

# Routing Misbehavior in MANets and How it Impact QoS!

<sup>1</sup>Avanaksh Singh Sambyal, <sup>2</sup>Prikhshayat Singh

<sup>1</sup>School of Computer and Systems Sciences, JNU, New Delhi, India

<sup>2</sup>6A, G/F, DDA Flats, Nirman Vihar, New Delhi, India

Email: <sup>1</sup>[avasisam@gmail.com](mailto:avasisam@gmail.com), <sup>2</sup>[psingh\\_bioc@rediffmail.com](mailto:psingh_bioc@rediffmail.com)

**Abstract-** Mobile Ad hoc Network is a collection of mobile nodes without support of any infrastructure. Routing in mobile ad hoc networks is achieved through mobile nodes acting as intermediate nodes. These nodes are responsible for receiving and forwarding data packets from one host to another in the network. Routing protocol in present mobile ad hoc network could be of two types: One, is *Proactive routing* which maintain routes to all nodes, including nodes to which no packets are sent (i.e., based on either link-state or distance vector principles) and other, is *reactive* routes establishments i.e., routes between nodes, are determined only when explicitly needed to route packets. *Reactive routing* algorithm is also known as *On-Demand Routing* algorithm. *Routing misbehavior* occurs when nodes agree to forward but some nodes agree and do not forward packets as the node is misbehaving, selfish, overloaded, broken or the software fault is present. Misbehaving nodes are significant problem in MANETs which severely effect the QoS mechanism of network.

**Key words-**Routing misbehavior; black hole attack; malicious node; AODV; NS2; MANets.

## 1. Introduction

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems work with the support of a centralized supporting structure such as an access point. The wireless users can be connected with the wireless system with the help of these access points, when they roam from one place to the other. Wireless systems adaptability is limited by the presence of a fixed supporting coordinate. It means that the technology cannot work efficiently in those places where there is no permanent infrastructure. Easy and fast deployment of wireless networks will be expected from the future generation wireless systems. This fast network deployment is not possible with the existing structure of present wireless systems. Recent advancements such as Bluetooth, Personal area network, IEEE 802.11 [1] a/b/g, etc., introduced a fresh type of wireless systems which is frequently known as *mobile ad-hoc wireless networks*. Mobile ad-hoc wireless networks or "short live" networks work in the absence of permanent infrastructure. Mobile ad hoc wireless network offers quick and horizontal network deployment in conditions where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." A wireless network is a growing new technology that will allow users to access services and information electronically, irrespective of their geographical position. Wireless networks can be classified in two types: - *infrastructure* network and *infrastructure less* (ad hoc) network. Infrastructure network consists of a network with

fixed and wired gateways. A mobile host interacts with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is in communication. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach, the base stations are fixed. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be set up quickly and inexpensively as needed. Such, a network may operate in a stand-alone fashion or connected to the internet. Multi-hop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. Our discussion is related with how routing misbehavior impact the QoS (Quality-of-Service) in MANets. First of all, we should know what the definition of routing misbehavior. Routing misbehavior [4] occurs when mobile node/s may agree to forward the packet/s, then failing to do so. This type of network (that is, MANets) is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. A mobile node may misbehave because it may be selfish, malicious, broken or overloaded. We will consider here Ad hoc On-demand Distance Vector (AODV) protocol implements the misbehaving nodes operating on this protocol. We will calculate parameter related to this protocol for misbehaving nodes present in the network and adversely affecting the quality of service (QoS [10]) of ad hoc wireless network.

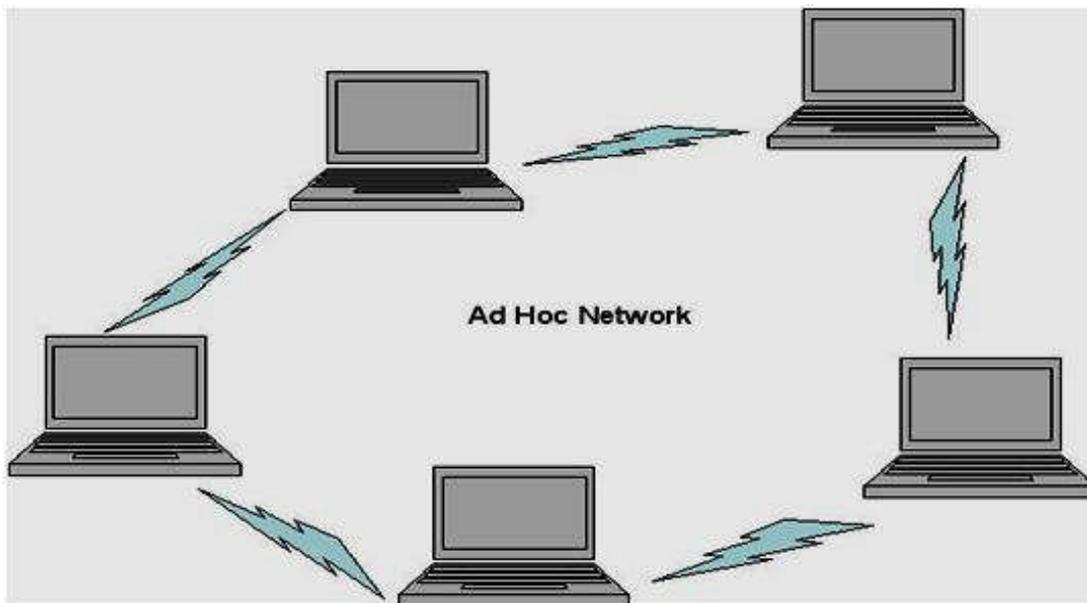


Figure 1. Ad hoc Network

### 1.1. Ad hoc on Demand Distance Vector (AODV)

Ad hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc wireless network [5]. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Due to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV protocol is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number, it (AODV) ensures loop freedom. AODV makes sure that the route to the destination does not contain a loop and has shortest path to its destination. Route Requests (RREQs), Route Reply (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. 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, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh route entry for the destination. Fresh one route means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with

the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards, the RREP message is unicasted to the source node. While the RREQ and the RREP messages are forwarded by the intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE\_ROUTE\_TIMEOUT, a constant value of AODV protocol. The default constant values of the AODV protocol are listed in RFC – 3561[5]. Sequence numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However, when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number means more accurate information and whichever node sends the highest sequence number, its information is considered for route to be established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number (i.e., 4294967295), then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message. In an ad hoc wireless network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets.

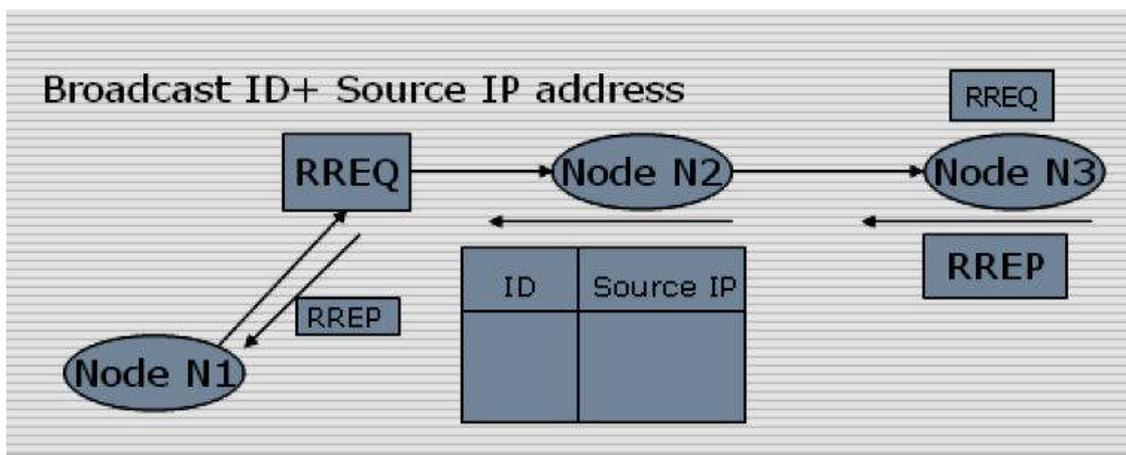


Figure 2. Illustration of AODV protocol

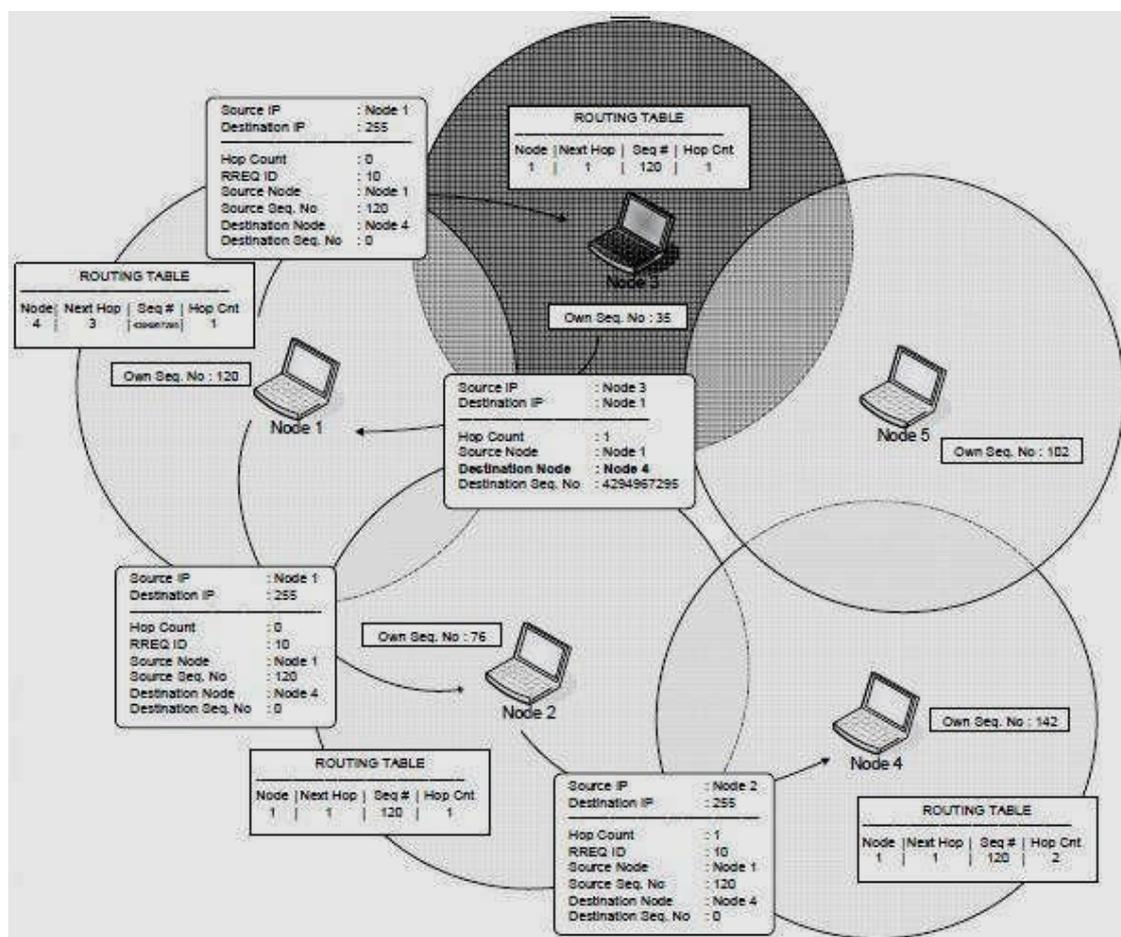


Figure. 3 Illustration of Black hole node misbehavior

### 1.2. Black hole node misbehavior

In this scenario, shown in figure below, we assume that the node 3 is the malicious node. When the node 1 broadcasts the RREQ message for the node 4, the node 3 (bhn)

immediately responds to the node 1 with an RREP message that includes the highest sequence number of the node 4, as if it is coming from the node 4. Node 1 assumes that the node 4 is behind node 3 (bhn) with 1 hop and discards the newly received RREP packet coming from the node 2.

Afterwards, the node 1 starts to send out its data packet to the node 3 (bhn), trusting that these packets will reach the node 4, but the node 3 (bhn) will drop all data packets.

## 2. Methodology used

In our measurement, we have made use of ns-2 simulator on ubuntu-linux OS. UDP, CBR traffic generator in 1000 x 500 m<sup>2</sup> topographical area was taken. 600 nodes were taken and the pause time was varied from 0 to 500 sec. The transmission range is 250 m. Misbehaving nodes were introduced in 8% to 35 % of the overall node. Ad hoc On-demand Distance Vector (AODV) routing algorithm was used to study various metrics namely: network size, bandwidth, traffic pattern, mobility rate and battery power. The metrics affected are packet delay, packet delivery ratio/fraction, overhead ratio and bandwidth utilization which will be used for performance evaluation of ad hoc wireless network. We have run the simulation for number of times until the exact values are obtained for the above said parameters. Thus, we have obtained the graphs of packet delivery fraction/ratio and illustrated the graphs.

## 3. Results and Discussion

In the figure 2 below, it is seen that the packet delivery ratio is lowest at 300 s and 600 s before it takes steep rise to below 80 % value. From this it is confirmed that in AODV, at 300 s and 600 s packet loss (i.e., 54.48 and 87.8) will be more due to the active participation of misbehaving nodes. In the figure 3 below, the delivery rate rises at 100 s then decreases up to 300 s simulation time and then increasing to some proportionate value and then decreasing to value at 600 s. This shows that either battery power is exhausted by some nodes or misbehaving nodes are selfish and assume that other nodes are forwarding the packets. But it is not so and the maximum packet loss is 85.8 % at 600 s simulation time. In the figure 4 below, the packet delivery ratio is at lowest and it is assumed that at initial stages misbehaving nodes have less effect on these parameters such as packet delivery ratio. First it decreases to some value at 200 s and then increases upto 400 s and then decreases to some value at 500 s and 600 s. Therefore, at these points, the packet loss will be more i.e., 87.4% and 89.5% respectively. This shows that misbehaving nodes are more prevalent in AODV as illustrated in graph below. It can be seen from the figure 5 below which shows that the packet delivery ratio first increases upto maximum value below 100 % at 300 s and then starts decreasing to minimum value at 400 s, 500 s and then 600 s respectively due to the presence of misbehaving node. Hence, the packet loss so far obtained is above 80% as can be seen from graph..

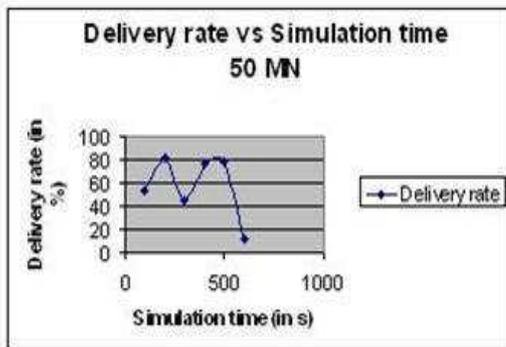


Figure 4. PDR versus Simulation time at 8% of Misbehaving nodes

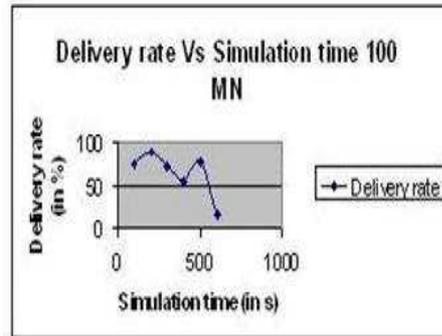


Figure 5. PDR versus Simulation time at 17% of Misbehaving nodes

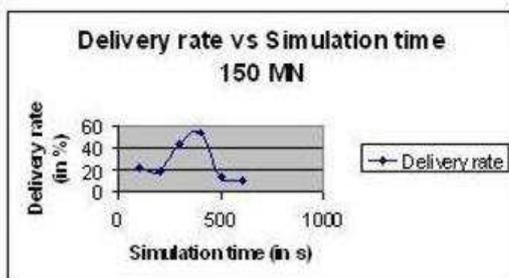


Figure 6. PDR versus Simulation time at 25% of Misbehaving nodes

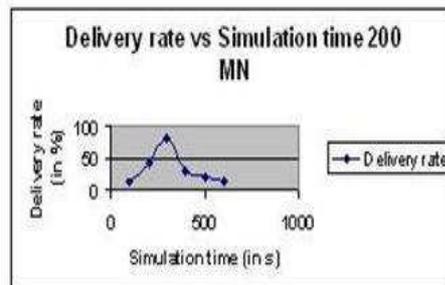


Figure 7. PDR versus Simulation time at 33% of Misbehaving nodes

## 4. Conclusion:

In this research paper,

- We have analyzed the effect of routing misbehavior such as black hole node in the ad hoc wireless network. For this purpose,

- We have designed a new AODV protocol such that the misbehaving nodes (i.e., black hole node) are introduced in MANets.
- We have simulated this protocol at the different simulation times and analyzed the packet loss. Moreover, we have simulated the parameter, namely packet delivery ratio using the different CBR sessions. We can interpret from the graph that the newly designed AODV protocol in MANets has overall 87% packet loss

## References:

- [1] IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard for Information Technology", 1999. <http://standards.ieee.org/catalog/olis/lanman.html>.
- [2] Murthy C. S. R., and Manoj B. S., "Adhoc Wireless Networks: Architecture and Protocols", Prentice Hall, June 2004, Chapter 5 - 12.
- [3] Perkins C. E., and Bhagwat P., "Highly dynamic destination sequenced distance vector routing (dsv) for mobile computers" ACM SIGCOMM: Computer Communications Review, vol. 24, no. 4, pp. 234-244, 1994.
- [4] Marti S., Giulì T.J., Lai K., and Baker M., "Mitigating routing misbehavior in mobile ad hoc networks", in *Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00)*, Boston, MA, August, 2000, pp. 255-265.
- [5] Perkins C., Belding-Royer E., and Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing", Feb.2003. <http://www.ietf.org/internet-drafts/draftietf-manet-aodv-13.txt>.
- [6] Ad hoc on-demand distance vector (aodv) routing. [Online] . Available: <http://www.ietf.org/rfc/rfc3561.txt>.
- [7] Dokurer S., Ert Y.M., and Acar, C.E., (2007). Performance analysis of ad hoc networks under blackhole attacks. *SoutheastCon, 2007, ProceedingsIEEE*, 148 – 153.
- [8] Shurman M. A., Yoo S. M., and Park S., "Black hole attack in wireless ad hoc networks", In: *Proceedings of the ACM 42nd Southeast Conference (ACMSE'04)*, pp 96-97, Apr. 2004.
- [9] Tamilselvan L., and Sankaranarayanan V., "Prevention of Black hole Attack in MANET", Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007. (AusWireless 2007).
- [10] Abbas, A.M. and Kure, Ø., "Quality of Service in mobile ad hoc networks: a survey", *Int. J. Ad Hoc and Ubiquitous Computing*, vol. 6 no. 2, pp. 75 – 98, 2010.
- [11] Zhang, Y. and Wu, L., "Rigid Image Registration by PSOSQP Algorithm", *Advances in Digital Multimedia*, vol.1, no.1, pp. 4-8, 2012
- [12] Iman Sadeghkhan, "Evaluation of Shunt Reactor Overvoltages Using Back Propagation Neural Network", *Advances in Digital Multimedia*, vol.1, no.1, pp. 46-51, 2012
- [13] Armin Ghabousian, Mousa Shamsi, "Segmentation of Apple Color Images Utilizing Fuzzy Clustering Algorithms", *Advances in Digital Multimedia*, vol.1, no.1, pp. 59-63, 2012