International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Secure AOMDV Protocol in MANET

Kanika Kamboj[1], Er. Vandana Singla[2]
[1]Student, Haryana Engineering College, Haryana, India
[2]Assistant Professor, Haryana Engineering College, Haryana, India

Abstract—

The crucial problem in the MANET is malicious nodes. When data is transmitted among nodes it may reach to the destination node with response time less than the threshold value. Such types of nodes are known as black hole nodes. In this paper, we try to analyze the problem issue, detect and remove the types of malicious nodes. This paper also proposes the Security Enhancement of AOMDV routing protocol, to detect as well as avoid the malicious nodes using the multipath route distance vector. The detection & Avoidance of malicious nodes during route discovery is carried out with a performance evaluation in the experimental results of proposed algorithm, Packets sent & received and Throughput.

Keywords—Blackholes, AOMDV, MANET, Ad-hoc

I. INTRODUCTION

A mobile Ad-hoc network (MANET) is a cluster of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks. Stands for "Mobile Ad-Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad-Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

The term MANET (Mobile Adhoc Network)refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time , without using any kind of fixed wired infrastructure. MANET are actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration.

In the popular field of MANET several previous works inspire me to work in this field, like the well known multi-cast protocols like ODMRP, SSSPST is a multi-cast protocol which maintains a multi-cast tree pro actively. We believe previous studies and researches improves the MANET working to a great extend but some of the previous researches can be slightly modified to gain better and fruitful results as compared to the previous studies. We have study previous defined AOMDV protocol which depicts the concept of avoidance of Black/Gray holes on the network. We have introduced a new concept of RIP (Restricted IPs) concept in our proposed work, taking previous AOMDV concept as base to the newly proposed work along with the older Black/Gray holes avoidance approach. This newly proposed work combining the older and new approach will be beneficial in avoiding the malicious nodes that affects the traffic on the network by imposing packet replay attack.

Because of such application there is requirement to improve MANET. But there is problem with MANET malicious node so there is the requirement to improve the performance of MANETs.

The above chapter discusses about the overview about the field of MANET. In this paper we shall perform the detection and avoidance of malicious attacks like Blackholes in MANET for a Secure AOMDV Protocol.

II. RELATED WORK

Many scholars and researchers studied a lot on MANET, different researchers' do different works using variety of simulators and code to support their proposed studies. Some does implements cross checks on the hoping of the IP packets while their journey. Some presented various new algorithms to avoid black/gray malicious nodes that decrease the network by slowing the network traffic by misguiding the packet to different flaw routes. Here is the review about the various works done in MANET field by various researchers of their field.

[1] Deng et. al. has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to their algorithm, any node on receiving a RREP packet, cross checks with the next hop on the route to the

destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other.

[2] S.Ramaswamy et. al. presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks .Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

[3] S.Banerjee et. al. has proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. Flow of traffic is monitored by the neighbours of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving, when in fact it is not.

[4] Neetika Bhardwaj, surveyed that Mobile Ad-hoc Networks are formed of several mobile devices which communicate over a shared wireless medium. Due to distributed, infrastructure-less nature and lack of centralized authority of MANETs, the Ad-hoc networks are vulnerable to various kinds of attacks. Because of the vast applications of MANET in fields of emergency networks, Secure Routing Protocols are a must for exploiting the functionality of it. Blackhole Attack is one of the most severe attacks because the attacker embeds itself into the route from source to destination by sending false RREP messages giving an impression that it has the freshest route to destination. Seeing its severity many researchers have addressed the problem of detecting and defending against Blackhole attack but the solutions presented so far suffered from one problem or the other. Also the false detection ratio of the approach is negligible

The above mentioned works that different researchers did is their immense contribution in the concept of MANET. Different researchers do work on different aspects in order to obtain the optimum benefit out of it and work to obtain the efficiency of the Ad-hoc networks by using support of different simulators such as NS2, Packet Tracer etc.

III. RESULTS AND DISCUSSION

We have taken total of 4 & 8 nodes in our simulation evaluation process as shown in the Figure 1 to Figure 2. In the figures it is being observed that in the starting of simulation process one every node is working in cooperation with each other to keep the network in communication but as we proceed further there are situations in between where we have emergence of malicious node and the network resulted into the packet loss later on in the simulation process. The second simulation has one malicious node that carries out the Black Hole Attack.

In our study, we try to compare the results of these two simulations to comprehend the network and node behaviors. We first try to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. We try to evaluate how many of the packets which could not reach the destination nodes are absorbed in the Black Hole Node.

We noticed that the percentage of data loss of the Black Hole AOMDV is increased more than the normal SAOMDV network simulations in all situations. We also understand that the packet loss already exists in the network. This is because packets drop at the node interface queue due to the density of the data traffic.

To minimize the data traffic, we alter node and packet parameters. Needing to evaluate the Black Hole effect in the network, we have to minimize the packet loss which happens at the network, except the Black Hole. In a wireless ad-hoc network which does not have any Black Hole, the data traffic might be dense and packets might get lost, for instance in a FTP traffic. Therefore, the data loss does not always say there was a Black Hole Node in the network. Performance evaluation metrics are:

1. Packets Sent & Received - Packets sent & received refers to the total packets transmitted by the CBR source to the total packets received by CBR sink at the corresponding destination nodes as compared with the existing AOMDV.

2. **Throughput**- Throughput refers to the total number of packets sent over one seconds time.

We discuss the scenarios, by varying the number of nodes to 4 & 8. In the first scenario where there is not a Black Hole AOMDV Node, connection between some nodes being simulated is correctly flawed when we look at the animation of the simulation, using NAM. The output can be analyzed by observing the screenshots of the NS2 network simulator.

Scenario 1:When number of nodes = 4

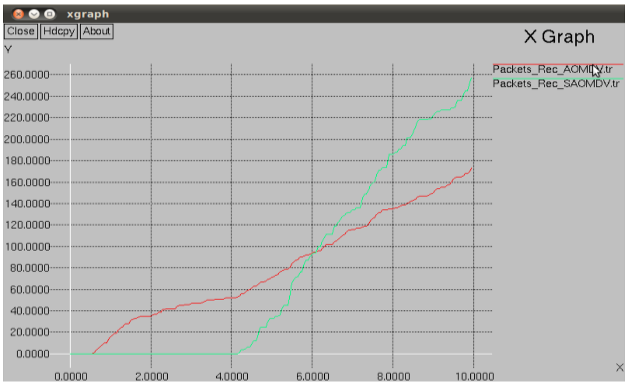

Fig.1 Representing Packets received in AOMDV & SAOMDV

Scenario 2: When number of nodes = 8

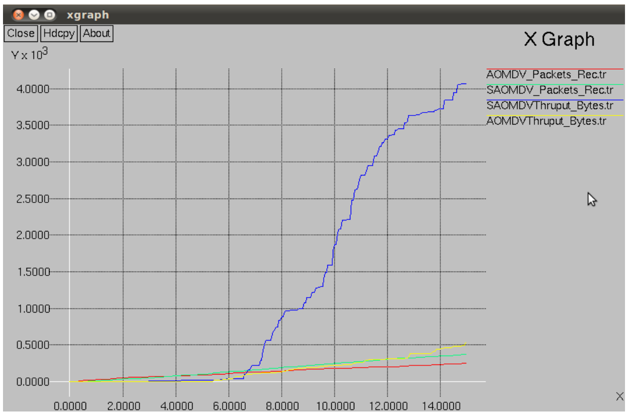

Fig.2 Representing Packets Received & Throughput in AOMDV & SAOMDV.

The output can be analyzed by observing the screenshots of the NS2 network simulator:

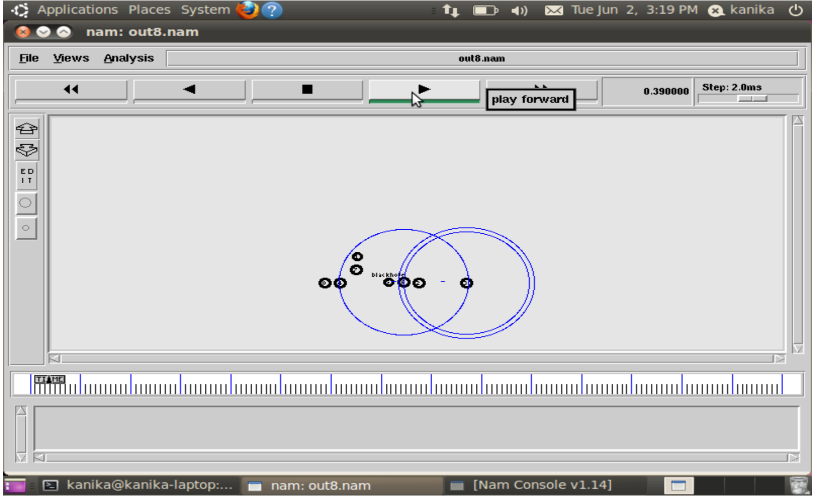

Fig.4 Nam output for one second

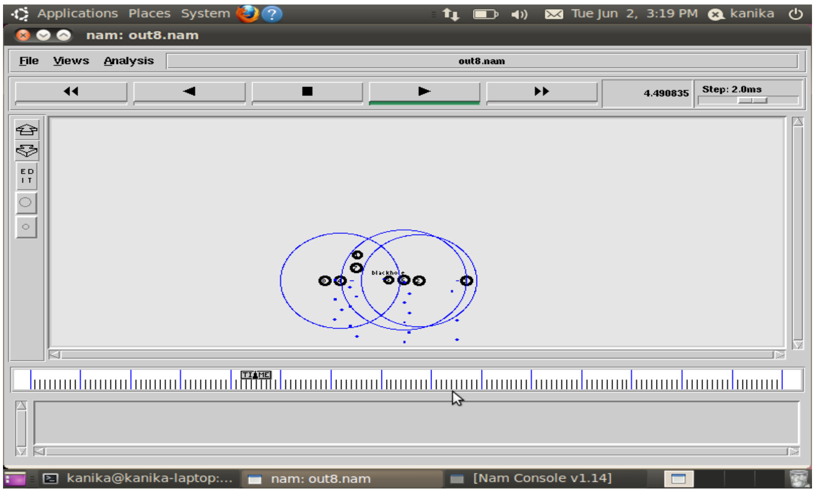

Fig.4 Nam output for 5.2 seconds

IV. CONCLUSIONS

Various malicious attacks hamper AOMDV. Black hole and gray holes attacks are the most important security issues in MANET. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. In proposed work focuses on detecting black and gray holes attacks, pointed out their advantages and disadvantages and at the end. Protection against both attacks in one detection system and decreasing number of errors is the main motive.

We have observed that the Black Hole affects the AOMDV protocol, also affects on packet loss is much lower as compared to effect on delay. As malicious node is the main security threat that effect the performance of the AOMDV routing protocol & their detection is the main matter of concern. In future this proposal is guided towards lessen the effect of Black Hole.

Ergo, it can be concluded that Multipath algorithm gives an alternative route by avoiding the malicious nodes in NS-2.

REFERENCES

[1] “Security Issues in Mobile Ad Hoc Networks- A Survey” Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.

[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, ”Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.Vijay Kumar, Rahul Gupta, “Change Detection on SAR data using PCA Algorithm”, International Journal of Computers and Technology, Vol.4, No.2(Mar-Apr 2013).

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.

[4] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AOMDV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.

[5] Sukla Banerjee “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks” Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[6] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[7] Wu B, Chen J, Wu J, Cardei M (2007) A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao Y, Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York.

[8] Raja Mahmood RA, Khan AI (2007) A Survey on Detecting Black Hole Attack in AOMDV-based Mobile Ad Hoc Networks. Paper presented at the International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007.

[9] Jain, S., Jain, M., and Kandwal H. 2010. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Computer Applications, Vol. 1, No. 7, 37-42.

[10] Neetika Bhardwaj, (2014) Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs, May 2014.