a destination node and send the RREP message, else it will forward the message to its nearby vehicles. Thereby black hole attackers cannot send the RREP message still compromised black hole attackers can still send RREP messages which is the major drawback.

Tyagi et al. [6] proposed a new algorithm to detect the black hole attackers in the vehicular network. It is based on sequence numbers, PPREP (Pseudo Reply Packet) is used by the source node to identify the attackers. Each node will maintain a look–up table which records the details of all the received messages. If the destination sequence number is greater than the source sequence number, then the node will be identified as an attacker. This solution is not suitable for collaborative black hole attack. Jhananie et al. [12] proposed a new handshake mechanism to detect black hole attacks. Nodes will generate same dynamic value periodically. Before accepting a packet, this periodically generated dynamic value will be checked first. If the value is not same then the received message is not accepted. It cannot provide security against collaborative black hole attackers.

Saad [10] proposed a new black hole detection scheme based on AODV protocol. It focuses on collaborative black hole attackers. It detects the black hole attackers in the network by sending the confirmation message in the route of the RREP message to find the gap between the destination. If the confirmation message is not transmitted to the destination, then the attacker is detected by checking the routing table. It has high delay since it sends a confirmation message before sending the data packets. Ahmed et al. [1] compared the impact of the black hole attackers in different routing protocols: DSR, AODV, OLSR and TORA. The performance in these routing protocols is compared to determine the best routing protocol for the vehicular networks.

Cherkaoui et al. [2] proposed a new scheme using quality chart to detect the black hole attackers in the network. It uses the packet loss ratio as a metric to select the black hole attackers and then compares the metrics measure with that of the chart parameters. If there is large deviation, then the network is considered to be under black hole attack. Malathi et al. [5] proposed a novel algorithm to identify the black hole attackers in the network. Initially, a source node will send a RREQ message with the invalid destination address to all its nearby two-hop neighbors. If it receives any RREP message from its neighbors, then it will be identified as an attacker. It then sends the RREQ message with the destination address. Since it sends RREQ messages with the invalid destination address before sending the real RREQ message, it has high overheads.

III. BACKGROUND OVERVIEW

A. AODV Protocol

Ad hoc On-Demand Distance Vector (AODV) protocol is one among the reactive protocols which finds routes on demand to the destination node. These routes will be updated in the routing table of the nodes. It has two processes: route discovery and route maintenance. The route discovery process is carried out whenever it is necessary. Initially, source node will check its routing table for the route to reach destination node. If there is no such routes to the destination or if the route is inactive, then the source node will find the route for the destination route by using Route REQuest (RREQ). RREQ message will be broadcasted by the source node to all its neighbors. It will be forwarded until it reaches the destination node or a node with the route to the destination. In such case, Route REPly (RREP) message will be sent to the source node in the same route in reverse direction. RREP is a unicast message, whereas RREQ is a broadcast message.

Thereby the source node will receive different routes to the destination from which it chooses an efficient route by using the sequence number. The higher the sequence numbers the fresher the route to reach the destination. If two paths have the same sequence number, then the path with less number of hop counts will be selected. The discovered routes are maintained in the route maintenance process, the route is maintained until it is needed by the source node. If there is a path failure, then a RERR (Route ERRor) message will be sent to the source node which finds the new route by using RREQ message if it is necessary. The AODV protocol is prone to different security attacks since it has no security mechanisms. One of such attack is the black hole attack.

B. Black Hole Attack

The black hole attack is a kind of Denial of Service (DoS) attack, where the attackers drop the received packets instead of forwarding it. When a source node broadcast RREQ message to discover a route to the destination, an attacker

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

will send a RREP message claiming that it has the freshest and shortest route to the destination as soon as possible without checking its routing table. Since the route with highest sequence number is considered as fastest route, the source node will send the data packets in the route with attacker and the attacker will just drop the packets without forwarding it. Hence the main aim of the black hole attack is to make the source nodes to transfer data packets in the route with attackers. An example of the black hole attack is given in figure 1.

As shown, Vehicle S tries to discover a route to the Vehicle D. Hence it broadcasts RREQ messages to the nearby vehicles. The only route to reach vehicle D is S-A-B-D. Vehicle D on receiving the RREQ message will send RREP message which will be transmitted in the same path in reverse direction. On receiving this RREQ message, an attacker C will send fake RREP message claiming that it has a faster route to vehicle D. Attacker C will send the RREP message as soon as possible since it doesn't check its routing table. On receiving these RREP messages, vehicle S will send data to the attacker considering it has freshest route to vehicle D. Attacker C on the other hand, drops the received data without forwarding it to other vehicles. This is the simple black hole attack in vehicular networks.

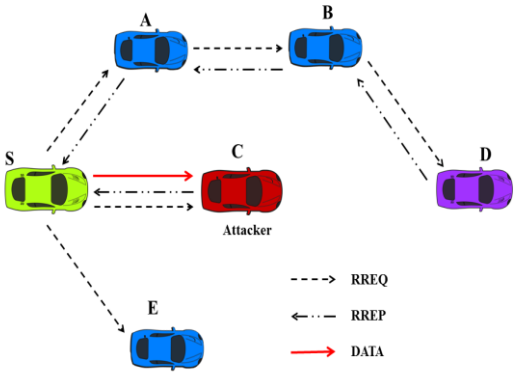

Fig. 1 Black Hole Attack

Collaborative black hole attack is done by using a group of black hole attackers [4]. These attackers will cooperate with one another and tries to receive and drop the data packets which are intended to be transmitted to the destination vehicle. An example of collaborative black hole attack is given in figure 2. As shown, both the route S-A-B-D, S-E-F-D has attackers B & F which claims that it has the fresher route to the destination node and drops the received packet. To detect such attack an efficient scheme is proposed which is explained in the next section.

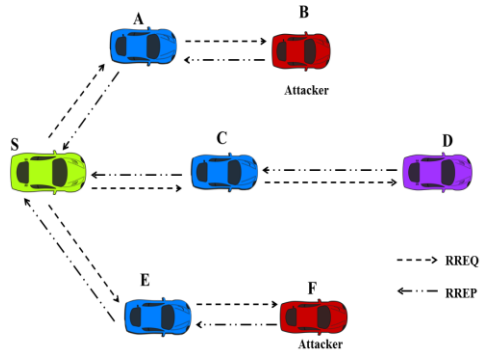

Fig. 2 Collaborative Black Hole Attack

IV. PROPOSED WORK

The proposed solution to detect and prevent black hole attackers in the vehicular network using slightly modified AODV protocol is explained in this section. Generally, in schemes based on AODV protocol, the source node will broadcast the RREQ message with the destination IP address to find a fresher route to the destination. The message format of the RREQ message is given in figure 3. In the proposed scheme, instead of 32 bit destination IP address, 32 bit hash value of the destination IP address is used. Here MD5 hash function is used to generate hash values of IP address. Since the 32 bit destination IP address is modified by the 32 bit hash value, the format of the RREQ message is slightly modified as shown in the figure 4. These hash values will be generated by TAs and disclosed to all the RSUs in that particular region. Since they are not reversible, the intended destination vehicle or the vehicle which has a route to the destination can only send the RREP message to the source. If an attacker tries to send a RREP message with some other IP address, it will be easily found during the verification process of the destination IP address and its details will be sent to nearby RSU which will be broadcasted to all the vehicles in its range.

The following are the steps involved in the proposed solution to prevent and detect black hole attack.

Step 1: When a vehicle S has data to be transmitted to the destination vehicle D, it checks whether it has a route to the D in its routing table. If it has a route, it then unicast the data in that route, else it will broadcast a RREQ message of the format as shown in figure 3 to all its neighbors.

Step 2: Intermediate vehicles on receiving a RREQ message, first checks whether the hash value of the destination IP address is its assigned hash value,

Step 2.1: If so, it is the destination to which the source is discovering a route to transmit data. Hence it will unicast the RREP message with its IP address in the same path in reverse direction.

Step 2.2: Else, it will check its routing table for a fresher route to the destination and unicast the RREP message with the destination IP address stored in its routing table to the source vehicle in the same path in reverse direction.it is not a destination and if it does not have a route to the destination, then it forwards the RREQ message to all its neighbors. This process is repeated until the destination or a route to the destination is found.

Step 3: After receiving the RREP message, vehicle S will first check the IP address of the destination,

Step 3.1: If it is the address of an indented destination, it then checks the sequence number of the received RREP message, if the received sequence number is <= the average of all the received sequence numbers of RREP messages, then the route is updated in its routing table and the data is transmitted in that route to the destination, else the route is discarded and the node from which it receives the RREP message will be detected as the black hole attacker.

Step 3.2: Else the route is discarded and the node from which it receives the RREP message will be detected as the black hole attacker. After detecting the black hole attacker, it will send attacker's information to the nearby RSU which will be broadcasted to all the vehicles and other RSUs in that region.

Thereby it detects both the simple as well as collaborative black hole attackers and prevents the network from the attackers by broadcasting attacker's to all its neighbors

V. SIMULATION RESULTS

The proposed scheme is simulated in NS2 with 125 nodes, 3 RSUs and one TA in the operating region of about 5000 x 5000m. AODV routing protocol is used and both the simple as well as collaborative black hole attackers are placed manually in the vehicular network. Vehicles communicate with other vehicles by transmitting packets, a size of about 512 bytes. The performance of the proposed scheme is analyzed with the parameters like Throughput, Packet Delivery Ratio and End-to-End delay. Comparison of the proposed scheme with that of the other related schemes is also given in this section.

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP address							
Destination sequence number							
Originator IP address							
Originator sequence number							

Fig. 3 Original Message Format of RREQ Message

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
32 bit Hash value (Destination IP address)							
Destination sequence number							
Originator IP address							
Originator sequence number							

Fig. 4 Modified Message Format of RREQ Message

Throughput is used to determine the amount of data which is sent from one node to another in a given time. It is the ratio of the size of the received data to that of the time difference between received and sent packets. The formula to compute throughput is given below,

Throughput = Size of Received Data / Received Time – Sent Time

The throughput of the proposed scheme is compared with other recent related schemes, which is given in figure 5. As shown the throughput of the proposed scheme on an average is 12%, 43.2% higher than Saad [10] and Lachdef et al. [8] schemes. Ahmed et al. [1] scheme has 35% higher throughput than the proposed scheme since it didn't focus on collaborative black hole attackers. Hence the proposed scheme has better throughput

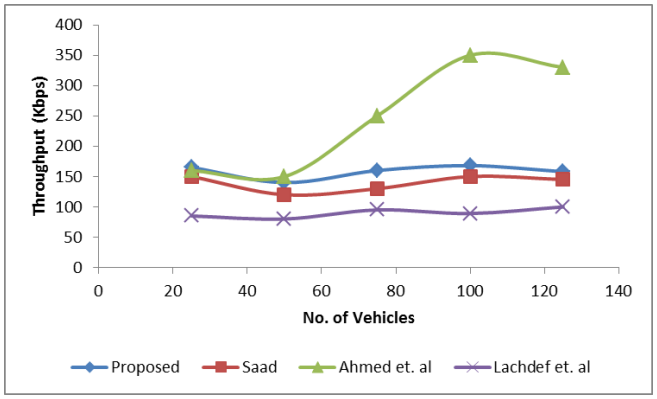

Fig. 5 Throughput for varying Number of Vehicles

End-to-End Delay is the time taken by a packet to reach the destination. The time to discover a route to the destination is also included. Delay is determined by finding the time difference between the received and sent packets as given in the formula below,

Delay = Received Time of Packet – Sent Time of Packet

The End-to-End delay of the proposed scheme is compared with other recent related works, which is given in figure 6. As shown the proposed scheme has less delay when compared to that of other schemes since the route discovered to send packets is the freshest and shortest route.

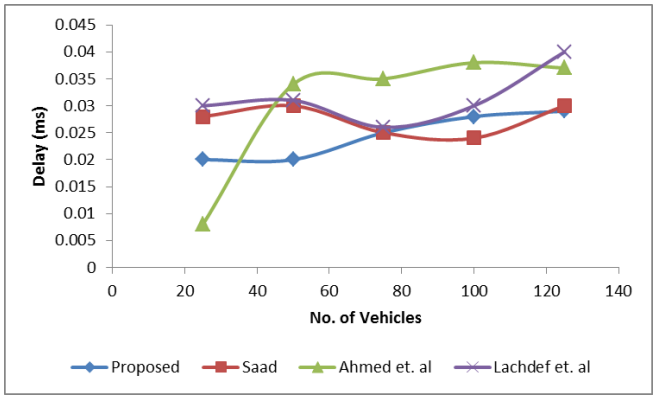

Fig. 6 Delay for varying Number of Vehicles

Packet Delivery Ratio (PDR) is the percentage of the number of packets dropped to that of the number of packets sent. The formula to compute PDR is given below,

PDR = (Packets Dropped / Number of Packets Sent) * 100

where, Packets dropped is the difference between the number of packets sent and received (Packets Dropped = Number of packets sent – Number of packets received). The PDR of the proposed scheme is compared with other schemes as shown in figure 7. As shown, the proposed scheme has a high PDR than other schemes since the number of packets dropped is reduced by detecting the black hole attackers in an efficient way.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The PDR in the proposed scheme is 71.9, 34.9% and 3% higher than Saad et al. [10], Ahmed et al. [1] and Lachdef et al. [8].

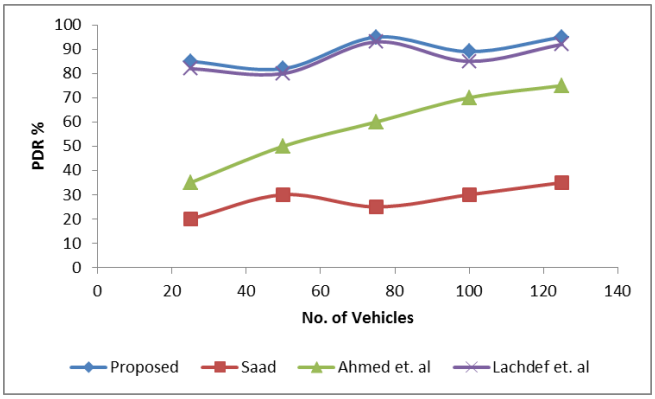

Fig. 7 PDR for varying Number of Vehicles

VI. CONCLUSION

An Efficient solution to detect black hole attackers in the vehicular network is proposed in this paper. Vehicles will use destination vehicle's hash value instead of IP address in the request message. Hence, only the respective destination vehicle can send the reply message with its IP address. Once a vehicle detects an attacker, it sends the information about the attacker to the nearby RSU which in turns forwards it to all the vehicles in its range and to the nearby RSUs. Thereby vehicles will not send packets in the route which has the attackers. Both simple as well as collaborative black hole attackers are considered and detected efficiently. Simulation results show that the proposed scheme has better performance in terms of PDR, throughput and delay. It has high PDR and throughput with acceptable delay.

REFERENCES

1. Ahmed, E.F., R.A. Abouhogail and A. Yahya, "Performance evaluation of black hole attack on VANET's routing protocols", Int. J. Software Eng. Applic., 8: 39-54, 2014.
2. Badreddine Cherkaoui, Abderrahim Beni-Hssane, Mohammed Erritali, "Quality Control Chart for Detecting Black Hole Attack in Vehicular Ad Hoc Networks", The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017), pp. 170-177, 2017.
3. Dokurer Semih, Erten YM, Acar Can Erkin, "Performance analysis of ad-hoc networks under black hole attacks", Southeast con. Proceedings, IEEE, pp. 148–53, 2007.
4. John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy, "An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs", 16th European Conference on Cyber Warfare and Security, Jun 2017.
5. Malathi and Sreenath, "Black Hole Attack Prevention and Detection in VANET using Modified DSR Protocol", International Journal of Computer Applications, pp.27-30, June 2017.
6. Parul Tyagi, Deepak Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)", pp. 133-139, Nov. 2016.
7. Raj Payal N, Swadas Prashant B, "DPRAODV: A dynamic learning system against black hole Attack in AODV based MANET ", Int J Comput Sci Issues, 2:54–9, 2009.
8. Salim Lachdhaf, Mohammed Mazouzi, Mohamed Abid, "Detection And Prevention Of Black Hole Attack In Vanet Using Secured Aodv Routing Protocol", Conf. Computer Science and Information Technology, pp. 25-36, Nov. 2017.
9. Sanzgiri Kimaya, Dahill B, "A secure routing protocol for Ad hoc networks", 10th IEEE international conference on network protocols (ICNP" 02), pp.78–87. Nov. 2002.
10. Taha Saad, "Performance Evaluation of Black Hole Attack on AODV in VANET", American Journal of Applied Sciences, pp. 141-148, 2014.
11. Yih-Chun, Perrig Adrian, Johnson David B. Ariadne, "A secure on-demand routing protocol for AdHoc networks", MobiCom'02 proceedings of the 8 annual international conference on mobile computing and networking, pp. 12–23, 2002.
12. Viswa Jhananie. K.R, Dr.C.Chandrasekar, "Detection and Removal of Black Hole Attack using Handshake Mechanism in MANET and VANET", IOSR Journal of Mobile Computing & Application (IOSR-JMCA), pp. 1-5, March 2015.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication