International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4

ISSN: 2454-4248
268 – 273

Comparative and Analytical Study towards Mitigation of Gray hole Attacks in VANET

Shiv Shankar[1]
[1]M.Tech. Scholar, Department of Cyber Forensic & Information Security, GITAM, Maharishi Dayanand University, Rohtak, Haryana, India.
Email-shiv200557@gmail.com

Dr. Neetu Sharma[2]
[2]Head of Department, Department of Cyber Forensic & Information Security, GITAM, Maharishi Dayanand University, Rohtak, Haryana, India.
Email-neetush75@gmail.com

Abstract:-Vehicular Adhoc Network is a type of (MANET) Mobile Adhoc Network that enables vehicles on the road to intelligently interact and communicate with other vehicle and road side infrastructure unit. It is prone to several type of attacks and one such attack is Grayhole attack. Gray hole attack is one of the attack on routing specification in which malicious node selectively drops packets coming from the source. Due to lack of security in Adhoc on Demand Distance Vector (AODV) routing protocol, Grayhole attack disrupts the performance of network and render communication impossible. This paper reviews various attacks in VANET including Grayhole attack on AODV routing protocol and provides a survey of existing defence approaches to mitigate them.

Keywords- *Mobile Adhoc Network (MANET), Vehicular Adhoc Network (VANET), Adhoc on Demand Distance Vector (AODV) Protocol, Route Request (RREQ), Rout Reply (RREP), Denial of Service Attack (DoS)*

*****

I. INTRODUCTION

Vehicular Adhoc Network (VANET) is a special kind of Mobile Adhoc Network (MANET) which uses vehicles as mobile nodes to communicate with each other and they are connected by wireless links. Vehicles exchange information between them without any fixed infrastructure [1]. VANET consists of wireless transmission device that is used for broadcasting information like short messages. The information is about velocity, control settings. Onboard sensor is used for broadcasting information. VANET provides wide range of applications like electronic toll collection, internet access, traffic reports and optimization, optimal route [2]. Security is of prime concern in a Vehicular Adhoc Network. Especially, where human lives are at stake, safety is of utmost concern. Henceforth, any illegitimate altercations and unwanted modification in life critical information must be strictly prevented. The very open nature and access method in VANET exposes its framework to severe complex kinds of attacks. In Grayhole attack, malicious node intends to drop packets selectively thereby hindering the communication between source and destination network. Grayhole attack is modified version of Blackhole attack in which it is difficult to predict the malicious node's behaviour. There exist data and control packets that are affected by this attack. Adhoc on Demand Distance Vector (AODV) routing protocol suffers from lack of security that makes that makes vulnerable to Grayhole attack. It cannot find and block a malicious code. This paper is divided into five sections; Section I describes the overview of VANET. Section-II describes about the AODV routing protocol .Section-III explains about the various attacks in VANET along with working of Grayhole attack in AODV routing protocol. Section-IV presents the analysis on related work and summarizes different mitigation techniques of Grayhole attack in VANET. Finally Section-V concludes the work and describes the future scope of work.

II. OVERVIEW OF AODV PROTOCOL

AODV is an on-demand routing protocol in which routes are created on demand. It adapts itself in accordance with change in the link conditions. Since links are created on demand, therefore it has low network utilization. When links fails, affected nodes invalidate all the routes through the failed link. Adhoc network build multihop routes when two nodes wish to communicate with each other. In this way multihop routes are formed. AODV works with three types of messages namely as route request, route reply and route error. These messages help in finding routes from source to destination. At first, route request packets are broadcasted from source whenever there is a need of finding new route to destination. This message reaches the next hop that may be a destination or has information related to destination. When intermediate node is having path to destination, it again rebroadcasts route request messages and at the same time update its route table in order to include a pointer reversing back to the source node. This whole process repeats until route to destination is found. Intermediate nodes keep track about route information of source and destination nodes. After source node receives route reply messages (RERP), it transfers data to destination node on the new route created. In case route reply message (RERP) does not come, source node again sends route request (RERQ) messages. When a link failure takes place, Route Error (RERR) messages are generated. When source node wants to

 ISSN: 2454-4248
268 – 273

choose the best path to transfer data to its destination, it broadcasts route request (RREQ) packet so that it reaches the whole network. When RREQ is received by nodes, they must find whether they are the destination node or not. If a node is not the destination node then it will rebroadcast the RREQ to its neighbours in the same manner as source if it doesn't have path to destination and update its route tale to include a reverse pointer that indicates path to the source node. Working is shown in fig.1 and fig.2.

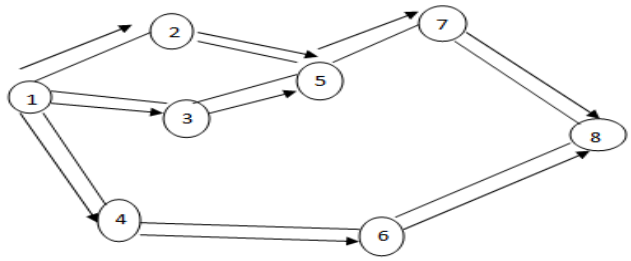

Fig.1. Route request packet from source 1 to destination 8

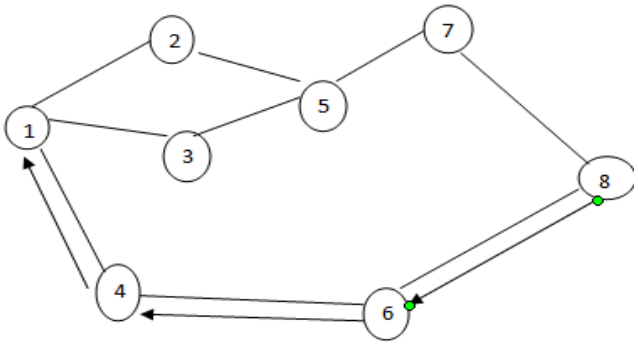

Fig.2. Route request packet from source 1 to destination 8

III. COMMON ATTACKS IN VANET

There are two types of attacks present in VANET which break the security of the networks. These attacks are discussed in detail in table 1 given below.

Table-I

Types of Attack

Types of attack	Characteristics	Example
Active Attack	Information is gathered from the network without disturbing it and it is difficult to detect	Snooping, Eavesdrop in, Traffic analysis, Monitoring.
Passive Attack	Termed as internal and external, it modifies and deletes information. Also impersonates a node.	Grayhole,Information disclosure,Black hole,Resource consumption

III.[1]. ROUTING ATTACK IN VANET

1. Denial of Service Attack: **-** This attack prevents a network from accessing the network from accessing the network service. The attack may overtire vehicles and network resources. Methods basically employed to carry this attack includes radio signal jamming and battery exhaustion. This attack can be made in two ways. In first the network DOS make use of the roadside units by comprising them or by making vehicle broadcast huge number of messages in a short span of time via Sybil attack. This makes the communication channel congestion with a lot of messages and disrupts the communication. In second, computational DOS targets the victim to spend all the time in making computations by forcing a vehicle to store too much information and by doing this it overloads the computation capabilities of a given vehicle, ultimately falling victim to this kind of attack [4].

2. Wormhole Attack:-This attack is called as tunnelling attack that can take place easily. In this attack, a high speed wireless link called wormhole link or tunnel is created between two nodes that are termed as malicious. Tunnels also called as worm-hole tunnel encapsulate data packets and also give false information about route lengths [3]. A large no of packets are allowed to transfer through these tunnels. Worms can drop data packets selectively or can obtain statistical information about the data. This attack is very difficult to detect and finally disrupts the network's performance by interfering with the route discovery process [5].

3. Black Hole Attack: **-** In black hole attack [5][6] black hole node advertise itself as having a valid and optimal route to the destination. It generates and disseminates bogus routing information in response to the received request packet [6].The black hole node replies with reply
Packet having tempering routing information to the requesting source node and thus, a bogus route will be created through it. Black hole attacker causes packet forwarding misbehaviour by intercepting and dropping all the received packets sent towards specified destined node. This is how, Black hole node launches DoS attack and absorb network traffic and thus, degrades performances of the network [7].
In this type of attack, intruder listens for the request of routes. When the request is received by the attacker, it creates a reply saying that it has shortest route to the destination and then starts dropping packets passing between them [6].

4. 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 attack, routing services are disrupted by

 ISSN: 2454-4248
268 – 273

dropping packets, forming route loops collision of packets on paths that are not optimal.

5. Reply Attack:- In this attack, instead of modifying packets'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].

6. 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 same frequency at which destination is receiving data through the transmitter thereby interfering with network operations [17].

7. Man in the middle attack:- This attack is performed by attacker by sitting between the sender and the receiver and any information that is exchanged between sender and receiver is sniffed by them. An attacker can also be claiming to be sender to talk with destination and vice versa [18].

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

III. (2) 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 different 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 it behaves as a normal node. These different types of behaviour makes attack difficult to detect. Grayhole attack finally disrupts the network's performance by interfering with the route discovery process [5].

GRAYHOLE ATTACK OPERATION

Fig.3 shows a VANET using AODV routing protocol. In the first figure, initially, node A acts as normal node and allows all incoming packets from source S to the required destination D. But afterwards as shown in second figure, it behaves as a malicious node and starts dropping packets that are sent from source S to destination D. After some time, A behaves maliciously for a certain period and becomes normal again. AODV routing protocol has no feature for finding and blocking a malicious node. Due to lack of security mechanism in AODV routing protocol, malicious nodes can perform many attacks. This attack is represented in fig 3. Given below

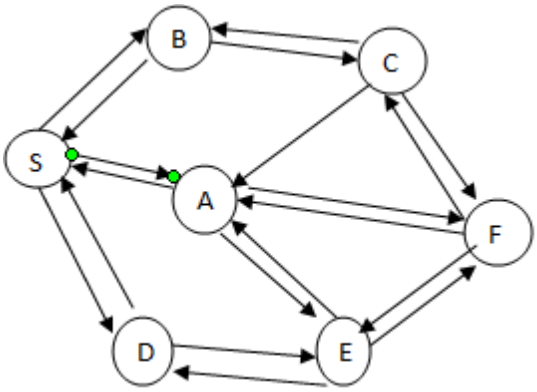

Fig.3. Grayhole attack

IV. 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 throughput 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 attack.

Piyush et.al [9] proposed a mechanism where backbone network on checking failure detects malicious nodes by initiating a protocol. It works on the principal 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 monitors all the packets flowing through them. After the data transmission is over, the destination sends postlude messages that indicates the number of packets

 ISSN: 2454-4248
268 – 273

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 next hop (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 are not possible in VANET.

Payal et.el [12] proposed a protocol called as DPRAODV. In this protocol, a threshold value is searched and compared with difference of sequence numbers 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 neighbour to inform that reply packets from the malicious node are to be discarded. ALARM packet adds to the higher routing overhead.

In [13] Jhaveri et.al. Proposed a method in which malicious node sending false information are detected by intermediate nodes. The routing packets also hold 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.

Bindra et.al [14] proposed a method to detect and remove the blackhole and greyhole attacks. Extended Data routing information (EDRI) table is maintained at each node in addition to the routing table of the AODV protocol. The proposed mechanism detects a malicious node in an efficient manner and keeps record of node's previous history regarding its malicious instances in order to deal with grayhole attack.

Krishnamurthi et.al [19] proposed an intrusion detection system (IDS) that calculates the difference abnormal difference in the number of data packets being forwarded by a node. Intrusion detection system is used for isolating malicious nodes on the network. When an abnormal difference is detected, IDS node present in the surrounding broadcast the block message. This block message informs all nodes on the network to isolate the malicious node from the network in a cooperative manner. This method is used to prevent selective blackhole attack by improving dynamic source routing protocol (DSR). This method is used to prevent selective blackhole attack by improving dynamic source routing protocol (DSR). This methods is also be implemented with some other protocols.

To summarize the above discussed work, the approach and limitations of previous techniques used in the mitigation of grayhole attack are discussed in table-2 given below.

TABLE-2
GRAYHOLE ATTACK MITIGATION TECHNIQUES

Techniques Used	**Approach**	**Limitations**
Flow Conservation [8]	1. Detects packet forwarding misbehaviour by flow conservation. 2. Highly robust method. Works with varying mobility.	Only packet forwarding misbehaviour addressed
End to End Checking [9]	1. End to End checking between source & destination that confirms whether packets have reached the destination or not. 2. Backbone network initiates a protocol for detecting single or cooperative malicious nodes.	Does not work well with all malicious nodes.
Prelude & Postlude messaging	1. Prelude messages used by source to alert destination. 2. Traffic monitored by neighbours. Postlude message sent by destination representing number of packets received. 3. Malicious nodes are removed by collecting response from monitoring node.	Analysis of proposed not done
Channel aware detection algorithm [11]	Hop by Hop loss observation by next hop (downstream node) and traffic monitoring by previous hop (upstream node) find out packet forwarding misbehaviour.	Nodes have no constraints on energy which is not possible in VANET
Anti Blackhole Mechanism (ABM) [15]	1.Suspicious value of node is considered 2.Based on suspicious value, block message is broadcasted by the detected node to all the nodes in order to isolate the suspicious node cooperatively.	It is assumed that a node ID cannot be forged and a block message sent by an IDS node cannot be modified.
Non Cryptographic technique [16]	Achieves degradation in packet loss rate without any computational complexity.	1.Caching performed by source node leads to memory over head 2. It also leads to packet delay i.e. slow process of delivery mechanism.

 ISSN: 2454-4248
268 – 273

V.CONCLUSION & FUTURE SCOPE

Vehicular adhoc network being highly critical in nature is highly critical in nature is susceptible to various kinds of attack. AODV routing protocol is vulnerable to Grayhole attack in VANET due to lack of security measures. In this paper, we provided a brief survey of various attacks including Grayhole attack on AODV routing protocol. Along with that we presented a review of various mitigation techniques that are used previously to defend against grayhole attack in VANET. Vehicular adhoc networks are not only meant for providing with a wide range of road traffic, life, life saving, infotainment related application but also a useful way of communication. The current solutions to defend against Grayhole attack do not serve as complete solution and suffer from drawbacks. Moreover Grayhole attack in AODV routing protocol in VANET also degrades various parameters that indicates the network performance like throughput, end to end delay etc. In future, our research closes towards the development of an effective defence mechanism to combat the Grayhole attack by using genetic algorithm (GA) to optimize the network.

ACKNOWLEDGEMENT

It is my pleasure to be indebted to various people, who directly or indirectly contributed in the development of this project work and who influenced my thinking, behaviour and acts during the course of study.

Apart from the efforts of me, the success of my project depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to my course coordinator, Dr. Neetu Sharma

Lastly, I would like to thank the almighty and my parents for their moral support and my friends with whom I shared my day-to- day experience and received lots of suggestions that my quality of work.

REFRENCES

[1] 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 Sci-entific and Research Publications: 825.

[2] Y. Qian and N. Moayeri, “Design of secure and application-oriented vanets,” in VTC Spring, 2008, pp. 2794–2799.

[3] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, “Study of Different At-tacks on Multicast Mobile Ad hoc Network”, Journal of Theoreti-cal and Applied information Technology, December 2009, pp. 45-51.

[4] Kim, Yeongkwun, and Injoo Kim. "Security issues in vehicular networks."Information Networking (ICOIN), 2013 International Conference on. IEEE, 2013.

[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. Jinwa-la,“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, 2010, pp: 54-59.

[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 MA-NET”,Computers & Electrical Engineering,Elsevier 2014

ISSN: 2454-4248
268 – 273

BIOGRAPHY

Shiv Shankar is currently pursuing M.Tech (CF&IS) from GITAM, Maharshi Dayanand University, Rohtak, India. He did his B.Tech (CSE) from Institution of Engineers (India), Kolkata. His areas of interests are Data security; cloud computing, DBMS, cyber forensic and information security.E.Mail-shiv200557@gmail.com

Dr. Neetu Sharma is currently working as Head of Department, Department of (CF&IS), GITAM, Maharishi Dayanand University, Rohtak, India. Her area of interest is cyber security, data security, web security & wireless security. E.Mail-neetush75@gmail.com