International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

A Study of Modified Routing Protocols in MANET

Dimpal Joshi[*1], **Nisha Velani**[2]
Department of Computer Engineering, SVIT, Vasad, Gujarat, India

ABSTRACT

A Mobile ad-hoc network is an infrastructure less network , that is self-configuring mobile nodes connected by wireless links. The open medium and the decentralized property of these nodes connected on each other to store and forward packets. But if the selected node becomes selfish or misbehave, it will affect the performance of the entire group communication. When misbehaving nodes likes Balckhole and Greyhole attack, the performance is degraded severely. This paper discusses some of the techniques to detect and prevent Blackhole attack and Greyhole attack in MANET using AODV protocol.

Keywords : MANET, Misbehaving Nodes, Blackhole Attack, Greyhole Attack.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a kind of Ad hoc network with mobile nodes.Ad Hoc network is a temporal network which is managed by autonomous nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. open network boundary made security highly challengeable in this network. In this network, all nodes are free to move in any direction, with anyspeed; which caused unpredictable topology of MANET. Securing routing protocols against misbehavior and malicious nodes is highly challengeable in MANET security In ad hoc networks one of the most challenging attacks to defend against is the blackhole attack and grey hole attack.[1,2,4].

The rest of the paper is organized as follows: Section II describes AODV protocol. Blackhole attack with its impacts is discussed in section III. Section in section IV discussed greyhole attack. different modified AODV protocol discussed in section V. Section VI concludes the paper.

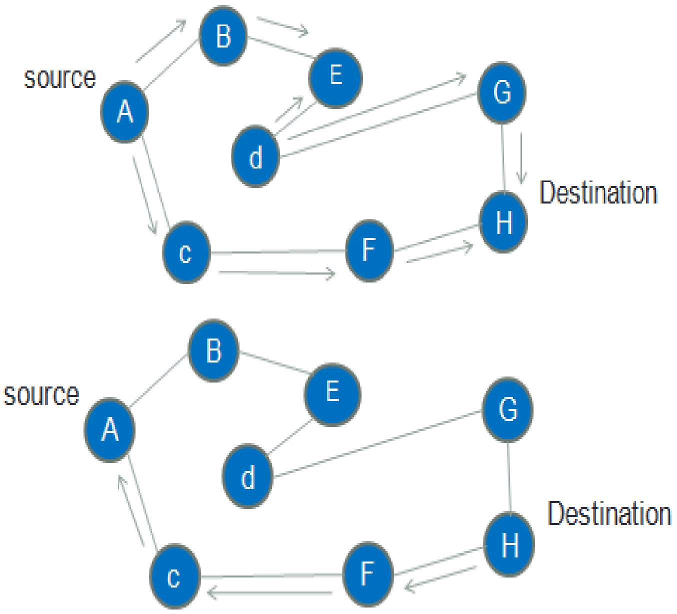

Fig 1. making path between node A and node G a RREQ BROADCAST b RREP forwarded path

II. AODV PROTOCOL

AODV is a reactive routing protocol in which the network generates routes at the start of the communication. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbour nodes. AODV routing

CSEIT1831351 | Received : 12 Feb 2018 | Accepted : 25 Feb 2018 | January-February-2018 [(3) 1 : 1621-1624]

protocol makes the paths by using an enquiry of wanting a path request and path answer. When a source node requests a path to end (destination), that node which now does not have the paths to destination-sends RREP-like broadcast all over the network. All the nodes that give this pack update their data depending on the source node data and create an entrance of reverse path for source node in the path charts. Ad hoc On-demand Distance Vector (AODV) is one of the widely used and the most effective routing protocol in MANET. In this protocol when a node needs a path to a destination, it has to find a path; therefore, it is categorized under reactive routing protocols . This protocol uses two routing packets which are: RREQ and RREP. Route Request (RREQ) packet generated by the source to find a path to the destination and Route Reply (RREP) is generated by Intermediate Nodes (IN)which have a fresh enough route to the destination. In AODV ,a fresh route is a route that has higher sequence number than the sequence number in RREQ. The sequence number increases by either the source node or RREP generator [3,4,8].

III. BLACKHOLE ATTACK

Blackhole attack is a kind of selfish node concerns with the network layer of MANET. It In black hole attack, an attacker or malicious node aims to consume all the data packets throughout the network. In black-hole attack, when the RREP message generated by source node, is received by maliciousnode, it generates a fake RREP and puts a very large value in Destination Sequence Number field and unicast it to the source node. On receiving this RREP,the source starts to forward data packets to maliciousnode, assuming that it is having shortest and freshest path to the destination and ignores other RREP packets.The data packets received by malicious node are not forwarded by it to any other node. This attack is called Black-hole attack because all the data packets are dropped by malicious node.[4,5,6].

IV. GREYHOLE ATTACK

Variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. In Gray Hole Attack a malicious node drops the packet and does not forward them. Gray Hole attack can be act as a slow poison in the network side that is the probability of packet loss is un determined . In this attack a malicious node behave as an truthful node during route discovery process and starts dropping the packets silently as soon as the packets start arriving [5,9].

V. MODIFIED AODV PROTOCOLS

IDSAODV protocol [3] which has resulted to earn new rules to identify the destructive nodes. By using this method, the security and efficiency of AODV protocol against the black hole attack has improved and so the identification percentage of the destructive nodes is higher. In this algorithm, the authors used a number of new rules to identify the destructive nodes, which caused a considerable decrease in the range of lost packets and endto-end delay in the proposed algorithm than AODV protocol. So the range of delivery packet and throughput of this algorithm increased more than the AODV protocol.

Checks both Next_Hop_Nodes (NHN) and Pervious_Hop_Nodes (PHN) [4] which detecting all malicious nodes in network by using a Data Routing Information (DRI) table. Our approach checks the Next_Hop_Node (NHN) and Pervious_Hop_Node (PHN) in a path to detect malicious nodes. When the source node detects malicious nodes, it broadcast the ID of malicious nodes to the network and all nodes set DRI entries for mentioned nodes to “NULL”. By using a data packet for PHNs, node’s DRI table updated and number of trustable nodes increases. reduced the packet overhead and processing time of detecting malicious nodes.

Tapping AODV [5] In this paper a technique is being proposed for detection of the black-hole or malicious node. In this technique, a new procedure a kind of trap method is added in AODV protocol for the detection of malicious nodes. When the Black-hole node is detected after that an alarming method is triggered to make other nodes aware of malicious nodes. This method is work in two phase (a). Route Discovery (b). Monitoring phase. Use traprequest based intrusion detection for detecting and preventing grayhole and blackhole attacks respectively.

TSAODV routing protocol [6] In this paper, The proposed work focuses on trust based computing to mitigate the effects of black hole, wormhole and collaborative black hole attacks. Trust value is computed on the basis of route request, route reply and data packets. After calculation get trust values between 0 to 1. If trust value is greater than 0.5 then marks node is reliable and allow on a network otherwise block. Network performance of proposed protocol trusted secure AODV routing protocol (TSAODV) is evaluated. The result shows performance improvement as compared to standard AODV protocol.

Two RREP packet verification [7] enhances the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks. Our solution avoids the black hole and the multiple black hole attacks. In our approach, like the standard AODV routing protocol, the destination node or intermediate node generates the RREP packet, but it also generates another RREP packet. It is a kind of confirmation of the first packet with a sequence number incremented by one. one with the normal sequence number and other with the normal sequence number + 1, and both have the field VERIFIED set to 0. appended field VERIFIED if it is set to 0 or 1. If it is 0, invalid packet. Otherwise the packet is verified and valid and it must be forwarded to the next node.

VI. CONCLUSION AND FUTURE WORK

This paper describe various type of modified AODV protocol which improve performance of routing protocol by detecting misbehaviour nodes in MANET. but routing overhead is one of the problem. we will discribe new algorithm soon to overcome drawbacks. we will show result using simulator.

VII. REFERENCES

[1]. Rasika R. Mali and Sudhir T. Bagade. "Detection of Misbehaving Node using Secure Acknowledgement in MANET."IEEE 2016

[2]. Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das "A Survey of Black Hole Attack Detection in MANET "IEEE 2014.

[3]. Sina Shahabi, Mahdieh Ghazvini and Mehdi Bakhtiarian. "A modified algorithm to improve security and performance of AODV protocol against black hole attack"20 auguest 2015 springer.

[4]. Ali Dorri and Hamed Nikdel. "A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET."IEEE 2015.

[5]. Neha Sharma, Anand Singh Bisen. "Detection As Well As Removal Of Black hole And Gray hole Attack In MANET."2016 IEEE.

[6]. Upendra singh, Makrand Samvatsar, Ashish Sharma and Ashish Kumar Jain "Detection and Avoidance of Unified Attacks on MANET using Trusted Secure AODV Routing Protocol "IEEE 2016.

[7]. Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif and Benachir El Hadadi. "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack."IEEE 2016.

[8]. Meenakshi Patel and Sanjay Sharma. "Detection of Malicious Attack in MANET A Behavioral Approach "IEEE 2012.

[9]. Pradeep R. Dumne and Arati Manjaramkar "Cooperative Bait Detection Scheme to prevent

Collaborative Blackhole or Grayhole Attacks by Malicious Nodes in MANETs "IEEE 2016.

[10]. Kriti Patidar, Vandana Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks "IEEE 2014.

[11]. P.Rathiaga and Dr.S.Sathappan "Hybrid Detection of Black hole and Gray hole attacks inMANET "IEEE 2016.

[12]. Kajal S. Patel and Dr. J. S. Shah. "Detection and avoidance of malicious node in MANET "IEEE 2015.

[13]. Sangeetha.V, S. Swapna Kumar "ZIDS: Zonal-based Intrusion Detection System for Studying the Malicious Node Behaviour in MANET ."IEEE 2015.