AODV ROUTING PROTOCOL WORKING PROCESS

[1]Asma Ahmed, [2]A. Hanan, [3]Izzeldin Osman
[1] University of Kassala, Kassala, Sudan, asma_mansori@yahoo.com
[2] Universiti Teknologi Malaysia, Johor, Malaysia, hanan@utm.edu.my
[4] Sudan University Science and Technology, Khartoum, Sudan,Izzeldin@Acm.org

Abstract

Ad hoc On-demand Distance Vector (AODV) is a reactive routing protocol in which the network generates routes at the start of communication. AODV has been developed specially for MANET. It obtains the routes purely on-demand which makes it a very useful and desired algorithm for MANETs. AODV use two different operations to find and maintain routes: the route discovery process operation and the route maintenance operation. There are four messages used in AODV to control the process of route discovery and route maintenance. In this paper the control messages that used in AODV ; RREQ, RREP and RERR; are classified, and the process of how AODV routing protocol is working was investigated as well as explain the reasons for why the AODV is the most desirable protocol for MANET environment.

Keywords*: AODV, MANET, RREQ, RREP, Sequence number*

1. Introduction

Reactive or on-demand routing protocols in MANET create routes only when they are needed [1]. Reactive protocols use two different operations to find and maintain routes: the route discovery process operation and the route maintenance operation. When a node requires a route to the destination [28], it initiates a route discovery process within the network [2]. This process completed once a route found, or all possible route permutations are examined. Route maintenance is the process of responding to changes in topology that happens after a route has initially been created. When link is broken, the nodes in the network try to detect link breaks on the established routes. AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol that is a simple, efficient on-demand MANET routing [2]. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs [5]. Each mobile node in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting.

The aim of this paper is to classify the control message that used in AODV and explained the process of how the AODV routing protocol is working. The paper is organized as follows: Section 2 explain the routing table. Section 3 describes the control messages and sequence number in AODV. Section 4 discusses the route discovery process of AODV. Section 5 explain the link breakage and the route maintenance process. The reasons of used AODV are explained in Section 6. Section 7 concludes the paper.

2. Routing Tables

In MANET, each mobile node in the network maintains a route table entry for each destination of interest in its route table. Each entry in the route table contains the following information:

- Destination Node Address.
- Next hop of the source node or intermediate node.
- Number of hops.
- Destination sequence number.
- Active neighbors of the route.
- Expiration time for this route table entry.

3. Control Packets

There are four messages used in AODV routing protocol [27]. These messages are used to control the process of route discovery and route maintenance.

3.1. Route Request Message (RREQ)

When the source node wants to connect with the destination node and it has no route entry to the destination node, a control packet; named Route Request message (RREQ); was broadcasted by the source node. RREQ contain the fields showing in Table 1.

Table 1. RREQ Format

Source Address
Request ID
Source Sequence No
Destination Address
Destination Sequence No
Hop Count

The request ID is incremented each time the source node sends a new RREQ. The pair (source address and request ID) identifies a RREQ uniquely. As RREQ travels from node to node, it automatically sets up the reverse path from all these nodes back to the source. Each node that receives this packet records the address of the node from which it was received. This process is called Reverse Path Setup (RPS) [27].

3.2. Route Reply Message (RREP)

If a node is the destination or has a valid route to the destination, it unicasts a Route Reply message (RREP) back to the source. The RREP has the format shown in Table.2.

Table 2. RREP Format

Source Address
Destination Address
Destination Sequence No
Hop Count
Life Time

The node on receiving RREQ message from a neighbor, it records the address of this neighbor. So when the destination node is found, the RREP message will travel along this path and no more broadcasts will be needed. RREP message travels back to the source based on the reverse path that it records. As the RREP travels back to the source, each node along this path sets a forward pointer to the node from where it is receiving the RREP and records the latest destination sequence number to the request destination. This process is called Forward Path Setup (FPS).

3.3. Route Error Message (RERR)

All nodes monitor their own neighborhood. When the route is broken or be invalid, a Route Error message (RERR) is generated to notify the other nodes that use this route, that the route becomes invalid. This messaege is generated to avoid retransmitting by that route.

3.4. HELLO Message

Each node can get to know its neighborhood by using local broadcasts, so-called HELLO messages. Nodes neighbors are all the nodes that it can directly communicate with them. HELLO message is used to inform the neighbors that the link is still alive.

3.5. Sequence Numbers

The sequence number is an important feature of AODV to determine the freshness of routing information and guarantee loop-free routes [2]. The destination sequence number for each destination node is stored in the routing table, and it is updated when the node receives a message with a greater sequence number. However the node it increases its sequence number in these cases:

- When the node sends RREQ message, its own sequence number is incremented.
- When the node responds to a RREQ message by sending a RREP, its own sequence number becomes the maximum of the current sequence number and the node's sequence number in the received RREQ.
- When a node sends RERR to indicate that the route is broken.

The higher sequence number is more accurate information, and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes [15].

4. Route Discovery Process

When a source node wants to send a data packet to a destination node; first, the source node checks with its routing table to determine if there is an available route to the destination node. If so, it uses this route to send the packets to the destination node. In the case where there is no route to the destination node, route discovery process is initiated by broadcasting a RREQ message. Each node checks the source address and the request ID on receiving a RREQ message. If the node has already received a RREQ with the same source address and request ID, the new RREQ message will be discarded. The RREQ ID is increased by one every time the source node sends a RREQ message. The Route Request contains the last known destination sequence number. Figure1 shows how RREQ message is propagating in MANET. In this figure, when the source node S wants to send a data packet to a destination node D, it has these steps:

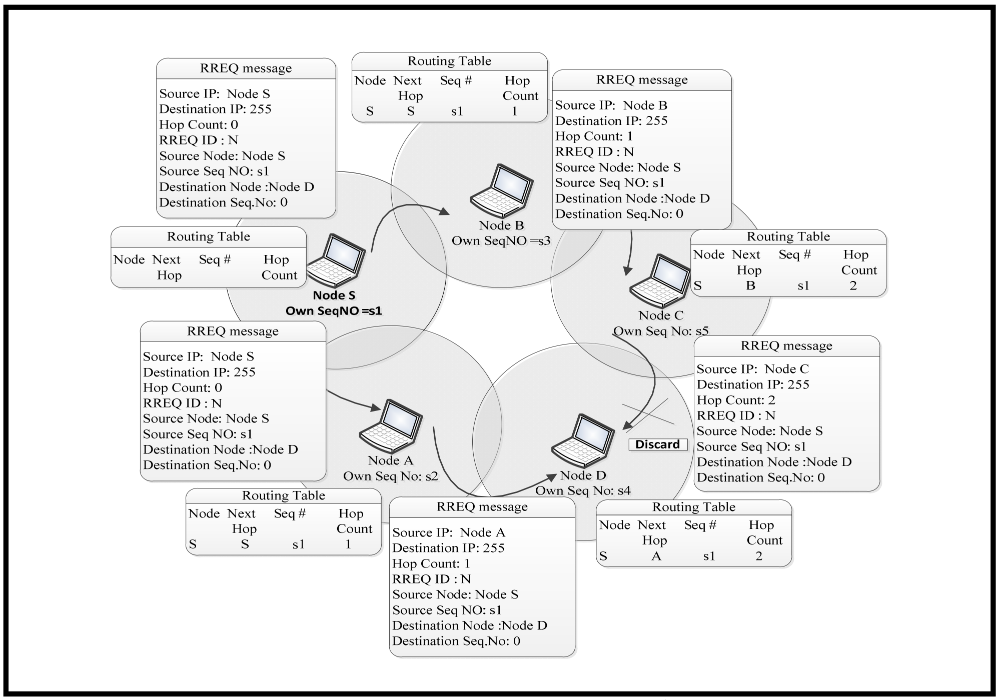
- Node S sends RREQ message to its neighbors; A, B.
- Node A sets up reverse path and forwards RREQ message to its neighbor D.
- Node B sets up reverse path and forwards RREQ message to its neighbor C.
- Node C sets up reverse path and forwards RREQ message to its neighbor D.
- When node D receive the RREQ from node C, it will discard it because it was already received it from node A.

If an intermediate node has a route entry for the desired destination in its routing table, it compares the destination sequence number in its routing table with that in the RREQ message. If the destination sequence number in its routing table is less than that in the RREQ, it rebroadcasts the RREQ to its neighbors. Otherwise, it unicasts a route reply message to its neighbor from which it was received the RREQ if the same request was not processed previously (this is identified using the request ID and source address). That means the node will be either:

(i) Broadcasts the RREQ with incremented hop count to its neighbors (if it has no route entry for the destination, or it has one but this it is not more an up-to-date route), or

(ii) Send back a Route Reply message (RREP) to the source node if it is the destination node or if it has a route to the destination with a sequence number greater than or equal to that of RREQ.

The exchange of route information will be repeated until a RREQ reaches destination node or an intermediate node that has a fresh enough route entry for the destination.



RREQ message
Source IP: Node S
Destination IP: 255
Hop Count: 0
RREQ ID : N
Source Node: Node S
Source Seq NO: s1
Destination Node :Node D
Destination Seq.No: 0

Routing Table

Node	Next Hop	Seq #	Hop Count
S	S	s1	1

RREQ message
Source IP: Node B
Destination IP: 255
Hop Count: 1
RREQ ID : N
Source Node: Node S
Source Seq NO: s1
Destination Node :Node D
Destination Seq.No: 0

Routing Table

Node	Next Hop	Seq #	Hop Count

Routing Table

Node	Next Hop	Seq #	Hop Count
S	B	s1	2

RREQ message
Source IP: Node S
Destination IP: 255
Hop Count: 0
RREQ ID : N
Source Node: Node S
Source Seq NO: s1
Destination Node :Node D
Destination Seq.No: 0

RREQ message
Source IP: Node C
Destination IP: 255
Hop Count: 2
RREQ ID : N
Source Node: Node S
Source Seq NO: s1
Destination Node :Node D
Destination Seq.No: 0

Routing Table

Node	Next Hop	Seq #	Hop Count
S	S	s1	1

RREQ message
Source IP: Node A
Destination IP: 255
Hop Count: 1
RREQ ID : N
Source Node: Node S
Source Seq NO: s1
Destination Node :Node D
Destination Seq.No: 0

Routing Table

Node	Next Hop	Seq #	Hop Count
S	A	s1	2

Figure 1. RREQ Message Propagating

When the destination or intermediate node that has route to destination receives the RREQ, it sends a RREP to the source node and updates its routing table with accumulated hop count and the sequence number of the destination node. Afterward, the RREP message is unicasted to the source node. When the source node receives the RREP, then a route is established. Figure 2 shows how RREP message is unicast in MANET. The explanation of the figure is as follows:

- Node D creates an RREP message and updates its routing tables with accumulated hop count and the sequence number.
- Then it unicast the RREP to node A.

When node A receives RREP from node D, it updates its routing tables with accumulated hop count and the sequence number of the destination node D.

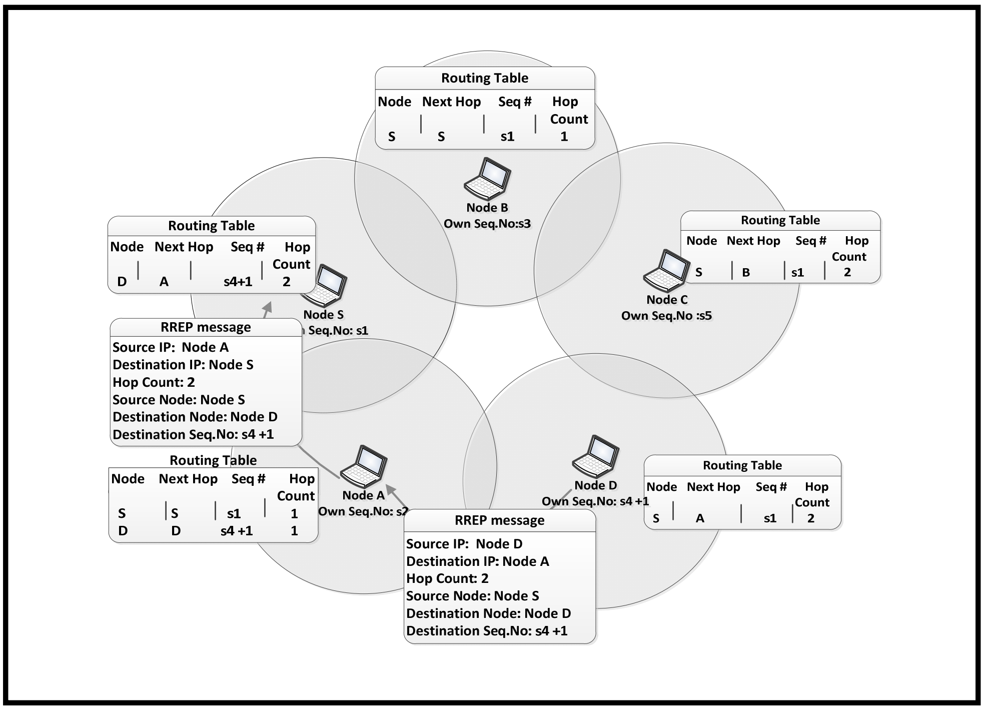
Then node A and sets up forward path and forwards RREP to source node S.

In case a node receives multiple RREPs, the RREP has largest Dst-Seq is selected. If Dst-Seq were the same, then the smallest hop count (HC) will selected.

The HC is used to determine the shortest path and it is increased by one if a RREQ or RREP message is forwarded each hop. That means the intermediate node updates routing information and unicast new RREP only in these cases:

- If the Destination sequence number is greater, or
- If the new sequence number is same and hop count is small.

Otherwise, it just skips the new RREP. This ensures that the algorithm is loop-free, and only the most effective route is used [5].



Routing Table

Node	Next Hop	Seq #	Hop Count
S	S	s1	1

Routing Table

Node	Next Hop	Seq #	Hop Count
D	A	s4+1	2

Routing Table

Node	Next Hop	Seq #	Hop Count
S	B	s1	2

RREP message

Source IP: Node A
Destination IP: Node S
Hop Count: 2
Source Node: Node S
Destination Node: Node D
Destination Seq.No: s4 +1

Routing Table

Node	Next Hop	Seq #	Hop Count
S	S	s1	1
D	D	s4 +1	1

Routing Table

Node	Next Hop	Seq #	Hop Count
S	A	s1	2

RREP message

Source IP: Node D
Destination IP: Node A
Hop Count: 2
Source Node: Node S
Destination Node: Node D
Destination Seq.No: s4 +1

Figure 2: RREP Message Unicasting

5. Link Breakage

Because a node in MANET can move at any time, link breakages can occur at any time [26]. If a node does not receive a HELLO message from one of its neighbors for a specific amount of time called HELLO interval, then:

- The entry for that neighbor in the table will be set as invalid.
- The RERR message will be generated to inform other nodes of that link breakage.

During the route discovery process if any node identifies a link failure it generates Route Error message (RERR) and puts the invalidated address of that node into list, then it sends it to all other nodes which uses that link for their communication to other nodes. RERR messages inform all sources using a link when a failure occurs [9].

6. Why AODV

AODV is one of the most popular routing protocols, which is a simple and efficient on-demand MANET routing protocol [13]. The concepts of AODV that makes it desirable for MANETs with limited bandwidth include the following:

- Minimal space complexity: The algorithm makes sure that the nodes that are not in the active path do not maintain information about this route. After a node receives the RREQ and sets a reverse path in its routing table and propagates the RREQ to its neighbors, if it does not receive any RREP from its neighbors for this request, it deletes the routing info that it has recorded.

- Maximum utilization of the bandwidth: This can be considered the major achievement of the algorithm. As the protocol does not require periodic global advertisements, the demand on the available bandwidth is less. And a monotonically increased sequence number counter is maintained by each node in order to supersede any stale cached routes. All the intermediate nodes in an active path updates their routing tables also make sure of maximum utilization of the bandwidth. Since, these routing tables will repeatedly be used if that intermediate node receives any RREQ from another source for the same destination. Also, any RREPs that are received by the nodes are compared with the RREP that was propagated last using the destination sequence numbers and are discarded if they are not better than the already propagated RREPs.
- Simple: It is simple with each node behaving as a router, maintaining a simple routing table, and the source node initiating path discovery request, making the network self-starting.
- Most effective routing info: After propagating a RREP message, if a node receives RREP with smaller hop-count, it updates its routing info with this better path and propagates it.
- Most current routing info: The route info is obtained on demand. Also, after propagating an RREP, if a node receives RREP with greater destination sequence number, it updates its routing info with this latest path and propagates it.
- Loop-free routes: The algorithm maintains loop-free routes by using the simple logic of nodes discarding the packets for same broadcast-id.
- Coping up with dynamic topology and broken links: When the nodes in the network move from their places and the topology is changed, or the links in the active path are broken, the intermediate node that discovers this link breakage propagates an RERR message. And the source node re-initializes the path discovery if it still desires the route. This ensures quick response to broken links.
- Highly Scalable: The algorithm is highly scalable because of the minimum space complexity and broadcasts avoided.

7. Discussions and Summary

Routing is an important function in any network; it be wired or wireless. Routing is the act of moving information from a source to a destination in an internetwork. AODV obtains the routes purely on-demand which makes it a very useful and desired algorithm for MANETs. The routing concept basically involves two activities: firstly, determining optimal routing paths to the destination and secondly, transferring the information through an internetwork. In AODV RREQ, RREP, RERR, HELLO messages are used to control the process of route discovery and route maintenance phases. Also, sequence number is an important feature of AODV to determine the freshness of routing information and guarantee loop-free routes.

This paper classified all control messages in AODV and explained how the sequence number determines the freshness route. It also analyzes the route discovery process and reasons of used AODV in MANET. In future work, AODV needs to be secure from being attack. Because AODV control packets carry important control information that governs the behavior of data transmission in MANET. Since the level of trust in a traditional network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter the control packets to disrupt communication.

8. References

[1] C.M barushimana, A.Shahrabi, “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[2] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[3] Farooq Anjum and Petros Mouchtaris, "SECURITY FOR WIRELESS AD HOC NETWORKS", by John Wiley & Sons, Inc Copyright © 2007.

[4] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Publications, 2002.

[5] Charles E. Perkins. Ad Hoc Networking. Addision Wesley, 2001.

[6] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[7] Manel Guerrero Zapata, "Secure Ad hoc On Demand Distance Vector (SAODV) Routing", Technical University of Catalonia (UPC), Mobile Ad HocNetworking Working Group, Internet Draft, 15 September 2005.

[8] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[9] M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for Mobile Ad Hoc Networks," Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[10] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, Mar. 2005.

[11] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Com- mun. Rev., pp. 234-44 Oct. 1994.

[12] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Publications, 2002.

[13] Junaid Arshad and Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", 1-4244-0626-9/06 © IEEE 2006.

[14] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[15] S.Thirumal . "Modified AODV to Prevent Black Hole Attacks in MANET", IJCSET Vol 1, Issue 8, 447-450, September 2011.

[16] Y. A. Huang and W. Lee, "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, Sept. 2004.

[17] T. Clausen, P. Jaquet, et.al. "Optimized link state routing protocol." Internet Draft, draft-IETF manet-olsr 06.txt, work in progress, 2001.

[18] G. Vigna, S. Gwalani, et al., "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks," in Proceedings of the Annual Computer Security Applications Conference (ACSAC), Tucson, AZ, December, , pp. 16–27 2004.

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

[20] D. B. Johnson, D. A. Maltz, and Y. C. Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), IETF Internet Draft, draft-ietf-manet-dsr-10, July 2004.

[21] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[22] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[23] Y. Xu and X. Xie, "Security analysis of routing protocol for MANET based on extended Rubin logic," in Proceedings of the IEEE International Conference on Networking, Sensing and Control (ICNSC '08), pp. 1326–1331, Sanya, China, April 2008.

[24] Levent, E., and Chavan, N. J. Elliptic "Curve Cryptography based Threshold Cryptography" (ECC-TC) Implementation for MANETs. IJCSNS International Journal of Computer Science and Network Security. 7(4), 48–61, 2007.

[25] Kim, J. and Tsudik, G. SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Networks. 7(6), 1097 -1109. ISSN 15708705., 2009.

[26] Asma Ahmed, Shukor A. R., A. Hanan, Izzeldin M., Yahia A., “Routing in Mobile Adhoc Network”, International Journal of Computer Science and Network Security (IJCSNS). Vol. 11, No. 8. ISSN 1738-7906, 2011.

[27] Asma Ahmed, A. Hanan, Izzeldin M., “ AODV Security Considerations”, in Proceedings of the 2013 International Conference on Wireless Networks (ICWN'13), July 21-24 Nevada, USA. 2013.

[28] Shamim Ripon, Sumaya Mahbub, K. M. Intiaz-ud-Din, “Verification of A Security Adaptive Protocol Suite Using SPIN” International Journal of Engineering and Technology, vol. 5, no. 2, pp. 254-256, 2013.