Asian Journal of Convergence in Technology *Volume III, Issue III*
ISSN No.:2350-1146, I.F-2.71

Modification in AODV for preventing Black hole Attack and increasing energy efficiency

Ruchi Kumari
Dept. of Computer Science and Engineering
Institute of Technology, Guru Ghasidas Vishwavidyalaya
Bilaspur, India

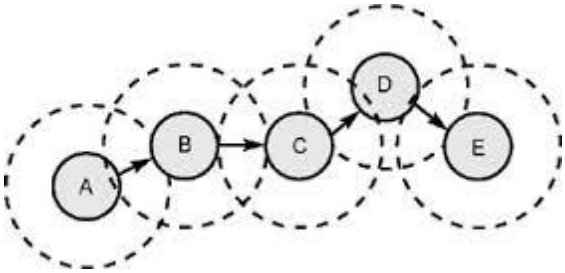
Nishi Yadav
Asst. Prof, Dept. of Computer Science and Engineering
Institute of Technology, Guru Ghasidas Vishwavidyalaya
Bilaspur, India

• *Abstract*— **Mobile Ad-hoc Network or MANET is basically a collection of mobile nodes. It is connected in a dynamic manner that is it has the property to change according to changing topology due to the lack of centralized nodes. Nodes are free to move about arbitrarily. This leads to difficult task of route maintenance in MANET. Nodes in MANET communicate with each other through various protocols. So, it is essential to identify which routing protocol works best for routing in MANET. For that we have analyzed most commonly used protocols viz AODV, DSR and DSDV on various parameters. We continue our study restricted to the AODV (Ad hoc On-demand Distance Vector) Routing protocol (since it is the most appropriate protocol for MANETs). The dynamic nature of MANET also poses a major problem for it. It is accessible to both legitimate user and attacker since it does not have a clear line of defense. A MANET becomes highly vulnerable to various attacks. The most common and prominent of all the attacks is Black Hole Attack. So we have to formulate a security solution to prevent the attacks. In order to do this, we have pre-identified all the malicious nodes in the network and then carry on routing so the network is not affected by malicious nodes and its performance not deteriorated by it. Also we make some improvements in physical nodes in order to improve the energy of nodes in the network.**

Keywords— MANET; AODV; blackhole attack

I. INTRODUCTION (*HEADING 1*)

MANET is a collection of various independent mobile nodes that are dynamic in nature. They communicate with each other via radio waves. It does not have a fixed infrastructure for instance access point etc. There is no centralized control or administration. The nodes act as both sender and receiver. The basic advantage of using MANET is that; MANET attracts different real world application areas where the networks topology changes very quickly. They are mainly useful at places where the communication cannot be done easily or through wired networks. There are many geographical routing protocols for MANET. Most primarily used are AODV, DSR and DSDV. We have simulated these protocols on NS2.35 and compared the results to see which protocol gives better results. MANETs are highly susceptible to attacks, they provide less security due to moving nodes. Power consumption also becomes considerable due to dynamic nature and changing topology. The bandwidth is limited and also the zone within which a node can send the data is limited.



A: Sender B: Reciever
Figure 1: Mobile Adhoc Network

A. MANET Routing Protocols:

The route is determined when source broadcasts RREQ message. Route in reactive protocols is determined if RREQ reaches destination or one of the intermediate nodes. The destination on receiving the packets sends RREP message to the source. In proactive protocols routes are decided on the basis of tables maintained by each node.

Proactive Routing (Table Driven): These are table-driven routing protocols that maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols enables updating of routing information and routing table according to the changes in network topology. The major disadvantages of these algorithms are- requirement for maintainence of a large amount of data at each node since all the nodes needs have the information of every other node and slow reaction on failures.

Eg: DSDV (Destination Sequence Distance Vector)

Reactive Routing Protocol (On-demand): Reactive Routing protocols create routes on demand and are seemingly more suitable for adhoc networks. The route in these kind of protocols are determined by flooding the network with Route Request (RREQ) packets.

Eg: AODV (Ad hoc On-demand Distance Vector),
DSR (Dymanic Source Routing)

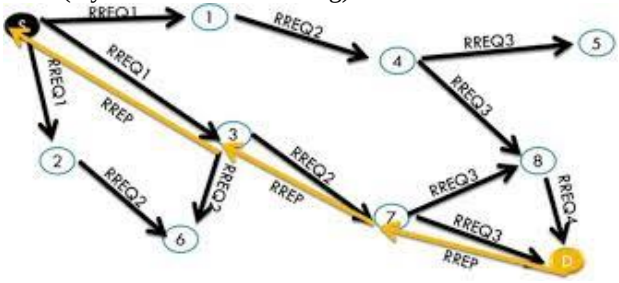


Figure 2: Route Discovery in MANET

B. AODV (Adhoc On Demand Distance Vector)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is based on the DSDV as well as DSR algorithm. AODV is an improvement on DSDV. It minimizes the number of required broadcasts by creating routes only when needed that is, on demand basis. It uses traditional routing tables, one entry per destination unlike DSR, which can maintain multiple route cache entries for each destination. AODV uses routing table entries to propagate an RREP the source and to route data packets to the destination. AODV uses sequence numbers maintained at each destination to prevent routing loops. All routing packets carry these sequence numbers. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighbouring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs.

II. ATTACKS ON MANET

The MANET (Mobile Adhoc Network) is vulnerable to several types of attacks. Due to unique characteristics of MANET, there is very much threat of malicious attacks on MANET. Attacks on mobile ad hoc networks can be classified into following two categories:

Passive Attacks:

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it.

Active Attacks:-

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

The most common of attacks in MANET is the Blackhole Attack. We will study the effect of this attack on AODV routing protocol (that is, the most suitable routing algorithm according to our results).

A. Black hole attack:-

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum or the shortest route and causes other good nodes to route data packets through the malicious one. If source node wants to send data packets to destination node it ignores all other reply messages and begins to send data packets to the malicious node since it claims that it has the shortest route to the destination. If the response from the malicious node reaches first to source node then node S thinks that it has the shortest route, when routing begins all packets through the malicious node is consumed or lost.

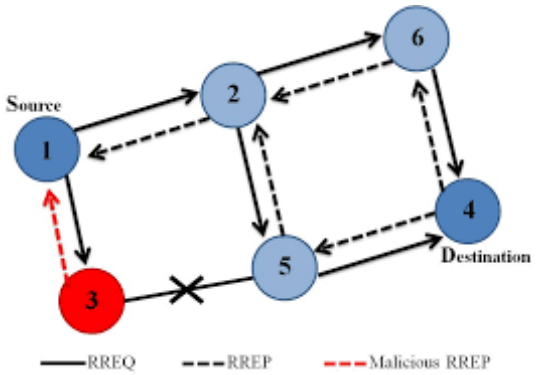


Figure 3: Black Hole Problem in MANET

B. Introduction to MAC layer of ns2.35:

The MAC layer or the physical layer is responsible to transfer packets from upper layer to lower layer. We can improve the energy consumption by improvement in these nodes.

III. PROPOSED APPROACH

We will study the effect of Blackhole attack on AODV protocol and also try to improve its efficiency. AODV proves to be better of the most commonly used protocols that is amongst DSDV, DSR and AODV.

Table I: Simulation Environment for mentioned protocols

Simulator	NS2.35

Protocols	AODV, DSR, DSDV
Simulation Time	500 msec
Topology	Random
Traffic Type	CBR (Constant Bit Rate)

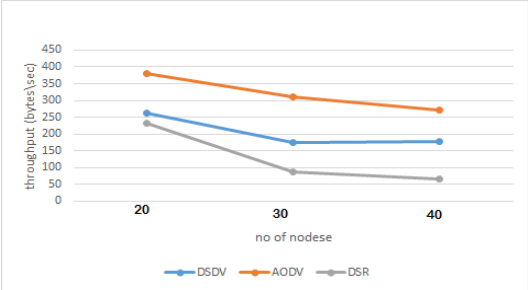


Figure 4: Throughput vs no. of nodes

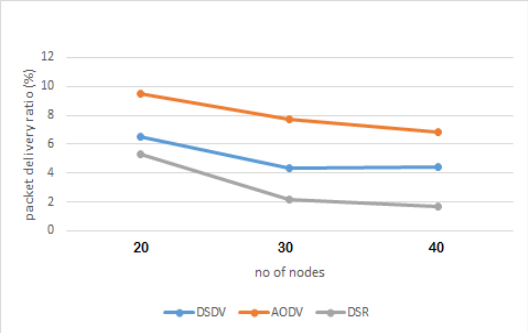


Figure 5: PDR vs no. of nodes

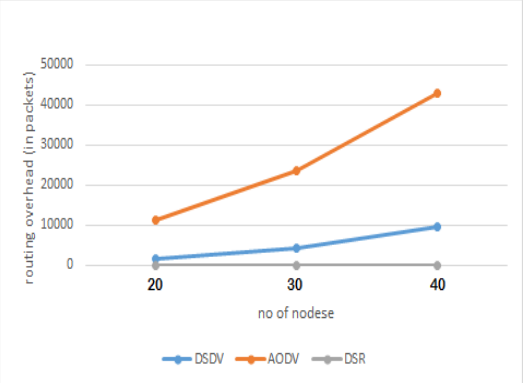


Figure 6: Routing Overhead vs no. of nodes

It is clearly evident that AODV protocol is better than other protocols in these parameters. Therefore we extend our analysis and study to AODV protocol.

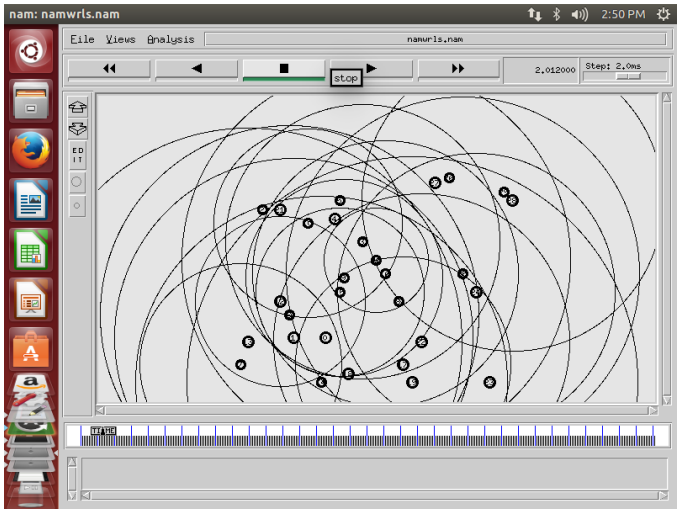


Figure 7: Simulation of AODV Protocol in NS2.35

A. Proposed Algorithm

1. Identification of malicious node
   - Step1: Source node broadcasts RREQ to neighbours
   - Step2: Source node receives RREP from neighbours
   - Step3: Source node selects shortest and next shortest path based on the number of hops.
   - Step4: Source node checks its routing table for single hop neighbouring nodes only.
   - Step5: If the neighbour node is in its routing table then route data packet
   - Else
   - The node is malicious and sends false packets to that node
   - Step 6: Invoke the route discovery
   - Inform all the neighbouring nodes about the stranger along with node sequence number.
   - Step 7: Add the status of stranger to the routing table of source node.
2. Improvement in energy
   - Step1: Keep a count of number of packets sent.
   - Assign priority on the basis of node sequence and shorter path and broadcast priority.
   - Start timer T.
   - Send the packets to the node with highest priority and check if a node has crossed the number of packets to be sent/received. If yes, make the node to sleep.
   - If timer lapses that is, T=0 make the node to sleep.
   - Make the node active after some time (say T).

We implement black hole attack on existing AODV and modified AODV and check for the differences between them and which protocol is better to withstand attacks.

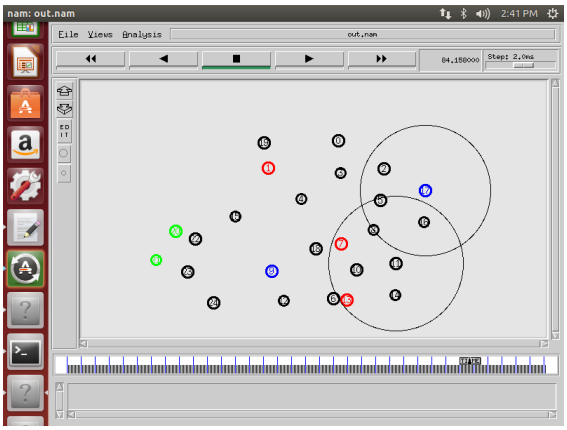


Figure 8: Simulation of Black Hole in AODV protocol Attack in ns2.35

Table II: Simulation Environment for comparison of AODV and modified protocol

Simulator	NS2.35 and NS2-VisualTraceAnalyzer
Protocol	AODV
Topology	Random
Traffic Type	CBR

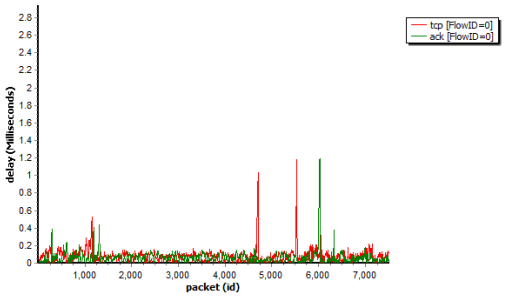


Figure 9: Delay in modified protocol after attack

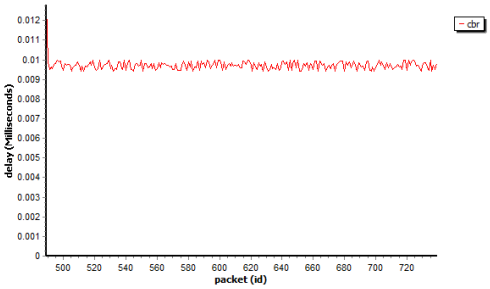


Figure 10: Delay in original protocol after attack

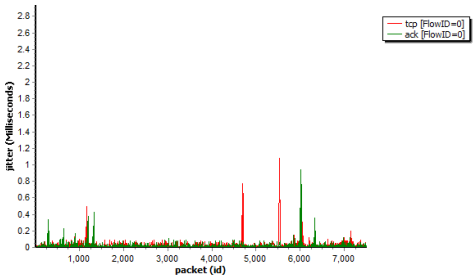


Figure 11: Jitter in modified protocol after attack

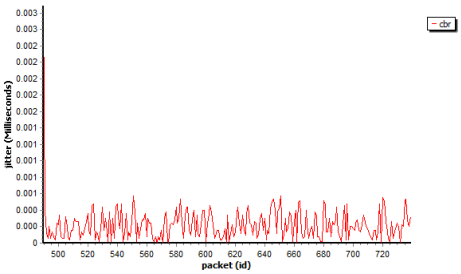
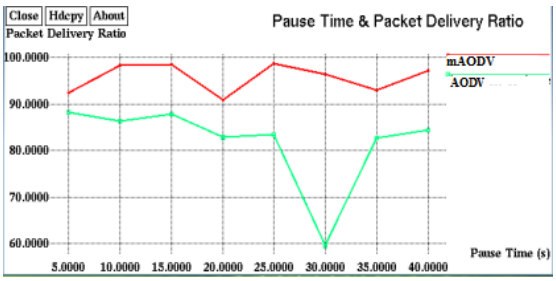


Figure 12: Jitter in modified protocol after attack



mAODV: Modified AODV

Figure 13: Comparison between modified and original protocol after implementation of Black hole Attack (after implementation of malicious node) [on PDR vs Pause Time].

The modified protocol offers better packet delivery ratio and works better even under attack therefore offers better routing efficiency. It offers lesser jitter and delay under attack. The new protocol thereby, offers better security feature and functions more efficiently under attack. The modified protocol detects and isolates malicious node while routing.

Our aim is also to minimize the energy consumption for this we make changes in the physical layer nodes. Physical layer is responsible for transferring packets from upper layer to lower layer and vice versa.

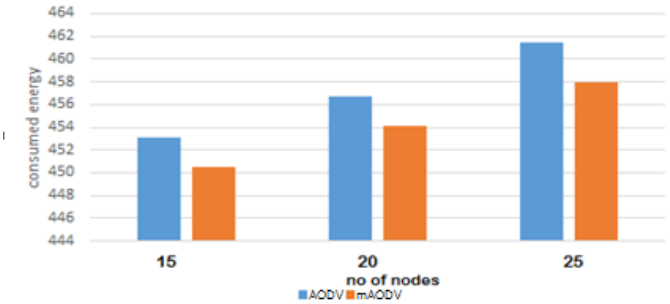


Figure 14: Energy consumption comparison between mAODV and AODV

We thus see that the energy consumption in modified protocol is lesser thus, it is more efficient.

IV. Litreture Review

[1] In Nov 2010, "Review of Security Attacks in Mobile Adhoc Network" by Priyanka Goel, Sahil Batra and Ajit Singh, it was stated that MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers.

[2] In June 2013, "A Survey of attacks in MANET" by Manjeet Singh and Gaganpreet Kaur analyzed the security threats an ad-hoc network faces and presented the security objectives that need to be achieved.

[3] In April 2012, "Issues and Behaviour of Routing Protocols in MANET" by Gurpinder Singh and Jaswinder Singh to provide a means of understanding the issues and protocol (OSPF, DSR, AODV, TORA, OLSR, DSDV) of MANET and investigating behavior of DSR,AODV,TORA.

[4] In 2013, "Performance Analysis of Black Hole Attacks in Geographical Routing MANET" by E.A. Mary and H.J. Shanthi. This paper aims to ensure security against the black hole attack and analyze the performance in geographical routing.

[5] In August 2016, "IEEE Risk Aware Mitigation for MANET Routing Attacks" by Sobin, stated that among various attacks of MANET routing attacks have received considerable attention since it could cause the most devastating damage to MANET.

Conclusion and Future Scope

We conclude that AODV is a better suited for MANETs on the parameter tested. Thus we analyze the effect of attacks on it for reference. We examine black hole attack deteriorates the efficiency of the AODV protocol by a very large extent. Thus we conclude it is important to predetermine the attack (malicious node) in order to prevent it.

In future works can be extended to other layers for efficiency and also we could append location aided path finding methods (using GPS) for better results. We could extend our study to other protocols and other attacks too.

References

[1] Priyanka Goel, Sahil Batra and Ajit Singh, "Review of Security Attacks in Mobile Adhoc Network" ,Nov 2010.

[2] Manjit Singh and Kamaljit Kaur, "Various Attacks in MANET and its Countermeasures", April 2014.

[3] Manjeet Singh and Gaganpreet Kaur, "A Survey of attacks in MANET", June 2013

[4] Gurpinder Singh and Jaswinder Singh, "Issues and Behaviour of Routing Protocols in MANET", April 2012.

[5] Amit Shrivastava, Nitin Chander, Avinash Mistry, Prashanth Patlolla, "Overview of Routing Protocols in MANET and Enhancements in Reactive Protocols", 2009.

[6] Shraddha Raut and S.D. Chede, "Detection and Removal of Black Hole in Mobile Adhoc Network", 2014.

[7] E.A. Mary and H.J. Shanthi, "Performance Analysis of Black Hole Attacks in Geographical Routing MANET", 2013.

[8] Identification and Alleviation of MANET Routing Attack Risks by Dakshayani G and Amol P Pandey, July 2013.

[9] Athira V Panicker and Disha G, "Network Layer Attacks and Protection in MANET", 2014.

[10] Arnab Banerjee and Dipayan Bose, "Different types of attacks in Mobile Adhoc Network: Prevention and Mitigation", 2013.

[11] Sobin on IEEE Risk Aware Mitigation for MANET Routing Attacks, August 2016.

[12] Qing Fang, Jie Gao and Leonidas J Guibas, "Locating and Bypassing Holes in Mobile Network", 2006.

[13] Mohammad A. Mikki, International Journal of Computer Science and Information Security, "Energy Efficient Location Aided Routing for Wireless MANETs", 2009.

[14] Sushil Kumar, Dinesh Singh & Mridul Chawla "Performance Comparison of Routing Protocols in MANET Varying Network Size"

[15] Nurul I. Sarkar & Wilford G. Lol "A Study ofMANET Routing Protocols: Joint Node Density, Packet Length and Mobility" 978-1-4244-7755-5/10/$26.00 ©2010 IEEE Page no. 515-520

[16] Vasudha Arora & C. Rama Krishna "Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions" 2010 2nd International Conference on Computer Engineering and Technology [Volume 6] 978-1- 4244-6349-7/10/$26.00 c 2010 IEEE

[17] Ian D. Chakeres and Elizabeth M. Belding-Royer. AODV Routing Protocol Implementation Design.

[18] Patel, B.; Srivastava, S.; , "Performance analysis of zone routing protocols in Mobile Ad Hoc Networks," Communications (NCC), 2010 National Conference on, vol.,pp.1-5, 29-31 Jan. 2010.

[19] Toh,C.-K.;Delwar, M.; Allen,D.;"Evaluating the communication performance of an ad hoc wireless network," Wireless Communications, IEEE Transactions on , vol.1, no.3, pp.402-414, Jul 2008

[20] [8] NS-2, The ns Manual (formally known as NS Documentation) available at http: //www. isi.edu/nsnam/ns/doc

[21] Mohammad Al-Shurman & Seong-Moo Yoo, Seungjin Park, (2004) "Black hole attack in mobile ad hoc networks", Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, pp. 96- 97.

[22] Gaurav Sandhu & Moitreyee Dasgupta, (2010) "Impact of blackhole attack in MANET", International Journal of Recent Trends in Engineering and Technology, Vol. 3, No. 2.