Research Paper

IMPACT OF MALICIOUS ATTACKS IN MOBILE ADHOC NETWORKS

Shirish Bhosale, Prof Deepak Mehetre

Address for Correspondence

Department of Computer Engineering, K. J. College of Engineering & Management Research

ABSTRACT

Computers, servers, mobile devices communicate with each other through a network infrastructure, irrespective to wired or wireless communication. This communication is done through intermediate networks devices like routers, intermediate network providers, etc. Communication over network layer is done by packets. This packets travels from source to destination through channel, this channel has to be secure. Unsecure channel can lead to malicious activity. Channel of mobile Adhoc networks(MANETs) are more vulnerable to malicious activities than fixed infrastructure networks. One of malicious activity is denial of service. Packet drop attack, black hole attack, gray hole attack are denial of service attack. This paper shows the effects of packet drop attack, black hole attack and gray hole attack on AODV protocol under different performance metrics like throughput, packet drop rate.

KEYWORDS—AODV, Denial of Service, Intermediate Node, MANET, Malicious Node, blackhole Node, Grayhole Attack, Network Simulator, RREQ, RREP.

I. INTRODUCTION

MANETs are multi-hop wireless network. It is dynamically formed amongst groups of mobile users having wireless net-work. It has different characteristics such as lack of centralized administration, distributed cooperation and changing topology. Wireless clients connect directly together without router or access point. MANETs nodes communicate with each other within the radio range through wireless links. There are different researches in MANET such as routing, power management, bandwidth management, radio interface and security issues. A MANET have a large number of potential applications like emergency services, tactical networks, sensor networks, commercial and civilian environments, home and enterprise networking, education, entertainment, context aware servicing and coverage extension.

A. Routings in Ad hoc Networks

If the nodes/devices are within the range of each other, then routing is not necessary as they can directly communicate with each other directly (neighboring nodes are source and destination). If a node (either source or destination) moves out of range, and they are not able to communicate with each other directly (within single hop), intermediate nodes are needed to establish communication between them. The purpose of a routing algorithm is to define a scheme for transferring a packet from one node to another. This algorithm takes decision to choose their next hop for communication based on criteria such as number of hops to communicate to destination, latency, transmission power, bandwidth, etc[10]. Ad hoc routing protocols can be classified as either proactive or reactive, depending on the method used to discover and maintain routes [1].

1) Proactive routing: Proactive routing algorithms are table driven using link state routing in which the algorithm maintains the partially copy of network and cost of communication needed to communicate with nodes in network, basically proactive algorithmic are used where the network topology is known or may not change by enough period of time. They can be optimized. eg Destination Sequenced Distance Vector (DSDV)[1].
2) Reactive routing: Reactive routing algorithms does not maintain any predetermined information of network, this algorithms are runtime in nature. Information are collected only when routes are to establish that is on demand, routes are discovered on when needed. They can be optimized up to certain limit. Proactive is more reliable than reactive. E.g. Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing(DSR) [1].

B. Challenges in Ad hoc Networks

- Due to mobility network topology is dynamic.
- Frequent network partitions and grouping of nodes.
- Routers are moving i.e. Intermediate node are mobile.
- Packet losses due to transmission errors.
- Flooding of Control message increasing routing over-head[10].

C. Issues in Ad hoc Networks

As nodes in ad hoc network are not static in terms of position and basically most of them are battery powered, this creates the power issue. Characteristics of joining and leaving network creates a problem in routing, checking the link are broken or not is one of the overhead due to mobility. Flooding of control message creates the routing overhead[10].

1) Mobility: Mobility depends on speed, pause time. E.g. Ad hoc networks of racing cars, here speed of each node varies. If on the way a car fails, hence that node waits for maintenance for some pause time. Mobility patterns may be different Student sitting in canteen (speed of mobility is less, all are within range). Racing car network (speed is higher; quickly nodes go out of range). Military movements (variable speed , variable range). Personal area network or WiFi ad hoc network of laptops (can be static for some time period).
2) Power: Devices in adhoc network can be laptop, palmtop, generator powered. Most of them battery powered. Wireless transmission, reception, retransmission, consumes power. E.g. Consider a ad hoc network established in forest by military, here there is no resources charging their devices, after certain time period battery may drain.

D. AODV Protocol

AODV is reactive routing protocol routes are created only when they are needed hence AODV discovers the route from source to destination only on demand rather than table driven approach, hence partial network copy is not maintained. It does not make sense to maintain due to mobility. AODV protocol has different processes like route discovery, route table management, route maintenance and local connectivity management. In route discovery process source node communicate to the destination node through intermediate nodes (routing nodes) if there is no direct connection between source and destination [12].

If there is no routing information available in the routing table of source node, route discovery starts by broadcasting route request (RREQ) packet to all the neighboring nodes within range of source node/IN nodes, RREQ goes on propagating through Intermediate nodes until valid path is not found.

Sequence numbers ensure the freshness of routes and guarantee the loop-free routing. Sequence numbers are always incremented. They are incremented only when RREP packets are received and RREQ packets are sent.

The reverse path sets up automatically when RREP packet is sent. Replying node (IN) generates the route reply (RREP) to the source (requesting) node. Source may receive multiple RREP. But the valid and shortest is selected. Forward path is the reverse of reverse path setup.

In path maintenance, continuously hello messages are used to ensure that neighbors links are available. If link is failed, route discovery process restarts and finds the route. In local connectivity management, nodes broadcast the hello messages to its neighbors node for checking its availability. Hello message does not change sequence numbers[12].

E. SECURITY ATTACKS ON ROUTING PROTOCOLS

1) Passive attacks: Attempts to learn or make use of information, they do not affect the system typically involve only eavesdropping of data (just to steal a confidential data).Goal is to obtain information that is being transmitted. It is an unauthorized interception of information. Passive attacks can be of two types Release of message content and traffic analysis[14].
2) Active attacks: They are based on modification of original message or creation of false message. Active attacks are mainly External attacks that are targeted to affect the performance of network. E.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can be prevented by using standard security mechanisms such as firewalls, encryption at hardware level or software level. Internal attacks are passive attacks, it is like Trojans A trusted node can be malicious and may work against network[14].

F. Denial of service

DoS attacks are malicious attacks to deny access to the system, network, application, or information to a user. DoS, unnecessarily uses bandwidth, computational and memory resources, and residual energy. Misdirection of traffic can also be denial of service attacks.eg packet drop, black hole/gray hole attack. Denial of service attacks in which the primary aim is to exploit the routing protocol to force unnecessary consumption of resources, so that other nodes cannot use the network for communication[1].

Such attacks include:

- Injecting routes to false destinations like in black hole attack.
- Flooding attacks involving control packets like RREQ,RRER, RREP.
- False removal of working routes.

1) Black Hole Attack: Black hole attack is kind of DoS attack where black hole node attracts all packets by pretending shortest route to the destination to route requesting node. It drops all attracted packets of source or intermediate nodes. As almost all packets of nodes within its range are attracted and dropped hence it degrades the performance of the network. Black hole node pretends that it has valid and shortest path with less hop count towards destination. Requesting node accepts it as next hop assuming cost of transmission through that node is less. Black hole intentionally attracts all packets so as to degrade performance of network[2].

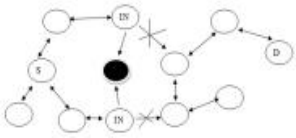

Fig. 1. Black hole pretending Intermediate nodes that it has valid and shortest path.

1) Gray Hole Attack: Gray hole attack is a specialized version of black hole attack, it has all characteristics of black hole attack. But gray hole switch its states from black hole to normal and vice versa any instance of time. Detection of gray hole attack is difficult because it cannot predicted when a node will be switched to normal mode and when in malicious mode[4].
2) Packet Drop Attack: Packet Droppers[1] are the malicious nodes which do not forward the packet(or route the packet through it) they just drop the packets routing through them. Packet drop attack is minor attack compared to black hole and gray hole attack Black hole intentionally attracts the packet towards them and drops them while packet dropping nodes drops only packets passing or trying to route through them. Packet drop attacks intention is not to degrade the overall performance of network but its purpose may be To save energy by not routing other nodes packets. To drop specific packets from specific nodes on specific routes.

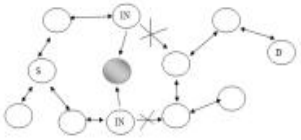

Fig. 2. Gray hole in malicious mode pretending Intermediate nodes that it has valid and shortest path.

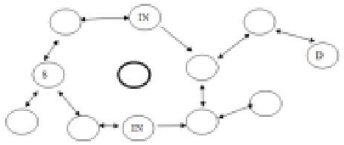

Fig. 3. Gray hole in normal mode, Intermediate nodes selects valid routes.

II. SIMULATIONS RESULTS

Malicious simulations are performed by using network simulator tool NS-2[13]. Routing protocol AODV has been considered for performance evaluation in this work.

A. Network Simulator NS (2.35)

Network simulator is an object oriented simulator. It is written in C++.OTcl is an interpreter as a front end. It supports class hierarchy in C++.The class hierarchy is within OTcl interpreter. The root of the hierarchy is the Tcl object. NS needs two languages such as C++ and OTcl. It is suitable to protocol implementation. It is useful for simulation configuration with the help of OTCL configuration[13].

B. Mobility Model

Movement of nodes is depends on the speed, direction and rate of change. Different mobility models study will help to check the behavior of the network. Mobility models are Random Waypoint Model, Gauss-Markov Model, Reference Point Group Mobility (RPGM) model, and Manhattan Mobility Model. Here we used Random Waypoint Model which first used by Jhonson and Maltz in evaluation of DSR routing protocol. This is a random based mobility model used in mobile management scheme. Mobile node moves randomly in simulated area. This area is in the rectangular. The speed of mobile nodes is uniformly distributed between the minimum speeds to the maximum speed. Pause time is defined as the time in which the nodes are stationary.

C. Traffic Type

Random traffic connections of Constant Bit Rate (CBR) and Transmission Control Protocol (TCP) can be set up between nodes in MANET. This CBR and TCP connections can be used in wireless nodes. For traffic connection generation the requirements are the type of traffic of connection, the number of nodes, and total number of connections between nodes etc.

D. Radio Propagation Model

The radio propagation model is used to predict the received signal power of each packet in MANET. There is receiving threshold at the physical layer of each mobile node. A single line-of-sight path between two mobile nodes is propagation. The two ray ground propagation model considers both direct path and ground reflection path. This model gives accurate prediction at a long distance.

E. Mac 802.11

Medium access control (MAC) 802.11 plays an important role in coordinating channel access among the nodes. MAC achieves maximum channel utilization. The channels in wireless communication are suffering from fading, path loss, and interference. Network topology may change continuously, cause frequent route breakages and again routing activity.

F. Performance Measures Used

- Throughput: It is defined as the amount of data transferred over the period of time expressed in kilobits per second (kbps).
- Packet Drop Rate: It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets.

G. Simulation Parameters

- Simulator - NS-2.35
- Simulated Attack - Packet drop attack, Black hole attack, Gray hole attack
- Channel Type - Wireless
- Antenna Type - Antenna/OminiAntenna
- Radio propagation model - Propagation/Two Ray Ground
- interface queue type - Queue/ Drop Tail / PriQueue
- Mac type - Mac/802 11
- Protocols - AODV
- Simulation time - 100 sec
- Pause time - 10 sec.
- Simulation area - 1500*1500.
- Number of Nodes in network - 60.
- Number of Malicious Nodes - 1 to 8.

H. Results

Figure 4, shows that as the malicious nodes are increased in the network through put goes on decreasing. Throughput is mostly impacted due to black holes than gray holes and packet droppers.

Figure 5, shows packet drop rate increases as numbers of malicious nodes are increased in the simulated network.

TABLE I:THROUGHPUT VS. NUMBER OF MALICIOUS NODES.

No Malicious Nodes	Packet droppers	Black holes	Gray holes
0	30.47	30.47	30.47
1	13.63	31.66	14.66
2	8.44	27.26	14.68
3	6.39	26.85	12.31
4	9.08	24.82	9.19
5	5.96	21.33	9.31
6	7.66	20.35	10.75
7	4.46	21.19	9.51
8	3.97	16.8	9.75

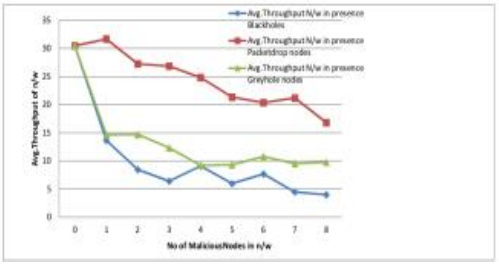

TABLE II: PACKET DROP RATE VS. NUMBER OF MALICIOUS NODES.

No Malicious Nodes	Packet droppers	Black holes	Gray holes
0	68.45	68.45	68.45
1	86.02	67.02	84.73
2	91.34	71.77	84.74
3	93.45	72.34	87.07
4	90.8	74.27	90.56
5	93.91	77.92	90.33
6	92.15	78.95	88.87
7	95.49	78.49	89.99
8	95.98	82.74	89.9

III. CONCLUSION

In this work, the performance of mobile ad-hoc network routing protocol AODV in the presence of black hole attack, packet drop attack and gray hole attack has been evaluated by using NS 2.35. Black hole attack is dangerous than packet drop attack and

gray hole attack. Due to changing state behavior of gray holes, results for gray hole attack is between black hole and packet drop attack. Simulation parameters used in this work is very important for evaluating the performance of networking protocol. As the numbers of malicious nodes increases the performance on the MANET goes down. The Fig. 5. Packet Drop Rate vs. number of malicious nodes. performance metrics used throughput, packet drop rate as the measuring metrics.

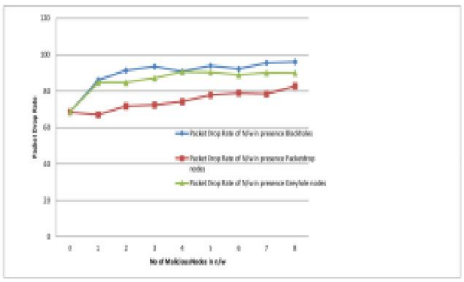

Fig. 5. Packet Drop Rate vs. number of malicious nodes.

ACKNOWLEDGMENT

I wish to thank Prof. D. C. Mehetre (Guide), Prof. M Nighot, Dr. S. J. Wagh who all have been a constant source of inspiration and guidance. I also acknowledge the research work done by all researchers in this Field.

REFERENCES

1. P.W.Yau,S.Hu and C.J.Mitchell, Malicious attacks on ad hoc network routing protocol, International Journal of Computer research ,15 no.1 (2007) 73-100.
2. S.Dokurer,Simulation of black hole attack in wireless ad-hoc networks, Atlm university.
3. Akanksha Saini, Harish Kumar, Comparision Between Various Black Hole Detection Techniques in Manet, NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.
4. Marjan Kuchaki Rafsanjani,Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV based MANET,IJCA Special Issue on Network Security and Cryptography NSC, 2011.
5. Hassen Redwan and Ki-Hyung Kim,Survey of Security Requirements Attacks and Network Integration in Wireless Mesh Networks,2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology.
6. Vesa Krpijoki,Security in Ad Hoc NetworksHelsinki ,University of Technology.
7. Semih Dokurer, Y. M. Erten, Can Erkin Acar,Performance Analysis of Adhoc networks under black hole attack, ATILIM University Ankara, Turkey.
8. Vivek Thaper, Performance analysis of adhoc routing protocols using random waypoint mobility model in wireless sensor networks, International Journal on Computer Science and Engineering (IJCSE).
9. P.Kuppusamy, Scenario Based Performance Evaluation of DSR and AODV Routing Protocols, IJCSET — July 2011 — Vol 1, Issue 6,320-323.
10. Iqbaldeep Kaur, Navneet Kaur, Tanisha, Gurmeen, Deepi, ”Challenges and Issues in Adhoc Network”, International Journal of Computer Science and Technology, Dec 2016 , ISSN : 0976-8491.
11. Carey Nachenberg VP, Fellow, ”A Window Into Mobile Device Security - Examining the security approaches employed in Apple’s iOS and Googles Android”, Symantec White paper.
12. Charles E Perkins , Elizabeth M Royer, ”Adhoc On Demand Distance Vector Routing”.
13. The network simulator-ns 2.35 http://www.isi.edu/nsnam/ns.
14. Hoang Lan Nguyen,Uyen Trang Nguyen, A study of different types of attacks on multicast in mobile ad hoc networks,Proceedings of 2006 IEEE International Conference on Networking (ICN 2006).