A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET

Kanika Lakhani[†] ,Himani bathla[††], Rajesh Yadav[†††]

Summary
An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. In mobile ad hoc network, each mobile node acts as a host as well as a router. These nodes communicate to each other by hop-to-hop communication. A number of routing protocols like Ad Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector (DSDV) and Temporally Ordered Routing Algorithm (TORA) have been implemented. AODV is a prominent on-demand reactive routing protocol for mobile ad hoc networks. But in existing AODV, there is no security provision against a well-known "Black Hole" attack. Black hole nodes are those malicious nodes that agree to forward packet to destination but do not forward packet intentionally. These black hole nodes participate in the network actively and degrade the performance of network eventually. This thesis proposes watchdog mechanism to detect the blackhole nodes in a MANET. This method first detects a black hole attack and then gives a new route bypassing this node. In this thesis an attempt has been made to compare the performance of original AODV and modified AODV in the presence of multiple black hole nodes on the basis of throughput and packet delivery ratio. With this new protocol, throughput increases 10-18% in the presence of 10% black hole nodes for different pause times.

Key words:
AODV, Black Hole, MANET, RREP, RREQ.

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the assistance of any stand-alone infrastructure or centralized administration [12]. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [14]. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi-hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network [13]. Figure 1 represents a MANET of 3 nodes. Node 2 can directly communicate with node1 and node 3, but any communication between Nodes 1 and 3 must be routed through node 2.

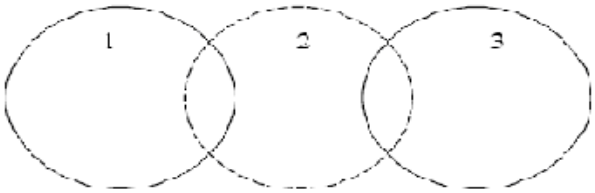

Figure 1: Example of simple MANET of 3-nodes

In mobile ad-hoc networks where there is no infrastructure support and since a destination node might be out of range of a source node transmitting packets, a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. A base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes.

2. AODV Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) [1] is an on demand routing protocol which is used to find a route between the source and destination node as needed. It uses control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from the source to the destination. Header information of these control messages are also explained in [1]. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, and received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ

Manuscript received May 5, 2010
Manuscript revised May 20, 2010

message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination in its routing table.

Fresh enough means that the intermediate node has a valid route to the destination established earlier than a time period set as a threshold. Use of a reply from an intermediate node rather than the destination reduces the route establishment time and also the control traf_c in the network. This, however, leads to vulnerabilities. Sequence numbers are also used in the RREP messages and they serve as time stamps and allow nodes to compare how fresh their information on the other node is. When a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is assumed to be more accurate information and whichever node sends the highest sequence number, its information is considered most up to date and route is established over this node by the other nodes.

3. Black-Hole Attack

The black hole attack [1] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough route to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. Vulnerabilities of ad-hoc networks against black hole attacks are studied by different authors. Deng et.al. [2] addresses the black hole problem and proposes a solution based on modification of the AODV protocol. The authors propose to check the route through the next hop in the agreed upon path. This solution means that next hop information shall be added to the standard AODV header. Similar approach is adopted in [3] where the nodes are asked to send their neighborhood sets once the route is established. In [4] two solutions are proposed for detecting the black hole attack in ad-hoc networks. First solution involves sending a ping packet to the destination to check the established route. If the acknowledgement does not arrive from the destination, presence of a black hole is deduced. The other approach proposed is based on keeping track of sequence numbers as black holes usually temper with these sending packets with unusually high sequence numbers.

4. Proposed Work

To investigate the effects of black holes we simulated the wireless ad-hoc network scenarios with and without a black hole node present in the network. To be able to do that we introduced a new protocol, which we called "Modified AODV. This new protocol, modified AODV is inherited from the existing AODV routing protocol. In Watchdog mechanism, each node maintains two extra tables, one is called pending packet table and another one is called node rating table. In pending packet table, there are four fields, Packet ID, Next Hop, Expiry Time and Packet Destination.

Packet ID	Next Hop	Expiry Time	Packet Destination

Table 1: Pending packet table

Packet ID: ID of packet sent.

Next Hop: Address of next hop node

Expiry Time: Time-to-live of packet

Packet Destination: Address of destination node.

In node rating table, there are also four fields, Node Address, Packet drops, Packet forwards and Misbehave. This table updated corresponding to pending packet table.

Node Address	Packet drops	Packet forwards	Misbehave

Table 2: Node rating table

Node Address: Address of next hop node.

Packet Drops: Counter for counting the dropped packet.

Packet Forwards: Counter for counting the forwarded packet.

Misbehave: It has two values 0 and 1, 0 for well behaving node, 1 for misbehaving node

Watchdog Mechanism: **-** In pending packet table, each node keeps track of the packets, it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node,

and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop.

In node rating table, each node keeps rating of nodes, which are adjacent to it (means nodes are within its communication range). This table contains the node address, a counter of dropped packets observed at this node and a counter of successfully forwarded packets by this node.

The fourth field of the above node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is considered as a misbehaving node), otherwise it is considered as a legitimate node. An expired packet in the pending packet table causes the packet drops counter to increment for the next hop associated with the pending packet table entry.

Each node listens to packet that are within its communication range, and only to packets belonging to its domain. Then it verifies each packet and prevent forged packet. If it observes a data packet in its pending packet table, then it removes this data packet from pending packet table after authenticating the packet. If it observes a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increments the packet forwarding value in node rating table.

For deciding whether a node is misbehaving or act as a legitimate one, depend on the selection of threshold value. For example if we take a threshold value of 0.5. This means that as long as a misbehaving node is forwarding twice packets as it drops it will not be detected. If we take a lower value of threshold then it will increase the percentages of false positives. After detecting a misbehaving node, a node will try to do local repair [2] for all routes passing through this misbehaving node. If local repair process fails, then it will not send any RERR packet upstream in the network. This process tries to prevent a misbehaving node from dropping packets, and also prevent blackmailing of legitimate nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop all RREP messages coming from nodes currently marked as misbehaving. To stop misbehaving node to act actively in a network, the entire packet originating from this node has been dropped as a form of punishment.

The algorithm for the proposed work is as follows:

1.Data packet forwarded or sent.
2.Copy and keep the data packet in pending packet table until it is expired or
forwarded
3.If (data packet forwarded)
{
Increment the corresponding *forwarded packet* in the node-rating table
and remove the data packet from pending packet table
}
4.If (data packet expires in the pending packet table)
{
Increment the corresponding *dropped packet* in the node-rating table and
remove the data packet from pending packet table
If (dropped packet >threshold(th1)) then
{
If (dropped packet /forwarded packet)> threshold(th2))
{
Node is misbehaving
Promiscuous node locally tells all the node of its wireless range that particular node is misbehaving node.
Discard RREP message coming from the misbehaving node
}
}
}

5. Simulation Model

The mobility simulations that have done in this thesis used the node movement pattern of 50 nodes in the area of 1000x1000 square meter and maximum speed of nodes will be 5 m/sec. Also the traffic pattern of 50 nodes in which there will be maximum 5 connections with CBR (constant bit pattern) and different seed value have been used in the simulation. Seed value is used for generating the random traffic pattern. By changing only the seed value for generating the CBR or TCP connections, it changes the complete traffic pattern files.

Communication Type	CBR
Number of Nodes	50
Maximum mobility speed of nodes	5 m/sec
Simulation Area	1000m x 1000 m
Simulation Time	200 sec
Packet Rate	4 packets/sec
Packet Size	512 bytes
Number of Connections	5
Transmission Range	250 m
Pause Times	0,40,120,160 sec
Number of malicious nodes	0, 3,5
Transmission Speed	10 Mbps

Table 3: Simulation Parameters

Throughput*:* - It is the total number of received packet per unit time.Throughput = Total No. of packet received / Total traversing time

End-to-end delay*:* - This is defined as the delay between the time at which the data packet was originated at the source and the time it reaches the destination. Delay = Receiving time – Sending time

First, results are calculated for throughput vs. number of black hole node with pause times 0 sec, 40 sec, when threshold value (th2 is 1.0).

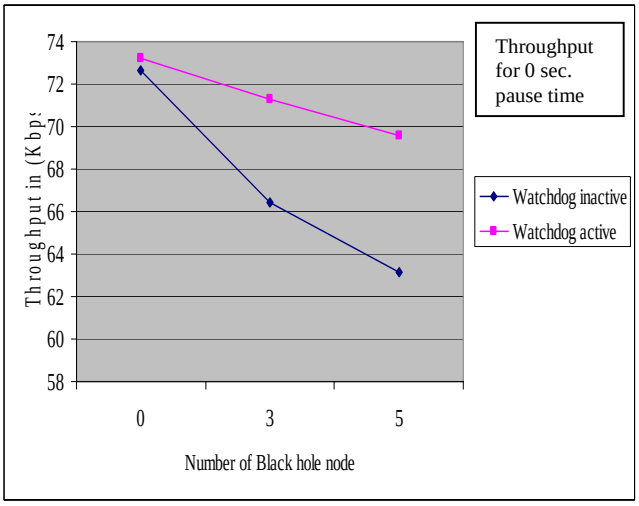

Figure 2: Throughput vs. Black hole nodes for 0 second pause time.

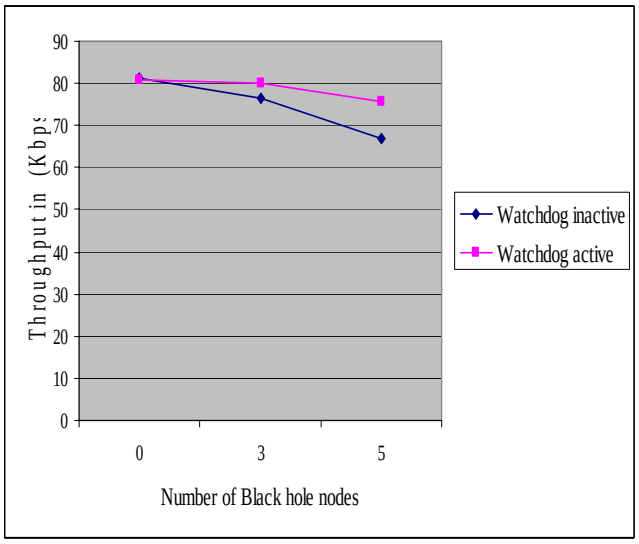

Figure 3: Throughput vs. Black hole nodes for 40 seconds pause time

The results are shown in table 2 increases in the value of throughput when the modified AODV based on watchdog mechanism is active in the presence of 3 black hole nodes, when scenario of node movement for pause time is 0 sec, 40 sec.

Pause Time (sec)	Throughput in (kbps) with Watchdog inactive	Throughput in (kbps) with Watchdog active	% Increase in Throughput
0 sec	63.42	71.61	7.81%
40 sec	76.62	80.11	4.55%

Table 4: Percentage increase in Throughput in the presence of 5 Black hole nodes

The results are shown in table 3 increases in the value of throughput when the modified AODV based on watchdog mechanism is active in the presence of 5 black hole nodes, when scenario of node movement for pause time is 0 sec, 40 sec.

Pause Time (sec)	Throughput in (kbps) with Watchdog inactive	Throughput in (kbps) with Watchdog active	% Increase in Throughput
0 sec	63.14	69.56	10.16%
40 sec	66.96	75.67	13.06%

Table 5: Percentage increase in Throughput in the presence of 5 Black hole nodes

Second, results are calculated for Packet delivery ratio vs. number of black hole node with different pause time 0 sec, 40 sec.

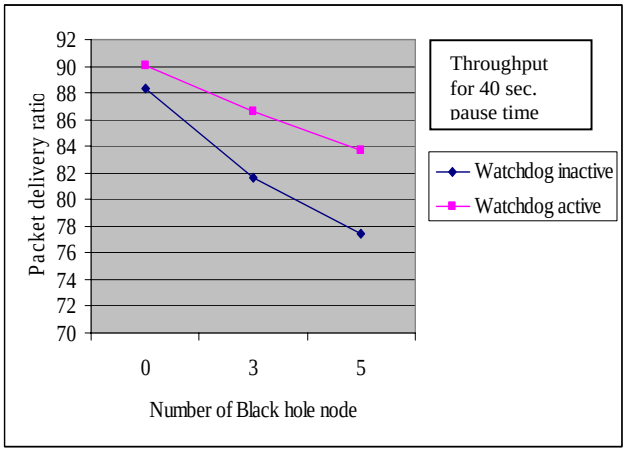

Figure 4: Packet delivery ratio vs. Black hole node for 0 second pause time

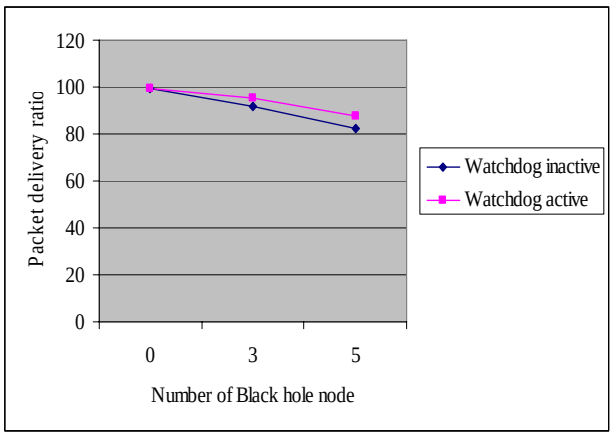

Figure 5 Packet delivery ratio vs. Black hole node for 40 seconds pause time

The results are shown in table 9 increases in the value of packet delivery ratio when the modified AODV based on watchdog mechanism is active in the presence of 3 black hole nodes, when the scenario of node movement for pause time is 0 sec, 40 sec.

Pause Time (sec)	Packet delivery ratio with Watchdog inactive	Packet delivery ratio with Watchdog active	% Increase in Packet delivery ratio
0 sec	81.82	86.62	5.86%
40 sec	91.36	94.56	3.50%

Table 6 Percentage increase in PDR in the presence of 3 Black hole nodes

6. Analysis

Simulated results are taken on ns-2.31 [8], [11] which runs on Red Hat Linux Enterprise Server. A network of 50 nodes was taken for simulation with different pause time i.e. 0, 40, 120 and 160 seconds. Throughput and packet delivery ratio was calculated for existing AODV running for different scenarios having 0, 3 and 5 black hole nodes.Using same simulation parameter modified AODV was tested on above-mentioned networks having 0, 3 and 5 black hole nodes, for both watchdog active and inactive mode. The experimental results show that when the black hole nodes is increased up to 6% of total network nodes then in the presence of watchdog active throughput increases up to 3% to 8% for different scenarios. When the black hole nodes is increased up to 10% of total network nodes then in the presence of watchdog active throughput increases up to 10% to 18% for different scenarios.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, *IEEE Communication magazine*, October 2002.

[2]C.E. Perkins, S.R.Das, and E.Royer, "Ad-hoc Demand Distance vector (AODV)", Mobile Ad Hoc Networking Working Group, *IETF Internet Draft*, http:/www.ietf.org/internet-draft/draft-ietf-manet-aodv-05.txt March 2000

[3] Lidong Zhou, Zygmunt J.Hass, "Securing Ad Hoc Networks", *IEEE Special Issue on Network Security*, vol-13, pp 24-30 Nov-Dec 1999

[4] P.Ning and K.Sum, "How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol", Tech Rep, TR- 2003-07, CS Department, NC University, April 2003

[5]L.Venkatraman and D.P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks", *IEEE Network Magazine*, vol. 13, no-6, Nov 1999

[6]S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of MOBICOM, Boston MA USA*, pp 255-265 2000.

[7] Elizabeth M.Royer and C.K.Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", *IEEE Personal Communication Magazine*, pp 46-55, April 1999

[8]The Network Simulator – ns-2 http://www/isi.edu/nsnam/ns.

[9] Kevin Fall and Kannan Varahan, editors. "NS Notes and Documentation", *the VINT Project, UCBerkeley*, LBL, USC/ISI, and Xerox PARC, November 1997.

[10]K.Gorantala, "Routing Protocol in Mobile Ad-hoc Networks," *Technical report Department of Computer Science from UMEA University*, June-2006.

[11]A tutorial named "NS by example": http://nile.wpi.edu/NS/, visited 2006-07-22

[12]David B.Johnson and Dravid A. Maltz, "Dynamic Source routing in ad hoc wireless networks", *Technical report, Carneigie Mellon University*, 1996

[13] M. Abolhasan, T. Wysocki, and Eryk Dutkiewicz, "A review of routing protocol for mobile ad hoc networks", *Technical report, University of Wollongong*, 2003

[14] X. Hong, Kaixin Xu, and Mario Gerla, "Scalable routing protocols for mobile ad hoc networks", *IEEE Network Magazine*, pp11-21, July-Aug 2002

[15] V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proc. INFOCOM*, Apr-1997.

[16] L.Buttyan and J.P.Hubaux, "Enforcing service availability in mobile ad hoc networks", *in Proceedings of MobiHOC*, USA, Aug 2000.
[17] S.Buchegger and J.Y.L.Boudec, "Performance analysis of CONFIDANT protocol: Cooperation of nodes", *In Proceedings of IEEE Workshop on MobiHOC*, Lausanne, June 2002
[18] P.Michiardi and R.Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", *in Proceedings of Sixth Conference on CMS 2002*. Portoroz, Slovenia, 2002
[19] B.Awebuch, D.Holmer and H.Rubens, "An on-demand secure routing protocol resilient to Byzantine failure", *in Procedding of Security Workshop on MobiCom*, 2002
[20] R. Ramanujan, S.Kudige, T.Nguyen and F. Adlestein, "Intrusion-resistant ad hoc wireless networks", *in Proceedings of MilCom*, October 2002

Kanika Lakhani received the B.E. degree in Information Technology and now pursuing M.Tech. degree in Computer Engineering.

Himani Bathla received the B.Tech and M.Tech degree in Computer Engineering.

Rajesh Yadav received B.Tech and now pursuing M.Tech degree in Computer Engineering.