A Review on Grayhole Attack and various Mitigation Techniques in VANET'S

Komalpreet Kaur[1] Prof. Rupinder Kaur[2]
[1]Student [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Punjabi University Patiala, India

Abstract— Vehicular adhoc networks (VANETs) is an advancing technology with a specific class of MANET. It does not have any fixed framework. Communication among vehicles is between vehicles and roadside units. So security is a powerful area for VANET. For authentication idea, lowers the execution and transmission capacity is high. And possibility of network must be recover when a node sends any required information to other node. The aim of this paper is to give an overview of VANETs with special effects of Gray Hole attack in Adhoc on demand distance vector Routing (AODV) protocol based on VANETs. We have used various execution metricals for Grayhole attack in VANETs. To simulate this attack we obtained simulation results NS-2.35 simulator. NS-2.35 has been used widely.

Key words: VANETs, AODV, Grayhole Attack, Initial Vector

I. INTRODUCTION

VANET is not same as MANET in the characteristic of higher mobility, isolation requirements. VANET is a special type of Mobile Ad hoc Network (MANET) that uses vehicles as mobile nodes to communicate with each other and they are associated by wireless channels. Vehicles interchange information between them without any fixed framework [1]. VANET is to make driving safer by possible communication between vehicles to get more appropriate roadside information. Vehicles essential OBU (On-Board Units) through they can communicate with each other and RSU (Roadside unit) associated to a network. VANET maintains right information, they should track with insurance necessities like isolation, understanding, purity to provide secure communication across attacker node [2]. Existence of vehicle and driver have to make known to RSU to communicate with them. [3]

VANET consists of wireless transmittal equipment that is used for telecasting information like brief messages. The information is about speed, control settings. On board sensor are used for telecasting information. VANET arrange broad area of functions like electronic toll collection, internet access, traffic reports and optimization, perfect route[4].

Security is of top mission in a Vehicular Ad-hoc Network. Specifically, where human lives are at stake, safety is of prime mission. The very open nature and contact method in VANET uncovering its structure to harsh, composite type of attacks. In Grayhole attack, malicious node aim to drop packet selectively thereby blocking the communication between source and destination network. Grayhole attack is a transformed version of Blackhole attack in which it is challenging to presume the malicious node's reaction .There remain data and control packets that are executed by this attack . AODV routing protocol be affected from absence of security that makes weak to grayhole attack. It cannot find and block a malicious node. The various types of communication in VANET are of following.

– Vehicle – to – Vehicle
– Vehicle – to – Infrastructure
– Inter roadside communication

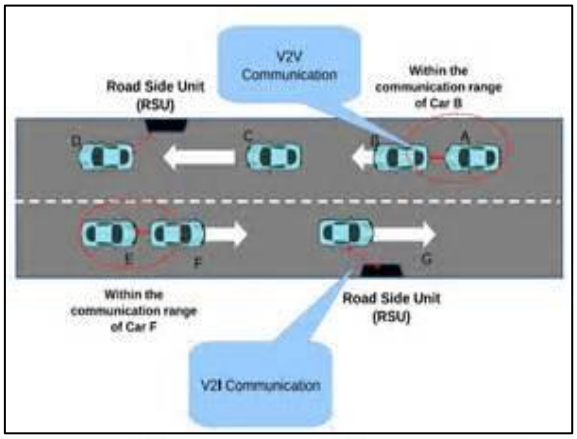

Fig. 1: Vanet

II. SECURITY REQUIREMENTS OF VANET'S

A. Authentication

Authentication is a primary fulfillment in VANET as it confirm that the messages are sent by the original nodes and hence attacks done by the grabby drivers or the other oppose it can be concentrated to a terrific limit.

B. Message Integrity

This is very much depend upon the confirmation of transferred messages are not changed in shipment that the messages the vehicle operator receives are correct.

C. Message Non-Repudiation

In this security based on system a sender cannot deny the fact having sent the message. But that doesn't mean that anybody can classify the sender only special authorities should be grant to classify a vehicle from the verified messages it sends.

D. Entity Authentication

It confirm that the sender who has developed the message is still in the network and that the driver can be ensured that the sender has send the message within a very short cycle. contact control it is demand to assure that all nodes action according to the roles and authority recognized to them in the network.

E. Message Confidentiality

It is a system which is demand when secure nodes wants to communicate in closet. But everyone cannot do that. This can only be done by the law compulsion mastery vehicles to communicate with each other to move closet information. An example would be, to find the location of a criminal or a terrorist.

F. Privacy

This system is used to protect that the information is not escaped to the unauthorized people who are not granted to view the information Third person should also not be ready to track vehicle speed as it is a cracking of own privacy.

G. Real Time Guarantees

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be fabricated into contracts to confirm that the time delicacy of security similar functions such as crash retreat is strike.

III. Common Attacks in VANET

There are two types of attacks present in VANET which break the security of the networks.

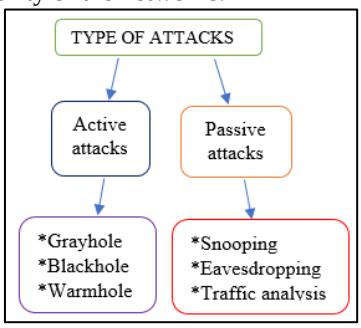

Fig. 2: Type of attacks

A. Eavesdropping Attack

Eavesdropping attack is the technique for collecting information by snooping on transmitted data on legitimate network. This information may incorporate the location, public key, private key or even password of the nodes. The assaulter detect the data variation in the network without tweak it. It is more vulnerable for MANET malicious nodes that can intercept the shared wireless medium.

B. Traffic Analysis

The principle task of this attack is to monitor and analyze which sort of the transmission is going on. Its point is to engage in convention or to provoke transmission between nodes. For this reason, the attacker may utilize a few methods, for example, time-correlation monitoring, traffic rate analysis, and so forth [5].

C. Black Hole

In a black hole attack a malicious node advertises itself as having a valid route to the destination node despite the fact that the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can totally suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.[6]

D. Gray Hole

In Gray hole Attack there is a node in the built up routing topology that selectively drops packet with certain probability causing network distraction. Gray hole may drop packets originating from (or destined to) certain particular node(s) in the network while forwarding every one of the packets for different nodes. Another sort of gray hole may carry on maliciously for quite a while period by dropping all packets yet may change to normal conduct later. A gray hole may likewise exhibit a conduct which is a combination of the above two [6].

E. Worm Hole

A worm hole attack is the place at least two malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The connectivity of the nodes that have set up routes over the wormhole link is totally under the control of the two colluding attackers. A worm hole demonstrates a valid route to the destination however it generally tunnels the packet to its malicious accomplice node. This attack is otherwise called burrowing attack[5]

F. Denial of Service Attack

DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Overflow the charge medium with high volumes of simulated developed messages, the network's nodes, onboard units and roadside units cannot comfortably proceeding the excess data.[6]

G. Byzantine Attack

Attacks where adversaries have full control of a number of authenticated devices and behave arbitrarily to disrupt the network are referred to as Byzantine attacks. [15] In this violation routing utility are confused by trickle packets, establish route circuits strike of packets on track that are not perfect.

H. Replay Attack

In this attack, instead of modifying packet's contents, intruder simply replays packets with the intension of exploiting battery power, bandwidth etc. This leads to congestion in the network because of different information flowing in the network among the routing nodes .This leads to conflict thus delaying delivery of packets and disrupting the communication among the nodes[16]

I. Jamming

These type of attacks are difficult to defend by using cryptographic methods. In this attack, intruder monitors the network to find the frequency received by destination node from the source. An attacker sends the signals to the destination using the same frequency at which destination is receiving data through the transmitter thereby interfering with network operations [17].

J. Man- in- the- Middle Attack

This attack is per- formed by attacker by sitting between the sender and receiver and any information that is exchanged between sender and receiver is sniffed by him. An attacker can also claim to be sender to talk with destination and vice versa.[18]

IV. Grayhole Attack in VANET

A. Grayhole attack

This is a message dropping attack that works in two phases. In first phase, a valid route to destination is advertised by nodes themselves. In second phase, nodes drop packets captured selectively [5].

B. Grayhole Attack in AODV

Grayhole attack is a modified version of blackhole attack in which it is difficult to predict the malicious node's behaviour. It can be performed by three ways. The first way is that malicious node may drop incoming packets while allow some packets to pass. In second malicious node may behave as normal for some time and malicious for a certain time. In third type, malicious node may drop incoming packets from some specified nodes for some time and later on it behaves as a normal node. These different types of behavior makes attack difficult to detect. Grayhole attack finally disrupts the network's performance by interfering with the route discovery process. [5].

C. Grayhole Attack Operation

Fig. 3 shows a VANET using AODV routing protocol. Initially, node A acts as normal node and allow all incoming packets from source S to the required destination D. But later as shown in figure, it react as a wicked node and starts trickle packets that are sent from source S to destination D. After some time, A act again as normal node as previous. Therefore A act wicked for a assured duration and becomes normal again. AODV routing contract has no detail for discovery and shut off a bad-natured node. Due to absence of insurance apparatus in AODV routing contract, wicked nodes can execute many breaks. This gray hole attack is described in fig.3 given here.

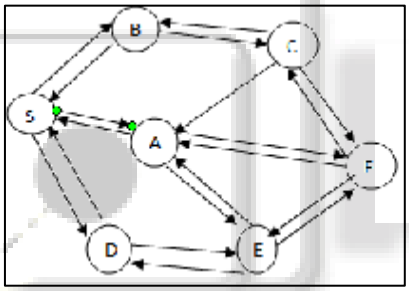

Fig. 3: Grayhole

V. GRAYHOLE ATTACK

A. Mitigation Techniques

1) Flow Conservation

Detects packet forwarding misbehaviour by flow conservation highly robust method works with varying mobility.

2) End to End Checking

In this technique end-to-end checking between source and destination to confirm the packet delivery.

3) Prelude and Postlude Messaging

Prelude messaging used by source to alert destination. Traffic monitored by neighbours postlude message give feedback by destination to source postlude message ack source by number of received packets. Malicious node are removed by getting information from monitoring node.

4) Anti-Blackhole Mechanism (ABM)

Broadcast by the detected node to all nodes in order to isolate the suspicious node cooperatively.

5) Non-Cryptographic Technique

Achieves degradation in packet loss rate without any computation complexity.

VI. RELATED WORK

Oscar et. al [8] proposed a solution that finds the nodes that are misbehaving in the network. This helps in finding out packet forwarding misbehaviour that happens in VANET. It makes use of an algorithm that takes considerable time to find out misbehaving nodes. Therefore, during this time malicious nodes can misuse the flow of packets before they are isolated from the network. A Selection of correct threshold of misbehaving nodes requires that well-behaved and misbehaved nodes are correctly distinguished. Therefore, average through- put cannot achieve the level with no misbehaving nodes in the network because the algorithm requires time to identify misbehaving nodes it also provides robustness in a network that is affected by Grayhole attacks.

Piyush et.al [9] proposed a mechanism where backbone net- work on checking failure detects malicious nodes by initiating a protocol. It works on the principle of end to end checking between source and destination nodes .This helps them to determine whether data packets have reached the destination or not. The proposed solution takes into consideration that network has more genuine and trusted nodes compared to misbehaving nodes. In case malicious nodes are more, this solution becomes vulnerable. The proposed solution may not work with all malicious nodes.

Sukla et.al [10] proposed a solution that uses a concept of in prelude and postlude messaging. In this, source node sends a prelude message to alert the destination before sending any packet so that it becomes aware about communication, neighbours monitor all the packets flowing through them .After the data transmission is over , the destination sends postlude message that indicates the number of packets received. If the data loss is out of acceptable range, the process of detecting and removing all malicious nodes is initiated. If difference between sent and received packet is out of tolerable range, a detection process is initiated and malicious nodes are isolated by collecting information from monitoring nodes.

Devu et.al[11] proposed a channel aware detection algorithm that makes use of two procedures in detecting misbehaving nodes. In first procedure, hop-by-hop loss observation by International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015 818ISSN 2229-5518hop (downstream node) is made and in the second procedure, traffic monitoring by previous hop is made. .In this node, upstream node assumes that nodes have no energy constraints which is not possible in VANET.

Payal et. al [12] proposed a protocol called as DPRAODV. In this protocol, a threshold value is searched and compared with difference of sequence number of reply packet and route table entry. If it exceeds threshold value, the node sending reply is added to a list of blacklisted nodes. Then it makes use of an ALARM packet that contains blacklisted node. This packet is sent to its neighbours to inform that reply packets from the malicious node are to be discarded. ALARM packet add to the higher routing overhead.

In [13] Jhaveri et al. proposed a method in which malicious nodes sending false information are detected by intermediate nodes. The routing packets also holds information about malicious nodes that is passed to all the nodes. All the malicious nodes are removed from the network that leads to safe and secure communication in the network.

VII. CONCLUSION AND FUTURE SCOPE

Vehicular ad hoc network being highly sharp in description is affected to different kinds of attack. AODV routing protocol is weak to Grayhole attack in VANET due to absence of insurance duration .In this paper, we provided a brief survey of different attacks including Grayhole attack on AODV routing protocol. .Along with that, we presented a review of different mitigation techniques that are used before to prevent network from grayhole attack in VANET. Vehicular ad hoc networks are not only meant for provision with a vast area of road traffic, life preserving, enfotainment relevant operations but also a useful way of communication. The current results to secure opposing Grayhole attack do not deal as complete results and be affected by weakness present into the network. Also Grayhole attack in AODV routing protocol in VANET also reduce various specification that specify the network execution like throughput, end to end delay, energy consumed, packetloss etc. In future our research close almost the advancement of a useful defender working to take action on the Grayhole attack by using RSA algorithm to secure channel establishment in the network.

ACKNOWLEDGEMENT

I would first like to thank my thesis Guide Er.Rupinder kaur of the ECE dept. at Punjabi University Patiala. The door to Prof. Rupinder kaur office was always open whenever I ran into a trouble spot or had a question about my research or writing. She consistently allowed this paper to be my own work, but steered me in the right the direction whenever she thought I needed it.

REFERENCES

[1] M.A. Razzaque, Ahmad Salehi S., and Seyed M. Cheraghi, "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead", Springer-Verlag Berlin Heidelberg, Vol No 2, Issue No 4, pp.107-132, 2013.

[2] Mohammed Saeed Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)", pp 1-9, 2012.

[3] Joshi, Ashish, Ram Shringar Raw, and Prakash Rao Ragiri. "A Counter Based Approach for Mitigation of Grayhole Attack in VANETs: Comparison and Analysis." International Journal of Scientific and Research Publications: 825.

[4] Y. Qian and N. Moayeri, "Design of secure and application- oriented vanets," in VTC Spring, 2008, pp. 2794 2799.

[5] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "DoS at- tacks in mobile ad hoc networks: A survey." Advanced Computing & Communication Technologies (ACCT), 2012 Second International Con-ference on. IEEE, 2012.

[6] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala,"Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP Journal of Com- puter Science, vol. 11 no. 1, March 2012, pp. 1-12.

[7] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analy- sis of MANET under Blackhole Attack", First International Con- ference on Networks & Communications, 2009, pp. 141-145

[8] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbe- havior in Mobile Ad-Hoc Networks ", Journal of Internet Engi- neering, vol. 2, no. 1, June 2008, pp. 181-192.

[9] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2nd international conference on Ubiquitous information management and communication, 2008, pp.310-314.

[10] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", World Congress on Engineering and Computer Science, October 2008, pp. 337-342.

[11] Devu Manikantan Shila, Yu Cheng_ and Tricha Anjali, "Channel- Aware Detection of Gray Hole Attacks in Wireless Mesh Net- works", IEEE Global Telecommunications Conference, Dec. 2009, pp. 1-6.

[12] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International journal of Computer Science Issues, Vol. 2, Issue 3,

[13] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala," A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", Second International Conference on Advanced Computing & Communication Technologies, Apr. 2012.

[14] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", International Conference on Sys- tem Engineering and Technology, September 11-12, 2012

[15] Awerbuch, Baruch, et al. "Mitigating byzantine attacks in ad hoc wireless networks." Department of Computer Science, Johns Hopkins University, Tech. Rep. Version 1 (2004).

[16] Virk, Gagandeep Kaur, and Dinesh Kumar. "Security Issues in ALARM Protocol for Mutual Authentication in MANET: A Re- view."

[17] Jyothi, V., U. Vidya Sagar, and S. Ramesh Kumar. "Prevention of Selective Jamming Attacks by Using Packet Hiding Meth- ods." IJCSNS 14.9 (2014): 56.

[18] Eriksson, Mattias, and Wenner-Gren Center. "An example of a man-in-the-middle attack against server authenticated SSL- sessions." international conference on applied cryptography and network security. 2003.

[19] M. Mohanapriya, Ilango Krishnamurthi," Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers & Electrical Engineering, Elsevier 2014

