A Counter Based Approach for Mitigation of Grayhole Attack in VANETs: Comparison and Analysis

Ashish Joshi, Ram Shringar Raw, Prakash Rao Ragiri

Department of computer science and engineering, Ambedkar Institute of Advanced communication technologies & Research, Delhi

Abstract**-** Vehicular Ad-hoc Networks (VANETs) are highly dynamic network and prone to many kinds of attacks. One class of attacks known as routing misbehavior targets the routing process of the networks. Grayhole attack is a malicious change in the routing process of effected nodes. Such node takes part in routing process but drops the packet when it is required to forward the packet to other nodes. This attack changes the performance of the network. Ad-hoc On-Demand Distance Vector (AODV) is prone to grayhole attack due to lack of central control and security. In this paper, we have proposed a counter based approach for mitigation of grayhole attack using freeway mobility model for highway scenario which is most suited for VANETs. Simulation results and analysis of proposed work has been carried out using NS-2. Further, the performance of the proposed work has been compared in terms of packet delivery ratio, normalized routing load, end to end delay and average throughput with grayhole attack in AODV and normal AODV protocol.

Index Terms**-** MANET, VANET, Freeway Mobility Model, AODV, Routing Misbehavior, Grayhole Attack.

I. Introduction

A VANET is a special type of Mobile Ad hoc Network (MANET). It is a self configuring network of mobile routers connected by wireless links which use vehicles as mobile nodes. VANETs enable the exchange of information between vehicles without any fixed infrastructure. It can be classified according to the type of infrastructure that is being used for communication. A Vehicle-2-Vehicle (V2V) communication is a pure ad-hoc communication in VANET consisted of vehicles mounted with communication devices. A Vehicle-2-Infrastructure (V2I) communication is infrastructure based communication in VANET which consists of vehicular nodes as well as fixed infrastructure along the road to deal with connectivity issues in VANET. The communication is carried using electromagnetic waves e.g. infrared, microwaves, VHF radio waves and short range radio waves. Mostly the VANET system is implemented using the IEEE 802.11 standard which is a class of standards for wireless communication. Some experiments also show that Universal Mobile Telecommunications System *(*UMTS*)* can also be used for communication in VANETs. IEEE P1609.1 is the standard for Wireless Access in Vehicular Environment (WAVE) based on DSRC. WAVE uses a modified version of IEEE 802.11a for MAC known as IEEE 802.11p. The IEEE 802.11p MAC/PHY layer standard is specially meant for VANETs which operate in wireless access for vehicular environment and uses a frequency band of 5.9 GHz and supports high mobility up to 150 kmph [8].

Routing is the integral part of ad-hoc networks. A routing protocol governs the way that two communication entities exchange information. It includes the procedure in establishing a route, decision in forwarding, and action in maintaining the route or recovering from routing failure. The two routing approaches that are being used for ad-hoc networks are reactive and proactive routing. In addition to both these approaches VANETs require some geographical information for efficient routing. This leads us to use location based routing in VANETs. Many researchers have proposed and simulated various routing protocols for VANET. Routing protocol must be designed carefully to serve the data dissemination issues such as reliability, minimum delay, efficiency and so on. The routing protocols may be classified as unicast and multicast routing. Some examples of unicast geographic routing protocols are Location Aided Routing (LAR), Most Forward progress within Radius (MFR), Border- node based MFR (B-MFR), Greedy Perimeter Stateless Routing (GPSR) etc. [9].

Routing misbehavior is the category of attacks in which the malicious node intentionally or unintentionally hinders the routing of data or control packets which may lead to collapse in a part or total network. One more important aspect in analyzing the VANETs is the mobility scenario. It determines the pattern of mobile node movement in the environment. A mobility model is representation of the mobility scenario in logical terms. As vehicles are generally used on roads, we will assume the scenario to be similar to the Yamuna Expressway in India. Traffic scenario determines the type of communication that is ongoing between the vehicular nodes in VANETs. Generally, traffic includes the type of data, protocols for transmitting packets, bit rates, and MAC characteristics of the communication. A traffic model represents traffic scenario in logical terms.

In this paper, we have proposed a counter based approach for mitigation of grayhole attack using freeway mobility model for highway scenario which is most suited for VANETs. This proposed algorithm overcomes the incapability of AODV to identify, block and mitigate grayhole attack in AODV. The rest of the paper is organized as following: section 2 introduces the related work. In section 3, the working of AODV and freeway mobility model is presented. Section 4 introduces the grayhole attack in AODV. In section 5, we have introduces the proposed work and its algorithms in brief. Section 6 shows the simulation and result analysis of the proposed work. Finally, we conclude the paper in section 7.

II. Related work

Piyush et.al [10] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

A mechanism is proposed by Sukla et. al [11] in which before sending any block, source sends a prelude message to destination to make it aware about communication where neighbors monitor flow of traffic. After end of transmission, destination sends postlude message containing 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 by collecting response from monitoring nodes and the network. The mechanism has routing overhead increased due to additional routing packets.

For detecting packet forwarding misbehavior, Oscar et. al [4] proposed an algorithm that use the principle of flow conservation and accusation of nodes that are constantly misbehaving. Selecting correct threshold of misbehavior allows distinguishing well-behaved and misbehaved nodes. However, the average throughput cannot reach that of a network where there is no misbehaving node present because the algorithm requires definite time to gather the required data to identify and to accuse misbehaving nodes. Therefore, misbehaving nodes can drop packets before being accused and isolated from the network during the preliminary phase.

Payal et. al [5] suggested a protocol DPRAODV that finds a threshold value and compares that with difference of sequence number of reply packet and route table entry. If it is higher than the threshold value, the node sending reply is added to a list of blacklisted nodes. Also an ALARM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. This protocol has higher routing overhead due to addition of the ALARM packets.

An algorithm is proposed by Deng et. al [6] in which when a source node receives a route reply packet, it cross checks with the previous node on the route to the destination to verify that the node sending reply packet indeed has a route to the destination as well as to the intermediate node. If it does not have, the node that sent the reply packet is judged as malicious node. The mechanism, though, increases end-to-end delay and due to the addition of further request and further reply packets in the algorithm, routing overhead also gets increased.

In [13] Jhaveri et al. proposed a scheme in which an intermediate node detects the malicious node sending false routing information. Routing packets are used not only to pass routing information, but also to pass information about malicious nodes. The proposed scheme not only detects but also removes malicious node by isolating it to make safe and secure communication in the network.

In [14] Bindra et al. proposed a mechanism to detect and remove the blackhole and grayhole attacks. The solution tackles these attacks by maintaining an Extended Data Routing Information (EDRI) table at each node in addition to the routing table of the AODV protocol. This mechanism is capable of detecting a malicious node. It also maintains a history of the node's previous malicious instances to account for the gray behavior.

III. AODV and Freeway mobility model

The framework proposed in this paper makes use of AODV protocol. In AODV the source node and the intermediate nodes store the next hop for each flow for data packet transmission. AODV uses a destination sequence number (DSN) for every route entry to resolve up-to-date and fresh path to destination [9]. During Route Discovery process, DSN is created by the destination. The DSN and the respective route information should be included by the nodes to find out the routes to destination nodes. Routes with the higher DSN are preferred in selecting the route to destination. Figure 1 shows AODV route discovery process. AODV uses Route Request (RREQ), Route Replies (RREP) and Route Error (RERR) in finding the route from source to destination by using UDP (user datagram protocol) packets. In the figure, a source node 'S' aiming to communicate with destination 'I' using the RREQ containing the source address and the broadcast ID address to its neighboring nodes to find the route to the destination. This broadcast ID is incremented by 1 for every new RREQ. When a neighbor notices a destination route it responds with RREP to the source. If the destination route cannot be found then it will re-broadcast the RREQ to its neighboring nodes by incrementing the hop count. In this process a node may receive multiple copies of the broadcast packets in transmissions from all the corresponding nodes. Now the node will check if the broadcast ID is new, if it is therefore, the node will process the request else it will ignore the re-broadcast.

During the Route Maintenance process, when a route breaks in AODV, which is determined by monitoring the periodical signals or by link-level acknowledgements, the end nodes are informed. When a source node notices the route break, it again sets up the route to the destination. If a route break is found at an intermediate node, the node tells the end nodes by sending unsolicited RREP with the loop count set to infinity. The source node re-launches the path finding mechanism with a new broadcast ID and the previous DSN. The nodes react to the any change in network topology and path failures. In case of the path failures the respective nodes are informed with the message, and then the affected nodes will withdraw the routes using the lost path. This makes the operation of AODV "Loop free".

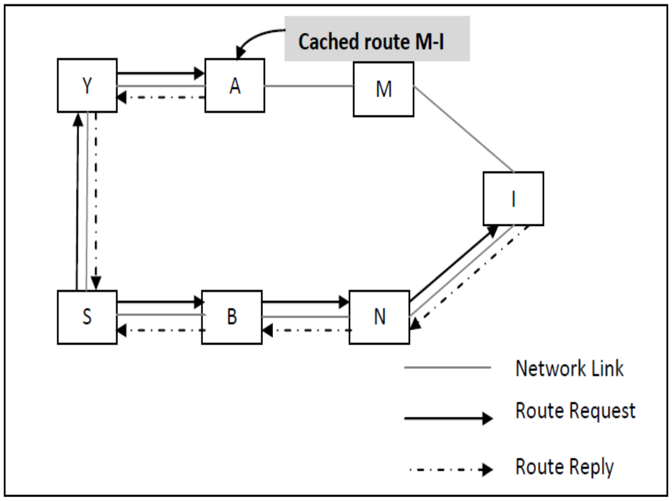

Figure 1 AODV Route Discovery Process

A mobility models in VANETs represent the way in which vehicular nodes might move in a real world traffic environment. A mobility model is designed to represent the movement patterns, their location at a particular instance of time, direction of movement, pause pattern, and speed changes over time of the mobile nodes in a given scenario. The freeway mobility model [6] represents the scenario of a freeway. We consider the freeway to contain 6 lanes; 3 lanes on either direction. Each lane has a defined speed and the defined velocity of that lane. When a vehicle has to change its lane it should either increase or decrease its speed.

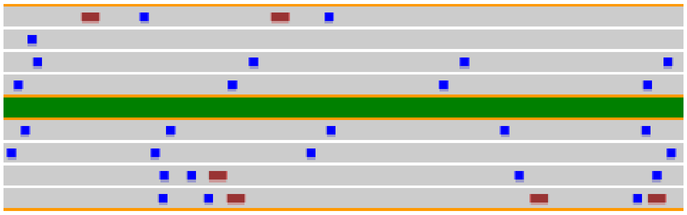

Figure 2. The freeway mobility model

Also it has to look for the space for moving left or right. Fig 2 shows the arrangement of nodes in freeway mobility model.

IV. Grayhole Attack in AODV

Routing misbehavior is the category of attacks in which the malicious node intentionally or unintentionally hinders the routing of data or control packets which may lead to collapse in a part or total network.

There are some shortcomings in AODV that makes it vulnerable to grayhole attack**.** AODV after finding the route to destination rely on the nodes falling in route for forwarding the message. AODV has any mechanism for finding and blocking a malicious node. It has no mechanism to deny a path that contains malicious node.

In AODV, whenever a sender has a path to destination, it starts sending packet to the next hop. Now each node will forward the packet to its next hop pertaining in the path to the destination. The malicious node

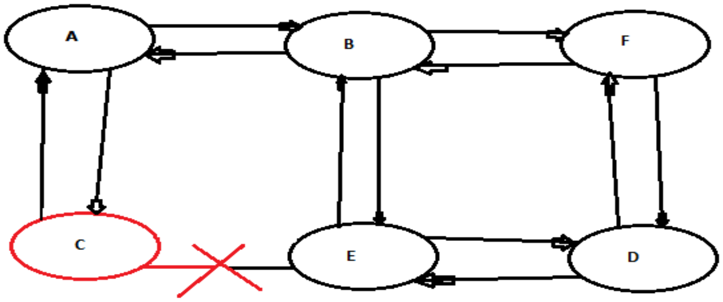

Figure 3 Grayhole attack in AODV

will take part in the routing process but will not forward a packet when required. It will simply drop all packets which come to it as shown in figure 3. Here node A wants to send packets to node D. The route that it has is A-C-E-D. When the packet comes to node C, which is the malicious node, it will start dropping packets and the communication will fail. The next section presents a possible solution to this misbehavior.

V. Mitigation of Grayhole Attack: A Proposed Framework

In this work, we have proposed a framework to mitigate the grayhole attack on AODV. For this purpose we need to redesign the functionality of AODV in such a way that it mitigates the grayhole attack. There are some pre-requisites that must be fulfilled in order to mitigate the effect of the grayhole attack. Every single node in the network must sense its neighboring nodes using HELLO or beacon messages with a fixed time interval T. This is necessary because there must be no ambiguity between link failure and Grayhole attack. Here T has to be defined earlier to the communication process. Apart from this the normal route finding and route maintenance process must carried out as the malicious node will take part in route finding process. The nodes that are added to the blacklist must not be considered for routing process.

The proposed mitigation framework based on number of times the packet is sent over a legitimate route but not acknowledged. A message transmission list has to be maintained which contain the packet number, time elapsed and Tries Counter (TC). The time elapsed is a counter that records the time elapsed when a specific packet was sent. TC will store the number of times a packet is retransmitted. The threshold of TC is defined as *A*. A blacklist table must also be maintained with each node in order to store the malicious nodes. A NACK message is also required which will contain the address of the malicious node. This NACK will be initiated by the intermediate node in the path and has to be sent back to the sender node. A blackcast message will contain the broadcast with malicious node address. The maximum time required for receiving an acknowledgement from destination is denoted by *t*, defined as:

$$t = 2 * n * D$$

Where *n* is number of hops remaining and D is the maximum delay between two hops. Here every node will be updated with the status of their neighbors using HELLO messages.

In this proposed framework whenever a sender has to send some message to destination, it initiates the normal route discovery process of AODV. When it finds the route to destination it makes an entry of message number in the message transmission list and initializes the TC to zero for each new message. Now it starts sending the packets to the destination. If acknowledgement is received, continue the transmission. If a NACK message is received it increments the TC by 1, it retransmits the packet and sets the elapsed time counter to 0. When the TC reaches *A* it puts the node address contained in the NACK to the blacklist and blackcast a message with the blacklisted nodes to its neighbors. Every time the sender node waits for time *t*, if TC reaches to be equal to *A* and no NACK is received, then it blacklists the next-hop and blackcasts a message to its immediate neighbors. Also it finds a new route to the destination excluding the nodes in the blacklist and retransmits those messages present in the message transmission list.

Every intermediate node will save every packet received into message transmission list. Whenever a NACK or ACK is received it will send it back to the sender. If no ACK or NACK is received and elapsed time reaches equal *t*, it will send a NACK message back to the sender node. If a blackcast is received it will forward it to all it neighbors. Result analysis says that the proposed framework enhances the throughput and packet delivery ratio when used in a grayhole attack scenario.

5.1 Algorithm for the sender node packet generation and transmission process

1. Start to send the data to the destination.
2. For each message wait for maximum threshold time (*t*) required for receiving an acknowledgement/ NACK from destination.
3. If acknowledgement is received then continue the transmission.
4. If NACK is received and TC < *A* then increment the TC by 1 and continue sending.
5. If NACK is received and TC = *A* then abort the transmission.
6. Abort the transmission of current message and blacklist the node.
7. Blackcast a message to all the neighbors.
8. Start route finding process for each route containing the malicious node and retransmit.
9. If no ACK or NACK is received after time *t*, the malicious node is the next hop node and goto 7.
10. STOP.

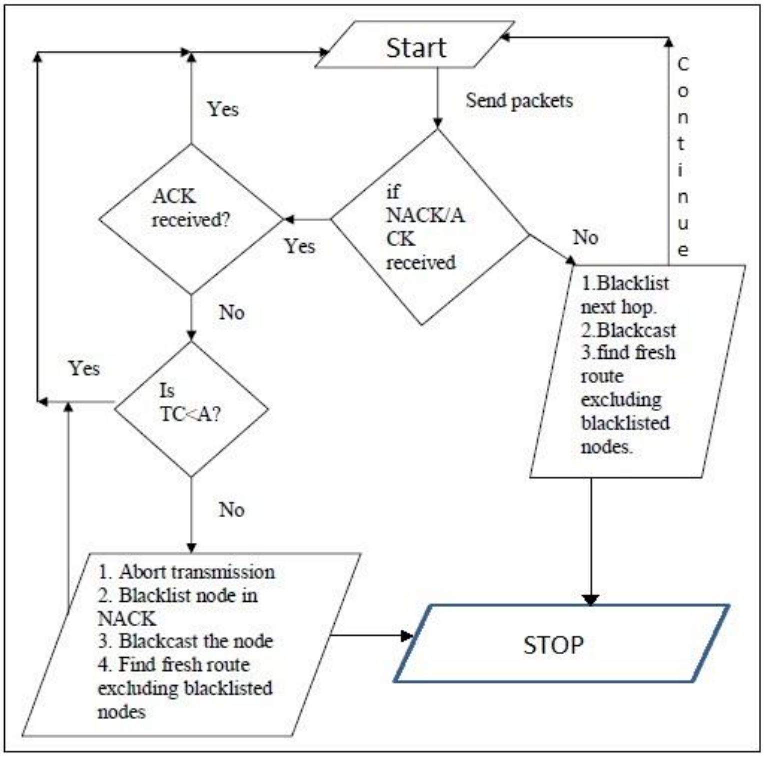

Figure 4. Flowchart for the sender node packet generation and transmission process

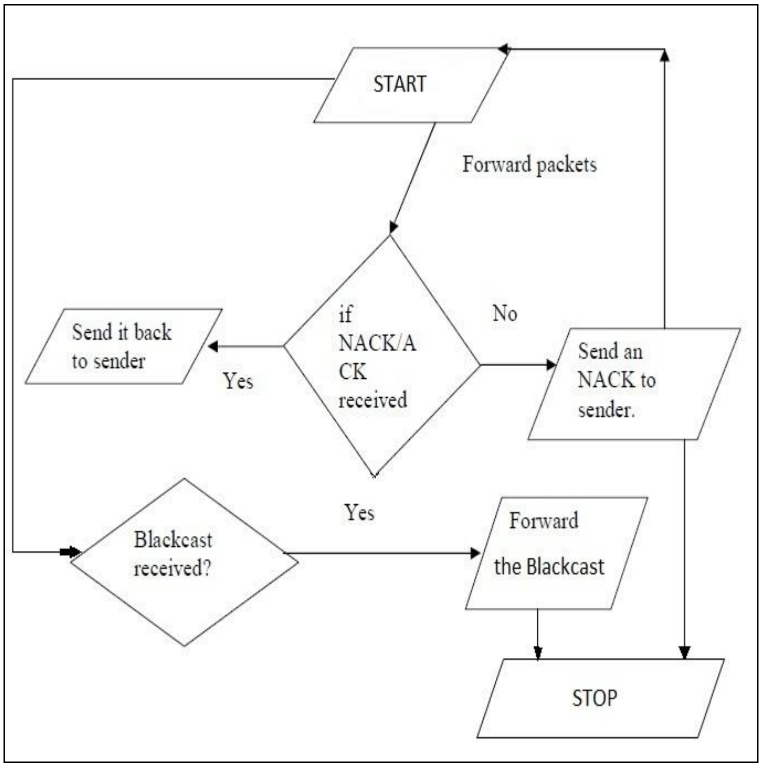

Figure 5 Flowchart for the processing of intermediate node

5.2 Algorithm for intermediate nodes

1. Forward the message towards destination.
2. Wait for maximum threshold time (t) required for receiving an acknowledgement from destination.
3. If ACK or NACK is received send it back to sender.
4. If no ACK or NACK is received after time t, send a NACK back to sender.
5. If a black cast is received, add node to blacklist and blackcast it further.
6. STOP.

VI. Simulation, Results and Analysis

The simulation is carried out using NS-2. For generation of freeway scenario C++ code and for generation of traffic CBRgen tool are used. Modified AODV protocol uses C++ and TCL to incorporate Grayhole attack and Mitigation Approach. The simulation parameters are as follows:

Table 1 simulation parameters

Parameter	**Value**
Number of nodes	10 to 100
Simulation area	1000*10
Simulation time	1000 seconds
Vehicle speed	100 Kmph
Mobility Model	Freeway
Traffic/ Connections	FTP over TCP
MAC	802.11
Transmission Range	150m
Protocol	AODV

The performance of proposed work can be analyzed and compare in terms performance metrics such as packet delivery ratio, normalized routing load, end-to-end delay, and average throughput. The next sections describes about these metrics and the resultant graphs of the simulation.

6.1 Packet delivery ratio

Packet Delivery ratio defines the efficiency of the network and hence signifies the efficiency of the routing protocol used. It is defined as

$$\boxed{\text{Packet delivery ratio} = \frac{\text{Total no of packets recieved}}{\text{Total no of packets sent}}}$$

Figure 6 shows the comparison between packet delivery ratio and number of nodes in the network. It shows that the packet delivery ratio decreases as the number of nodes increases. It is because link failures halt the transmission and hence resulting in packet drop. Our mitigation approach slightly enhances the packet delivery as compared to grayhole attack.

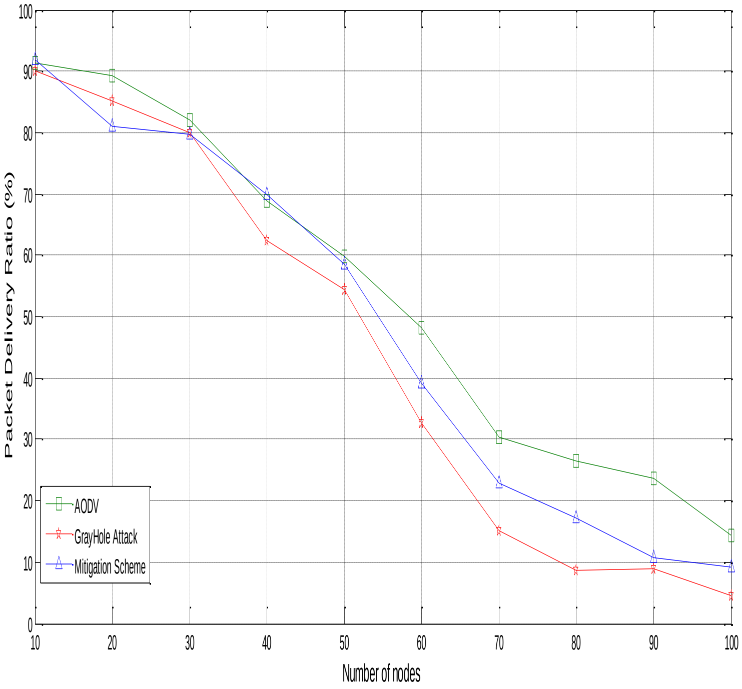

Figure 6 Packet delivery ratio Vs. number of nodes

6.2 Normalized routing load (NRL)

Normalized routing load signifies the stress that a specific protocol offers. It is defined by the mathematical formula as

$$\boxed{\text{Normalised Routing Load} = \frac{\text{Number of routing packets sent}}{\text{Number of data packets sent}}}$$

Figure 7 shows the effect of normalized routing load when the number of nodes increases for three different scenarios. In this simulation, NRL initially remains constant for all the scenarios. With the increase of the number of nodes in the network the routing load increases drastically. Our mitigation approach decreases the load on the network as compared to the grayhole attack in AODV and normal AODV.

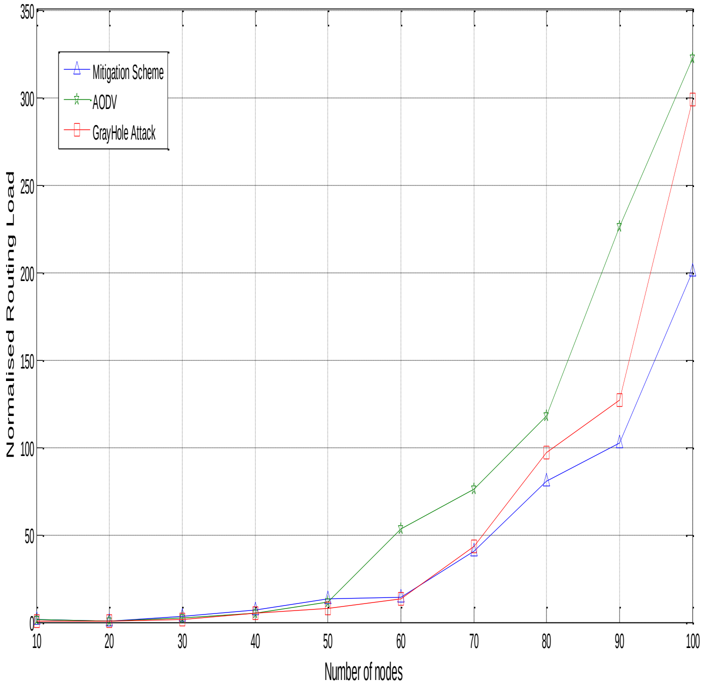

Figure 7 Normalized routing load vs. number of nodes

6.3 End–to-end delay

Average end-to-end delay signifies the total congestion factor in the network. It is defined as

$$Average\ End\ to\ End\ delay = \frac{\sum_{i=0}^{no.of\ packets} end\ time(i) - start\ time(i)}{Total\ no\ of\ packets}$$

Figure 8 depicts the average end to end delay for all three scenarios. It increases for all three with the increase in the size of the network. Our mitigation approach increases the efficiency of the network by decreasing the end to end delay.

6.4 Average Throughput

Average throughput tells us about the actual data rate of the network. It is defined by the mathematical formula.

$$Average\ Throughput = \frac{Total\ data\ sent(Kb)}{Total\ time\ (s)}$$

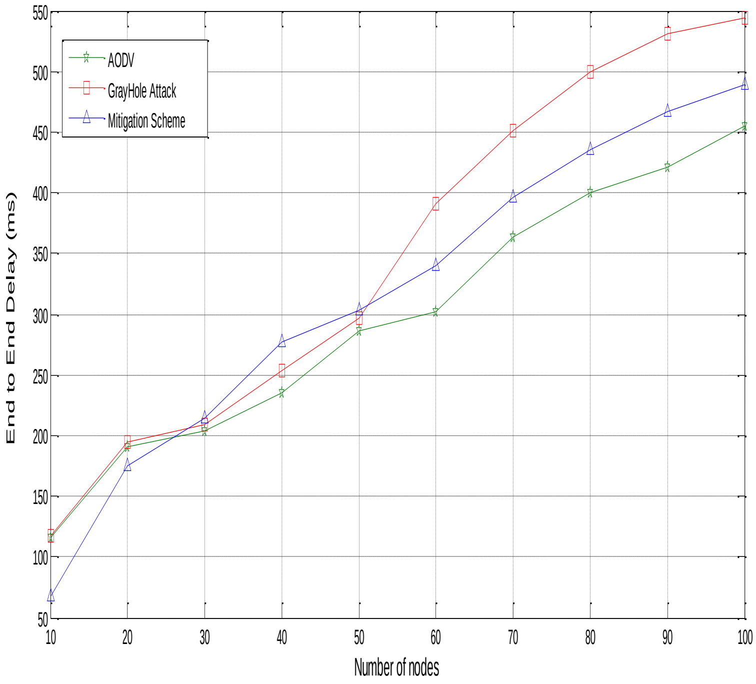

Figure 8 End-to-end delay vs. number of nodes

Figure 9 shows the comparison graph for average throughput of the network with AODV, grayhole attack and proposed mitigation approach. This graph clearly indicates that with the increase of nodes in the

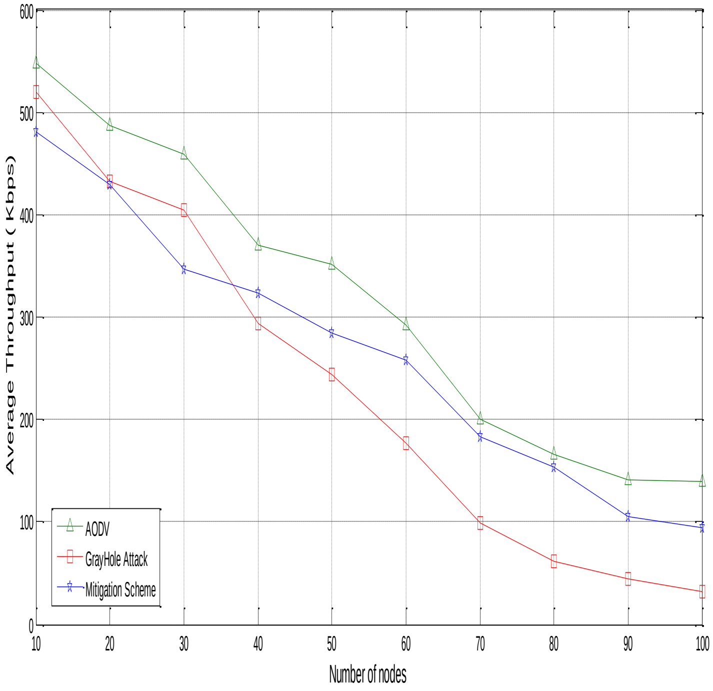

Figure 9 Average throughput vs. number of nodes

network throughput decreases. This is true for AODV, grayhole attack and our mitigation scheme. Initially the throughput for all three is closer to each other but as the number of nodes increases our approach mitigates the drop in throughput.

The aforementioned comparisons and analysis of all the four metrics show that our proposed counter based mitigation approach performed better and efficiently. It not only enhanced the throughput and packet delivery ratio but also performed better in terms of end to end delay and normalized routing load as compared to grayhole attack in AODV and normal AODV protocol.

VII. Conclusion

This paper presented a brief framework for mitigating grayhole attack in AODV. The paper showed that grayhole attack affect the performance of VANETs even at a high speed of 100 Kmph. This framework is tested and analyzed using NS-2 simulation tool. The simulation generated a scenario using freeway mobility model and AODV protocol. The proposed framework is implemented for varying number of nodes and number of misbehaving nodes for different scenarios. The comparison and analysis has been done on the basis of average throughput, packet delivery ratio, normalized routing load and average end to end delay. We found that our proposed solution helps in mitigating grayhole attack on VANETs.

References

[1] C.Siva Ram Murthy and B. S Manoj, “Ad Hoc Networks: Architectures and Protocols”, Pearson Education, Inc., 2007.

[2] Bijan Paul, Md. Ibrahim and Md. Abu Naser Bikas,” VANET Routing Protocols: Pros and Cons”, International Journal of Computer Applications (0975 – 8887), Volume 20, Issue 3, April 2011

[3] Purushottam Patel and Rupali Soni,” Defense Against Selfishness and Countermeasure”, International Journal of Computer, Information Technology & Bioinformatics (IJCITB) Volume-1, Issue-1,2012

[4] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, “Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks “, Journal of Internet Engineering, vol. 2, no. 1, June 2008, pp. 181-192.

[5] 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.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing security in Wireless Ad-hoc Network”, IEEE Communication Magazine, Issue 40, 2002, pp 70–75

[7] Atulya Mahajan, Niranjan Potnis, Kartik Gopalan and An-I A. Wang,” Urban Mobility Models for VANETs”,Computer Science Magazine, Florida State University,2011

[8] Yasser Toor, Paul M.,Anis l., and Arnaud F. “Vehicle ad-hoc networks: applications and related technical issues”, ieee communication surveys,vol 10 ,no. 3,2008,pp.74-88

[9] Loay A.,Ashfaq K.,Mohsen G.,”A survey of mobile ad hoc routin protocols”,IEEE communication surveys, vol 10, no. 4,2008

[10] 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.

[11] 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.

[12] Charles E. Perkins and Elizabeth M. Royer. “Ad-Hoc On- Demand Distance Vector Routing”. In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999, pp. 90-100.

[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 System Engineering and Technology, September 11-12, 2012

Authors

First Author – Ashish Joshi is a Research Scholar at AIACTR, New Delhi. He holds a bachelors degree in Computer Science and Engineering and pursuing post graduation in Information Security. His areas of interest are MANET and Network Security., Email: ashishium@gmail.com

Second Author – Dr. Ram Shringar Raw is an Asst. Professor in Computer Science Department at AIACTR, New Delhi. He holds Doctorate from School of Computer and Systems Sciences of Jawaharlal Nehru University, Delhi, India. He has over 12 years of teaching and research experience. His current research interest includes Mobile Ad hoc Networks, Vehicular Ad hoc Networks and Web and Data mining. He has published more than 45 papers in International Journals and Conferences including IEEE, Springer, Inderscience, American Institute of Physics, AIRCC, etc., Email: rsrao08@yahoo.in

Third Author – Prakash Rao Ragiri is an Asst. Professor in Computer Science Department at AIACTR, New Delhi. He holds M. Tech degree in Computer Science and Technology from Andhra University. He has 6 years of teaching and research experience. His areas of interest are MANET and Network Security., Email: prakashraoragiri@gmail.com