ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 06, pp.32484-32486, June, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

STUDY FOR PERFORMANCE ANALYSIS OF AODV WITH AND WITHOUT BLACK HOLE NODES

***Shikha Sharma**

Research Scholar, CSE, CGCCOE, Landran (Mohali)

ARTICLE INFO

Article History:
Received 23rd March, 2016
Received in revised form
19th April, 2016
Accepted 26th May, 2016
Published online 15th June, 2016

Key words:
AODV,
Routing,
Blackhole,
Protocols.

ABSTRACT

Mobile ad hoc network (MANET) is a group of portable hosts without the required intrusion of any existing arrangement or centralized access point such as a base station. Due to the major characteristic of MANETs i.e. vigorous topology and lack of centralized management security, MANETs are vulnerable to attacks. Black hole attack is one of the possible attacks in MANET. A black hole attack is network layer attack in which the mischievous node misleadingly advertises to the source node that it is having shortest path to the destination and actually it does not have and drops the packets and as a result the destination node never receives that packet. In this paper, we study the behavior of AODV (Ad hoc on Demand Distance Vector Routing Protocol) with and without black hole nodes on various parameters like End to End delay, Packet delivery ratio, Throughput and Routing Load. All the parameters are analyzed using NS2 simulator.

Citation: Shikha Sharma, 2016. "Study for performance analysis of AODV with and without black hole nodes", *International Journal of Current Research*, 8, (06), 32484-32486.

INTRODUCTION

When there is no infrastructure to communicate or the equipment's which are to be used are expensive then the wireless mobile users can communicate through an ad hoc network. In the ad hoc network the nodes which are involved act as a host and also as a router. The communications between the nodes are quickly and spontaneously. The route between the nodes in the network could be several different paths. (Choudhary and Kunal, 2012) This permits the network to have different connection with in the network.

Routing Protocols

The primary goal of routing protocols in ad hoc network is to found the best path between source and destination with minimum overhead and minimum bandwidth utilization so that packets are delivered in a appropriate manner to the appropriate destination. Routing protocols are divided into three categories proactive, reactive and hybrid protocols, depending on the topology in which the nodes are arranged in the network. Proactive protocols are typically table-driven. Reactive or source-initiated on-demand protocols, in opposing, do not occasionally update the routing information. It is propagated to the nodes on demand. Hybrid protocols involve both types of protocols reactive and proactive approaches.

Proactive Routing Protocol

In a network where the protocol which is used is Proactive Routing Protocol, each and every node maintains various tables in order to maintain the information regarding the topology of the network. These tables are updated whenever any change is there in the topology due to dynamic topology in the network. These tables have up to date information about the topology of the network on regular basis. On the other hand the routes which are provided will be available on the request. Example of Proactive routing protocol is OLSR (Optimized Link State Routing Protocol).

Reactive Routing Protocol

In reactive routing protocols are the protocols which work when the network requests. Routing information is updated whenever it is needed and route is determined depending on sending on sending the queries throughout the network.

Example of Reactive routing protocol is AODV (Ad hoc on Demand Distance Vector Routing Protocol).

****Corresponding author: Shikha Sharma,***
Research Scholar, CSE, CGCCOE, Landran (Mohali)

Hybrid Routing Protocol

In hybrid routing protocol is the combination of Proactive and Reactive routing protocol and all the nodes are ordered in groups so as to which node is Proactive or Reactive. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. (Lakshmi *et al*., 2010)

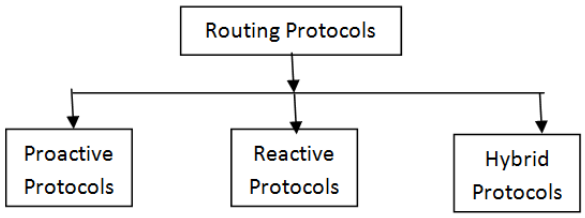

Fig. 1. Types of Routing Protocols

Working of AODV

AODV (Ad hoc on Demand Distance Vector Routing Protocol) is a reactive protocol in which the routing information is updated on need. This protocol is divided into two categories (1) Route Discovery and (2) Route Maintenance. AODV uses Route Request (RREQ) and Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. In AODV, when a source node needs to converse with other node for which no routing information is updated then Route Discovery process gets initiated by sending a Route Request (RREQ) to all its neighbors. Once the neighboring nodes wants to reply the request then Route Reply (RREP) is sent back to the source node or the neighboring nodes can send the RREQ to their own neighbors. Whenever the frequency of sending the RREQ is increased the value of hop_count field also get increased. The sequence number for the nodes specifies the freshness of a path to the destination.

Routing table has the below information:

- Destination node
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for the route
- Expiration timer for the route table entry (Lakshmi *et al*., 2010)

If the link is broken then the node receives the notification about the broken state of link and the RERR control message is broadcasted to the nodes which are involved. And then the source node of the network again starts with the discovery process.

Blackhole Attack

Routing protocols are visible to a variety of attacks. Black hole attack is one of the attacks and it is a kind of Denial of Service (DoS) attack in which a mischievous node makes use of the weaknesses of the route discovery packets of the routing protocol to announce itself as having the optimal path to the destination whose packets it wants to catch. When the Route Discovery process starts, the source node sends RREQ packets to the in-between nodes to find fresh path to the planned destination. Mischievous nodes reply immediately to the initiating node as these nodes do not discuss with the routing table. The initiating node assumes that the route discovery process is complete, disregards other RREP messages from other nodes and selects the path through the mischievous node to route the data packets. The mischievous node does this by assigning a sequence number which is high to the reply packet. The black hole node now drops the message received in its place of relaying them as the protocol requires.

Related Work

In (Perkins and Bhagwat, 1994), the authors discuss a protocol in which the intermediate nodes send RREP message with the next hop information regarding that node. When the source node gets the hop and reply information, then the source sends a RREQ to the following hop to confirm that the target node really has a route to the in-between node and to the destination. When the next hop receives a Further RREQ Request, it sends a Further RREP Reply which includes the result of confirmation to the source node. Based on information in Further Reply, the target node comes to know about the validity of the route. In this protocol, the RREP packet is changed to contain the information about next hop. When RREP message is received, the source node again sends request to the node specified as the next hop in the received reply. Obviously, this increases the routing overhead and end-to-end delay. In (Shurman *et al*., 2004), the authors define a protocol in which the source node confirms the validity of a node that starts sending RREP by finding multiple routes to the destination. When source node receives RREPs, if one node is sharing more than one route to destination, source node can identify a safe and optimal route to destination.

In Sanjay Ramaswamy, *et al*. (Huang and Lee, 2004) suggested a method for recognizing multiple black hole nodes. They are the first authors to propose clarification for cooperative black hole attack. They modified AODV protocol by introducing data routing information table (DRI) and cross checking. Each and every changed behavior of the node is maintained by the table. They trust on the nodes which are reliable to transfer the packets. In (Huang and Lee, 2004) the authors defined a solution which can avoid the multiple black holes with the various changes in the AODV protocol. It was supposed that the nodes which are participating are valid nodes and can get involved in the communication. In this solution the node which is participating is given a fidelity level which assures the reliability of that node and this level is stored in the fidelity table. If the fidelity level of any node is 0 then that node is malicious and it is removed from the network itself. In (Bala *et al*., 2009) authors studied the behavior of ad hoc network under black hole attack on AODV routing protocol. Black hole attack is simulated with the help of network simulator (NS-2). The results show the packet loss, throughput, and end-to-end delay in both the scenarios with black hole and without black hole. It has been examined that the packet loss increases if

there is a black hole node in the network. It has also been observed that the throughput and end to end delay decreases with a black hole node.

Conclusion

Black hole attack is the major security difficulty in MANET. In this attack the malicious node advertises itself that through this path the optimal route will be followed but as a result the black hole node actually drops that message in between and destination node never receives that message packet. In this review paper, different methods for analyzing the behavior of AODV with and without black hole attack has been studied with the parameters like End to End delay, Packet delivery ratio, Throughput and Routing Load. After studying the behavior of the parameters it concludes that the throughput and packet delivery ratio decreases due to black hole nodes because in between these nodes drop the messages. Whereas the delay and routing load increases as the black hole node increases congestion in the routes which are revealed. These results of the metrics conclude that the network performance is degrading predominantly in the presence of black hole attack.

REFERENCES

Bala, A., Bansal, M., Singh, J. 2009. "Performance Analysis of MANET under Blackhole Attack" In Proceedings of IEEEInternational Conference on Networks and Communications, NETCOM '09., pp.141 – 145

Choudhary A. and Kunal, 2012. "Performance Evaluation of AODV under Blackhole attack", *International Journal of Emerging Technology and Advanced Engineering IJETAE*, ISSN: 2250-2459, Volume 2, Issue 5.

Ghonge M. and S.U. Nimbhorkar 2012. "Simulation of AODV under Blackhole attack in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering IJARCSSE*, ISSN:2277 128X, Volume 2, Issue 2.

Huang Y. A. and W. Lee, 2004. "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera.

Lakshmi, K., S. ManjuPriya, A. Jeevarathinam, K.Rama and K. Thilagam, 2010. "Modified AODV Protocol against blackhole attacks in MANET*", International Journal of Engineering and Technology,* Vol 2(6), 444-449.

Perkins C. and P. Bhagwat, 1994. "Routing over multihop wireless network for mobile computers". SIGCOMM '94 : Computer Communications Review: 234-244.

Shurman M. A., S. M. Yoo, and S. Park, 2004. "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97.

Tamilselvan, L. Sankaranarayanan, V. 2008. "Prevention of Blackhole Attack in MANET", *Journal of Networks*, Vol.3, No.5.

****