Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic

P. V. Venkateswara Rao
Research scholar,
Dept. of CSE,
JNTUK,
Kakinada-530003.

S. Pallam Setty, PhD
Professor,
Dept. of CS&SE, AUCE (A),
Andhra University,
Visakhapatnam-530003.

ABSTRACT
MANETs are vulnerable to different kinds of attacks due to inherent properties such as wireless medium, dynamic topology, distributed operation and constrained capability. One of the well-known attacks is the Black Hole attack which is most common in the on-demand routing protocols such as AODV. In this paper, we simulate the Black-hole attack in AODV using NS2 Simulator for both SANETS and MANETS by varying node density in the context of responsive and non-responsive traffic. From the simulation results, the impact of Black-hole attack on the performance of AODV QOS metrics i.e., throughput, packet delivery ratio is less, for end-to-end delay, routing load is high in MANET and SANET under responsive (TCP) and non-responsive traffic (UDP).

General Terms
TCP, mTCP, UDP, mUDP.

Keywords
MANETs, SANETs, AODV, black hole attack, NS2, throughput, end-to-end-delay, packet delivery ratio, normalized routing load.

1. INTRODUCTION
Ad hoc networks are limited capacity networks with no network infrastructure and no dedicated routing devices. Moreover, every node in such networks has to take care of its routing module itself. The main advantage of wireless network is communicating with rest of the world while being mobile. A Mobile Ad-hoc Network (MANET) is a collection of independent mobile users that communicate with available bandwidth and limited power. As the nodes in a MANET are mobile, the network topology may change rapidly [1]. The most important characterizing feature of a MANET is that no one among all has the central role. So there is a big scope of secure algorithm which can serve the best in this mobile scenario.

A MANET can also be known as the mesh network as these communicate with each other randomly and the routes of communication are created as per on-demand. The MANETs do not have to have the fixed infrastructure like a head/base station hence it provides very high flexibility and they communicate quickly and spontaneously. There are several routing protocols of MANET like AODV, DSDV, and DSR Routing in ad-hoc network involves determining a path from the source to the destination data can be communicated and the delivery of the packets to the destination nodes while nodes in the network are moving freely. Due to this node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility, nodes need to maintain routes in the network [2]. Routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid and location-based categories depending upon how nodes can establish and maintain paths. Pro-active routing protocols are table-driven protocols that maintain up-to-date routing table using the routing information learnt from the neighbors on a continuous basis. Routing in such protocols involves selecting a path form the source to the destination, where the source node and each intermediate node selects a next hop, by routing table look up, and forwarding the packet to next hop until destination receives the packet [3].

A drawback of such protocols is the proactive overhead due to route maintenance and frequent route updates to cope with node mobility. Examples of this class include DSDV, WRP. Reactive routing protocols are demand-driven protocols that find path when necessary. In such protocols, establishing a new route involves a route discovery phase consisting of route request (flooding) and a route reply (by the destination node). Nodes maintain only the active routes until a desired period or until destination becomes inaccessible along every path from the source node. A drawback of such protocols is the delay due to route discovery. Examples of this class include AODV and DSR protocols [3] [4].

Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Thus mechanism for ensuring packet delivery in Pro Active and Reactive can be apply together in this category [4] [5].

The paper is organized as follows: In section 2, **AODV routing protocol** is discussed. In section 3, **Black hole attack** is explained. Section 4 provides **Methodology** followed. Section 5 provides **Simulation and Parameter setting.** Section 6 **provides Results and Analysis** observed**.** In section 7 **Conclusion and future work** is discussed.

2. AODV ROUTING PROTOCOL
In Ad-hoc On-demand Distance Vector Routing (AODV), a node discovers and maintains a route to the destination as and when necessary [6]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination that is actively communicating with each other. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination.

The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. Thus, each node maintains a sequence number for itself and the respective source(s) and destination(s).Anode increments its sequence number if it initiates a new route request or if it detects a link- break with one of its neighbors.

Ad-Hoc On-Demand Distance Vector (AODV) is a dynamic protocol which actuates on demand routing algorithm and multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. To establish a path to the destination, a source node broadcasts a route request (RREQ) packet [6] [7]. The RREQ packet contains the source ID, the destination ID, sequence number of the source, and the latest sequence number of the destination node that is known to the source node. When a node receives a RREQ packet, it makes an entry for the route request in the route-request cache, and stores the address of the node from which it received the request as the next hop towards the source in its routing table. If receiving node is the destination or it has a fresh route to that destination1, then it responds with a route reply (RREP). Otherwise, it rebroadcasts the RREQ to its neighbors. When a node receives a RREP, it stores the address of the node from which it received RREP as the next hop towards the destination in its routing table and unicast the RREP to the next hop towards the source node. Once the source receives the RREP packet, it starts transmitting data packets along the path traced by the RREP packet. Due to the node mobility, path(s) established by a source node may break. When a node detects a path-break, it drops the packet for the destination and generates a route error (RERR) packet for the destination and sends the RERR to the source. Upon receiving a RERR, the source node buffers data packets for the destination and tries to re-establish a path to the destination. This is illustrated in figure 1.

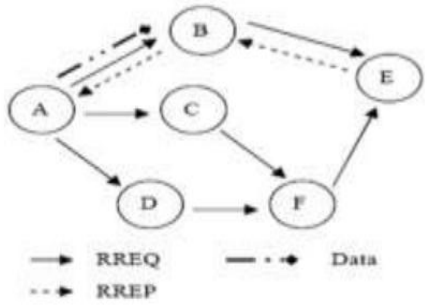

Figure 1: RREQ and RREP propagation from Ato E

3. BLACK HOLE ATTACK

An attack is an assault to system security derived from intelligent threat [9].

3.1 Security Attacks

The attacks [11] in MANET can roughly be classified into two major categories-passive attacks and active attacks, according to the attack means [12] [13].

3.1.1 Passive Attacks:

A passive attack obtains data exchanged in the network without disrupting the operation of the communications.
Ex: eavesdropping, traffic analysis, and traffic monitoring

3.1.2 Active Attacks:

An active attack involves information interruption, modification, or fabrication.
Ex: jamming, impersonating, modification, denial of service (DoS), and message replay.
Black hole attack comes under Active attack.

The Black Hole attack is a powerful attack in MANET. In this Malicious Node attract all traffic by claiming the route to the destination which then absorbs the packets without forwarding them to the destination. Co-operative Black hole means the malicious nodes act in a group. The attacker injects falsified routing packets to attract traffic. The attacker intercepts or drops control as well as data packets to deny services to authentic nodes. This attack can be prevented by establishing routes free of such nodes or by removing them from existing routes [8]. In the following illustrated fig. 2, imagine a malicious node ‘M’. When node ‘A’ broadcasts a RREQ packet; nodes ‘B’ ‘D’ and ‘M’ receive it. Node ‘M’, being a malicious node, does not check up with its routing table for the requested route to node ‘E’. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node ‘A’ receives the RREP from ‘M’ ahead of the RREP from ‘B’ and ‘D’.

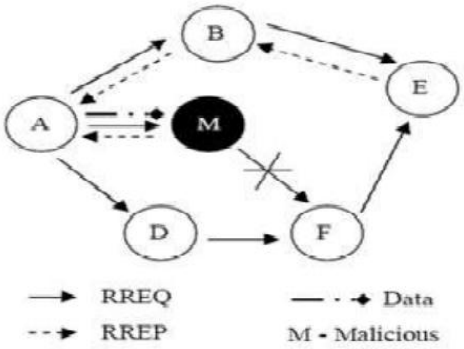

Figure 2: Black hole attack

Node ‘A’assumes that the route through ‘M’ is the shortest route and sends any packet to the destination through it. When the node ‘A’ sends data to ‘M’, it absorbs all the data and thus behaves like a ‘Black hole’.

4. METHODOLOGY

Several researchers have been proposed several solutions to support QoS in the dynamic MANET environment but they are not taking care about the provisioning of security requirements in hand held devices where the resources are scare. The security provision will cost more resources and minimizing the network life, it may be adversely affect the QoS. Thus it may be necessary to consider both provisioning of security and minimizing the energy consumption to provide network life in an integrated manner. To evaluate the designs proposed in this paper to choose the most suitable evaluation methodology. Three evaluation methodologies were identified

1. Simulation,
2. Experimental and
3. Mathematical

Simulation was chosen, as experimental methodology was not practicable and mathematical methodology is highly restrictive. The research method was to evaluate the collection of the results, and the results were analyzed and compared with those from the work, conclusions were drawn from evaluations of the proposed routing protocol.

4.1 Algorithm for SAODV:

Algorithm used to implement Black hole attack in AODV routing protocol:

1. Add the field malicious in header file of AODV(aodv.h)
2. By default, malicious value is set to false, but in the TCL script if malicious node is set then it is checked in aodv.cc and set the malicious value to true.
3. Changes to be made in aodv.cc for malicious node, set route reply parameters with highest sequence number and low hop count to the source node in order to make malicious node to be in the route though it does not have the route to the destination.
4. Once the route discovery process is completed and the route is set with malicious node as intermediate, data transfer starts, packets coming towards malicious node are dropped.
5. This causes low throughput, packet delivery ratio and high end-to-end delay, routing ahead.

5. SIMULATION

The routing protocol AODV is under the analysis for this paper. The Linux UBUNTU OS 12.04 LTS is used to run the Simulation Software NS2 (Network Simulator 2) version 2.35 for the performance evaluation.

The performance of AODV routing protocol with Black hole attack in SANETs and MANETs is observed at various pause time intervals, with TCP and UDP, with the number of nodes (40 and 60) which move randomly 1500m X 1500m range. There are modifications done to the original **aodv.cc** and **aodv.h** files as mentioned above (section 4) of the NS2 to simulate the Black Hole behavior.

Table 1.The simulation parameters are shown in table

Parameter	value
Simulator	Ns-2
Protocol	AODV
Simulation time	600 seconds
Pause time	0sec(MANET), 600sec(SANET)
Number of Nodes	40,60
Transmission Range	1500m x 1500m
Mobility Model	Random way point
Propagation model	Two-Ray Ground Reflection
Traffic Type	TCP (responsive), UDP (non-responsive)
Application Type	FTP,CBR
Maximum speed	10m/s
Malicious nodes	1

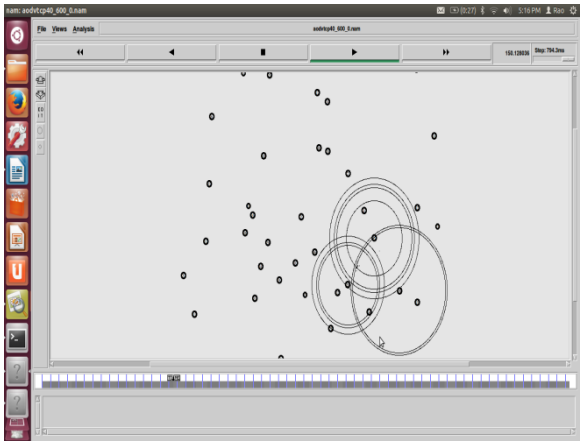

Figure 3: Simulation scenario for 40 nodes

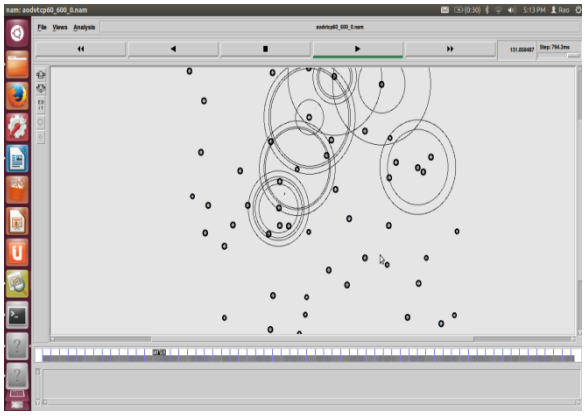

Figure 4: Simulation scenario for 60 nodes

6. RESULTS AND ANALYSIS

From the experimental results of QoS metrics [9] – average throughput, average end-to-end delay, packet delivery ratio, routing overhead the following are observed.

6.1 Average Throughput (bits/s):

The rate of successfully transmitted data per second in the network during the simulation is called Average Throughput. From the graph below it is observed that average throughput is decreased in both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) when malicious node is introduced.

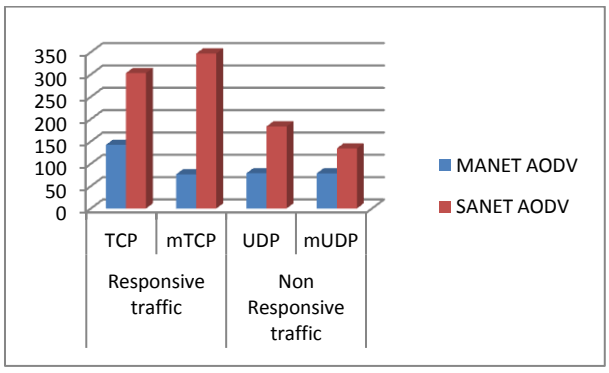

Figure 5: A graph for average throughput for both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) with and without malicious node.

6.2 Average end-to-end delay(s):

The time taken for a packet to travel from a source to destination is called Average end-to-end delay. From the graph below it is observed that average end-to-end delay is increased in both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) when malicious node is introduced.

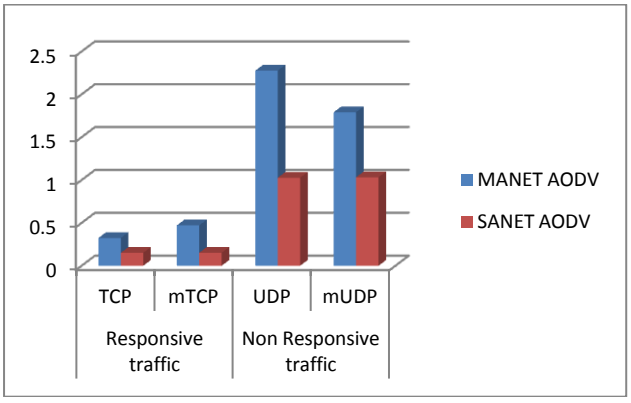

Figure 6: A graph for average end-to-end delay for both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) with and without malicious node.

6.3 Packet Delivery Ratio:

The ratio of the number of packets originated by the "application layer" to the number of packets received by the destination is called Packet Delivery Ratio.

From the graph below it is observed that average packet delivery ratio is decreased in both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) when malicious node is introduced.

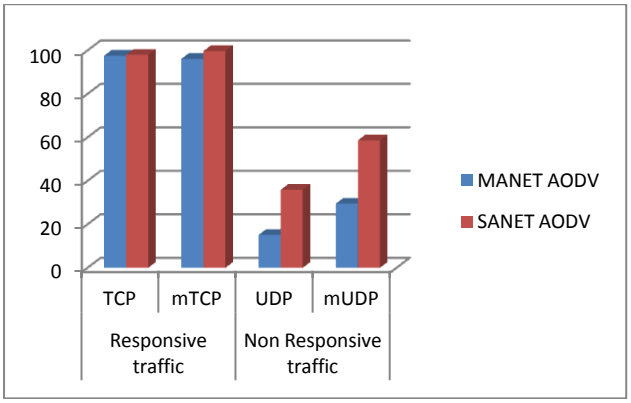

Figure 7: A graph for packet delivery ratio for both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) with and without malicious node.

6.4 Routing Overhead:

The number of control packets produced per mobile node for data packets. Control packets include route requests, replies and error messages.

From the graph below it is observed that routing overhead is decreased in both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) when malicious node is introduced.

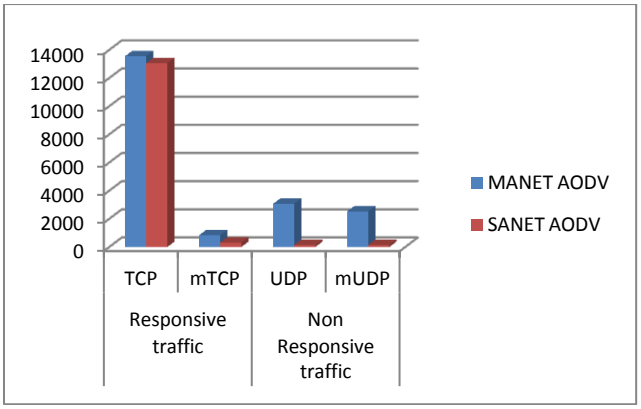

Figure 8: A graph for routing overhead for both MANET and SANET for responsive (TCP) and non-responsive traffic (UDP) with and without malicious node.

7. CONCLUSION AND FUTURE SCOPE OF WORK

Impact of malicious nodes on the performance of AODV routing protocol on throughput is maximum for responsive traffic when compared to non-responsive traffic. Impact is maximum in SANETs and minimum in MANETs.

Impact of malicious nodes on the performance of AODV routing protocol on delay is maximum for non-responsive traffic when compared with responsive traffic. Again when compared with MANETs and SANETs impact is maximum in MANETs.

Impact of malicious nodes on the performance of AODV routing protocol on packet delivery ratio for both MANETs and SANETs is minimum for non-responsive and maximum for responsive.

Impact of malicious nodes on the performance of AODV routing protocol on routing overhead for responsive traffic is high, low for non-responsive traffic and high in MANETs and low in SANETs.

In the future scope of work, we would extend different types of attacks on different routing protocols in MANETs.

8. REFERENCES

[1] S. Corson and J. Macker, "RFC 2501Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration ,"1999.

[2] Constantine Manikopoulos and Li Ling "Architecture of the Mobile Adhoc Network Security (MANS) System" CONEX Laboratory, NJWINS Center

[3] Hsu J.,Bhatia S., Takai M.,bagrodia R. and Acriche M.J.,(2003),"performance of mobile Ad Hoc Networking routing protocols in realistic scenarios", proceeding of IEEE conference on military communications, Vol. 2,pp. 1268-1273.

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

[5] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[6] J. Broch, D. Maltz, D. B. Johnson, Yih-Chun Hu, J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing protocols."Proceedings of the Fourth Annual ACM/IEEE on Mobile Computing and Networking, MOBICOM 98, October 1998.

[7] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv- 05.txt

[8] D.Djen, L. Khelladi, and A.N. Badache, "A survey of of Security issues in Mobile Ad Hoc Network," Communication Surveys & Tutorials , IEEE, vol. 7 no. 4,2005,pp. 2-28.

[9] Cryptography and Network Security – Willian Stallings

[10] Venkataramana Attada, and S. Pallam Setty, "Cross Layer Design Approach to Enhance the Quality of Service in Mobile Ad Hoc Networks" Wireless Personal Communications, DOI 10.1007/s11277-015-2609-6, May 2015, Springer.