International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

MAS-AODV: Mobility Aware Secure AODV to Prevent Gray Hole Attack in MANETs

Namrata Jain[1], Yogesh Rathore[2]

[1, 2]Department of Computer Science and Engineering, Raipur Institute of Technology, Mandir Hasaud, Raipur (C.G), India

Abstract: ***Security in mobile ad hoc networks (MANETs) is still a crucial issue as the protocols devised till now are still under experimental RFCs and thus no protocol could be standardized to date to stand against the weaknesses of MANETs. In this paper we present Mobility Aware Secure AODV referred to as MAS-AODV, which is an AODV based routing algorithm, to protect MANETs from a selective forwarding attack known as gray hole attack. MAS-AODV uses the speed of movement of nodes for the detection of gray hole nodes and thus termed as mobility aware. If a node moves around in the network with speed greater than the threshold, the node is identified as gray hole node. Apart from this, an added security in the algorithm is through digital signature. All the nodes taking part in the path formation are first verified using digital signature so that no malicious nodes can interfere the transmission of data. Simulation of MAS-AODV shows that the algorithm performs better than AODV in terms of packet delivery ratio (PDR) and throughput at a cost of routing overhead and delay in some cases.***

Keywords: MANET, Gray hole attack, AODV, MAS-AODV, Reactive Routing Algorithm.

1. Introduction

In the present era, mobility is on its verge as day to day needs demand mobility and Mobile Ad-hoc Networks (MANETs) are therefore much in demand. MANET is a network paradigm which is wireless and ad-hoc in nature i.e., different devices on the fly can communicate to each other without any pre-existing network infrastructure. MANETs are also dynamic i.e., devices can join or leave the network at any time due to which it does not have any secure boundaries like in wired networks and also hold a dynamic topology. Due to such vulnerabilities[1] of MANETs and lack of centralized management facility MANETs are prone to many attacks mainly categorized as[3] passive attacks, which does not harm the networks like eavesdropping, traffic analysis etc, and active attacks that interrupt the network operations like DOS, replay, selective forwarding attack etc.

In this paper, we propose an algorithm to defend a network layer, selective forwarding attack known as gray hole attack [7][8]. The algorithm is referred to as MAS-AODV i.e. Mobility Aware Secure-AODV. In the gray hole attack, the attacker selectively forwards packets to the destination by displaying false routing information to the source so that the source diverts the traffic to the attacker node and the node can thus launch the attack. When this attacker node drops all the data packets that are routed to it, the attack is known as black hole attack but due to the selective dropping nature of the gray hole attack, the attacker more intelligently hides itself from being discovered.

MAS-AODV is an AODV based algorithm as studies show that proactive routing protocols are left behind in performance by reactive protocols [6]. MAS-AODV enhances the security of AODV against gray hole nodes by the use of cryptography and also by examining the speed of mobility of nodes. Malicious nodes tend to move more speedily around the network in search of its victim than a normal node. This fact is utilized and malicious nodes are traced by noticing the node speed. Even if the node acts normal, the digital signature verification scheme secures the network.

In the rest of the paper, we first discuss the AODV protocol in section II on which our proposed algorithm is based on. In section III, the proposed approach is discussed and section IV shows the simulation results of comparison of MAS-AODV with AODV protocol. Section V concludes the paper.

2. AODV: Ad-hoc On demand Distance Vector

AODV [5] is a reactive routing protocol and one of the most popular routing protocols for MANETs. Many other researchers take AODV as their basis for further research and development of more secure versions. Like other reactive routing protocols [2], AODV establishes a path for transmission of data packets on demand and does not maintain routing information beforehand like in proactive routing protocols[2],[10]. The most distinguishing feature of AODV from other routing protocols is the use of the destination sequence number (DSN).

Whenever a path needs to be discovered, the source node broadcasts a route request (RREQ) packet. Any intermediate node having an updated path to the destination or the destination itself replies with the route reply (RREP) packet which contains the route to the destination. Any intermediate node receiving the RREQ packet updates its path to the destination if the DSN in the RREQ is greater than the previous DSN stored in it and further broadcasts the RREQ packet, and if the DSN in RREQ is smaller, then the IN is considered to have an updated path and it remits the RREP back to the SN. When the source node receives the RREPs, it decides which route to select on the basis of hop count. This is the route discovery method of AODV and route maintenance is done with the help of periodical beacons and acknowledgement messages.

AODV is essentially a combination of both DSR [4] and DSDV[9]. The on-demand mechanism of route discovery is borrowed from DSR and from DSDV it takes hop by hop routing, sequence numbers and periodic beacons. One main thing to be noticed is AODV does not provide any type of security.

3. Proposed algorithm: MAS-AODV

3.1 Overview

MAS-AODV is an extension of one of the popular reactive routing algorithms, AODV. AODV is security wise enhanced to detect gray holes or probable gray holes in the network by taking into consideration the speed of movement of the nodes. The fact that malicious nodes tend to move more speedily in the network in search of victim nodes compared to normal nodes , is utilized in designing the algorithm. Also digital signature is added for enhanced verification of nodes contributing in the data transfer path even if the node speed is normal. MAS-AODV is explained in detail next.

3.2 Detailed Description

MAS-AODV secures the network by enhancing AODV as follows. Whenever a source(S) needs to send data packets to the destination (D), it floods the network with route request (RREQ), like in AODV, to establish the path for transmission. If an intermediate node (IN) has an updated path to the destination, it sends route reply (RREP) back to the source and if no IN has an updated path, the RREQ packet is broadcasted till it reaches the destination and the RREP is generated by the destination and sent back to the source. The secure aspect of the algorithm starts when the source receives the RREP packet. As soon as the source receives the RREP, it first checks if the RREP is from the destination node or an IN. if the RREP is generated by the destination, the source without any further enquiries transfers the data to destination. And if the RREP received is from an IN, the source checks for the node speed. If the speed of the node from which S received RREP is greater than a threshold value, the IN is treated as a gray hole node. If not, the source starts a verification of the node using digital signature. If the digital signature of the node matches, then the IN is considered to be a normal node and data is routed to the destination through the IN. A flow chart for MAS-AODV is shown in Figure 1.

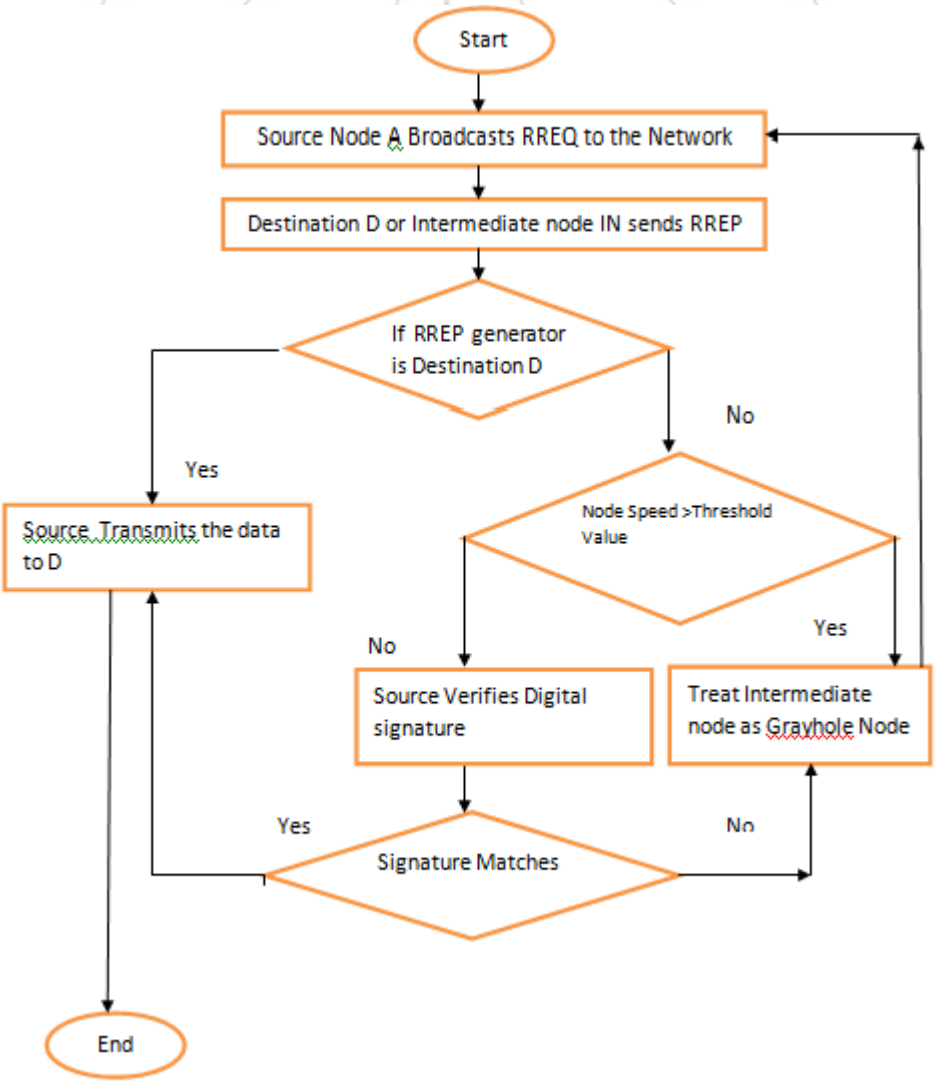

Figure 1: Flow Chart of MAS-AODV

4. Performance Evaluation

4.1 Simulation Model

To simulate MAS-AODV and compare it with AODV we have used the network simulator NS-2 [11][12]. The simulation model consists of flat grid topography of 1000 x 1000 meters. Channel type is wireless with randomly placed nodes having property of random movement. When a node needs to send data packets, it initiates constant bit rate (CBR) traffic with user datagram protocol (UDP) for the intended destination. Mac type used is IEEE 802.11. Three different cases with varying number of mobile nodes are taken into consideration for comparison of the two algorithms under different conditions. An instance of the simulation is shown in figure 2.

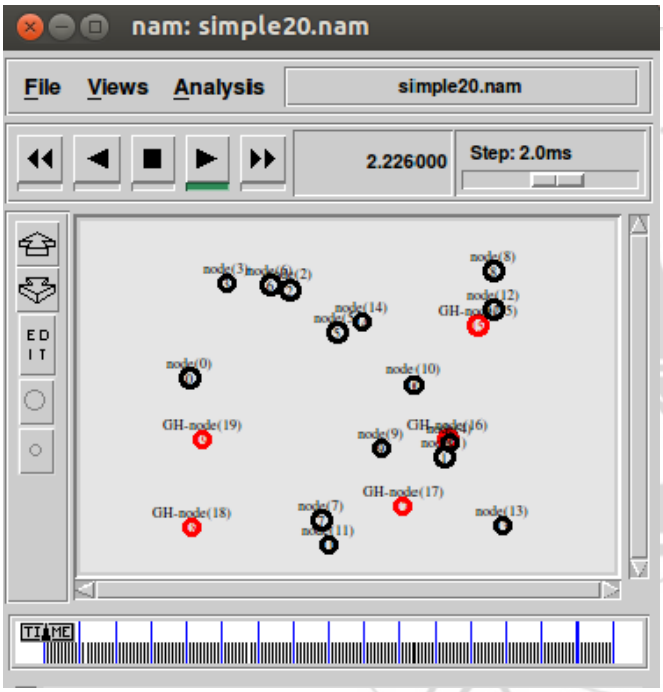

Figure 2: An Instance of Simulation Environment

4.2 Performance Metrics

MAS-AODV is compared with AODV in terms of packet delivery ratio (PDR), normalized routing load (NRL), throughput and end to end delay (E2E). The parameters for comparison are explained below:

Packet delivery ratio: Packet delivery ratio compares the total number of packets sent by the sender to the number of packets actually received at the receiving end. The result of this comparison is represented by a metric derived by taking a ratio of the two. This ratio defines the percentage of data successfully delivered.

Normalized Routing load: NRL is the Load on the network due to the routing protocol apart from the data packets to be routed. Routing load is calculated as the ratio of the routing data transmission known as control packets to the data packets transmitted in the same transmission. This is the overhead of transmission incurred by the routing protocol apart from the data to be transmitted.

Throughput: Throughput is the amount of data transmitted per unit of time. It is generally calculated by dividing the total amount of data received by the receiver to the time taken by the destination to receive the final packet.

Average End to End delay: This is the average time taken by the network to transfer a data packet from one end to other i.e. the delay in transfer of a data packet to the destination from the source.

4.3 Simulation Results

The algorithms are compared in environments with varying number of nodes. The comparisons can be seen with the help of xgraph tool available with NS-2. Figure 3 shows the graph for PDR of both the algorithms with varying number of nodes. The green line in the graph refers to MAS-AODV and the red line refers to AODV. From the figure, we can see that the PDR for MAS-AODV is way much higher than AODV which proves that the security mechanisms implemented in MAS-AODV works fine to keep the gray hole nodes away from dropping data packets. Thus the ratio of the packets delivered to packets sent is higher. The network is thus more secure to gray hole attacks as compared to AODV. We take for instance the case of 20 nodes. In an environment of 20 nodes with gray hole nodes present, the PDR in under AODV protocol is 38.40% and under the proposed protocol is 74.54% , which shows that the PDR is almost doubled in this case.

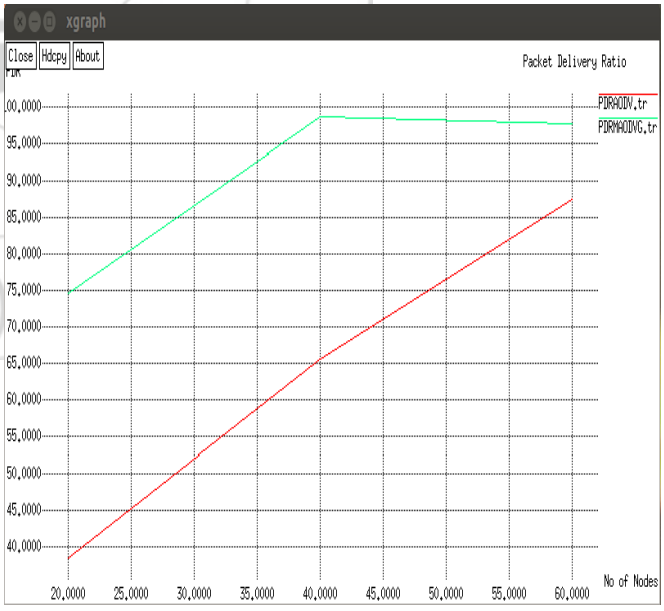

Figure 3: Packet Delivery Ratio

Figure 4 shows the results for throughput and here again MAS-AODV takes a lead on AODV by giving higher throughput in the presence of gray hole nodes than under the AODV protocol. In the same 20 nodes case, the throughput under AODV protocol is .4840 in kbps and under MAS-AODV is .9385. so the data transmitted per second also increases to nearly double. The graph in figure 4 in the same

way shows how the throughput varies under the two algorithms.

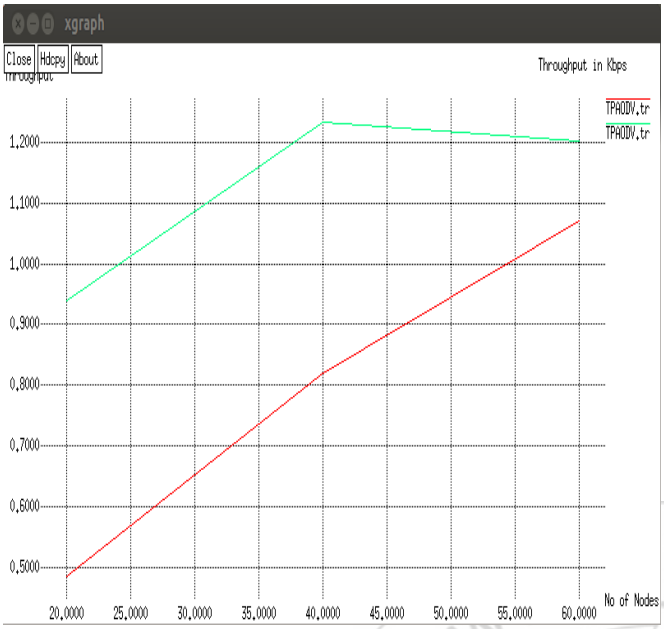

Figure 4: Throughput

In figure 5, the graph for the normalized routing load is shown. From the graph it is clear that MAS-AODV is providing better performance at the cost of overhead of control packets. MAS-AODV incurs more routing overhead as compared to AODV. The routing load increases with increasing number of nodes in the network. The routing load is .6364 under AODV for 20 nodes environment and 3.3314 under MAS-AODV. This can be a drawback in case where cost matters more than security and performance.

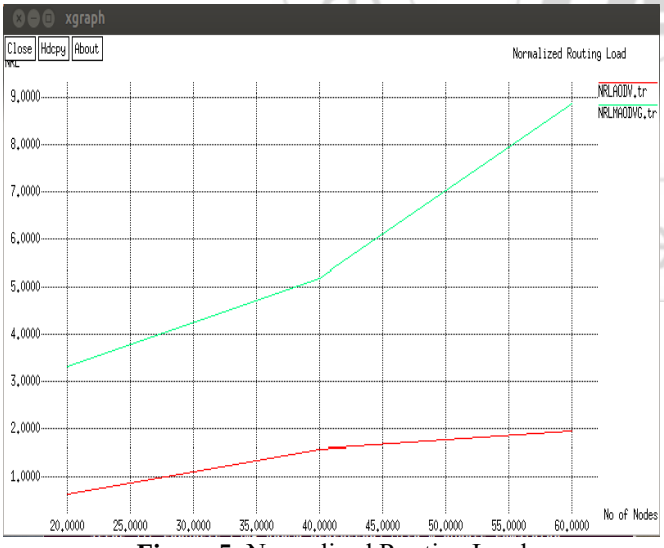

Figure 5: Normalized Routing Load

Next we analyze end to end delay, the results for which are shown in figure 4 with the help of graph. Due to the load of the extra routing information under MAS-AODV, the E2E delay is more for less number of nodes in the network as compared to AODV. But as the number of nodes increases, the E2E delay decreases bringing it lower than AODV for number of nodes higher than 55. Thus we can see that for a network with less number of nodes, the E2E delay of the nodes is higher than AODV but for a network with nodes higher than 55, the E2E delay decreases for MAS-AODV as compared to AODV.

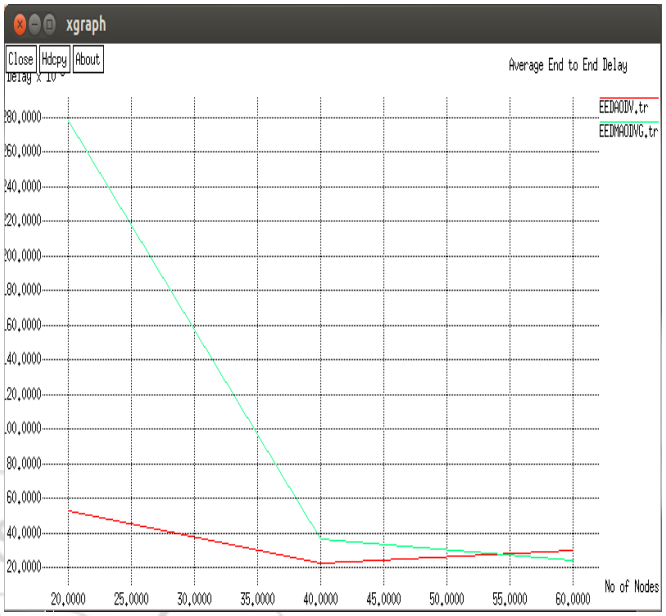

Figure 6: End to End Delay

5. Conclusion

In the paper we have presented an AODV based routing algorithm to make the network more secure against gray hole attacks. In gray hole attack, the attacker selectively drops data packets and is difficult to detect due to its nature of selective dropping using which the attacker can conceal its existence in the network. MAS-AODV identifies the suspected nodes with the help of speed of movement of nodes and apart from this digital signature is used to verify each and every node that takes part in the path formation for data transmission from source to the destination. We have also seen simulation results which help in analyze the performance of MAS-AODV. The simulation results realize that MAS-AODV performs better in case of packet delivery ratio and throughput at the cost of extra routing load. The end to end delay for MAS-AODV is also more when there are less number of nodes in the network, but when the number of nodes increases more than 55, the end to end delay decreases as compared to AODV. So the trade-off is between performance and cost.

References

[1] Zaiba Ishrat, “Security issues, challenges & solution in MANET”, IJCST Vol. 2, Issue 4, Oct. - Dec. 2011
[2] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani Loay , “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008
[3] Siddharth Gupte, Mukesh Singhal, Secure routing in mobile wireless ad hoc networks, science@direct, 2003
[4] D.B. Johnson and D.A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, vol. 353. Kluwer Academic, 1996.

[5] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. Workshop Mobile Computing Systems and Applications (WMCSA '99), Feb. 1999.
[6] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. MobiCom, pp. 85-97, 1998.
[7] Snehal P. Dongare, Ram S. Mangrulkar, "Implementing Energy Efficient Technique for Defense against Gray-Hole and Black-Hole Attacks in Wireless Sensor Networks", IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015
[8] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", IEEE ICICS, 2007.
[9] A. A. Chavan , Prof. D. S. Kurule, Prof. P. U. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", ScienceDirect, 2016
[10] Israat Tanzeena Haque, "On the Overheads of Ad Hoc Routing Schemes", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 2, JUNE 2015.
[11] Eitan Altman, Tania Jimenez, "NS Simulator for Beginners", Sophia-Antipolis, France, December 4, 2003
[12] Paul Meeneghan and Declan Delaney, "An Introduction to NS, Nam and OTcl scripting", National University of Ireland, Maynooth, Department of Computer Science Technical Report Series, 2004-05.

Author Profile

Namrata Jain received the degree of B.E in Information Technology Engineering Branch from Government Engineering College, Jagdalpur (C.G) in 2011 and is presently persuing her M.Tech in Computer Science and Engineering Branch form Raipur Institute Of Technology, Raipur(C.G).Meanwhile she has rendered her service as a lecturer in GEC Jagdalpur. Her areas of intrest include Networking, mainly Ad-Hoc Networks and also programming.

Yogesh Rathore received the degree of B.E and M.Tech in Computer Science and Engineering Branch form Raipur Institute of Technology, Raipur (C.G) in the year 2005 and 2010 respectively. Presently he is working as an Assistant Professor in Computer Science and Engineering Branch in Raipur Institute of Technology, Raipur and has already provided 10 years of dedicated service there in this field since 2006. His areas of intrest are Image Processing, Video Processing and Networking