A Modified approach to Detect & Prevent Grayhole Attack in MANET

Ankita Prajapati[1], Krunal Panchal[2]
[1]Student LJIET, Ahmedabad, India, [2]Assistant Prof. LJIET, Ahmedabad
[1]IT Engineering
[1] LJIET, Ahmedabad, India,

Abstract: *Mobile Ad hoc Network (MANET) has distributed mobile wireless nodes, which do not have pre-determine topology and pre-existing infrastructure mobile nodes that can arbitrarily change their geographic locations and random mobility with constrained resources, ad hoc networks are vulnerable due to their structure less property. During the Grayhole attack, a Grayhole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. In these proposed detection mechanisms for In this paper we represent a mechanism which is helpful for prevention of grayhole attack, through observing the delay of different path to receiver and verification using authentication approach. Our mechanism helps to protect the network by detecting and reacting to malicious activities of any node. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently. Simulation will be carried out by using network simulator tool so as to address the problem of detection & prevention of grayhole attack in mobile ad-hoc network.*

Keywords: *MANET, AODV, Black-hole-attack, Gray-hole Attack.*

I. INTRODUCTION

Mobile ad hoc network (MANET)[7] is an emerging area of research which is infrastructure less network that enables the user to communicate without any fixed infrastructure. MANET[8] is a wireless network that can transfer the information from source to destination wirelessly.The nodes are movable which communicate and coordinate with the other nodes[7].Now days this network is widely used all around the world because it does not require any fixed wired network to establish communication between the source and the destination. The entire network can be established by using transmitter, receiver, processor and the battery[8]. In today’s scenario the mobile ad hoc network used in many real time applications like military surveillance, disaster management, air pollution monitoring etc[8].There are many issues in MANET like Security, Routing, Medium access scheme,Self Organization, Multicasting, Energy Management etc[6].

Taking into consideration the constraints of MANETs, most routing protocols are fairly simple, and therefore quite vulnerable to attacks.Some of these attacks are: Eavesdropping, Rushing attack ,Byzantine attack ,Location disclosure attack, Sleep deprivation attack, Routing table overflow attack ,Black hole attack ,Grayhole attack ,Wormhole attack,Denial of service, Impersonation attacks, Man-in-the-Middle attacks etc[13].

GRAYHOLE ATTACK:

In Grayhole attack, the attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication[8].Gray Hole attack execute malicious activity by dropping the packet selectivity by launching a single malicious layer[7]. They mislead the source node by pretending for shortest path.Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path[7]. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. Gray-hole attack [9] may apply through two ways which are listed below:

1. Dropping all incoming UDP packets.
2. Partial dropping of UDP packets with random selection process.

In Grayhole attack, the nature of the malicious node is highly unpredictable. It behaves as genuine legitimate node for a short duration and behaves as a malicious node for other duration. Thus we can say that the Grayhole attack is the extension of the Blackhole attack. Grayhole a ttack acts as a slow poison because the probability of the packet loss cannot be determined perfectly [12].

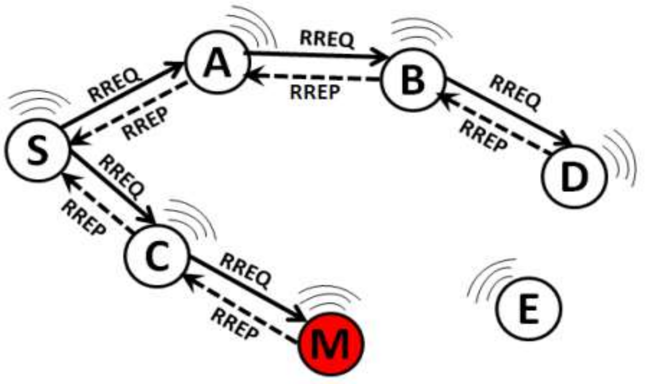

Fig. 1: Grayhole Attack in MANET[14].

II. RELATED WORK

In [1] False reply count and TrueLink based Path Authentication scheme, False reply count is very help full to detect gray hole without increasing routing overhead. The algorithm is executed on every node in the network at the local level, due to this it takes minimum time and faster than existing technique. This technique never exchanges black list and never send ALARM packets to inform other nodes about malicious node. This property reduces network traffic. TrueLink is facilitated for path authentication. As false reply count technique executes during route discovery process, any honest node can switch in the blackhole after route establishment between source and destination. Hence it is important to detect gray hole and verify link.

In [2] IDS-agent approach to detect highest sequence number node. When it detects the suspicious node, it adds it into blacklist of source node to avoid further transmission. Simulation of proposed solution observes that prevention technique not only detect malicious node but also help to prevent it.

In [3] MGAM (Mitigating Grayhole Attack Mechanism), that mitigates the impact of the smart gray hole attack. which is mainly used to compute the number of packets dropped by the particular node.When any anomaly is detected by the G-IDS nodes, an ALERT message is broadcasted by it, alerting all nodes in the network for blocking the malicious node. All normal nodes upon receiving the ALERT message issued by G-IDS nodes will include the malicious node in their blacklist table, The simulation results show that our proposed mechanism improves the network performance in terms of PDR, PLR and average throughput.

In [4] The Sequnce number based bait detection scheme (called SNBDS) for AODV protocol which is based on the destination sequence number. The scheme attempts to counter Grayhole attack during route discovery phase without introducing additional control packets to propagate information about malicious nodes to other nodes in the network..

In [5]A packet update scheme and even advise the elimination scheme by discovering all the malicious nodes.The overall simulation performance is demonstrate that the Grayhole attack scenario provides good result and even normalize the Grayhole effect network which results in normalizing effects, of Grayhole.Concept has shown improved result after elimination of the Grayhole attack in the simulation result.

III. PROPOSED SYSTEM

In blackhole or grayhole attack, malicious nodes drop the packets fully or partially. To affect the performance of network these type of malicious node attracts the traffic by sending fake route reply (RREP) to the requesting node. This type of fake reply referred as FALSE REPLY. FALSE REPLY is fake reply received from the malicious node.

In this methodology, detection of a malicious node is depending on a number of FALSE REPLY received from a node. Detection of a malicious node is done during the path establishment i.e. route discovery process. It decides to blacklist that node or not. The grayhole/malicious node is blacklisted by using this approach. The grayhole switches to the honest node and vice versa. When an honest node converts in black hole / malicious node, it generates false reply due to this it detect that node as a grayhole.

The false reply count technique runs at each and every node in the network. The counter is maintained in local RAM of the node to count a number of received false replies from replying node. To add a node in blacklist, the condition is e.g. if the first false reply is detected from the honest node, it would not add to black list. But if a number of false replies are detected from a node, it would consider as malicious and get added to the blacklist.

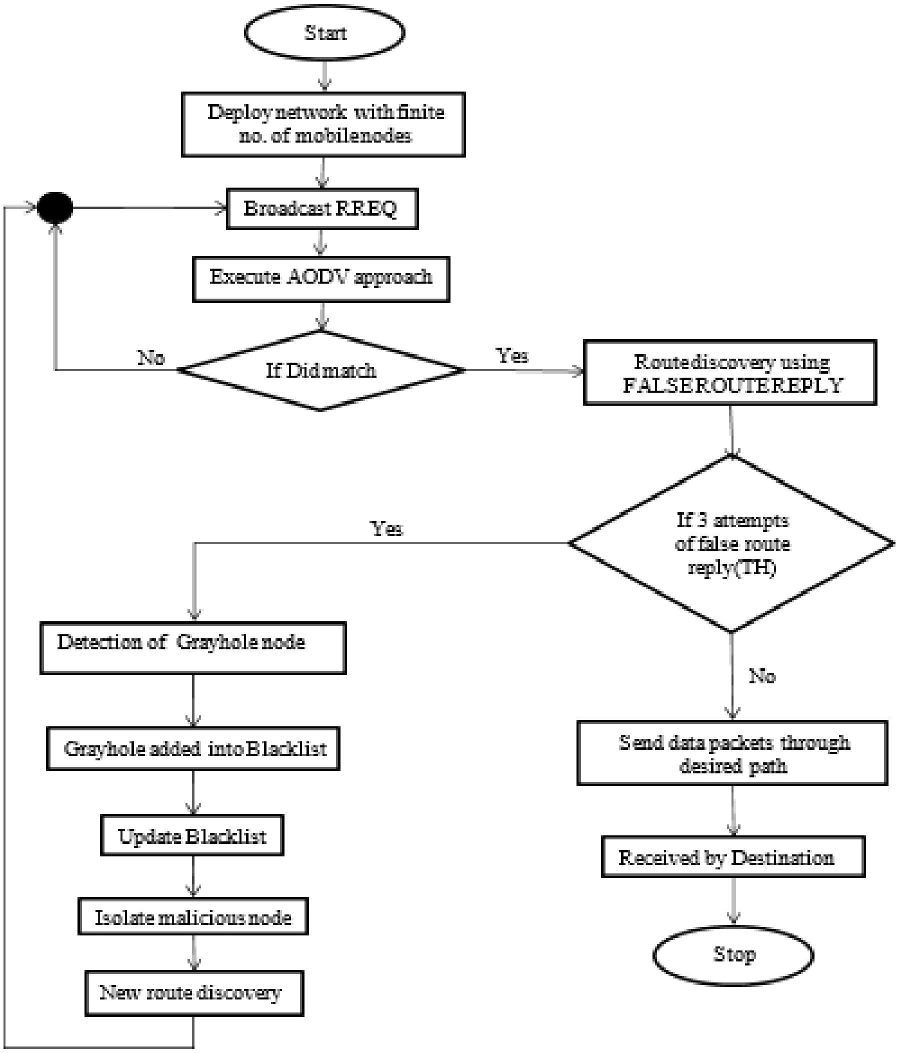
Start
Deploy network with finite no. of mobilenodes
Broadcast RREQ
Execute AODV approach
If Didmatch
No
Yes
Routediscovery using FALSEROUTEREPLY
If 3 attempts of false route reply(TH)
Yes
No
Detection of Grayhole node
Grayhole added into Blacklist
Update Blacklist
Isolate malicious node
New route discovery
Send data packets through desired path
Received by Destination
Stop

Fig- 2 Proposed System

IV. SIMULATION ENVIROMENT ANDRESULT ANALYSIS

In this section the simulation results are shown for parameters like Packet delivery rate, Packet loss rate, Normalized Routing overhead and average throughput of the packets at destination. In each scenario, all nodes were located in different positions and moved with different mobility speed of 5, 15, 25 and 35 m/s. The wireless ad-hoc network environment is formed using network simulator- 2.35. The following table indicates the simulation parameters.

Table-1 Simulation parameters

Parameter	***Value***
Dimension	*1000 X 1000 m*
Total number of nodes	*50*
Simulation Time	*500s*
Propagation radio model	*Two ray ground*

Traffic type	*CBR*
Packet size	*512 bytes*
Connection	*TCP*
Mobility model	*Random waypoint*
MAC layer	*IEEE 802.11*
Mobility speed (varying)	*5, 15, 25, 35 m/s*
Protocol	*AODV*

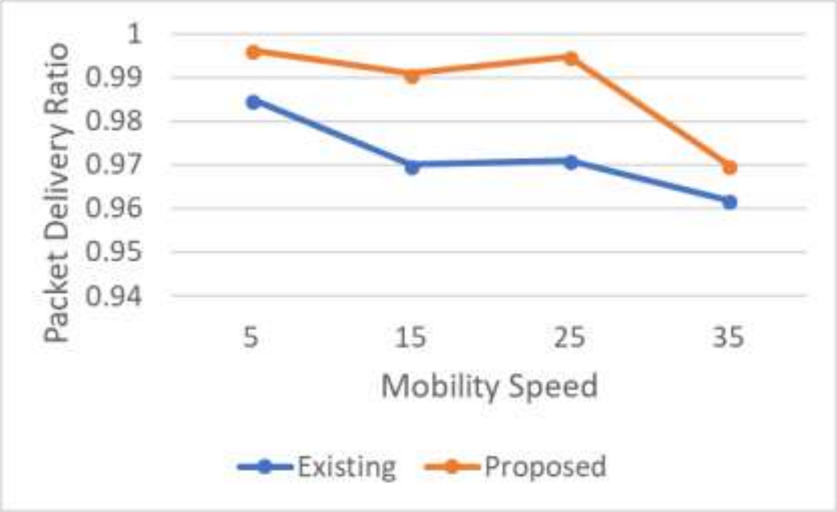

Fig . 3. Packet delivery rate

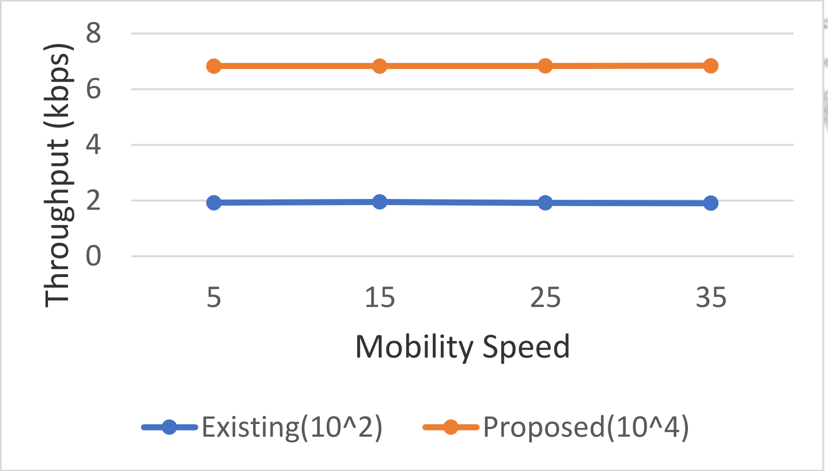

Fig . 4. Average throughput

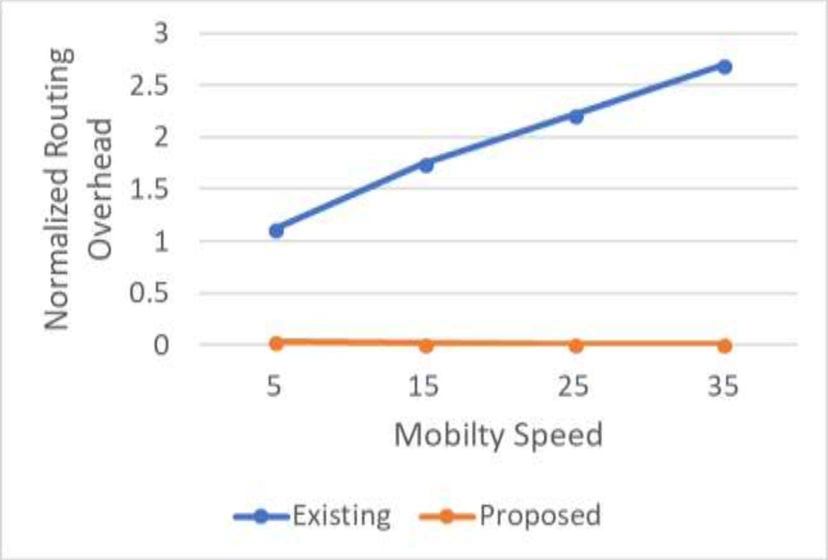

Fig . 5. Normalized Routing Overhead

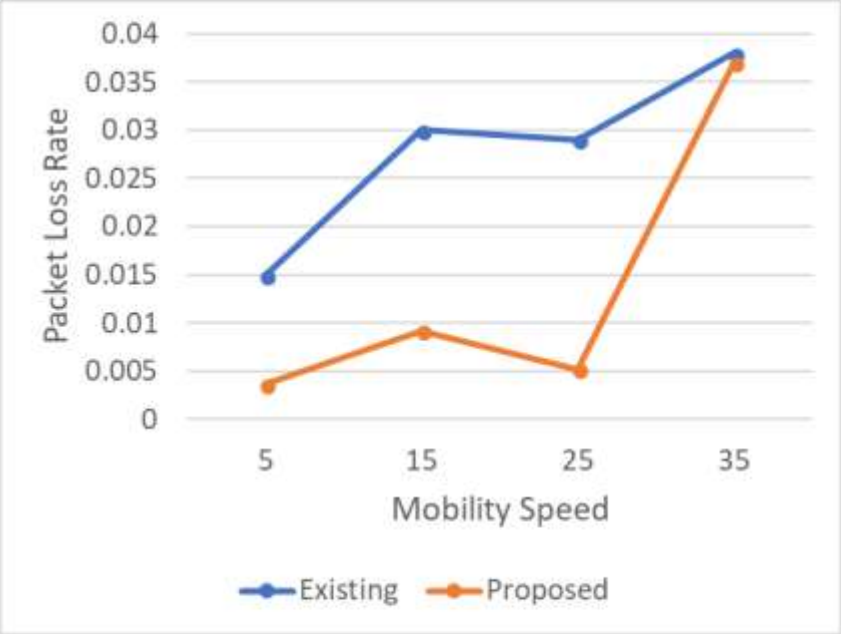

Fig- 6 Packet Loss rate

V. CONCLUSION

Ad hoc networks are more vulnerable to attacks. The Grayhole is able to change its behaviour honest node to a black hole and vice versa. This kind of node drops packets partially or fully passing through them. There are several techniques to mitigate grayhole attack but in these techniques there are many of issues like: Complex Architecture, Network congestion issue, bring down the network performance, Increase routing overhead, Time consuming etc. So that the proposed False reply count technique doesn't increase routing overhead. It takes minimum time and faster than existing technique and also reduces network traffic.Also it improves PDR,PLR,Routing overhead,Throughput etc.

VI. REFERENCES

[1] Yugandhara S. Patil, Dr. Ashok M. Kanthe.” Gray Hole Attack Detection using False Reply Count and TrueLink based Path Authentication in MANET” Computer Engineering Department, Sinhgad Institute of Technology, Lonavala.Pune, India.IEEE-2016.

[2] Sudheer Kumar, Nitika Vats Doohan ” A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol”. Medi-Caps Group of Institution Indore,India.IEEE-2016.

[3] Shashi Gurung, Siddhartha Chauhan.” A novel approach for mitigating gray hole attack in MANET”. Department of Computer Science and Engineering, National Institute of Technology, Hamirpur, Hamirpur, HP, India.Springer-2016.

[4] Rutvij H. Jhaveri,Narendra M. Patel.” A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks”. Department of Computer Engineering, CSPIT, Charotar University of Science & Technology, Changa 388 421, India, Department of Computer Engineering, Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar 388 120, India.Springer-2015.

[5] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai and Roy David Margalit.” Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks”.IEEE-2016.

[6] AD HOC WIRELESS NETWORKS by C.Siva Ram Murthy and B.S.Manoj-Pearson publication.

[7] Jyoti Prabha Singh,Savita Shiwani,Dinesh Goyal,Vishal Gaur“Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach” 2017,3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT) 978-1-5090-6218-8/17/$31.00 ©2017 IEEE.

[8] Rupali Sharma “Gray-hole Attack in Mobile Ad-hoc Networks:A Survey” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460.

[9] V. SHANMUGANATHAN, Mr.T.ANAND “A Survey on Gray Hole Attack in MANET” IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012.

[10] Ruchi Tiwari, Jyoti Jain “Exposure and Mitigation of the Gray Hole Attack from AODV in Mobile Ad hoc Network: An Approach” International Journal of Computer Applications (0975 – 8887)Volume 165 – No.5, May 2017.

[11] Subhankar Dhar “MANET:Applications, Issues, and Challenges for the Future”Int’l J. of Business Data Communications and Networking, 1(2), 66-92, April-June 2005.

[12] Mr. Ankit D. Patel,Mr. Kartik Chawda,“Blackhole and Grayhole Attacks in MANET” 2014,ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE.

[13] Nabil Nissar, Najib Naja,Abdellah Jamali,“Lightweight Authentication-based Scheme for AODV in Ad-hoc Networks” 2017,978-1-5090-6681-0/17/$31.00 ©2017 IEEE.

[14] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala,“ A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks” 2012, 978-0-7695-4640-7/12 $26.00 © 2012 IEEE.