Detection and Prevention from Black Hole attack in AODV protocol for MANET

Abhilasha Sharma
RKDF Institute of Science Tech. Bhopal, India

Rajdeep Singh
RKDF Institute of Science Tech. Bhopal, India

Ghanshyam Pandey
RKDF Institute of Science Tech. Bhopal, India

ABSTRACT
Mobile ad hoc network is dynamic in nature and vulnerable for several attacks to be arising in it. Mobile nodes frequently disconnect and join the network; they can arbitrarily moves from one place to another. There are several attacks in MANET. One of the attacks is Black hole attack, it is a kind of active attack, it drops the entire incoming packet between one source and destination. Black Hole nodes or Black Holes actually send a fake RREP packet and advertise itself as the shortest route is found. Sender starts transmitting packets to Black Hole, But packet do not reach the destination node on account of this attack and data packets are also lost .In our work we tried to secure the AODV protocol, so that it can withstand the attack by adding an IDS_node to AODV protocol. We have seen that packet drop ratio is decreased by desirable amount. This will help to improve the performance of Mobile Ad hoc network and decrease the Packet loss ratio, which increased due to the attack. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the Black Hole attack. In this paper, we simulated the attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations.

General Terms
MANET, IDS_Node

Keywords
Black Hole attack, IDS_Node, AODV, Sequence Number

1. INTRODUCTION
As ad-hoc networks are composed of autonomous and self-managed nodes without any infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In this attack, a Black Hole node absorbs all data packets in itself, in this way; all packets in the network are dropped or captured by Black Hole node. A Black Hole node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Black Holes node do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the Black Hole node to the destination assuming it is a true path. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 [8] contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first added a new Black Hole node into the NS-2. Having implemented a new node which simulates the Black Hole we performed tests on different scenario to compare the network performance with and without Black Hole attack in the network. As expected, the throughput in the network was deteriorated considerably in case of Black Hole. Afterwards, we proposed a solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2. and evaluated the results as we did in Black Hole implementation.

The rest of the thesis is organized as follows: In chapter 2 we presented security vulnerabilities in adhoc network, including Black Hole attack. In Chapter 3 we described the AODV protocol and how Black Hole Attack causes the protocol to misbehave. Chapter 4 presents NS (Network Simulator) and our contribution (proposed work) to this software. Chapter 5 describes the results of the network behavior due to the Black Hole attack and Chapter 6 explained the conclusion and future work.

2. SECURITY VULNERABILITY IN ADHOC NETWORK

2.1 Attacks in Adhoc network
Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. These will be detailed in the subsequent sections. Another malicious behavior of the nodes is selfishness. Black Holes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore; failed and Black Holes also affect the network performance as they do not correctly process network packets, such as in routing mechanism.

2.2 Understanding Black Hole Attack
MANET is vulnerable for many attacks; one of them is Black Hole attack. Black Hole attack [1] is a kind of active attack. In this attack, Black Hole waits for neighboring nodes to send RREQ messages. When the Black Hole receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over

itself, gives a high sequence number to make entry in the routing table of the victim node, before other nodes send a true RREP. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Black Hole attacks all RREQ messages this way and takes access to all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. There are two major behavior that Black Hole attack actually possess. They are as follows:-

1. Black Hole node advertise itself by showing larger or highest possible destination sequence no. as we know larger the sequence [1] no. means the route is fresh and latest for a particular destination. This way malicious node bluffs the source node, who wants to initiate communication.
2. It is a active DoS attack in MANET [5], which intercepts all incoming packets from an intended source. A black hole node absorbs the network traffic and drops all packets.

The malicious node is supposed to be positioned in center of the wireless network.

3. BACKGROUND OF AODV

3.1 Working

AODV [2] is an adhoc on demand distance vector reactive routing protocol; that do not maintain any routing information. AODV has borrowed the concept of destination sequence number from DSDV [7], to maintain the most recent routing information between nodes. Whenever a source node needs to communicate with another node for which it has no routing information, it will initiate Route Discovery process by broadcasting a Route Request (RREQ) packet to its neighbors. Each neighboring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbors after increasing the hop_count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup. The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. If the intermediate node has a route entry for the desired destination, it determines whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQ's sequence number for the destination is greater than the recorded by the intermediate node. Instead, the intermediate node rebroadcasts the RREQ packet. If a node receives more than one RREPs, it updates its routing information and propagates the RREP only if RREP contains either a greater destination sequence number than the previous RREP, or same destination sequence number with a smaller hop count. It restrains all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then later updates its routing information of better route to the destination node. Each route table entry contains the following information:

• Destination node
• Next hop
• Number of hops
• Destination sequence number
• Active neighbors for the route
• Expiration timer for the route table entry

The route discovery process is reinitiated to establish a new route to the destination node, if the source node moves in an active session. As the link is broken and node receives a notification, and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process.

As the routing protocols typically assume that all nodes are cooperative in the coordination process, malicious attackers can easily disrupt network operations by violating protocol specification. This paper discusses about Black Hole attack and routing security in AODV by purging the threat of Black Hole attacks.

3.2 Simulation of AODV

In this paper to provide trust based communication in MANET, we have used AODV-IDPS (ad-hoc on demand distance vector with Intrusion detection and prevention system) against the Black Hole attack. Our basic approach to analyze the behavior of Black Hole attack, normal time network behavior analyzes and also after the AODV-IDPS module through protects the selfish behavior of the node and comparative analysis find out.

In our simulation we use ns-2 simulator and analyze the performance of the network on the bases of flowing parameter like throughput, average end-to-end delay, routing load, packet delivery ratio, TCP flow analysis and UDP packet analysis.

- **Routing overhead:** How many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.
- **Average Delay:** Represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination
- **Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps
- **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

4. PROPOSED SCHEME

4.1 NS-2 Simulation

In our approach we have inbuilt IDS module with AODV routing and Black hole behavior module (named as Selfish module). Very first we attach IDS and Selfish module in the NS-2 package and update the make file through following command:

selfish/selfish_logs.o selfish/selfish.o selfish/selfish_rtable.o selfish/selfish_rqueue.o\idsaodv/idsaodv_logs.oidsaodv/idsaodv_rtable.o idsaodv/idsaodv_rqueue.oidsaodv/idsaodv.o \

After that we update the packet.h file through PT_idsAODV= "IDSAODV"; and PT_selfish= "Selfish"; and compile the internal module if new object file generated then we create TCL (tool command language script) for the scenario creation and create the MANET scenario, TCL invoke the new module Selfish and IDS module and gives the behavior according to selfish and IDS module. Then we create two different type of Output file name as .tr (trace file) and .nam (network animator file) through TCL script. Trace file contain each and every event information in particular discrete event of simulation and that file passes to awk (abstract window tool kit) and get the output in the form of routing overhead, throughput, average end-to-end delay etc. Here we create three module names as AODV simple routing, IDS (intrusion detection and prevention system) module and Black hole module (named as selfish module) step by step.

4.2 AODV

AODV classify as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. The working of AODV is mentioned in above section.

4.3 Black Hole Module

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole attack we added a malicious node that exhibits Selfish behavior and capture the UDP packet and block the TCP packet or can't forward the TCP data to actual destination. In a Black Hole attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the Black Hole still manages to mislead the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

4.4 IDPS (Intrusion Detection & Prevention System)

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. In our simulation module we apply IDS module that protect through the Black Hole behavior if Black Hole node in the range of IDS. Very first IDS check which node update the routing table and send higher sequence number to the sender node, if find out so IDS sends the message to the sender node for elimination of that particular path where belongs Black Hole and search new route according to IDS instruction. Here IDS internal module provides only protection of misbehave and provide trust communication between sender and destination. After prevention we detect Black Hole node via trace analysis and provide secure communication in MANET.

5. RESULTS

5.1 TCP analysis graph

Here in this graph we can see that how many TCP packets are received/sec by the destination in all the 3 cases i.e.

1. In case of normal AODV "TCP-AODV.tr" (Red colour line)
2. In the presence of Black Hole attack "TCP-Selfishnode.tr" (Green colour line)
3. After creating IDS_node "TCP-IDS-Selfish.tr" (Blue colour line)

The graph shows that In case of IDS_node maximum no. of packets/second are delivered and in case of Black Hole no packets are delivered. For example after 60sec around 40 no. of packets are delivered in case of normal AODV, 90 packets are delivered in case of IDS node and zero packet in case of Black Hole.

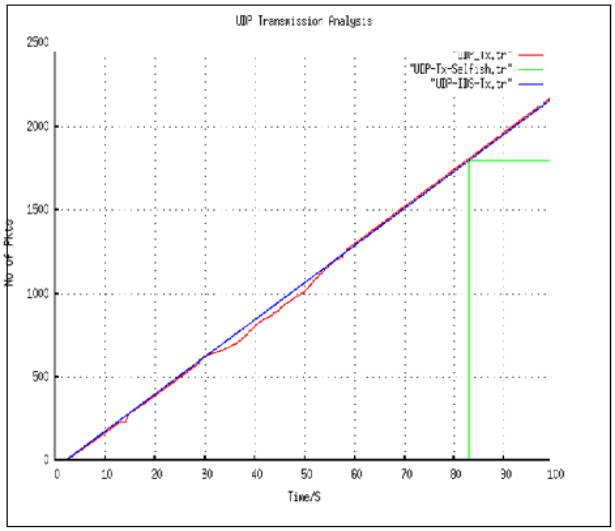

Figure 1

5.2 UDP Transmission Analysis

The graph shows the no. of packets transmitted/second in case of UDP packet transmission. We can observe that there are around same no. of packet transmitted in case of normal AODV and Ids_node. But in case of Black Hole transmission start after 82 seconds, before that no packets are transmitted.

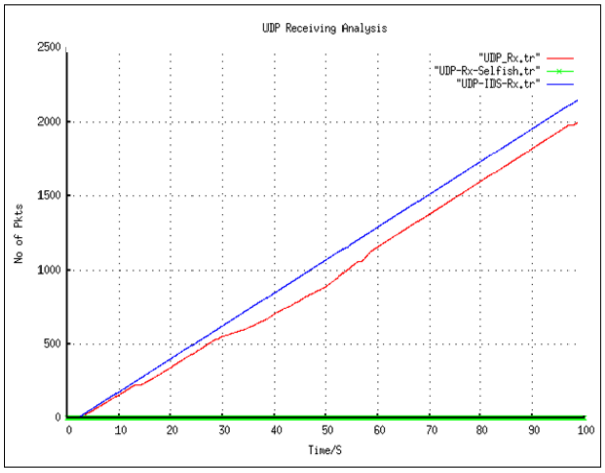

Figure 2

5.3 UDP receiving Analysis

Graph shows the no. of UDP packets received/sec in all the three cases. We can see that no packets are received in the presence of Black Hole attack. While in case of IDS node maximum no. of packets are received.

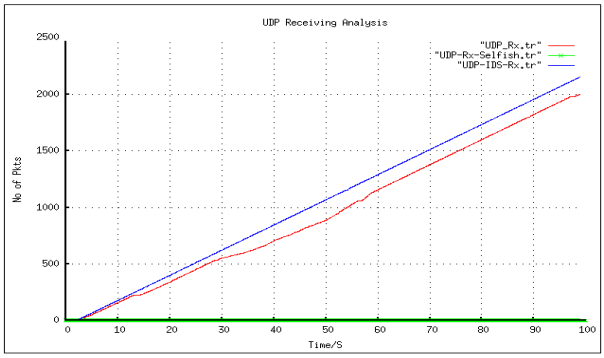

Figure 3

5.4 UDP Lost Analysis

Graph shows the no. of UDP packets lost/sec. In case of IDS node no packet is lost all the packets are received by the destination. In case of Black Hole all the packets which are transmitted are lost. And in case of normal AODV some packets are lost.

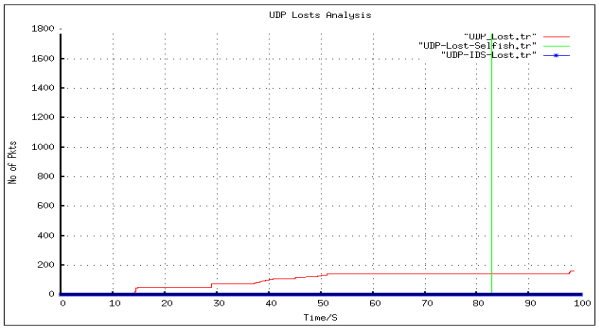

Figure 4

6. CONCLUSION AND FUTURE WORK

In this paper, we have analyzed effect of the Black Hole attack in an AODV protocol of MANET. For this purpose, we have simulated an AODV protocol and its behavior in the presence of Black Hole attack in NS-2. We have simulated three scenarios where each one has 20 nodes that use AODV protocol and also simulated the same scenarios after introducing Black Hole attack into the network. Moreover, we have also simulated a solution that attempted to reduce the Black Hole attack effects in NS-2 and simulated the solution using the same scenarios. We have also detected the Black Hole node by analyzing the .tr files. In .tr file if any node creates *loop* then it is detected as Black Hole. Simulation results are analyzed below:

Having simulated the Black Hole Attack, I saw that the packet loss is increased in the ad-hoc network. The figure of simulation results shows the graph, which shows the difference between the numbers of packets lost in the network with and without a Black Hole Attack. The result also shows that AODV network has normally 95 % packet delivery fraction and if a Black Hole Node is introducing in this network data packets delivered up to 0.14 %. Black Hole attack increases data loss. When I used IDS_AODV in the same network, the packet delivery fractioned is increased up to 99 %. These results show that my solution reduces the Black Hole effects in a network by using IDS_AODV.

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. There are many techniques to prevent and investigate [3], [9] AODV from the Black Hole attack. These could be tested to determine which one is the best to prevent the Black Hole. We have analyzed effect of the Black Hole in an AODV Network. Our solution tries to eliminate the Black Hole effect by making an entry of secure route. This could be a possible solution to make secure entries in the routing table, where each node is known to rest of the nodes present in the Ad hoc network. If a new node wants to join this network, it has to ensure its authenticity. Then authenticity should be well tested and black hole must be detected at that point. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period.

In future this approach can be extended to other proactive and reactive routing protocols. We can also extend this research to secure routing protocols against other attacks such as Wormhole attack, Jellyfish attack etc.

7. REFERENCES

[1]. Mangesh Ghonge and Prof.S.U.Nimbhorkar "Simulation of AODV under Blackhole Attack in MANET" IJARCSSE, Feb 2012.

[2]. C. Perkins, E. Belding-Royer, and S. Das. AODV RFC3261, experimental edition, July 2003.

[3] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET", Journal of Networks, Vol.3, No.5, May 2008.

[4]. P.-W. Yau and C. J. Mitchell, "Security Vulnerabilities in Ad hoc Networks," Proceedings of the 7th International Symposium on Communication Theory and Applications (ISCTA), pp. 99–104, 2003.

[5]. D. Chen, J. Deng, and P. K. Varshney, "Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming (research poster)," Proceedings of the 9th ACM International Conferenceon Mobile Computing and Networking (MobiCom), 2003.

[6]. C. Silva Ram Murthy and C. Siva Ram. Ad Hoc wireless networks : architectures and protocols. Prentice Hall PTR, 2004.

[7]. C. E. Perkins, P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," In ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, pp. 231–241, 1994.

[8] Marc Greis, "Tutorial for the Network Simulator (NS2)"

[9] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.

[10] Reena Karandikar, Rashmit Kaur Khanuja, Surendra Shukla "proposed solution to prevent black hole attack in manet" Volume 2, Issue 2 (February 2012) IJRIM.

[11] Madhusudhananagakumar KS, G. Aghila "A Survey on Black Hole Attacks on AODV Protocol in MANET" International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011.