Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.324 – 330

RESEARCH ARTICLE

Impact of AODV under Black Hole and Flooding Attack

Sunanda Puri, Mr. Harish Saini
M.Tech Scholar & GNI, Mullana, India
Associate Professor, Department of CSE & GNI, Mullana, India
sunandapuri83@gmail.com; harishsaini@gni.edu.in

Abstract—Mobile Ad Hoc Networks (MANETs) is a collection of wireless mobile nodes connected by wireless links forming a temporary network without the aid of any infrastructure or any centralized administration. Owing to its mobility and broadcast nature MANETs are particularly vulnerable to attacks over traditional wired networks finally makes them susceptible to various active and passive attacks. In particular, black hole attacks and flooding attacks can be easily deployed into the MANETs by the adversary. In the black hole attack, a malicious node falsely replies to the route request that comes from a source node showing it has enough routes to your destination even it does not have any route to the destination. In this way, the malicious node can drop, delay and modify the packets from the source node. On the other hand the attacker nodes in case of flooding attacks generate the false route requests after a very short interval of time thus flooding the network with false route request packets. Our objective is to thoroughly capture and analyse the impact of Black Hole attacks and flooding attacks on MANET performance using reactive (Ad hoc On-Demand Distance Vector-AODV) routing protocol with varying number of Black Hole nodes in the MANET. We have used Performance Metrics i.e. Throughput, Packet delivery Ratio and end to end delay to analyse the impact of both attacks on AODV Routing Protocol in MANET using the network simulator NS-2 simulator

Keywords— MANET, NS, AODV, FLOODING, BLACKHOLE

I. INTRODUCTION

Mobile Adhoc networks (MANETs)[1] are usually formed by a group of mobile nodes interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. If a node claims, it has path to a certain node, the claim is trusted; similarly, if a node reports a broken link, the link will no longer be used. They can form arbitrary topologies depending on their connectivity with each other in the network. The nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. 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 makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

Security in MANETs is the most important concern for the functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs suffer from security attacks because of its features like open medium, dynamically changing topology,

no central monitoring and management, cooperative algorithms and no defence mechanism. This assumption introduces vulnerability to several types of denial of service (DoS) attacks [5], particularly packet dropping attack. Adversary can easily join the network and drop routing packets passing through it that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes.

II. SECURITY ISSUE IN MANET

2.1 Wireless Medium

Wireless medium is free to access by everyone and it's prone to bit errors or interfacing problem.

2.2 Lack of Centralized Management

There is no central authority to monitor the traffic in a highly dynamic and large scale ad-hoc network and that makes the detection of attacks difficult.

2.3 Resource Availability

An attacker can easily become an important routing agent and disrupt the network operation by disobeying the protocol specifications as a Mobile Adhoc network is based on cooperative environments.

2.4 Infrastructure Less

There are no specific infrastructures for addressing, key distribution, certificates etc.

2.5 Scalability: The protocols and services that are applied to the adhoc network should be compatible to the continuously changing scale of the adhoc network.

2.6 Dynamic topology

Dynamic topology may violate the trust relationship among the nodes.

2.7 Restricted power supply

Node in mobile ad-hoc network can behave in a selfish manner when there is consumption of battery to support some functions in the network.

2.8 Bandwidth constraint

Cooperation based security solutions must consider the bandwidth limitation associated with links.

2.9 Multi hop Routing

As the nodes are dependent on each other for routing, adversaries can generate fabricated routes to create routing loops, false routes etc.

III.SECURITY ATTACKS IN MANET

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behaviour of the attack i.e. Passive or Active attack.

3.1 Internal attacks

These types of attacks have a direct impact on the nodes that are working in a network. Internal attacks may broadcast wrong type of information to other nodes. These types of attacks are more difficult to be handled as compared to external attacks as internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes.

3.2 External attacks

External attacks are carried out by nodes that do not belong to the domain of the network. Unlike internal attacks external attacks are mainly due to the nodes outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations.

3.3 Black Hole Attack in MANET'S

Black hole attack is a kind of Denial of Service (DoS) attacks in MANET. In this attack, a malicious node waits the Route Request message (RREQ) from the neighbour nodes. When it receives the RREQ message, it sends immediately a false RREP with high sequence number to the source node. The source node assumes that the route is fresh route. However, when the source node sends the data packet to the destination node by using this route, the malicious node does not relay the packet and absorbs all data packet. This is called as black hole attack. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack.

3.4 Flooding Attack in MANET'S

Flooding attack is a attack which is present at the network layer by the malicious/attacker node. This attack is based on DOS in which the attacker node broadcast the false packet in the network. The main aims of attacker node to consume the available resources like bandwidth, battery power etc. so that legitimated user are not able to use these network resources for valid communication. Flooding attack is easy to implement but it can cause severe damages. The flooding attack can be differentiating it into two categories Data flooding or RREQ flooding. In RREQ flooding the attacker nodes floods the RREQ in the complete network that takes a lot of resources of the network . In data flooding the attacker nodes makes a paths between all the nodes in the whole network .The attacker nodes sends a unlimited amount of useless and unnecessary data packets into the network once they established a path which is directed to all the other nodes in the network. These unlimited & unwanted data packets in the network and it cause to congest the whole network. Any node at that time to serves as destination node will be busy all the time by receiving useless, false , unnecessary and unwanted data packets in the network at all the time**.**

IV.MATERIAL & METHODS

Our work is to analyze the impact of Black hole attack and Flooding Attack in AODV routing protocol based on throughput, packet delivery ratio and end to end delay. We analyzed the Black Hole attack and flooding attack with different scenarios of the network by varying the number of Black hole nodes and the flooding nodes by keeping the total number of nodes fixed to analyze the performance of the network with AODV routing protocol without attack and under the attack.

4.1 Parameters

4.1.1 Throughput

The average rate at which the total number of data packet is delivered successfully from one node to another over a communication network is known as throughput. The result is found as per KB/Sec. It is calculated by
Throughput= (number of delivered packet * packet size) / total duration of simulation.

4.1.2 Packet delivery Ratio

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

4.1.3 End-to-End delay

It refers to the time taken for a packet to be transmitted across a network from source to destination. This metric includes all possible delay that may be caused by buffering during route discovery, queuing at the interface queue, retransmission delay at the MAC layer, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination. The simulation work is done by using the NS-2 simulator.

4.2 Network Simulator (NS-2)

Network simulator (NS-2) is an open source, discrete event simulation tool. It provides support for simulation of routing, multicast protocols and IP protocols over wired, wireless and satellite networks. It can generate graphical details of network traffic through the NAM. It is written in the C++ programming language with the Object Tool Common Language (OTcl) as the front-end interpreter. For this dissertation NS-2(version NS-2.33) was chosen as a network simulator.

4.2.1 NS-2 Structure

To simulate the network, user has to program with OTcl script language to initiate an event scheduler and set up the network topology using the network objects and tell traffic sources when to start and stop transmitting packets through the event scheduler. OTcl script is executed by NS-2.

4.2.2 NAM

The Network Animator NAM is a graphic tool used with NS-2. It requires a nam-trace file recorded during the simulation and will then show a visual representation of the simulation.

4.2.3 Agents

Agents are defined as the endpoints where packets are created and consumed. The agents are all connected to their parent class, simply named Agent. This is where their general behavior is set and the offspring classes are based on some alterations to the inherent functions in the parent class. The modified functions will overwrite the old and thereby change the performance in order to simulate the desired protocol.

4.2.4 X-Graph

One part of the NS-allinone package is 'xgraph', a plotting program which can be used to create graphic representations of simulation results.

4.3 Performance Analysis

To investigate the effects of blackhole and flooding attack in AODV routing protocol, we have simulated the scenarios of MANET with and without black hole nodes and the flooding nodes.

To test the protocol, we used simulations of a network with 20 nodes with and without the black hole attack and the flooding attack. We have conducted four scenarios of the network with AODV routing protocol by increasing the numbers of black hole nodes and the attacker nodes for flooding node firstly two then four and finally six. We then compared the results of these simulations under various scenarios.

Simulator	**NS-2 (ver. 2.33)**
Simulation Time	500(s)
Number of Mobile Nodes	20
Mobility Model	Random Waypoint Model
Black hole / Flooding Node	0,2,4,6
Topology	750m x750m
Transmission Range	250m
Routing Protocols	AODV
Traffic	Constant Bit Rate(CBR)
Pause Time	2(s)
Packet Size	512 bytes
Data Rates	10 Kbits

Table: 4.1 Simulation Setup

V. RESULTS & DISCUSSIONS

We compared the results of these simulations to understand the network and node behaviours. The results of the simulation show that the packet loss in the network increases with increase in number of attacker nodes. This is due to increased congestion in the routes towards the attacker nodes. Mobile Ad hoc networks may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the variation of data loss due to network parameters such as the distribution of the nodes changed.

5.1 Throughput

The average rate at which the total number of data packet is delivered successfully from one node to another over a communication network is known as throughput. The result is found as per KB/Sec.
It is calculated by Throughput= (number of delivered packet * packet size) / total duration of simulation
It is obvious that the throughput for AODV is some time high and sometimes low. The malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.
The results of the simulation show that the throughput in the network with a Blackhole node decreases by increasing the number of blackhole nodes in the network. In the case of flooding attack the throughput also decreases with the increase in the flooder node. But the impact of the Blackhole attack is more severe than flooding attack. The performance of the network degrades much higher in presence of the blackhole attack as compared to flooding attack. It is obvious that the throughput for the case with AODV, without attack, is higher than the throughput of AODV under attack as also shown in figure 3.8. The throughput keeps on decreasing as the numbers of malicious nodes/ flooding nodes are increased in the network keeping the total number of nodes constant in each scenario. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination and the flooding nodes consume the bandwidth, thus effecting throughput. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet

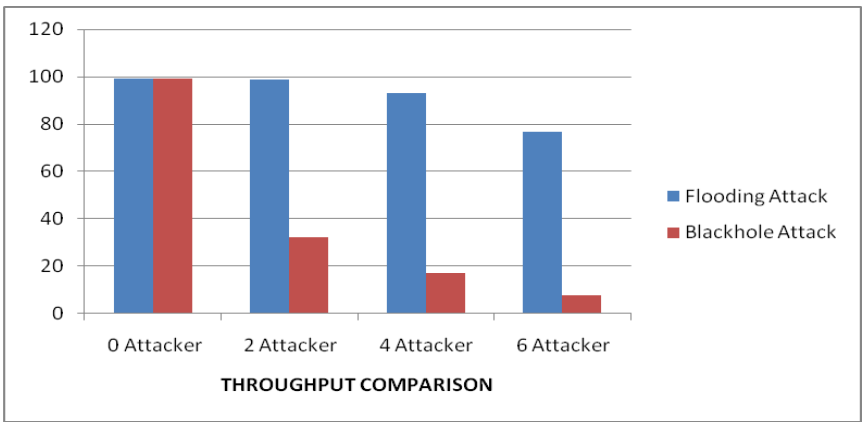

Fig-5.1.Throughput for AODV Protocol with Black Hole Node/Flooding Node.

5.2 Packet delivery Ratio (PDR)

The results of the simulation show that the number of packets successfully delivered in the network with a Black hole node/Flooding node decreases by increasing the number of attacker nodes in the network. This is due to increase in the probability that more number of packets that pass through the black hole node increases with increase in the number of the black hole node. The malicious node discards the data rather than forwarding it to the destination. In the presence of more flooding attacker nodes the congestion in the network is increased. As such nodes are increased in the network more and more packets are discarded thus affecting the delivery ratio of the network.

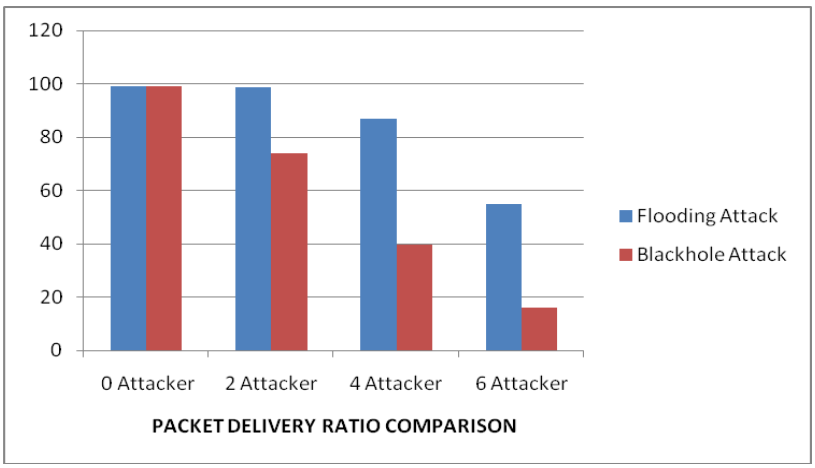

Fig-5.2.Packet Delivery Ratio for AODV Protocol with Black Hole Node/Flooding Node

5.3 End to End Delay (E2E delay)

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. This metric includes all possible delay that may be caused by buffering during route discovery, queuing at the interface queue, retransmission delay at the MAC layer, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination.

The results of the simulation show that the end to end delay keeps on increasing as the number of attacker nodes are increased in the network. The attacker nodes present in the network drop the packets and hence a retransmission is required. As such nodes are increased in the network the probability of the packet being getting dropped also increases thus more and more retransmissions are required and thus increasing the overall end to end delay with the increase in attacker nodes.

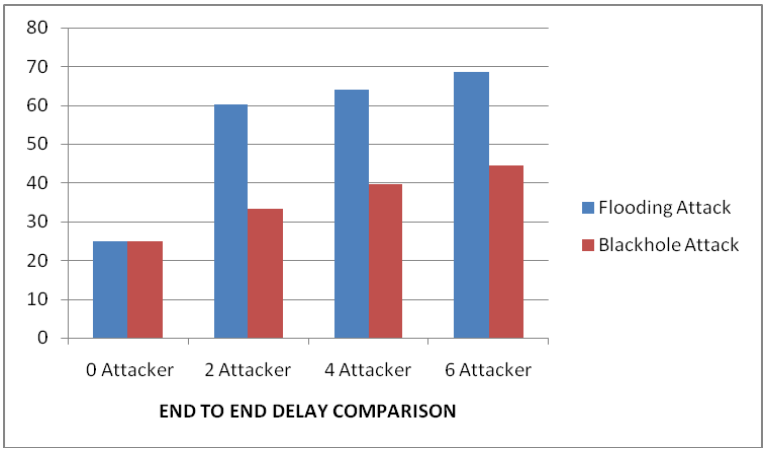

Fig-5.3.End to End Delay for AODV Protocol with Black Hole Node/Flooding Node

VI. CONCLUSION

The future of ad- hoc networks is really appealing, giving the vision of anytime, anywhere and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. We tried to discover and analyze the impact of Black Hole attack and the flooding attack in MANETs using AODV routing protocol by generating the traffic using the CBR, the same needs to be tested for the other ways of generating traffic i.e. exponential or the Poisson. There is a need to analyze Black Hole attack and the flooding attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of one attack, it cannot be applicable in case of other attacks. The detection of the Black Hole attack and the flooding attack as well as the elimination strategy for such behaviour has to be carried out for further research.

REFERENCES

[1] Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang 2011 “Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges” publish in IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011

[2] www.wikipedia.org

[3] Harjeet Kaur , Manju Bala , Varsha Sahni “Study of Blackhole Attack Using Different Routing Protocols in MANET” published in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013

[4] Bala, Anu, Munish Bansal, and Jagpreet Singh. "Performance analysis of MANET under blackhole attack." Networks and Communications, 2009. NETCOM'09. First International Conference on. IEEE, 2009

[5] X. Wu and D. K. Y. Yau, "Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach", *In Proc.* 3*rd International Conference on Security and Privacy in Communications Networks*, Nice, France, September 2007.
[6] Monika Roopak, Prof.BVR Reddy, " Blackhole Attack implementation in AODV Routing Protocol" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 402 ISSN 2229-5518.
[7] Panos C. Lekkas Randall K. Nichols. "Wireless Security - Models, Threats and Solutions" Mc Graw Hill, 2002
[8] Preetee K. Karmore,Gaurishankar L. Girhe " Detection of Blackhole Attack on AODV based Mobile Ad hoc Networks using K-means Clustering Technique of Data Mining" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905
[9] Bhuvaneshwari. K, Dr.A.Francis Saviour Deva raj," Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation" Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages:1695-1699 (2013)
[10] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava, "Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 7, JULY 2013 ISSN 2277-8616
[11] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma " Performance analysis of AODV, DSR & TORA Routing Protocols" IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010
[12] Preetee K. Karmore,Gaurishankar L. Girhe " Detection of Blackhole Attack on AODV based Mobile Ad hoc Networks using K-means Clustering Technique of Data Mining" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905
[13] http://www.ijstr.org/finalprint/july2013/Simulation-And-Analysis-Of-Performance-Parameters-For-Black-Hole-And-Flooding-Attack-In-Manet-Using-Aodv-Protocol-.pdf
[14] Usha and Bose "COMPARING THE IMPACT OF BLACK HOLE AND GRAY HOLE ATTACKS IN MOBILE ADHOC NETWORKS" Journal of Computer Science 2012, 8 (11), 1788-1802 ISSN 1549-3636
[15] Bhuvaneshwari. K, Dr.A.Francis Saviour Devaraj,"Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation"
[16] Madhavi, S. and K. Duraiswamy, "FLOODING ATTACK AWARE SECURE AODV" Journal of Computer Science, 9 (1): 105-113, 2013

