ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SIMPLE APPROACH TO DEFEND BLACKHOLE ATTACK IN MANETS

Biswaraj Sen [*], Kalpana Sharma, Mrinal Kanti Ghose
[*] Computer Science & Engineering Department, Sikkim Manipal University, India

DOI: 10.5281/zenodo.46527

ABSTRACT

The interest in the field of Mobile Ad hoc Network (MANET) is growing since last few years because of its practical applications in mobile devices. MANET is particularly vulnerable to security attacks in comparison to wired network or infrastructure-based wireless network due to its fundamental characteristics such as the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring and management. In order to provide secure and good communication and transmission, researchers have worked specifically on the security issues in MANETs and many secure routing protocols and security measures were proposed. The black hole attack is one of the most prominent security threats which disrupt the routing in Mobile Networks. The scope of this work is to understand the effects of Black hole attack in MANET and devise a strategy to mitigate the attack for Ad-Hoc on Demand Distance Vector (AODV) Routing Protocol in MANETs.

KEYWORDS: MANET, Blackhole, AODV

INTRODUCTION

A mobile Ad-hoc network (MANET) is one of the recent active fields and has received spectacular attention because of their self-configuration and self-maintenance. The functioning of Ad hoc networks is based on mutual trust and cooperation between the nodes of the ad hoc networks thus in these networks besides acting as a host, each mobile node also acts a router and forward packets to the correct node in the network once a route is established.

Though MANETs are easily deployed networks, they often suffer from security attacks because of their features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism to counter threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also make the MANETs more susceptible to attacks, which makes it easier for the attacker to go inside the network and get access to the ongoing information. Mobile nodes present within the range of wireless link can overhear and even participate in the network. The proposed work will analyze the effect of black hole on single and multiple malicious nodes in a MANET based on various parameters. A mechanism has been deployed to identify the malicious nodes and then a combined result showing the behavior of AODV in different changing scenarios has been presented. At the same time, a point where the whole network drops would be found. The proposed work will also try to find a defense mechanism for the black hole nodes so that the black hole nodes are avoided and the black hole attack against the network is stopped.

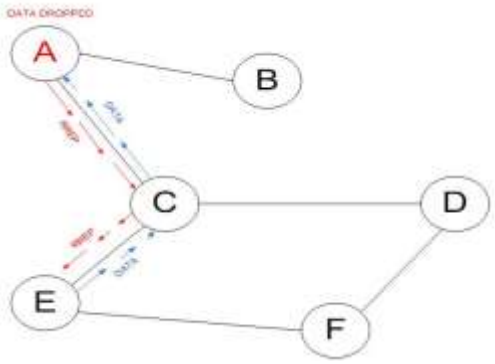
BLACKHOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh

routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [4]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [5]. The method how malicious node fits in the data routes varies.

Fig. 1 shows how black hole attack happens in AODV. The black hole node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

Fig 1: Blackhole attack in AODV



METHODOLOGY

The approach to understand the effect of Blackhole attack in AODV has been implemented by using Network Simulator2 (NS2) simulator tool which is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks**.** Using NS-2, initially we will simulate the AODV protocol without any malicious nodes so that we will be able to compare its results with results of our defense mechanism as well as to find the maximum destination no possible in the network. The next step is to simulate AODV protocol that will have black hole nodes in the network. The presence of black hole nodes will vary from 5%, 10% 20%, 30%, 40% and finally 50%. We will try to find the percentage of black hole nodes for which the network will have zero throughputs. This will give us the breaking point of the network for black hole attacks.

Then we will simulate the AODV protocol with our defense mechanism for which we have thought of identifying the black hole nodes by checking the destination sequence number of the RREP packet. In a black hole attack, the malicious nodes have a characteristic that while false advertising it sends a very high destination sequence number in its RREP packet and with the minimum hop count possible, this tricks the source node to select the route that includes the black hole node. So by identifying the packets with a high destination sequence number we will be able to drop the RREP packets of the black hole nodes in the intermediate nodes itself. This would prevent a source node from ever choosing a path containing the malicious nodes

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

SIMULATION ENVIRONMENT

Table 1: Simulation parameters

Parameters	Valus
No of nodes	25, 50, 100
Traffic Type	Constant Bit Rate
Map Size	1000 X 1000 meters
Transmission range	250 meters
Simulation Time	200 ms
Pause time	0,2,4,6,8,10 ms
Mobility model	Random waypoint
No of connections	1

PERFORMANCE METRICS

Throughput: This is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source, both at the application layer. Packets that are sent but not received are lost in the network due to malicious drops, route failures, congestion and wireless channel loss.

End to End Delay: Packet end to end delay in case of black hole depends on the protocol routing procedure and number of nodes involved during a black hole attack there is no need of RREQs and RREPs because the malicious nodes ds its already sends its RREPs to the sender node before the destination nodes reply.

RESULTS AND DISCUSSIONS

Results have been obtained by using NS2 simulator and analyzing the trace files. Throughput and End-to-End delay were calculated by using AWK scripts. The following graphs depicts the results from various simulations.

Fig 2.1: Throughput at 2m/s node speed

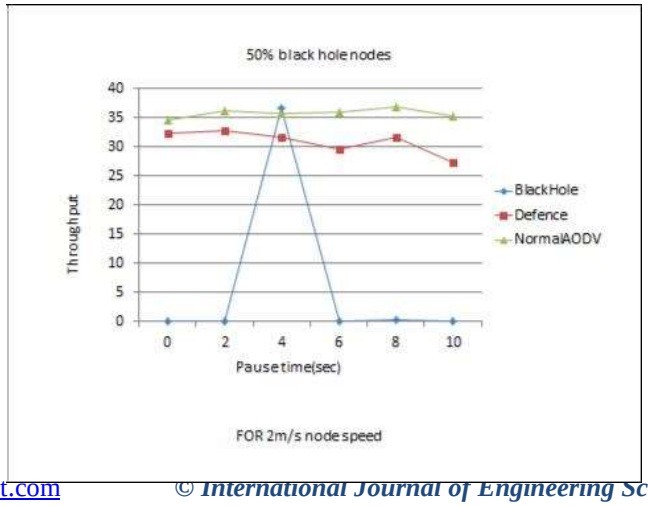
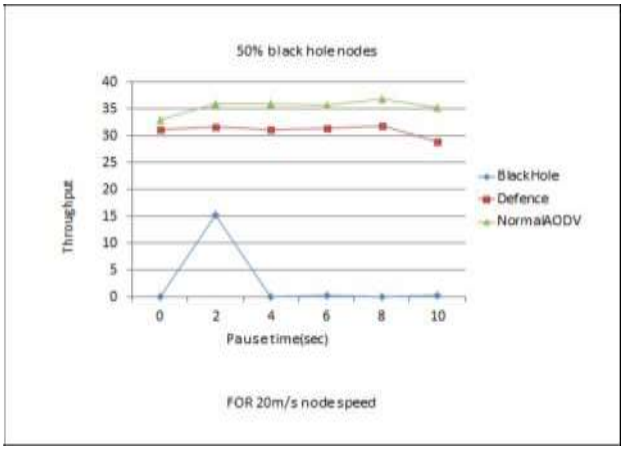


Fig 2.2: Throughput at 20m/s node speed



From Graph 2.1 and Graph 2.2 we found that the throughput of the normal AODV and our defense mechanism is almost same which indicates that the malicious nodes are successfully avoided, and our defense mechanism is successful.

Fig 2.3: End to end delay at 2m/s node speed

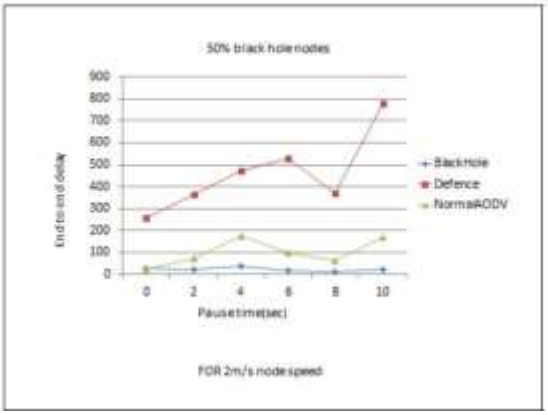
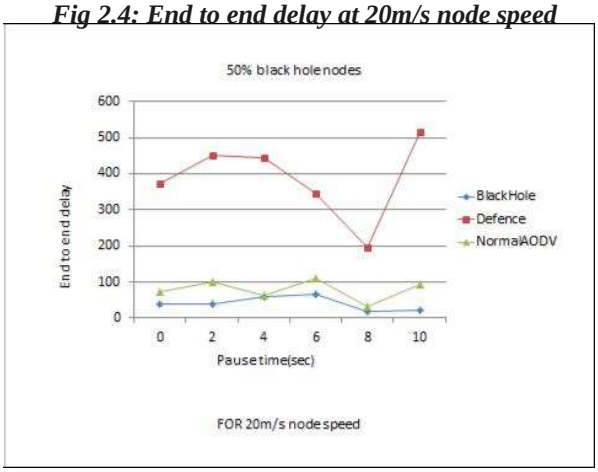


Fig 2.4: End to end delay at 20m/s node speed



ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

Analyzing the graph 2.3 and 2.4 for end to end delay vs. pause time for normal AODV, black hole AODV and defense mechanism we see that the end to end delay for black hole attacks are low as they do false advertising. The end to end delay for our Defense mechanism is very high as the black hole reply packets are dropped and new path found out ignoring the black hole nodes.

Fig 2.5: Throughput for defense mechanism

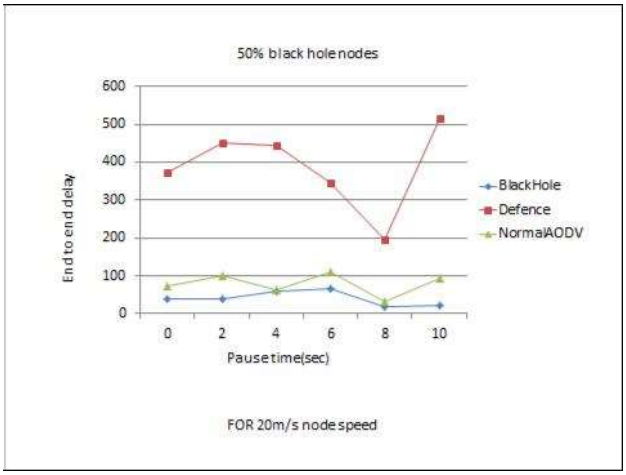
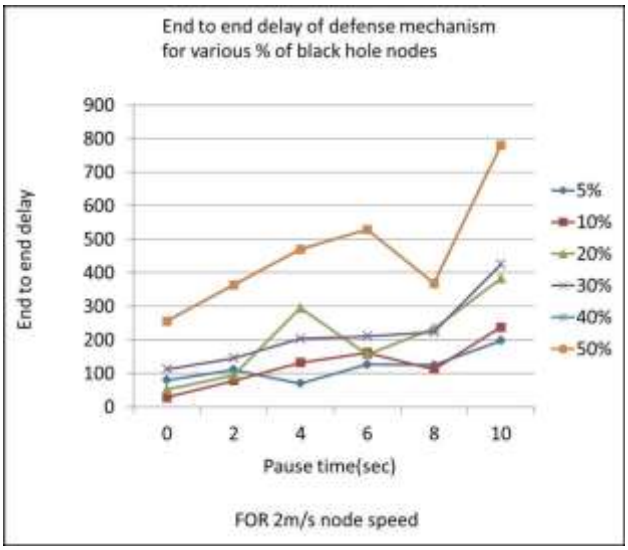


Fig 2.6: End to end delay for defense mechanism



We can see from the graph that as the percentage of black hole nodes in the network increases even in the defense mechanism the throughput of the network decreases. But the decrease in the throughput is very less as compared to the percentage increase in the no of Black hole nodes. We can see from the graph that when we increase the percentage of black hole nodes in the system the end to end delay of the system increases drastically and this increases in accordance with the increase in the pause time.

CONCLUSION

This work aims to develop a defense mechanism to successfully detect and avoid black hole attacks and compare the performance of AODV by varying the number of black hole nodes under different parameters along with the defense mechanism. The simulation results show that the throughput of the defense mechanism is almost at par with the throughput of the Normal AODV. However, this defence technique result in a higher end to end delay. Also it was observed that as long as the percentage of black hole nodes is less than 30% the network throughput never falls to zero whereas the upper limit of black hole nodes required to bring down the complete network is 50% and the average was approximately 40%. Another prominent outcome of this work is - the more stable the network, higher will be the end to end delay.

REFERENCES

1. Biswaraj Sen, Achute Sharma, Varsha Mintri, Kalpana Sharma, M.K Ghose, "Impact of Varying Node Density and Pause Time in AODV", SSRG International Journal of Computer Science and Engineering(SSRG-IJCSE)- volume 1, issue 6, August 2014.
2. Monika Roopak et al., "Performance Analysis of AODV protocol under Black Hole Attack", International Journal of Scientific & Engineering Research Volume 2, Issue 8, August-2011.
3. Mehdi Medadian, Mohammad Hossein Yektaie, Amir Masoud Rahmani, "Combat with Black-hole Attack in AODV routing protocol in MANET", Communications (MICC), 2009 IEEE 9th Malaysia International Conference, page no:-530-535, 15th -17th December, 2009.
4. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 200
5. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006
6. Al-Shurman M, Yoo S-M, Park S, "Black Hole Attack in Mobile Ad Hoc Networks", 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.
7. Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.