INTERNATIONAL JOURNAL OF COMPUTATIONAL MATHEMATICAL IDEAS
ISSN: 0974-8652 / www.sijcmi.weebly.com / VOL 7-NO3-PP 8344-8348(2015)

# IMPLEMENTATION OF RUSHING ATTACK IN MANETS

**J.RAJU PRASAD**
**jogiraju797@gmail.com**

**D.V.RAJESH BABU**
**vrajeshbabud@gmail.com**

**Abstract:** Mobile ad-hoc network (MANETS) is a self-arranging system that is framed suddenly by a gathering of mobile devices by means of remote correspondence channels. Hubs in such a system coordinate by sending data-packets for one another. This permits them to convey past direct remote transmission range. MANETSs don't have brought together organization or settled system foundation. They are frequently conveyed in circumstances where there is no settled system framework. Applications, for example, military portable systems, debacle alleviation and mine site operations, advantage from this kind of systems administration. Attributable to the qualities of MANETSs, for example, absence of infrastructural bolster, powerfully changing system topologies, transparent obliged channels and heterogeneous gadgets, planning specially appointed directing conventions to helps hubs to locate a most suitable routes in such a dynamic domain have been a fascinating examination point as of late. But secure routing is most critical problem various kinds of attacks are possible on MANETSS in those rushing attack is a most focused attack. It effects the performance of the network drastically. Particularly, in this paper we evaluate the rushing attack on AODV and measure the performance using NS2.

## Introduction

Mobile Ad hoc Network (MANETS) is as self-administering arrangement of mobile gadgets dedicated by remote connections, not as a matter of course with any backing from the current framework or whatever other sort of stationary stations, thus it gives high adaptability and they convey rapidly and suddenly. Each gadget works like a framework which forward the information bundle to the following hub subsequently functioning as the switch for the other conveying hosts. Different directing conventions in MaNETSs have been foreseen and these conventions [1] can be ordered into the three classifications: Static (or Proactive), in static routing protocols routes are established before transmission of data happen so for each and every node must maintain some small amount memory.

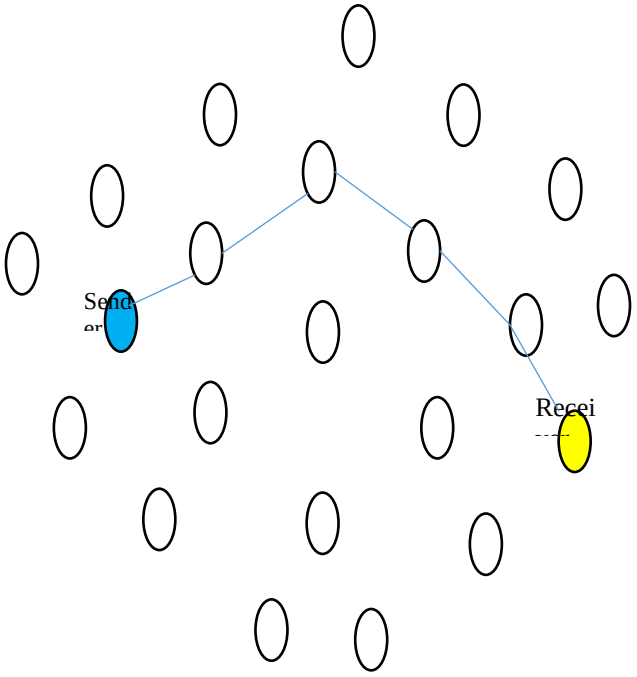


Figure-1: illustration of AODV in MANET

Proactive routing protocols are enclosed with routing information tables at each and every host. And all hosts continuously updates the routing information tables to maintain latest view on the network topology. Dynamic (or Reactive) protocols [1] are establish routes whenever they wants to transmits the data. And

the routes are maintained until the willing ness of the intermediate nodes and the completion of the communication between communicating parties. So here the risk is to establish perfect routes. And Zone based (or Hybrid) routing protocols use both the properties of static and dynamic approaches to make routing. Numerous tests have been done to locate the best routing strategies out of the accessible routing protocols. All experimentations lead to the most utilized and solid convention particularly Ad hoc On-interest Distance Vector (AODV) [2], which is an enthusiastic directing

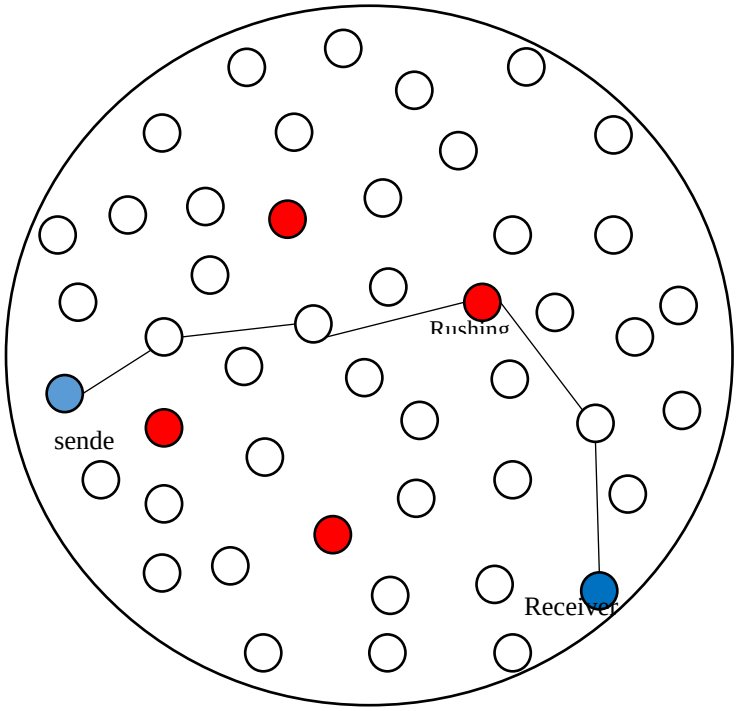


Figure-2: Rushing attacker in MANET

Convention. Be that as it may, the AODV convention has no efforts to establish safety in-implicit it. In this way, it is vulnerable to a few sorts of assaults. The main and most dangerous attack is rushing attack which rushes the routes or channels of the network. So the data items are dropped or not reached to the target. The left behind of the paper is planned as follows section deals with previous works, section-3 deals with impact of the rushing attack on AODV, section-4 focus on simulation modeling and section-5 concludes the paper.

**Existing work:**

We introduce here a new attack, which we call the rushing attack that acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols, including protocols that were designed to be secure. In an on-demand protocol, a node needing a route to a destination floods the network with ROUTE REQUEST packets in an attempt to find a route to the destination. To limit the overhead of this flood, each node typically forwards only one ROUTE REQUEST originating from any Route Discovery. In particular, existing on-demand routing protocols, such as AODV, DSR, LAR, Ariadne, SAODV, ARAN, AODV secured with SUCV, and SRP, only forward the REQUEST that arrives first from each Route Discovery. In the rushing attack, the attacker exploits this property of the operation of Route Discovery. We now describe the rushing attack in terms of its effect on the operation of DSR Route Discovery; other protocols such as AODV [34], Ariadne, SAODV, and ARAN are vulnerable in the same way.

**Impact of rushing attack on AODV:**

AODV is an assortment of Destination-Sequenced Distance-Vector (DSDV) routing strategy which uses the few properties of DSDV. Main working of AODV is composed with two key operations one is route-finding and another is

route-up-dating. Route-finding: A source hub send a RREQ bundle to its neighboring hubs if no path is accessible for the sought destination then the hub shows the route ask for info-packet (RREQ) to achieve the destination. Route-

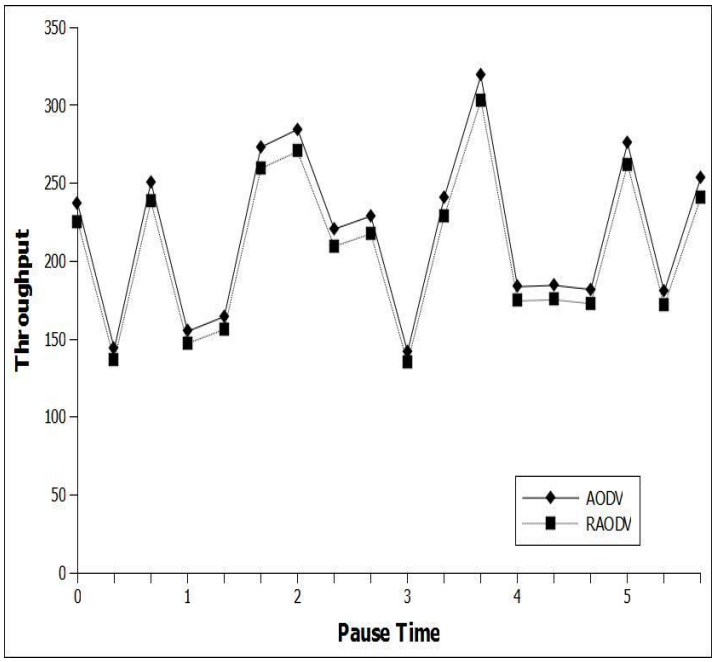


Figure-3: Throughput

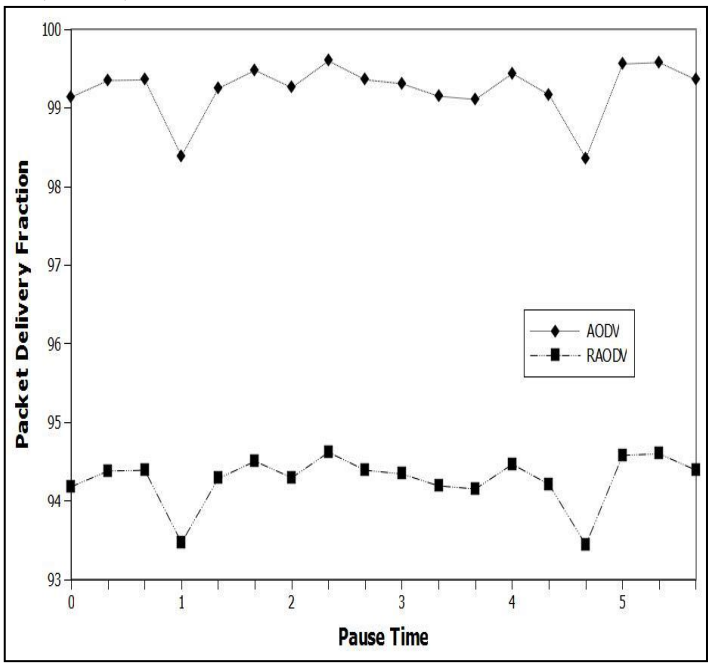


Figure-4: Packet Delivery Fraction

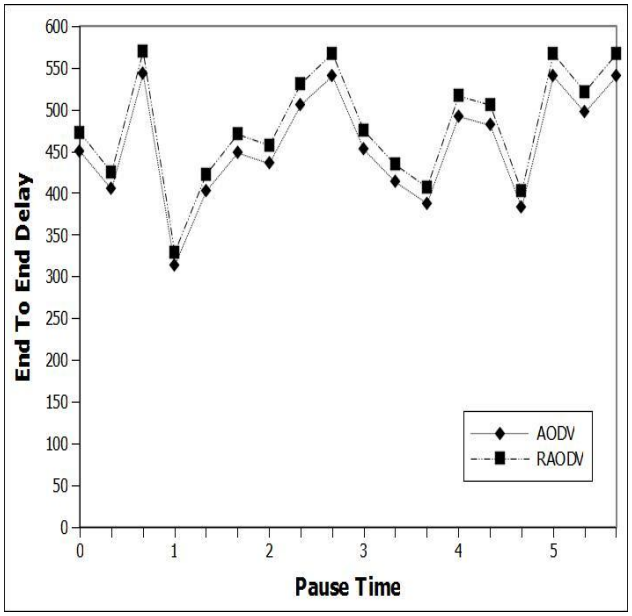


Figure-5: End To End Delay

pointers stay informed concerning the halfway hubs while message being sent to destination hub. At last, when RREQ came to the destination hub, it then send back the RREP message to the source by means of the in the middle of hubs and the retrogressive pointer stays informed regarding the hubs. Course Maintenance: Three sorts of messages traded in the middle of source and destination, for example, course mistake message, hi message and time out message. Route error message guarantees that this message will be broadcast to all hubs in light of the fact that when a hub watches a fizzled path, it will engender this message to its upstream hubs towards source hub just. Hello message guarantees the onward and in opposite pointers from close. Time out message ensures the erasure of connection when there is no movement for a sure measure of time in the middle of source and the destination hub.

AODV directing is totally irritated when there is a worm opening in the system. AODV routing is completely disturbed when there is a rushing attacker in the network. In AODV routing protocol the initiator node initiates a route discovery for the target node. If the route requests for the discovery forwards by the attacker are the first to reach each neighbor of the target node then any route discovered by the route discovery will include through the attacker. That is when a neighbor of the target receives rushed route request from the attacker, it forwards that Request and will not forward any further requests from the route discovery. When non-attacking Requests arrive later at these nodes, they will discard these legitimate Requests. As a result the initiator will be unable to discover any usable routs. In general terms an attacker forwards more quickly then legitimate nodes request this leads more chance of getting routes to the target via an attacker node presents in the routes. So the rushing attacker increase the rush in the paths by forwarding more unnecessary packets in the paths. It leads in decreasing of the routing protocol performance.

**Performance analysis:**

The simulations were performed using Network Simulator 2 (NS-2.35). Random waypoint model is used to generate the mobility scenarios and the nodes moving in a territory area of 1000 X 1000 meters. Hear we uses moderate packet rate and varying pause times to simulation. The simulation parameters are summarized in Table 1.

| Parameter | Values |
|---|---|
| Traffic type | CBR. |
| Number of nodes | 100 |
| Simulation time | 1000 sec. |
| Pause time | 0, 1, 2, 3, 4 and 5. |
| Simulation area | 1000 X 1000 meters. |
| Mobility | 0 to 20 meter/sec. |
| Performance metrics | End to End Delay, Throughput and Packet delivery fraction. |

**Table1: Simulation parameters**

**Performance Metrics:**

This paper analyze the rushing attack in MANET routing protocols under the following three performance metrics.

1. *Packet delivery Fraction/Ratio:* It is the ratio of the number of data packets successfully conveyed to the destination to the number of data packets sent out by the source.
2. *End-to-end Delay:* It is the time taken by the data packets to propagate from source to destination across the network. It contains all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc.
3. *Throughput:* It is the portion of channel capacity used for successful data transmission.

**Performance analysis**

Hear figure-3 shows that the comparison of AODV and rushing attacker AODV under throughput. Rushing attack is a most dangerous attack which is in middle of the source and destination that is in the route and rush the channel between the nodes. So the communication fails between the nodes. Through put means the number of data packets transferred from source host to target. Throughput of AODV is good. But under rushing attacker AODV the throughput decreased drastically.

Hear figure-4 shows that the comparison PDF of normal AODV and RAODV. Due attacker node in the routing AODV performance is decreased largely.

Hear figure-5 shows that the comparison of end-to-end delay of normal AODV and RAODV under end. Rushing attacker is a most dangerous attack which is in middle of the source and destination that is in channel the attacker sends more unnecessary packets. So the communication fails between the nodes. Delay from one end to another end the time taken to travel a packet from source to destination. Delay

done by one end to another end of AODV is high. RAODV having very high End-to-End delay compared to normal AODV.

The performance results shows that the comparison of AODV and RAODV with three performance metrics those are throughput, PDF and delay from one end to another end. Black hole decrease the network performance severely proved by simulation results.

**Conclusion:**

In MANETSS secure routing is most critical problem various kinds of attacks are possible on MANETSS in those rushing attack is a most concentrating attack. It effects the performance of the network drastically. The performance results shows that the comparison of AODV and RAODV with three performance metrics those are throughput, PDF and End-to-End delay. Rushing attack decrease the network performance drastically proved by simulation results.

**References**

[1] S.J. Lee, W. Su, M. Gerla, 2002. On-demand Multicast Routing Protocol in Multihop Wireless Mobile Networks, ACM/ Kluwer Mobile Networks and Applications 7 (6) 441–453.

[2] E.M. Royer, C.E. Perkins, 1999. Multicast operation of the Ad-Hoc On-demand distance vector routing protocol, in: Proceedings of MobiCom'99, Seattle, WA.

[3] Van der Merwe, J., Dawoud, D., and McDonald, S., 2007. A survey on peer-to-peer key management for mobile Ad-Hoc networks. ACM Comput. Surv. 39, 1, Article 1.

[4] Wua, B., Wua, J., Fernandeza, E., Ilyasa, M. , Magliveras ,S., 2005. Secure and efficient key management in mobile Ad-Hoc networks. Elsevier.

[5] Gerla, M., 2005. Ad-Hoc Networks. Springer.

[6] Giordano, S., 2002. Mobile Ad-Hoc Networks.Wiley.

[7] Wu, J., Stojmenovic, I., 2004. Ad-Hoc Networks. IEEE Computer Society.

[8] Hu, Y-C., Perrig, A., Johnson, D., 2003. SEAD: secure efficient distance vector routing for mobile wireless Ad-Hoc networks.Elsevier B.V.

[9] R.V. Boppana, S. Konduru, 2001.An adaptive distance vector routing algorithm for mobile, Ad-Hoc networks, in: Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001).

[10] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, 2001. Optimized Link State Routing Protocol, Internet-draft, draft-ietf-manet-olsr-05.txt.