Simulation Study of Black Hole and Jellyfish attack on MANET Using NS3

Nidhi Purohit
Information Technology Dept.,L.D. College Of Engineering,Ahmedabad, India

Richa Sinha
Information Technology Dept.,L.D. College Of Engineering,Ahmedabad, India

Hiteishi Diwanji
Information Technology Dept.,L.D. College Of Engineering,Ahmedabad, India

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). The attacks studied in this paper are against the routing protocols in Mobile ad hoc network. We have used AODV for simulating this attacks using NS3. Black hole attack is one of the security threat in which the traffic is redirected to such a node that drops all the packets or the node actually does not exist in the network. Black holes refer to places in the network where incoming traffic is silently discarded or dropped. Jellyfish (JF) attack is a type of selective black hole attack. When JF node gets hold of forwarding packet it starts delaying/dropping data packets for certain amount of time before forwarding normally. Since packet loss is common in mobile wireless networks, the attacker can exploit this fact by hiding its malicious intents using compliant packet losses that appear to be caused by environmental reasons

General Terms

Table, Graphs and results

Keywords

AODV protocol, Black hole & Jellyfish attack, Mobile ad hoc networks (MANETs), Network Simulator-3

1. INTRODUCTION

The mobile ad-hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices connected by wireless links [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The strength of the connection can change rapidly in time or even disappear completely. Nodes can appear, disappear and reappear as the time goes on and all the time the network connections should work between the nodes that are part of it. As one can easily imagine, the situation in ad hoc networks with respect to ensuring connectivity and robustness is much more demanding than in the wired case.

Such types of dynamic networks are more vulnerable to attack than compared to wired network. This is because of the following reasons:

Open Medium

Dynamically Changing Network Topology

Cooperative Algorithms

Lack of Centralized Monitoring

Lack of Clear Line of Defence

Therefore, MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself [3]. Simulation and study of such attack has become necessary in order to provide defend mechanism between these types of attacks.The remainder of this paper is organized as follows: In section II, we have introduced some background study and related work that gave the motivation of this paper. In section III, we give overview of AODV. In section IV, we discuss both Jellyfish and Black hole attack. In section V, we present simulated results based our study and set up on NS3. Finally, section VI concludes the paper with some future research enhancement.

2. BACKGROUND AND RELATED WORK

In ad hoc networks, routing has become the big challenge due to presence of Wireless network [4]. Dynamic routing protocols are of two types. First is proactive routing likes DSDV [5] which are table driven and second is reactive protocol like AODV [6] and DSR [7] which are on demand routing. MANETs are dynamic in nature and follow up on demand nature so AODV and DSR can be used because network will force the host to rely on each for maintaining stability. In these protocols forma every node (or Radio terminal) communicates with its partner so as to perform peer to peer communication. If the required node is not a neighbour to the initiated call node, then the other intermediate terminal are used to perform the communication link. This is called multi-hop peer to peer communication [2]. The collaboration between these nodes is very important in the ad hoc networks. Now, in this type of scenario if some misbehaving nodes[8] first agrees to send the packet and refuse to do so because of node's overhead , connection broken, node selfishness and maliciousness, then successful transferring of data will be compromised. Node overhead is done due to increase in CPU cycle, there is no buffer space availability and connection can be broken because of dynamicity of the network. In such case network suffers the general issues for packet lost. But when a node is getting selfish for saving its own resource

[9] or becoming malicious [10] by indulging DoS attack by dropping packets then in such case network suffers a genuine packet loss.

In our analysis we will provide with the simulation of DoS attacks [11] [16] like Black hole and Jellyfish attacks. The

DoS attack can be done by node selfishness or becoming malicious [15]. In Black hole attack [13], suppose if a node tries to communicate with the other node out of its range then intermediate selfish node will drop its packet. So data gets compromised. Similarly, Jellyfish attack [14] is type of Black hole attack in which data gets compromised but till certain time only. We have used AODV as the reference protocol to simulate the node selfishness or malicious using NS-3[12]. This study will show the simulation of Black hole and Jellyfish attacks and a performance analysis of networks is done.

In [17], an anomaly detection scheme is proposed using dynamic training method in which training data is updated at regular time intervals.

In [18], the rushing attack implemented on AODV protocol by malicious nodes.

In [19], a schema is proposed in which multiple Black holes are seen cooperating with each other and thus discovering a solution for safe route avoiding cooperative Black hole attack.

In [20], we found that Jellyfish attack can increase the capacity of ad hoc networks as they will starve all multi-hop flows and provide all resources to one-hop flows that cannot be intercepted by Jellyfish or Black Holes. By measuring the effects of various performance factors for a node like number of attacking nodes, mobility model, detection time, system size, etc., a quantitative study of the performance impact and scalability of DoS attacks in ad hoc networks is done.

All material on each page should fit within a rectangle of 18 x 23.5 cm (7" x 9.25"), centered on the page, beginning 2.54 cm (1") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (.75”). The text should be in two 8.45 cm (3.33") columns with a .83 cm (.33") gutter.

3. OVERVIEW OF AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) Routing[21] is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. In AODV, every node maintains a table, containing information about which neighbor to send the packets to in order to reach the destination. Sequence numbers, which is one of the key features of AODV, ensures the freshness of routes.When a node source node wants to send a packet to another node destination node, the source node performs a Route Discovery by broadcasting a ROUTE REQUEST (RREQ) packet to the destination node, which is flooded throughout the network in a controlled manner. A ROUTE REPLY (RREP) packet is unicasted to source node from either the destination node, or another intermediate node that knows a route to destination node. Every node forwarding the RREQ message caches a route back to the source node S.Routes are maintained by using ROUTE ERROR (RERR) message, which is sent to notify other nodes about a link breakage. HELLO messages are used by the nodes for detecting and monitoring links to their corresponding neighbours.

4. EXPLANATION AND IMPACT OF BLACKHOLE AND JELLYFISH ATTACK

According to the layered network reference model, MANETs are vulnerable to the DoS attacks on the link layer and the network layer. A DoS attack[16] is said to be on the link layer when it can be launched by exploiting any vulnerabilities of data link layer protocols. For example, an attacker may use the binary exponential back-off scheme of IEEE 802.11 to deny access to the wireless channel from its local neighbours.

Correspondingly, DoS attacks on the network layer take the advantage of the vulnerabilities of the network layer protocol, which can be further classified into three types,

1) Routing disruption

2) Forwarding disruption, and

3) Resource consumption attacks.

For example, Wormhole (Rushing), and Black Hole attack are routing disruption attacks, and Jellyfish, directional antenna abusing, and dynamic power abusing attacks are forwarding disruption attacks, while Packet injection attacks and control packet floods are resource consumption attacks. In MANETs, malicious nodes can launch DoS attacks, which can isolate a node even if the isolated node has active neighbours. This is called Node Isolation Problem.

4.1 Black Hole Attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. This is called black hole attack. It is a passive attack and is also a simple way to perform a Denial of Service. Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipients. The method how malicious node fits in the data routes varies [22].

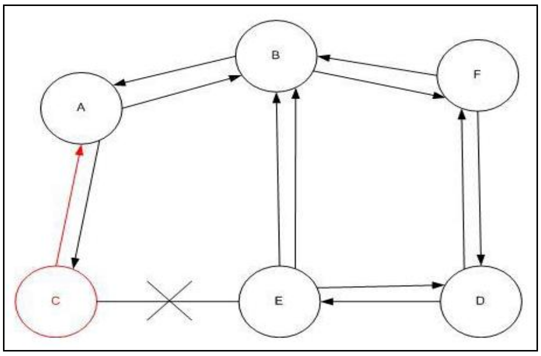

Figure-1: Black hole attack scenario

Figure-1 shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

4.2 Jelly Fish

When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. The Jellyfish attack is one of those kinds. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. Reference also described that malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviours of dropping packets [16].As shown in Figure-2, node JF is a Jellyfish, and node S starts to communicate with node D after a path via the Jellyfish node is established. Then the DoS attacks launched by node JF will cause packet loss and break off the communications between nodes S and D eventually.

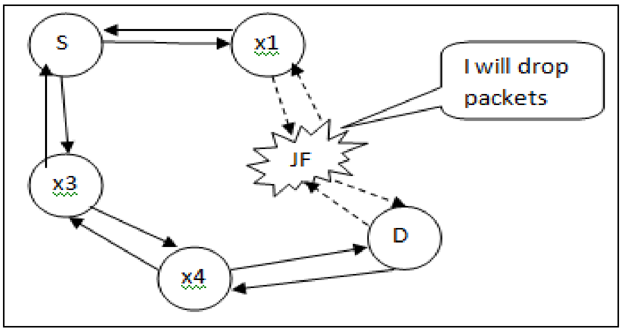

Figure-2: Jellyfish attack scenario

Three attacking ways of Jellyfish

a. JF Reorder Attack

b. JF Periodic Dropping Attack

c. JF Delay Variance Attack

5. SIMULATION RESULTS AND DISCUSSIONS

Simulation results and discussions

For simulation of the above attacks we have used Network simulator-3. NS-3 is a discrete-event network simulator in which the simulation core and models are implemented in C++ .It is built as a library which may be statically or dynamically linked to a C++ main program that defines the simulation topology and starts the simulator .It also exports nearly all of its API to Python, allowing Python programs to import an “ns3” module in

much the same way as the ns-3 library is linked by executables in C++. The core of the simulator is those components that are common across all protocol, hardware and environmental models. The simulation core is implemented in src/core. Packets are fundamental objects in a network simulator and are implemented in src/network.

In order to perform and calculate impact of blackhole and jellyfish attack in MANET, the AODV implementation was modified using the NS-3 simulator. Table-1 represents the simulation parameters along with their corresponding values. The networks constructed for simulation consist of 20 nodes placed randomly 100 meters apart. Each node has a transmission range of 250 m and moves at a speed of 10 m/s. The total sending rate of all the senders of the multi-cast group, i.e. the traffic load is 1Mbps.It sends 64bytes/sec to ping the remote node.

Table-1 Simulation parameters

Parameter	Value
Routing Protocol	AODV
Simulation time	20s
Number of Mobile Nodes	25
Transmission Area	50x100
Mobility Model	Constant Position
Traffic type	CBR
Data Packet Size	64bytes
Rate	64 Bytes/ Sec

One node was selected as route selfish for this simulation, and packet loss in the network was observed. These nodes simply discard routing control packets like RREQs/RREPs/etc.

We have plotted graph as shown in Figure-3 which shows a clear representation of the packets received at the malicious node 4 and the receiver node. The malicious node continues receiving packets while the receiver node is starved

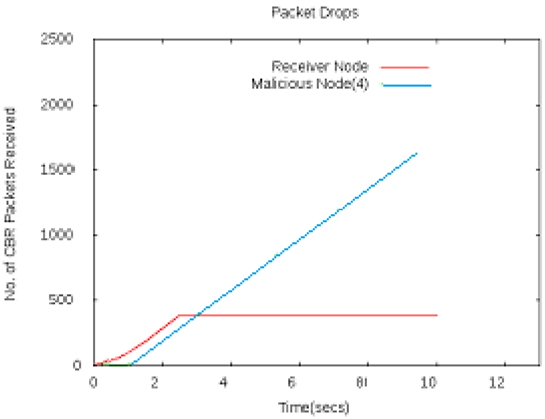

Figure-3: Black hole attack, Packets lost by Receiver node with node 4 malicious

From Figure-4, for 25 nodes, it is obvious that the throughput for AODV is high compared to that of AODV under attack. Also in AODV throughput for the case with no attack is higher than the throughput of AODV under attack. 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, thus effecting throughput.

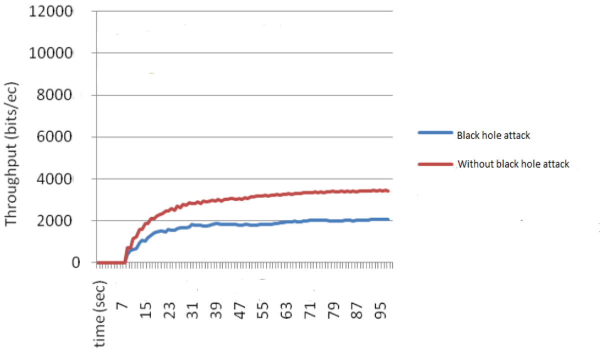

Figure-4: Throughput of AODV with v/s without black hole attack

Figure-5 depicts the results of simulation experiments with the JF periodic dropping attack. Consider first the upper curve in which the path consists of a source, a single relay node (a JF), and a destination. A time period of 0 indicates no attack and the flow again obtains a throughput of 800 kb/s. To obtain the null at 1 second, the JF drops packets for 90 ms every 1 second, which results in dropping 40% of the time, and forwarding 60% percent of the time, values easily incurred by a congested node

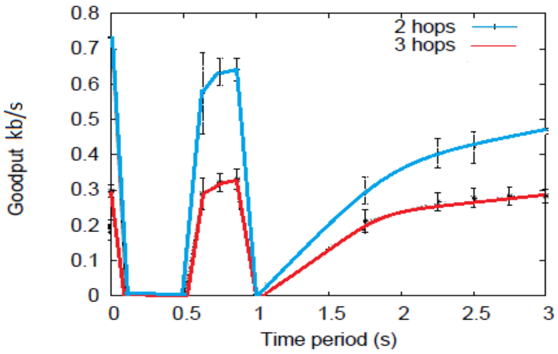

Figure-5: Jellyfish dropping attack impact on throughput

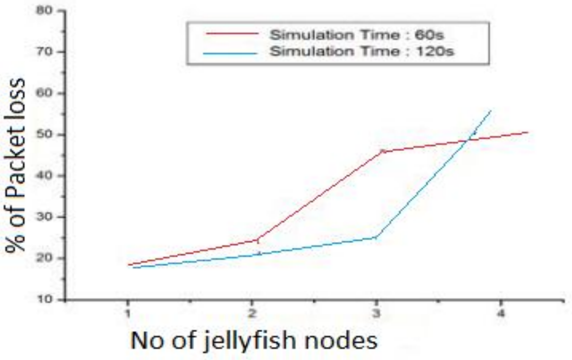

Figure-6: % of packet loss vs. No of jellyfish node

6. CONCLUSION AND FUTURE WORK

In this paper, we studied Black hole and Jellyfish: periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is protocol-compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. For completeness, we have also considered a well known attack, the Black Hole attack, as its impact on open-loop flows is similar to the effect of Jellyfish on closed-loop flows. We studied these attacks by simulating on NS-3 and have provided a quantification of the damage they can inflict. It showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multihop flows and provide all resources to one-hop flows that cannot be intercepted by Jellyfish or Black Holes. As such a partitioned system is clearly undesirable; we also consider fairness measures and the mean number of hops for a received packet, as critical performance measures for a system under attack. A well and good monitoring mechanism must be implemented in the MANET nodes in order to identify and isolate the selfish nodes from the network. Some sort of incentive mechanism may also be incorporated in the network to enforce cooperation among all the nodes in MANET to improve the overall network performance.

7. REFERENCES

[1] Perkins, Charles E, “Ad Hoc Networking,” Addison-Wesley, 2001.

[2] Suma R, Sridevi K N, Mozil M , Mungara J.N ,Sethi P, “Random-Cast: An Energy-Efficient Communication Scheme for Mobile Ad Hoc Networks,” European Journal of Scientific Research,2011

[3] T. Karygiannis and L. Owens, “Wireless Network Security, 802.11, Bluetooth and Handheld Devices,” NIST Publication, p. 800(48), November 2002

[4] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz,“A review of routing protocols for mobile ad hoc networks”, Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

[5] C. Perkins and P Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers”, In ACM SIGCOMM’94 Conference on Communication Architectures, protocols and applications, 1994

[6] C.E. Perkins, E. Belding Royer, and S.R. Das, “Ad hoc On demand distance vector (AODV) routing”, IETF RFC 3561, July 2003

[7] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007 [8] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker,

[8] “Mitigating routing misbehavior in mobile ad hoc networks”, International Conference on Mobile Computing and Networking, Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, Boston, Massachusetts

[9] P. Sankareswary, R. Suganthi, G.Sumathi, “Impact of selfish nodes in multicast Ad hoc on demand Distance Vector Protocol”, in Wireless Communication and Sensor Computing, 2010

[10] A. Babakhouya, Y. Challal, and A. Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks", in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008

[11] V. Gupta, S. Krishnamurthy, and M. Faloutsos, .Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks,. in Proc. of IEEE MILCOM ’02, 2002

[12] NS -3 manual (Release ns-3.11)

[13] Irshad Ullah and Shoaib ur Rehman, “ Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols”

[14] B. B. Jayasingh and B. Swathi, “A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network”, BVICAM’S International Journal of Information Technology

[15] Satyanarayana Vuppala, Alokparna Bandyopadhyay, Prasenjit Choudhury and Tanmay De, “A Simulation Analysis of Node Selfishness in MANET using NS-3”

[16] Fei Xing Wenye Wang, “Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks”

[17] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[18] Moitreyee Dasgupta, S. Choudhury, N. Chaki, “Routing Misbehavior in Ad Hoc Network”, International Journal of Computer Applications,2010

[19] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”

[20] Imad Aad,y JeanPierre ,Hubaux,y and Edward W. Knightly, “Denial of Service Resilience in Ad Hoc Networks”

[21] RFC 3561: Ad hoc on demand Routing protocol

[22] E. A .Mary Anita and V. Vasudevan “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining”, International Journal of Computer Applications.