Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/6120
DOI URL: http://dx.doi.org/10.21474/IJAR01/6120

RESEARCH ARTICLE

AN APPROACH TO ISOLATE BLACKHOLE ATTACK USING AODV IN VANET.

[1]Srishti and Sapna Yadav[2].

1. Mody University of Science and Technology.
2. Lakshmangarh, Sikar, Rajasthan, India.

Manuscript Info

Manuscript History

Received: 21 October 2017
Final Accepted: 23 November 2017
Published: December 2017

Abstract

Vehicular Ad Hoc Network (VANET) is the special branch of the Mobile Ad Hoc Network. MANET has un-controlled moving patterns of a number of nodes where as VANET has restricted node movement by factors like a road course, traffic and traffic regulations because VANET is formed mainly by vehicles. VANET is the collection of information on moving vehicles throughout the period of communication. Security in VANET is a complex issue. Black hole attack is one of the possible attacks on AODV routing protocol in vehicular ad hoc networks. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to it. The effect of Black hole attack on Adhoc network using AODV as a routing protocol will be studied in this paper. The proposed solution that is capable of detecting and removing Black hole nodes in the VANET.

Introduction:-

Nowadays, road traffic activities are one of the most important daily routines worldwide. Passenger and freight transport are essential for human development. Thus, new improvements on this area are achieved every day - better safety mechanisms, greener fuels, etc. Driving is one of the most incident factors of traffic safety, so there is a clear need to make it safer. Apart from partially automating this task, reliable driver data provisioning is critical to achieve this goal. An accurate weather description or early warnings of upcoming dangers (e.g. bottlenecks, accidents) would be highly useful for drivers. For this purpose, a new kind of information technology called VANET (Vehicular Ad-hoc Network) is being developed.

VANETs are a subset of MANETs (Mobile Ad-hoc Networks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications). Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads.

Corresponding Author:- Srishti.
Address:- Mody University of Science and Technology.

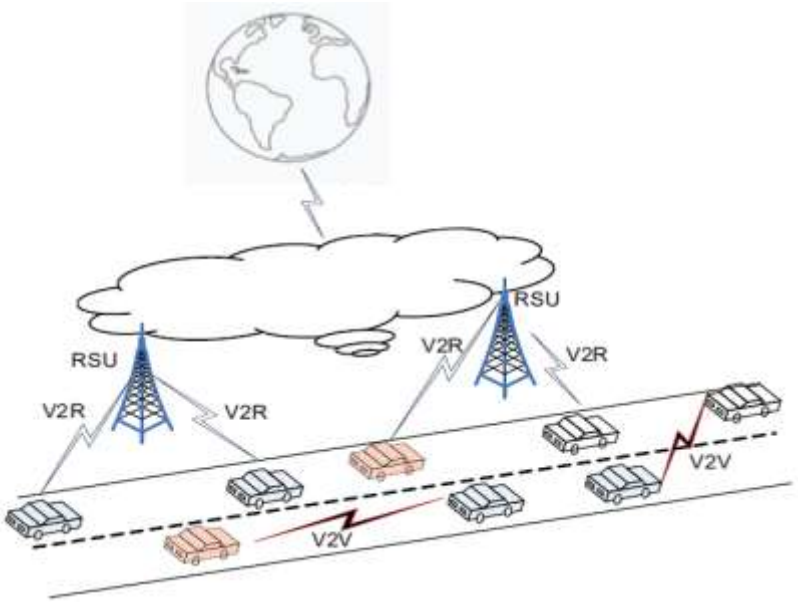

Figure 1:- Communication Network in VANET

Security is an important issue especially in this kind of network where one altered message can creates problem for the users in many ways. Attackers create problem directly and indirectly by launching different kind of attacks.

Attacks on Vehicular Networks:-
Before designing any security solution for VANETs [2, 3], we should know different types of security threats, their capabilities, and the types of attackers also.

Classification of Attackers:-
External attackers:-
External attackers are attackers that are not legally part of the network. They could be part of another network which is linked to the target network using the same infrastructure or same communication technology. These nodes can carry out attacks without being authorized on the target network.

Internal attackers*:* Internal attackers are compromised nodes which are authorized on the target network. These nodes are capable of more sophisticated attacks because they are seen as authorized by the network and fellow nodes. As an example they can produce false routing information to the network.

Passive Attackers:-
Passive attackers do not disrupt service. Eavesdropping is a good example of a passive attack, in this attack the attacker only listens to traffic that it can intercept. The attacker does not do anything active in the sense of attracting traffic to itself through the network.

Active attackers:-
Active attackers alter data, disrupt the operation or cut off nodes from neighbors. An active attacker must be able to inject packets to the network. Active attackers can target the physical layer by jamming the transmissions of wireless signals or by destroying the hardware at certain nodes.

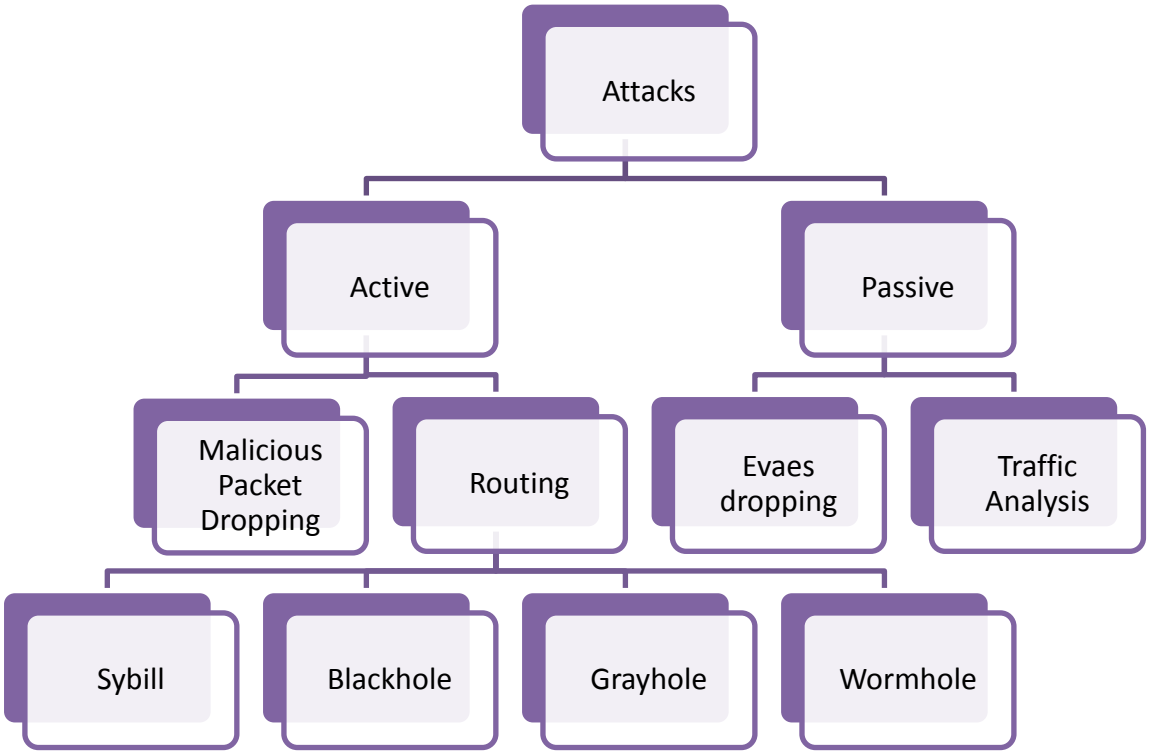

Figure 2:- Attacks in VANET

Different attacks in VANET:-

Table 1:- Attacks and their effects on each layer of Network

Layer	Attacks	Effect
Physical layer	Jamming	Interrupt the entire network and blocks the path between sender and receiver.
	Tampering	Can extract sensitive information such as cryptographic keys or other data on the node
Data link layer	Collision	Packets discarded as invalid.
	Resource exhaustion	Exhaustion of network resources
	Unfairness	degradation of real-time applications
Network layer	Spoofed routing information	Generate fake error messages to disrupt traffic in the network
	Black hole attack	Node does forward the packets to next intermediate nodes and drops the packets.
	Sink hole attack	Neighbor nodes choose the compromised node as the next-hop node.
	Sybil attack	Mislead other nodes by presenting identities of multiple nodes.
	Wormhole attack	low latency link between two portions of a network over which an attacker replays network messages
	HELLO flood	Overwhelm the node with hello packet requests.
	Acknowledgment spoofing	Attacker spoof the acknowledgments and provides false information to the nodes
Transport layer	Flooding	All available resources are used up and cause DoS
	Desynchronization	Cause drainage of energy of legitimate nodes.

Application layer	Overwhelm attack	Consumes network bandwidth and drains node energy by overwhelm network nodes
	Path based DoS attack	starve the network of legitimate traffic by consuming resources on the path to base station

Proposed Algorithm:-

Description of Black Hole attack:-

Security is the major issue in VANET. Majority of the attacks were against Physical, MAC and few more layers which deals with routing mechanism of Vehicular ad hoc network. Primarily the attacks were classified based on the purpose i.e. not forwarding the packets through routing mechanism, which affects sequence number and hop count. In the Black Hole attack malicious vehicle waits for the neighbors' to initiate a RREQ packet. Since the receivable RREQ Packet reaches the vehicle, it will immediately send a false RREP packet with a modified higher sequence number. A malicious vehicle where there is a possibility of Black hole VANET attack which submerge all data packets of all objects and the packet will not be distributed further. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each vehicle of the network has to shares their routing tables among each other. Black-Hole attack involves some modification of the data stream or the creation of a false stream [9]. Figure 2 below show a simple scenario of this attack with one malicious vehicle.

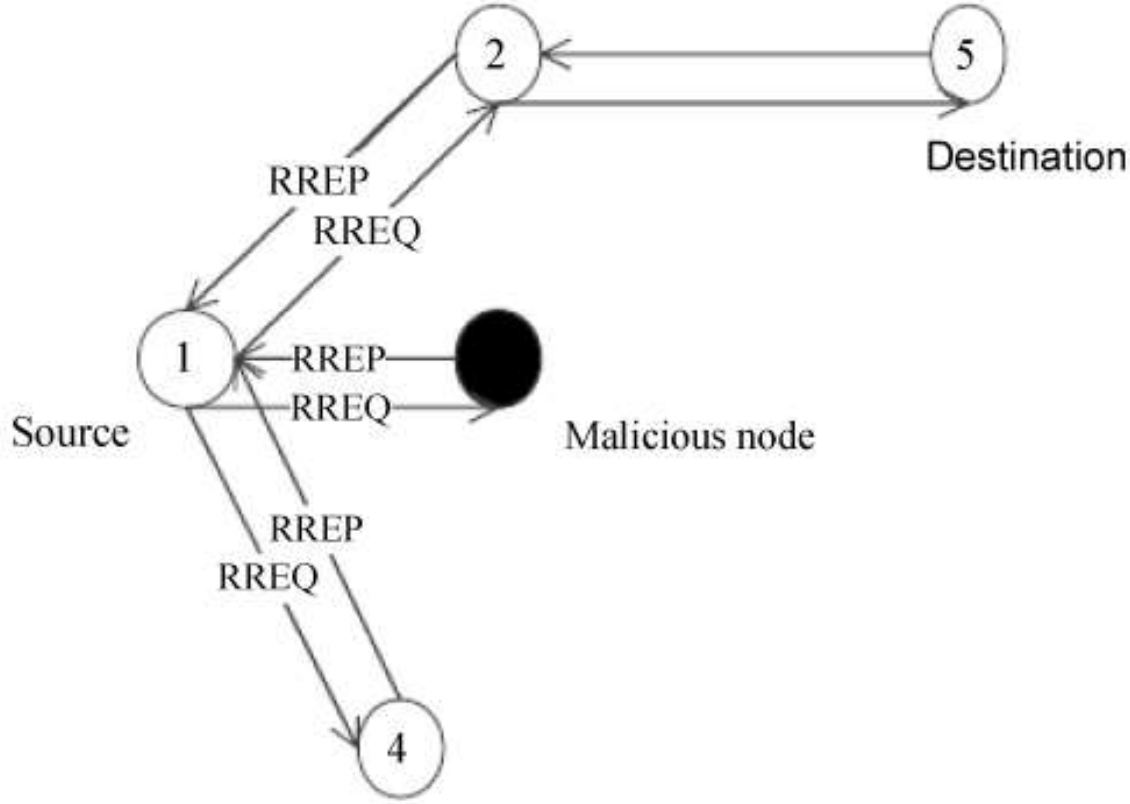

Figure 3:- Black-hole attack in progress

The AODV protocol is vulnerable to the well-known black hole attack. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a vehicle selects the route with the highest sequence number. If multiple routes have the same sequence number, then the vehicle chooses the route with the shortest hop count. A malicious vehicle sends Route Reply (RREP) messages without checking its routing table for a fresh route to a destination. As shown in Figure 3: above, source vehicle 1 broadcasts a Route Request (RREQ) message to discover a route for sending packets to destination vehicle 5. A RREQ broadcast from vehicle 1 is received by neighboring vehicles 2, 4 and 3. However, malicious vehicle 3 sends a RREP message immediately without even having a route to destination vehicle 5. A RREP message from a malicious vehicle is the first to arrive at a source vehicle. Hence, a source vehicle updates its routing table for the

new route to the particular destination vehicle and discards any RREP message from other neighboring vehicles even from an actual destination vehicle. Once a source vehicle saves a route, it starts sending buffered data packets to a malicious vehicle hoping they will be forwarded to a destination vehicle. Nevertheless, a malicious vehicle (performing a black hole attack) drops all data packets rather than forwarding them on.

Recovery of Black hole Attack:-
The proposed algorithm performs Efficient Routing in VANET; it detects and recovers the Black hole attack. Here, we modified the header of AODV by trust on vehicle. The trust value is used to verify the malicious vehicles. The recovery approach is included in the proposed algorithm as shown in below.

Proposed Method:-
Step 1: Base node send bogus Request in network with the destination set to some randomly generated Address in network (assuming that it is not present in network)
Step 2: On receiving of the first Reply, it starts the timer for receiving replies
Step 3: All the replies received before the timer expire are stored in RREP table.
Step 4: Once the timer expires, it check for the replies.
Step 5: Genuine nodes do not send reply as the dummy RREQ is for node that do not exist in network.
Step 6: Base node will generate an Alarm packet containing the Id of all nodes generated reply for Bogus Request broadcast this packet in network
Step 7: Every node that receives this alarm packet will add the Node Ids in block table and block that node from any further communication in network
Step 8: As a punishment any communication started by malicious node will also be blocked by other nodes of network
Step 9: This process gets repeated after every time interval, so if in some node which was initially good and later start acting as Blackhole will also be detected.

Simulation Results:-

Once a malicious vehicle is detected by the protocol, packets sent to it will automatically be dropped and stop further communications to the vehicle and it is isolated from the communicating environment. The performance of the vehicle in the network is demonstrated using the metrics packet delivery ratio and end to end delay.

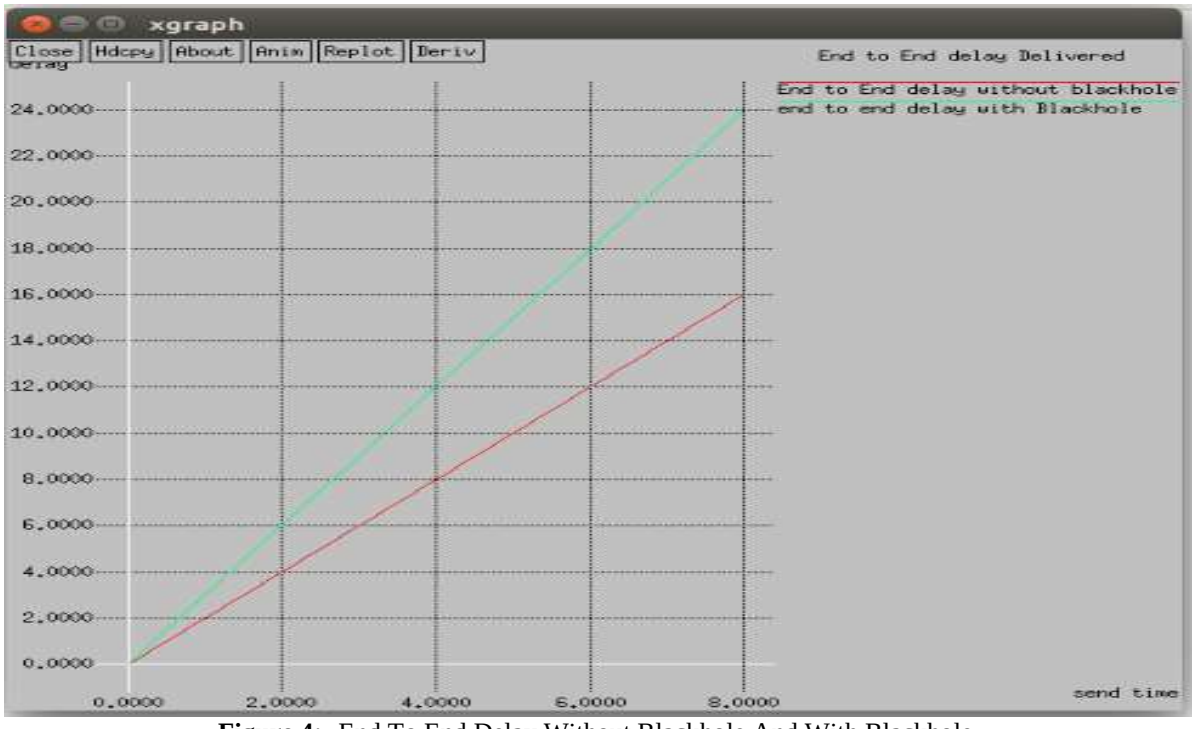

Figure 4:- End To End Delay Without Blackhole And With Blackhole

Figure 4 shows that end to end delay in malicious vehicle is greater than non malicious vehicle with increase in send time.

Figure 5:- Packet delivery ratio without Blackhole and with Blackhole

Figure 5 show that packet delivered in malicious vehicle is lesser than non malicious vehicle with increase in packet received time.

Conclusion:-

VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. Cooperation between the vehicles is essential to communicate with each other because of the short range of wireless communication medium. The attacker generates problems in the network by getting full access of communication medium due to open nature of the medium. In the black hole attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other. By this research, Black hole attack is efficiently removed by using proposed method. In this technique black hole attack is easy to detect, manage and recover. Here packet delivery ratio is increased and end-to-end delay gets decreased. In future we will working on another attacks to protect and safe the vehicles as well as passengers and drivers from the malicious vehicles.

References:-

1. K.R.Viswa Jhananie, Dr.C.Chandrasekar,(2015) " Detection and Removal of Blackhole Attack Using Handshake Mechanism in MANET and VANET", In Proceeding of IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
2. Ms Annu, Ms Sarul,(2015)" DETECTION OF BLACK HOLE ATTACK IN VANET", In Proceeding of 2nd conferences of science technology and management.
3. A.P.Jadhao, Dr.D.N.Chaudhari,(2014) "Security Aware Adhoc on Demand Distance Vector Routing Protocol in Vehicular Adhoc Network", In Proceeding of International Journal of Innovative Research in Computer and Communication Engineering.
4. Sonal Dhingra1, Komal Arora,(2013)" Detection and Prevention of Black Hole Attack in VANET", In Proceeding of IJCSMS International Journal of Computer Science & Management Studies. Bernsen, J. Manivannan, D.,(2008) "Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service" In the fourth international conference on Wireless and Mobile Communications.
5. T. Leinmuller, E. Schoch, and C. Maihofer, (2007) "Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference on Wireless on Demand Network Systems and Services.
6. M. Raya and J.-P.Hubaux,(2007)" Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.
7. T. Leinmuller, E. Schoch, and C. Maihofer, (2007) "Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference on Wireless on Demand Network Systems and Services.
8. P. Papadimitratos, V. Gligor, and J. P. Hubaux, (2006) "Securing vehicular communications— assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars (ESCAR).
9. Aijaz, B. Bochow, F. Dtzer, A. Festag, M. Gerlach, R. Kroh, andT. Leinmuller, (2006) "Attacks on inter-vehicle communication systems—an analysis". In Proceedings of the 3 rd international Workshop on Intelligent Transportation (WIT).
10. Raya, M., &Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.