Black Hole Attack Prevention and Detection in VANET using Modified DSR Protocol

A. Malathi
Research Scholar
Department of Computer Science
Pondicherry Engineering College
Puducherry

N. Sreenath, PhD
Professor
Department of Computer Science
Pondicherry Engineering College
Puducherry

ABSTRACT
Vehicular Ad hoc Network is one of the interesting and attractive topics in the recent years. It has a potential to achieve intelligent inter vehicle communication for the benefit of the vehicle user. The VANET has lot of challenges. These decentralized dynamic networks require a secure communication. These networks are vulnerable to various attacks. In this paper the security features of routing protocols and about the black hole attacks are examined and an enhanced DSR algorithm called MDSR protocol to detect and prevent from black hole attack is proposed. The simulation is performed in NS2. The simulation result ensures that the attack detection by using Modified DSR (MDSR) protocol for message authentication provides a secured communication.

General Terms
Security, Black Hole Attack, Modified DSR.

Keywords
VANET, security, AODV, DSR, Black Hole attack, Packet delivery Ratio, End-to-end delay

1. INTRODUCTION
VANET is an important component of Intelligent Transportation System. VANET creates a mobile network among moving vehicles with or without the support of infrastructure or Roadside Unit(RSU) for providing a intelligent services like Real-time traffic, Co-operative Message Transfer, Post Crash Notification, Road Hazard Control Notification, Cooperative Collision Warning, Traffic Vigilance, Route Diversions, Active Prediction etc. VANET utilizes the dedicated short-range communications (DSRC) frequency bands to provide the wireless access to interact with vehicles as well with the infrastructure. The wireless access in vehicular environments (WAVE) is significantly different from the Wi-Fi and cellular wireless networking environments. The specifications of DSRC/WAVE networks are defined by IEEE802.11P and IEEE1609. The structure of VANET is shown in Figure1.

The main intention of the VANET is to enhance vehicle user's safety. Efficient routing of the data is a challenge to VANET. Although the designing and maintaining a routing protocol is a difficult task, the wireless medium is vulnerable to several attacks. These attacks mislead the communication process and other operations. In this perspective security is an obligatory in VANET communication process. Security is an important and challenging issue in VANET.

A security of the Vehicular ad hoc network has to be maintained by satisfying the requirements like Authentication, Authorization, Data Consistency, Confidentiality, Integrity, Availability, Non Repudiation, Driver Privacy etc..

In order to provide a secure communication all these requirements need to be addressed. The various attacks in VANET against security requirements are Impersonate, Session hijacking, Identity revealing, Location Tracking, Repudiation, Eavesdropping, Denial of Service, Routing attack. The susceptibility of network layer routing protocols are subjugated in routing attacks. The attacker either drops the packet or disturbs the routing process of the network in the routing attack. The most common routing attacks in the VANET are Black Hole attack, Worm Hole attack, Gray Hole attack. The Black Hole attacks and a solution for prevention of Black Hole attack is focused in this paper.

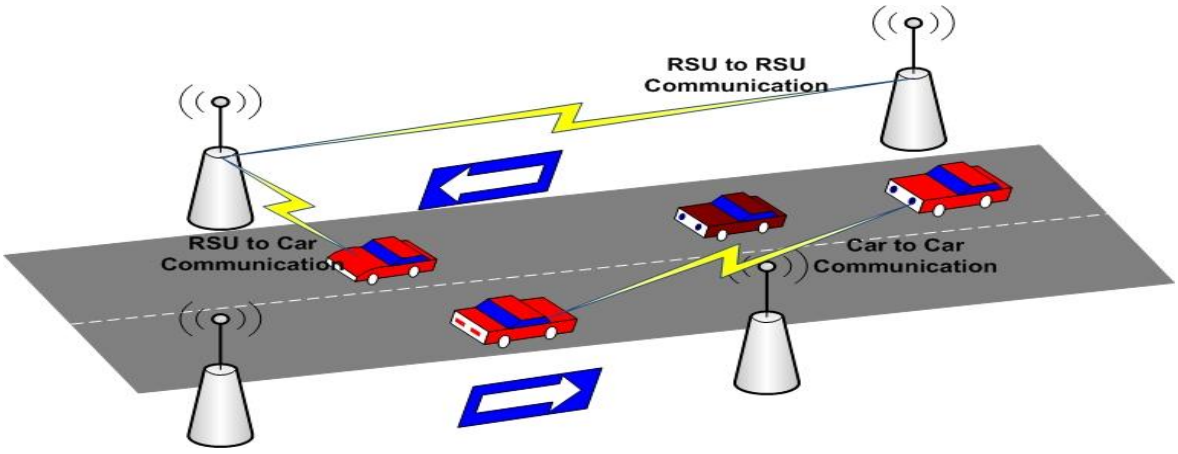

Fig1: The structure of VANET

The rest of the paper is organized as follows: The related work in the security aspects of routing protocols is discussed in Section 2. The Security issues in VANET are analyzed in Section 3. The proposed solution to detect and prevent the black hole attack is presented in Section 4. The experimental results are briefed in Section 5 and the conclusion and future directions are presented in Section 6.

2. RELATED WORKS

The research community in VANET has proposed many solutions to overcome the security challenges of routing protocols caused by various attacks. Some of them are described as follows: The author Yi et al. [1] examined unauthorized and malicious nodes and represented flaws in the security aspects of ad-hoc network communication.

In Authenticated Routing protocol for ad hoc Networks (ARAN) Sanzgiri et al. [2] proposed a method to resolve the security issues based on cryptographic public-key certificates. ARAN is efficient in maintaining and discovering the route but used larger packets resulting to overall higher routing overhead.

Secure Efficient Ad hoc Distance Vector Routing Protocol (SEAD) was proposed by Hu et al. [3] . It was based on hash chain sequences to authenticate hop counts between nodes. The security features in Distance Sequence Distance Vector (DSDV) protocol was enhanced by the sequence numbers. The packet delivery ratio of SEAD is better than DSDV. But due to increase in number of routing advertisement network overhead is also increased.

A secure on- demand routing protocol for AdHoc networks was proposed by Ariadne Perrig [4]. The algorithm was based on Dynamic Source Routing (DSR). It shared the secret key between two nodes. Though these distributed and independenet developments have provided an analysis of network security features, still there is a lack in protocol standards.

A novel mechanism was proposed by Shurman et al. [5] in which the source node has a computational capabilities to verify the authenticity of the node initiating the RREP messages. The possible paths to the destination could be identified by the node and compute the safest route to the destinations. The routing delays are increased in this method.

Dokurer et al. [6] solved group attack problem by ignoring the first route by the assumption that the first RREP message might be from a malicious node. This method ignored the possibility of the second RREP message from a malicious node. Thus, the method was vulnerable to Black Hole Attacks as it lack identifying and deleteting attacker node from the network.

An enhanced model to detect Black Hole Attacks proposed [7] by Raj and Swadas. The source continuously monitors the RREP destination sequence number and compares it with a periodically updated threshold. When the value is higher than the threshold it is suspected that RREP from malicious node. The presence of the malicious node is informed to the neighbors by an ALARM packet and the routing overhead is increased. It increases Packet Delivery Ratio.

A dynamic training method was proposed by Kurosawa et al. [8] for anomaly detection. In this scheme training data is renovated at regular time intervals and analyzed Black Hole Attack in the network. In MOSAODV Mistry et al. [9] proposed an algorithm to verify the authenticity of RREP destination sequence number. This algorithm analyze the predefined waiting period heuristically. A high sequence number marked the sender of RREP as malicious node. When there was no attack the node suffers out of latency and the routing overhead is also increased.

Even though the methods and algorithms brought some novelty to the attack detection scheme, they suffer from routing overhead issues on intermediate and source node. A new modified DSR algorithm with the following objectives of preventing and detecting Black hole attack node, to increase packet delivery ratio and to reduce the End to end delay is proposed.

3. SECURITY ISSUES

Securing vehicular communication is an important task in VANET. There are certain security requirements that have to be considered to overcome the vulnerability and various attacks. Therefore the security of the VANET is confirmed with the following requirements:

3.1 Authentication

A node in VANET should acknowledge only to the authenticated messages. Thus, it is very necessary to authenticate every message by the sender for secure communication to overcome from various attack.

3.2 Data Consistency

The messages in VANET communication should be consistent with time and location which is an important requirement for safety applications.

3.3 Confidentiality

In VANET's confidential communication refers that no one in a network except the members are able to decrypt the messages that are broadcasted to every member of the group.

3.4 Data Integrity

A Secure communication of VANET should ensure that data or messages are not modified by attackers. Otherwise, it will affect users of the VANET.

3.5 Availability

Vehicular system must be available to the applications of vehicular systems in real time even if the attacker attacks the network.

3.6 Non-repudiation

A secure VANET should able to identify the attackers even after the attack. That is when a node sends out a message, it shouldn't be able to later deny sending that message.

3.7 Privacy

Security should ensure that personal and private information's of data are not accessible by other users or attackers.

Though VANET offers various benefits it also imposes certain security challenges. The security attack is one among them. These attacks are created by the attackers. In the impersonation attack the attacker change his identity, acts like a source and changes original message for his benefit. In Sybil attack, the attacker sends multiple messages to other vehicles with different source identity (ID) to enforce other vehicles on the road to leave the road for its benefit. Attackers take control of session between nodes in session hijacking. Repudiation is an attack where attacker attempt to deny a node involved in communication. In this attack the legitimate user is prevented to use the service by the attacker. In the

routing attack the attacker disturbs the network routing process and drops the packet. The most common routing process attacks are Black Hole Attack, worm Hole attack and Gray Hole attack.

In Black Hole attack, the attacker node attracts the other nodes to transmit the message through itself by sending a malicious route reply. When the message is forwarded through this node it drops the packet. In warm Hole attack the attacker tunnels the packet received at one point to another point and replays them from that point. A Gray Hole attack is the extension of Black hole attack where the malicious node drops the packet selectively.

The focus of this paper is to detect and prevent Black Hole Attack. In search of shortest possible route to the destination the source node broadcast Route Request (RREQ) packet to the nearby nodes. The receiving intermediate node transmits the RREQ packet to the neighboring node to find the route to the destination. If the intermediate node is the malicious node it transmits false Route Reply packet (RREP) to the source node. Then the sources node starts transmitting all the packets to the malicious node which never transmits them to the intended receiver and at the same time genuine paths are omitted by neglecting the other RREP.

4. THE PROPOSED WORK

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol. DSR protocol maintains the route cache to store the route to the mobile node it is aware [10]. This protocol is composed of two major phases: route discovery and route maintenance. Whenever any node has the data to send, first it checks the route cache for the route to the destination. If it has the unexpired route, then it use otherwise initiate a route discovery process by broadcasting the RREQ (Route Request) packet which contains the source address and destination address. Whenever any intermediate node receives the RREQ, and it does not have the route to the destination it adds its own address in the route record and forward to its neighbor. RREP (Route Reply) is generated whenever RREQ reaches to destination node or intermediate node which has the route to destination in its route cache. Route maintenance mechanism is used to detect whether the path to the destination exist or not. Route maintenance uses the route error message and acknowledgement. Route error (RERR) message is initiated whenever the destination's data link layer recognizes any transmission error.

Route discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

Route maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, scan and attempt to use any other route it happens to know to D, or it can invoke Route Discovery again to find a new route for subsequent packets to D. Route Maintenance for this route is used only when S is actually sending packets to D.

The proposed routing is based on DSR with modification for detection of black hole attack. It is divided into two phases: Detection before route establishment and avoidance of malicious nodes during data forwarding. The proposed scheme is used for detecting malicious nodes in dynamic scenarios. When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black hole node. Such kinds of black hole attacks are discovered by using modified DSR protocol more effectively rather than preceding protocols.

This algorithm is designed based on the concept that malicious node may drop the packet or modify the packet. During detection phase, the nodes first send a RREQ to the entire two hop neighbor node id's and RREQ packet which consisting of invalid data destination to its two hop neighbors. If the receiving node states that it has the route to the invalid destination in its cache, and has forwarded the data packet to next hop then the node is assumed to be a black hole malicious node. This information about the maliciousness is stored in the nodes. During route discovery, the nodes cross check the routes in its cache and if the route consists of a malicious node, the node invalidates that route and starts a fresh route discovery avoiding the malicious node. Thus, the proposed mechanism reduces the black hole attack and avoiding it in any of the routes during transmitting data packets.

1. Begin
2. Set nodes $N = \{n_1, n_2, \ldots \ldots n_n\}$
3. Set path $P = \{p_1, p_2, \ldots \ldots p_3\}$
4. When Route _ Request _ Packets are acquired by node
5. Update information for all nodes $n_1, n_2, \ldots \ldots n_n$
6. if trust information in Route _ record then update distance, path and node information
7. Discover attack node using source id, trust value and route _ record information
8. Drop the black hole attack nodes
9. Compute the parameters of node and it must be higher throughput, packet delivery ratio, minimum distance and lower end to end delay
10. Choose the best node
11. Update route record employing route discovery and route maintenance process
12. End

5. EXPERIMENTAL RESULT

In this segment, by means of NS2 simulator, the recital outcome of the proposed MDSR approach is compared with AODV and DSR approaches. The simulation parameter are presented in the Table 1

Table 1: Simulation Parameters

Parameter	**values**
No. of Nodes	500
Area Size	3000 X 4000 m
Routing protocol	AODV, DSR
No. of malicious node	1
Simulation Time	500 sec
Traffic Source	CBR
Transmission range	250m
Metrics	Packet delivery ratio, End to end delay

5.1 Packet delivery ratio

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. The packet delivery ratio decreases when there is a

malicious node in the network because some of the packets are dropped by the malicious node.

Fig 2 illustrates that the comparison of packet delivery ratio for existing and proposed methodologies. It is calculated by amount of packets established alienated by amount of packets essentially sent. The simulation proves that the proposed MDSR approach provides higher packet delivery ratio rather than the existing AODV and DSR approaches.

5.2 End to end delay

The average time used by a packet to reach target node. It includes the delay in the path finding process and in the queue. The end to end delay decreases with black hole attack as the black node replies immediately without checking the routing table. Fig 3 portrays that the comparison of end to end delay performance of AODV and DSR with MDSR approaches. The nodes are varying from 100 to 500 and end to end delay is plotted for such nodes in nano seconds (ns). In x axis, the number of nodes are taken and in y axis end to end delay is taken. The experimental result shows that the proposed MDSR approach provides lower end to end delay performance when compared with AODV and DSR approaches.

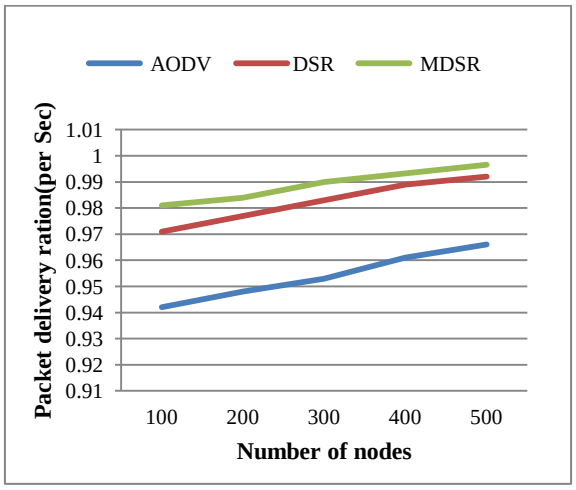

Fig 2: Number of nodes Vs Packet Delivery Ratio

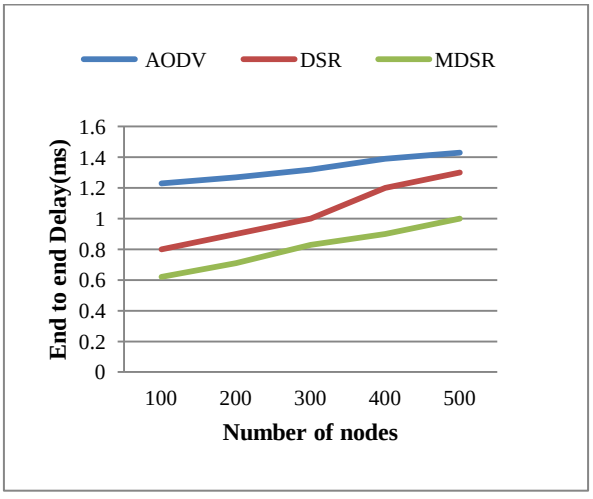

Fig 3: Number of nodes Vs End to End Delay

6. CONCLUSION

Security is an important feature in VANET. This research is focused on analysis of the black hole attack in vehicular ad hoc network (VANET). The existing mechanism for black hole detection and prevention are not applicable to the extent that the VANETs are secure from black hole attack. Comparison of the routing protocols AODV, DSR and the proposed MDSR is carried out. From the experiments and simulation the MDSR performance is better than AODV and DSR with and without black hole attack. In all scenarios, MDSR outperforms in terms of packet delivery ratio and delay as compared to AODV and DSR. Results shows that MDSR is much scalable than other routing protocols. So MDSR is a well suited routing protocol to be deployed in VANET.

In this paper only the Black hole attack prevention techniques and solution is proposed. Similarly other attacks like Greyhole attack, Jellyfish attack, and Wormhole attack need to be studied in VANET. The analysis of other attacks, prevention techniques and solutions are future work of this paper.

7. REFERENCES

[1] Yi S, Naldurg P, Kravets R. Security-aware ad hoc routing for wireless networks. In: Proc. 2nd ACM symp. mobile Ad Hoc networking and computing (Mobihoc‟01), Long Beach, CA, October. 2001. p. 299–302.

[2] Sanzgiri Kimaya, Dahill B. A secure routing protocol for Ad hoc networks. In:10th IEEE international conference on network protocols (ICNP‟ 02). 2002. p.78–87. Nov.

[3] Hu YC, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks. Ad Hoc Networks J 2003;1:175–92.

[4] Yih-Chun, Perrig Adrian, Johnson David B. Ariadne: a secure on- demand routing protocol for AdHoc networks. In: MobiCom'02 proceedings of the 8th annual international conference on mobile computing and networking. 2002. p. 12–23.

[5] Shurman MA, Yoo SM, Park S. Black hole attack in mobile Ad Hoc networks. In: ACM Southeast Regional Conference. 2004. p. 96–7.

[6] Dokurer Semih, Erten YM, Acar Can Erkin. Performance analysis of ad-hoc networks under black hole attacks. In: Southeast con. proceedings. IEEE; 2007.p. 148–53.

[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 2009;2:54–9.

[8] Kurosawa Satoshi et al. Detecting black hole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. Int J Network Security 2007;5(3):338–46. Nov.

[9] Mistry NH, Jinwala DC, Zaveri MA. MOSAODV: solution to secure AODV againstblack hole attack. (IJCNS) Int J Comput Network Security 2009;1(3). December.

[10] Hu, Y., and Maltz, D. The Dynamic Source Routing Protocol (DSR) for Mobile Ad hoc Networks for IPv4. RFC 4728, February 2007, pp. 2-100.