ISSN:0975-9646



# A Survey on Intrusion Detection in MANET through AODV

Divya Patidar[1],Jigyasu Dubey[2]

*Department of Information Technology*
*SVITS College Indore(MP),India*

***Abstract*— Mobile ad hoc networking has been a popular research area for last Decade. Security is an essential requirement in mobile ad hoc network (MANETs). In comparison with wired networks, Mobile ad hoc networks are more vulnerable to security attacks due to the lack of a centralized authority and limited resources. The security of the ad hoc network is compromised by a various type of attacks because of malicious nodes present in the network. This paper provides a survey on how AODV detect the Attacks using different methods. We discuss several methods of secure routing and intrusion detection mechanisms using AODV Protocol.**

***Keywords*— MANET, AODV, Attacks, Malicious nodes etc.**

## I. INTRODUCTION

A mobile ad hoc network (MANET) is a system of wireless mobile nodes that can freely and dynamically self-organize in arbitrary and temporary network topologies without the need of wired backbone or centralized administration [1]. The goal of mobile ad hoc networking is to support robust and efficient operation in mobile wireless network by incorporating routing functionality into mobile nodes. Ad hoc network have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as router, which discover and maintain routes to other nodes in the network.

Mobile ad hoc networks are infrastructure less and self-organized or configured network of mobile devices connected with radio signals. There is no centralized controller for the networking activities like monitoring, modifications and updating of the nodes inside the network. There have been serious security threats such as various kinds of attacks (active and passive), blackhole, wormhole, flooding attack, denial of service attack etc. in MANET. These usually lead to performance degradation, less throughput, congestion, delayed response time, buffer overflow etc.[2].

Protocols in MANET allow user of mobile devices to communicate over the wireless links. There are mainly two types of routing protocols: Proactive Protocols (Table Driven) and Reactive Protocols (On Demand). Proactive protocols such as DSDV, OLSR, and TBRPF maintain routing information in network in tables. And reactive protocols such as AODV, DSR etc. finds the route on demand [3].

## II. AODV

Ad hoc on demand distance vector (AODV) is consisting of two phases: route discovery and route maintenance. In route discovery phase Route Request (RREQ) and Route Reply (RREP) control messages are used and in Route Maintenance phase Route Error (RERR) control message are used. The source node sends RREQ packets to all its immediate neighbours in route discovery phase. The node sends RREP packet to the sender node if the corresponding node is a destination node. In the other case, the nodes check whether it has entry for the route to the destination in their routing table. If yes, they send the route request RREQ to their further neighbours. This process will continue until the destination node or an intermediate node having a fresh route to the destination. If the routing table doesn't contain any entry to the destination then next step comparison of sequence number. If destination sequence number is greater than or equal to the new sequence number than it denotes the fresh route and packet can be send through this route. Then this intermediate node sends a RREP packet to the requested node. The RREP packet sends back to the source through the reverse route. Then the source node updates its routing table and sends packets through this route. . In route maintenance phase, if during the operation, if link failure is identified by any node, respected node sends a RERR (Route Error) packet to all other nodes in a network that uses this link for their communication to other nodes [4].

## III. RELATED WORK

The nodes in an ad hoc network also function as routers whose work is to discover and maintain routes to other nodes in the network. The main goal of a MANET routing protocol is to establish a correct and efficient route between nodes so that messages may be delivered with in a time. The entire network can be paralysed, if routing is misdirected. Thus, security during the routing plays an important role in the security of the whole network.[routing security in wireless ad hoc]. This section describes how various routing techniques are helpful to remove security threads in MANET[5].

The Mr. Nallamala Sri Hari, Dr. N. Srinivas Rao, Dr. N. Satyanarayan["A Novel Routing attack in mobile ad hoc networks", Indian Journal of Computer Science and Engineering Vol. 1 No. 4 382-391] describe a set of generic mechanism that together defend against the ad hoc flooding attack: neighbour suppression. This method is used to prevent flooding of RREQ packets. In neighbour

suppression method each neighbour calculates the rate of RREQ originated by intruders. If this rate exceeds the pre-defined threshold, all neighbours will not receive and forward packet from intruder. To calculate the rate of RREQ and find the intruder, they give algorithms to calculate REQ_time and then check REQ_time > threshold. If the time exceeds the threshold, we may make a judge that it is intruder. But there are some drawbacks in this method: This method efficiently defences the Ad Hoc Flooding Attack with little overload i.e. performance of network can't bear heavy load as if attacking packets are more[6].

To avoid the blackhole attack authors Seungjoon Lee, Bohyung Han, Minho Shin ["Robust Routing in Wireless Ad Hoc Networks" Parallel Processing Workshops, 2002 ISSN :1530-2016] Introduce the route confirmation request (CREQ) and route confirmation reply (CREP) packets. On finding a route to the destination in its cache, an intermediate node sends RREP back to the source. At the same time, the intermediate nodes send CREQ to its next hop node toward the destination. Then, after receiving CREQ, the next hop node looks up its cache for a route to the destination. If it has one, it sends CREP with its route information to the source. Then, the source is checks whether the path in RREP is valid by comparing the information with CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that, if two consecutive nodes work in collusion they can't avoid blackhole attack as the next node is a colluding attacker sends CREPs that supports the incorrect path[7].

The authors Rutuja Shah, Lakshmi Rani, S. Sumathy ["Node Monitoring with Fellowship Model against Black Hole Attacks in MANET", International Journal of Computer Science and Business Informatics, ISSN: 1694-2108 | Vol. 14, No. 1. JUNE-JULY 2014**]** introduce a mechanism to reduce the packet-drop attacks by implementing "node monitoring with fellowship" technique. They introduce an obligation on the nodes to render services to network. If services are not rendered, the particular node will be expelled outside the performance. They also introduce a "fair-chance" scheme for all nodes to find genuine node or malicious node. In this method they calculate the equivalence ratio as number of incoming packets and number of outgoing packets is same. If that count is same, there is uniform distribution and forwarding of packets among the nodes inside network. And if the count is not same, then that particular node is kept under "observance zone" in order to monitor its suspicious behavior. Then this suspected node is given "fair-chance" treatment in observance zone. Then that suspected node have to submit its "status-message" to neighboring nodes to prove its genuineness of performance inside network. Status-messages will be entertained only up to threshold level which was set up unanimously amongst neighboring nodes inside a network. One drawback of this approach is that there is an overhead of exchanging more number of messages among the neighboring nodes in forwarding status messages[8].

The authors Vikas kumar upadhyay , Rajesh K Shukla["WPAODV: Wormhole Detection and Prevention Technique", Int. J. Advanced Networking and Applications Volume: 05, Issue: 03, (2013) ISSN : 0975-0290] presents a mechanism to provide wormhole free path from source to destination by adding an extra feature in AODV routing protocol. To find the wormhole, the WPAODV uses divide and conquer technique over the suggested path by AODV. For taking decision WPAODV uses Neighbour node concept along with Statistics Based scheme and graphical based solution of wormhole problem. To discover wormhole in the route suggest by AODV maximum number of intermediate node between nodes to its next to next node with alternate route are discovered. If alternate route between any pair of node to next to next node with the path discover by AODV is greater than threshold, then there is wormhole between its next node and next to next node. Threshold is calculated on the basis of hop-count and neighbour node. For calculating threshold each and every node of network find the path having the largest number of node over the entire possible path between it and its next to next node and consider average value highest hop count of the entire node. The drawback of this method is that the detection technique works efficiently but having some overhead, control packets are more[9].

The author Saurabh Upadhyay and Aruna Bajpai ["Avoiding Wormhole Attack in MANET using Statistical Analysis Approach", International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012] proposed wormhole attack model method which works without any extra hardware requirements, they use the basic idea of wormhole attack reduces the length of hops and the data transmission delay. They proposed algorithm in which they randomly generate a number 0 to maximum number of nodes, and make the node with same number as transmitter node. Then from the selected transmitting node to destination node generate the route. Using reactive routing technique sends RREQ and initiate counter. After Receiving the RREP packet from the each path; associate it in route list with time delay. Then calculate the average time delay. Then Select the route within covariance range of average delay. The routes are black listed which are not within the covariance range hence they are not involved in future routes discovery. Whole process is repeated for limited assumed time. The main drawback of this method is that the algorithm avoids the wormhole route so the route discovery time is increases. This Statistical analysis approach is useful if the sufficient information about the routes is available from multi path routing and can detect the wormhole[10].

The authors Avenash Kumar , Meenu Chawla["Destination based group Gray hole attack detection in MANET through AODV", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012 ,ISSN (Online): 1694-0814] proposed a method to detect and prevent the group grayhole attack in MANET using ad hoc on demand protocol. Methodology works in three steps: Store the RREP packet on previous node, Check 2 hop distance of a suspected node and lastly Rejection of RREP packet. In this paper RREP message replies to previous node and should attach the one hop distance node of replying node (suspected node) otherwise

previous node will reject the RREP message. The main drawback of this method is that there is extra overhead of hop distance[11].

## IV. PROPOSED CONCEPT

A conventional intrusion detection approaches detects various types of attack in a MANET through AODV routing. These conventional approaches find the malicious node during the maintenance phase of routing that increase end-to-end delay. So require to design an approach that detects malicious nodes during the route discovery phase to reduce end to end delay. The proposed solution is the prevention technique that prevents the ad-hoc network from the various kinds of routing attacks such as Packet dropping attack, Flooding, Blackhole by removing malicious node during the route discovery process. The proposed approach increases the network performance in terms of PDR, throughput and end to end delay.

## V. CONCLUSIONS

In this paper we have study the different methods to provide security in MANET. We also studied many solutions have been proposed to recover MANET attacks, but still MANET has several issues and challenges so need to design new method or algorithm which will address these issues. There are still work required in terms of packet delivery ratio, throughput, and end to end delay. The future work should be focused on performance of secure network in terms of PDR, end to end delay, throughput etc.

## REFERENCES


[1]. D. D. Perkins, H. D. Hughes & C. B. Owen, (2002) "Factors Affecting the Performance of Ad Hoc Networks," Proceedings of the IEEE International Conference on Communications (ICC), 2002, pp.2048-2052.

[2]. Nishu Garg, R.P.Mahapatra "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[3]. Basu Dev Shivahare ,Charu Wahi , Shalini Shivhare " Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol property", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 3, March 2012.

[4]. Pardeep Saini, Ravinder Chouhan "An Analysis For Recognition And confiscation Of Black Hole In MANETS", International Journal of Innovative Research in Advanced Engineering (IJIRAE), ISSN: 2349-2163, Volume 1, Issue 5 (June 2014).

[5]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, October 2002, ISSN :0163-6804,Volume:40 , Issue:10.

[6]. Mr. Nallamala Sri Hari, Dr. N. Srinivas Rao, Dr. N. Satyanarayana "A Novel Routing Attack In Mobile Ad Hoc Networks", Nallamala Sri Hari et. al. / Indian Journal of Computer Science and Engineering Vol. 1 No. 4 382-391.

[7]. Seungjoon Lee, Bohyung Han, Minho Shin "Robust Routing in Wireless Ad Hoc Networks" ,Parallel Processing Workshops, 2002 ISSN :1530-2016.

[8]. Rutuja Shah, Lakshmi Rani, S. Sumathy "Node Monitoring with Fellowship Model against Black Hole Attacks in MANET", International Journal of Computer Science and Business Informatics, ISSN: 1694-2108 | Vol. 14, No. 1. JUNE-JULY 2014.

[9]. Vikas kumar upadhyay , Rajesh K Shukla "WPAODV: Wormhole Detection and Prevention Technique", Int. J. Advanced Networking and Applications Volume: 05, Issue: 03, (2013) ISSN : 0975-0290.

[10]. Saurabh Upadhyay and Aruna Bajpai "Avoiding Wormhole Attack in MANET using Statistical Analysis Approach" ,International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012.

[11]. Avenash Kumar , Meenu Chawla "Destination based group Gray hole attack detection in MANET through AODV", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012 ,ISSN (Online): 1694-0814.

[12]. Meenakshi Sharma and Davinderjeet Singh, "Implementation of a Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in Manet", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161©2014.

[13]. Komal, Sonam Dhawan, "An Improved Performance of MANET using AODV Protocol for Black Hole Detection", International Journal of Research in Computer and Communication Technology, Vol 3, Issue 5, May- 2014.

[14]. Kritika Sharma, Parikshit Singla "Robust Security Solution to Countermeasure of Malicious Nodes for the Security of MANET", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4364-4368.

[15]. Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, Mobile Ad Hoc Networking, IEEE Press, A John Wiley & Sons, INC., Publication,2004