GADL Journal of Inventions in Computer Science and Communication Technology (JICSCT)
Volume 1 – Issue 1, December, 2015

A Survey on Route Maintenance and Attacks in AODV Routing Protocol

Pushpendra Dwivedi
Pranveer Singh Institute of Technology
Kanpur, U.P. (208020)
U.P.T.U., Lucknow

Saurabh Gupta
Pranveer Singh Institute of Technology
Kanpur, U.P. (208020)
U.P.T.U., Lucknow

Abstract: Mobile ad-hoc network is a self configuring multi hop wireless network that's infrastructure and topology changes frequently. As the links in the wireless networks goes down very frequently due to highly dynamic environment, therefore, routing becomes a critical task. In the genre of reactive protocols, Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in Mobile ad-hoc Networks (MANETs). The no. of broadcasts are minimized by AODV, with the creation of routes only when the routes are needed. Routes are maintained locally. This protocol is loop free and single path. This Paper is a survey about what are the different types of attacks can occur in AODV routing Protocol and How the route Maintenance works in this protocol. This paper shows the process of creation of routes, then the types of maintenance and then at last the possible route attacks in AODV.

Key Words: *MANET, routing protocol, node, packet, route.*

I. INTRODUCTION

Rapidly changing technology of wireless communication network allows people to share information any time and from anywhere. An Ad-hoc network [1] is a self configuring network it means that it will be configured automatically and collection of autonomous mobile nodes in which connection is establish for one session and after the establishment of connection any router or wireless base station is not required. A wireless network can be classified on the basis of how the nodes are interconnected. They can be classified in two main categories network with fixed infrastructure (centralized) and wireless Ad-hoc network (non-centralized). A wireless network faces many challenges [2] like transmission area, nature of wireless medium, mobility, battery constraints and security. Selecting the best possible path in a network (it can be wired or wireless) and also considering the challenges of wireless network is called the routing. Routing [3] becomes a key issue in wireless mobile network due to its distributed and dynamic nature. The wireless routing protocols are categorized into three basic categories [4]. Proactive routing protocols that are table driven, reactive routing protocols that are on demand and hybrid routing protocols means the mixture of both proactive and reactive. The proactive routing protocols that are also called table driven, generally use an algorithm that is link state routing algorithm. To maintain up to date information of routes the topology information need to be exchange between the nodes frequently, it causes high overload on the network. Reactive protocol that are also called on demand protocols, these finds routes on Demand by flooding the network with RRP''s that is Route Request packets. The reactive routing protocol generally uses distance vector algorithms that generally have information about next hop of the neighbor node and cost for all known destinations. Hybrid protocols are the protocols, those are combined with both reactive and proactive routing protocols. On the other hand the main advantage is that the route will be always remains on demand. Various protocols have been developed for network having no fixed infrastructure (non-centralized). Selection of routes affects the performance if the network in terms of power consumption.

This paper provides a brief review of AODV (Ad-Hoc on Demand Routing) protocol, the properties of AODV, merits and demerits and comparison with different protocols.

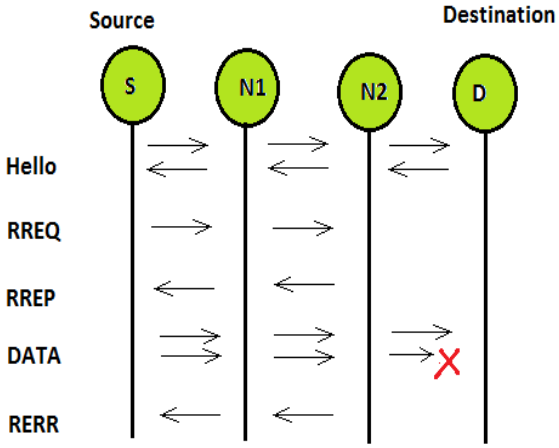

Figure 1 AODV Protocol Messing

II. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

AODV [5, 6] is widely used routing protocol in wireless ad-hoc network. It is based on the approach of Bellman-Ford algorithm. AODV works on wired as well as wireless medium when a link between sources to destination exists. AODV follows a proactive (on demand) approach hence AODV does not require the periodic exchange of routing table.

The main advantages of AODV are that quickly adaptation of dynamic link conditions, network utilization is low, low processing overhead and a unicast route is determined from source to destination. The entries of routing table will be checked when a source node wants to send the data to destination node, to check the validity of the route to destination. AODV uses Hello message (Beacon) to determine link to its neighbor. Each node periodically broadcast Beacons to its entire neighbors. Any node that receives a Beacon is considered as a neighbor node and added to its routing table. If a node does not receive any Beacon then there is a link break.
Control messages: Route request, Route reply, Route error, Hello messages are the control messages [6, 7] used in AODV.

III. ROUTE CREATION

The process of route creation starts from checking the routing table entries for the path or link to destination when a source node has data packet to send. When the valid route is not found in routing table from source to destination, then in AODV protocol a route request (RREQ) packet has been broadcasted across the network [8]. AODV ensures loop free routing by using sequence number. A parameter that is called DestSeqNum that is destination sequence number is used by AODV protocol to determine the path to the sink. If the destination sequence number of the packet received is greater than or equal to the last destination sequence number then the route of the node is updated. When a node recives a RREQ then it will either forward it to to a valid route or it is a destination node. When a RREP is received by a source node then it copies the route from it and can begin transmission of the data.

A route request contains following entries in its routing table:

- Source address
- Destination address
- Request id
- Source sequence number
- Destination sequence number
- Time to live
- Hop count

If a node receives an already processed RREQ packet then it discards the packet. The validity of a node is determined by comparing the sequence number at that node with the destination sequence no in the route request packet. All intermediate nodes including destination node having valid route to the destination are allowed to forward the route reply packet to the source node. Sequence number is incremented when a source node initiates a route request (RREQ) packet or when a destination node replies a route reply (RREP) packet.

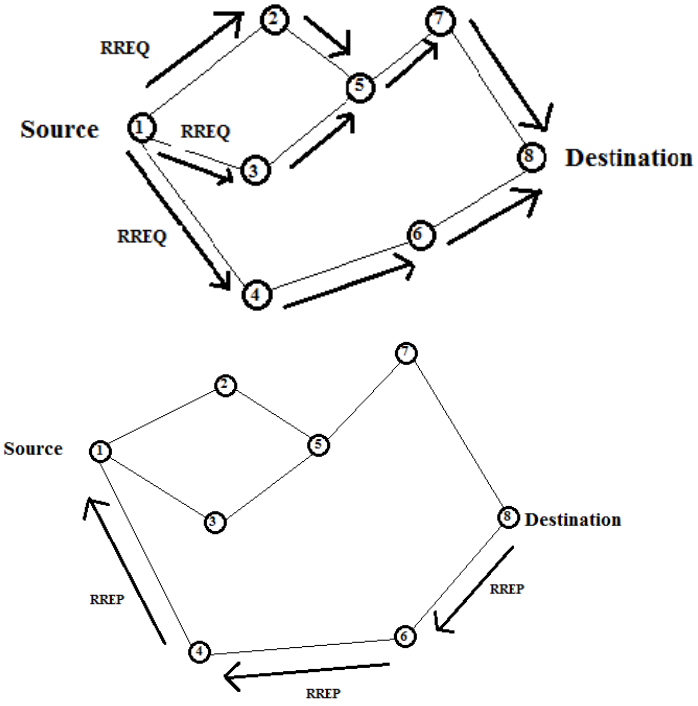

Figure 2 Route creation in AODV

Each RREQ contains a time to live (TTL) field. This field specifies that how many times the message should be re-broadcasted. This TTL value is set to a predefined value and is incremented with every re-broadcast. The re-broadcast is done when a node does not receive any reply. Generally TTL value is set to a value greater than the value of diameter of network so that the message may reach all nodes and guarantee a successful path discovery in one broadcast.

I. Route Maintenance:

Now we will discuss the maintenance of a route in AODV routing protocol. A route will be maintained only and only if the route is active. When a route is active, it means that the data packets are periodically travelling from one node to other or we can say that from the source to the destination. The links are called to timeout when the source stops sending data packets on that path or link and then they will be deleted from the node routing tables. A routing error message will be propagated to the source node to inform that the destinations are now unreachable, if a link break occurs while the route is active[6]. This is a RERR message. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

AODV maintains routes for as long as the route is active [9]. This includes maintaining a multicast tree for the life of the multicast group. Because the network nodes are mobile,

it is likely that many link breakages along a route will occur during the lifetime of that route. The author of [5] suggests that a link failure can a link failure can also be determined using link layer acknowledgement (LLACKS).

IV. MERITS AND DEMERITS OF AODV

Merits:

- It establishes routes on demand
- Uses destination sequence number to find latest route to destination
- Requires less time in setting up a connection

Demerits:

- Periodic beaconing leads to unnecessary Bandwidth consumption
- Multiple RREPs in response to a single RREQ can lead to heavy control overhead
- Intermediate nodes have stale entries

V. POSSIBLE ATTACKS IN AODV

A. Denial of Service Attack:

The denial of service[10] attack is also known as route request (RREQ) flooding attack that aim to flood the network with the large number of RREQ packet to the receiver in the network. In this attack the malicious node generates a large number of RREQ in the network until the network is saturated with the RREQs and it is unable to transmit the data packet. Many on demand protocols suffer from this attack. In route discovery the sender broadcasts the network with RREQs. If the received RREQ at intermediate node or at receiver is a duplicate packet or same sequence number it is dropped. For an Ad-hoc network Traffic load and energy consumption are two major factors. The RREQ consumes more band width than data packet. Attacker uses this disadvantage and initiates a large number of RREQ and leads to the denial of service attack.

B. Black Hole Attack:

The Black Hole Attack [11] is a common denial of service attack in MANETs. In this attack a malicious node take part in the route discovery process using a fake sequence number or hop count information. The malicious node pretends that it has the best possible path to reach the destination. The RREP from the attacker M appears to be much fresh than the genuine one as the former has a higher sequence number. As a result, a route from node S to node M is established because the source node feels that packet p is the latest one. The malicious node M can now drop all packets sent by S to D, which passes through M. The impact of black hole attack [12] is that when source node starts sending data packet to destination using route via malicious node, the malicious node drops all the packets hence leads to black hole attack.

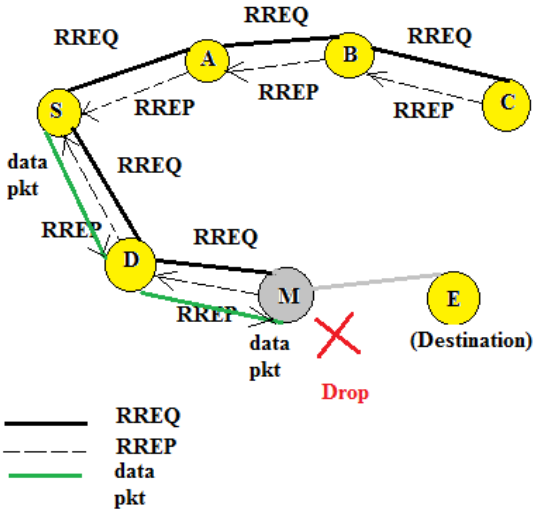

Figure 3 Black hole attack in AODV

COMPARISON WITH OTHER REACTIVE PROTOCOLS:

Type of Packet	Type o f protocol	Name of protocol	Rate selection criteria	Route	Beacon	Message overhead	Protocol used	Routing Structure
RREQ, RREP,	Reactive	AODV	Shortest path	Single	Yes	High	Source routing	Flat
	Reactive	DSR [15]	Shortest path	Multipl e	No	High	Source routing	Flat
QRY, UPD,CL R	Reactive	TORA [16]	Shortest path	Multipl e		Moderat e	Link reversal	Flat
	Reactive	ABR [17]	Link stability	Single	Yes	High	Source routing	Flat

VI. Conclusion and Future Scope:

AODV routing protocol is designed for Mobile Ad-hoc networks with dynamic architecture. AODV can handle large number of mobile devices and varying data rate of traffic. It assumes the there is no intruder node. AODV is designed for reducing the use of control messages and eliminate overhead on data traffic to improve the scalability and performance. In multipath AODV there is a large research area to reduce the overhead of route discovery process. Security and energy efficiency is one of the main concerns in MANETs. The detection and prevention of black hole attack in the network exists as a challenging task. It can also be done in other routing protocols.

References:

[1.] S.Misra, I.Woungang and S.C. Misra, "Guide to Wireless Ad Hoc Networks", Springer science, 2009.

[2.] Goldsmith AJ, and Wicker SB. "Design challenges for energy-constrained ad hoc wireless networks." IEEE Wireless Communications 2002; 9(4): 8–27.

[3.] AI-Karaki, IN.; and Kamal, A.E., "Routing techniques in wireless sensor networks: a survey", Wireless Communications, IEEE , vol.ll, no.6, pp. 6-28, December 2004.

[4.] Shiv Prakash, J.P.Saini, S.C.Gupta, " review of Energy Efficient Routing Protocols for Mobile Ad Hoc Wireless Networks", International Journal of computer Information System Vol. 1, No 4, 2010

[5.] Royer E.M., Perkins C.E. "Ad-hoc on-demand distance vector routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, p.90, 1999.

[6.] Das S. Perkins C.E., Belding-Royer E.M, "Ad-hoc on-demand distance vector (aodv) routing" RFC 3561, IETF Network Working Group, 2003.

[7.] M. K. Marina and S. R. Das, "On-Demand Multipath Distance Vector Routing for Ad Hoc Networks," Proc. of the Int. Conf. on Network Protocols (ICNP), pp. 14-23, Nov. 2001.

[8.] Perkins C.E. Lee S.-J., Belding-Royer E.M., "Scalability study of the ad-hoc on-demand distance vector routing protocol", Int. J. Netw. Manag., 13(2), 2003.

[9.] Ochola EO & Eloff MM, "A review of black hole attack on AODV routing in MANET".

[10.] M. A. Shurman, S. M. Yoo, and S. Park,"Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[11.] Ei Ei Khin Thandar Phyu, "Impact of black hole attack on aodv routing protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[12.] V. Kanakaris*, D. Ndzi and D. Azzi, "Ad-hoc Networks Energy Consumption: A review of the Ad-Hoc Routing Protocols", Journal of Engineering Science and Technology Review 3 (1) (2010) 162-167

[13.] A. Iwata, C. C. Chiang, G. Pei, M. Gerla, and T.W. Chen, "Scalable Routing Strategies for Ad-Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.

[14.] David B. Johnson, Davis A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer, 1996, pp. 152-81.

[15.] VD Park and MS Corson "A highly adaptive distributed routing algorithm for mobile wireless networks", Proc. INFOCOM'97, Apr. 1997, 9 pages

[16.] Chai-Keong Toh, "A novel distributed routing protocol to support Ad hoc mobile computing" Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480-86