GNITED MINDS
Journals

Journal of Advances in Science and Technology

Vol. IV, No. VII, November-2012, ISSN 2230-9659

AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ALONG WITH EXPANDING RING SEARCH TECHNIQUE WITH REFERENCE TO BENEFITS AND LIMITATIONS OF AODV

www.ignited.in

Journal of Advances in Science and Technology
Vol. IV, No. VII, November-2012, ISSN 2230-9659

Ad Hoc On-Demand Distance Vector (AODV) Along With Expanding Ring Search Technique With Reference To Benefits and Limitations of AODV

Teja Singh[1] Dr. Pradeep Goel[2]

[1]Research Scholar, CMJ University, Shillong, Meghalaya

[2]Associate Professor, M.M. College, Fatehabad

Abstract – AODV is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol which is collectively based on DSDV and DSR. It aims to minimize the requirement of system-wide broadcasts to its extreme. It does not maintain routes from every node to every other node in the network rather they are discovered as and when needed & are maintained only as long as they are required. The requests are sent using RREQ message and the information in connection with creation of a route is sent back in RREP message. The source node broadcasts the RREQ packet to its neighbors and then sets a timer to wait for a reply.

Key Words; Destination-Sequenced, Broadcast ID, Requirement Of System.

--------------------------♦----------------------------

INTRODUCTION

MANETs can communicate with different networks that are not ad-hoc. Therefore, they can communicate with wired networks creating hybrid networks. In the ad-hoc networks, the mobility of the nodes makes that the topology changes continuously. Hence, a specific dynamic routing protocol for MANETs which discovers and maintains the routes, and deletes the obsolete routes continuously is necessary.

The routing protocols for MANETs try to maintain the communication between a pair of nodes (source-destination) in spite of the position and velocity changes of the nodes. To achieve that, when those nodes are not directly connected, the communication is carried out by forwarding the packets, by using the intermediate nodes.

Currently there is research on the behaviour of a lot of those routing protocols and the IETF (Internet Engineering Task Force) is working on the standardisation of some of them. The protocols that are in experimental phase RFC (Request For Comments) include DYMO (Dynamic MANET On demand Routing Protocol) [DYMO_06], OLSR [OLSR_03], AODV [AODV_03], DSR (Dynamic Source Routing) [DSR_04] and TBRPF (Topology Dissemination Based on Reverse Path Forwarding) [TBRPF_04].

The origin of MANETs begins in the 70's for the military necessity of the interconnection of different hosts. This type of networks was implanted to avoid the need of a central base of communications. With these networks it was expected to transmit information in a fast and stable way as well as to cover the major part of the possible range without the necessity of having a previous infrastructure.

REVIEW OF LITERATURE

Kimaya Sanzgiri et al [30] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server.

Hubaux, et al. have proposed a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [31]. Kong, et al. [32] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the MAC address of multiple other nodes. Yi, et al. [33] also have proposed a general framework for secure ad hoc routing called the SAR.

Papadimitratos and Haas [34] proposed a protocol (SRP) that can be applied to several existing routing protocols. SRP requires that, for every route discovery, source and destination must have a security association between them.

Ariadne [35], by the same authors, is based on DSR [1] and TESLA [29] (on which it is based its authentication mechanism). It also requires clock synchronization.

S. Buchegger, and J.-Y. Le Boudec [36] proposed CONFIDANT routing protocol extension over DSR to provide security.

MATERIAL AND METHOD

AODV is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol which is collectively based on DSDV and DSR. It aims to minimize the requirement of system-wide broadcasts to its extreme. It does not maintain routes from every node to every other node in the network rather they are discovered as and when needed & are maintained only as long as they are required. The key steps of algorithm used by AODV for establishment of uncast routes are explained below.

A. Route Discovery

When a node wants to send a data packet to a destination node, the entries in route table are checked to ensure whether there is a current route to that destination node or not. If it is there, the data packet is forwarded to the appropriate next hop toward the destination. If it is not there, the route discovery process is initiated. AODV initiates a route discovery process using Route Request (RREQ) and Route Reply (RREP). The source node will create a RREQ packet containing its IP address, its current sequence number, the destination's IP address, the destination's last sequence number and broadcast ID. The broadcast ID is incremented each time the source node initiates RREQ. Basically, the sequence numbers are used to determine the timeliness of each data packet and the broadcast ID & the IP address together form a unique identifier for RREQ so as to uniquely identify each request. The requests are sent using RREQ message and the information in connection with creation of a route is sent back in RREP message. The source node broadcasts the RREQ packet to its neighbors and then sets a timer to wait for a reply. To process the RREQ, the node sets up a reverse route entry for the source node in its route table. This helps to know how to forward a RREP to the source. Basically a lifetime is associated with the reverse route entry and if this entry is not used within this lifetime, the route information is deleted. If the RREQ is lost during transmission, the source node is allowed to broadcast again using route discovery mechanism.

B. Expanding Ring Search Technique

The source node broadcasts the RREQ packet to its neighbors which in turn forwards the same to their neighbors and so forth. Especially, in case of large network, there is a need to control network-wide broadcasts of RREQ and to control the same; the source node uses an expanding ring search technique. In this technique, the source node sets the Time to Live (TTL) value of the RREQ to an initial start value. If there is no reply within the discovery period, the next RREQ is broadcasted with a TTL value increased by an increment value. The process of incrementing TTL value continues until a threshold value is reached, after which the RREQ is broadcasted across the entire network.

C. Setting up of Forward Path

When the destination node or an intermediate node with a route to the destination receives the RREQ, it creates the RREP and uncast the same towards the source node using the node from which it received the RREQ as the next hop. When RREP is routed back along the reverse path and received by an intermediate node, it sets up a forward path entry to the destination in its routing table. When the RREP reaches the source node, it means a route from source to the destination has been established and the source node can begin the data transmission.

D. Route Maintenance

A route discovered between a source node and destination node is maintained as long as needed by the source node. Since there is movement of nodes in Wireless network and if the source node moves during an active session, it can reinitiate route discovery mechanism to establish a new route to destination. Conversely, if the destination node or some intermediate node moves, the node upstream of the break initiates Route Error (RERR) message to the affected active upstream neighbors/nodes. Consequently, these nodes propagate the RERR to their predecessor nodes. This process continues until the source node is reached. When RERR is received by the source node, it can either stop sending the data or reinitiate the route discovery mechanism by sending a new RREQ message if the route is still required.

E. Benefits and Limitations of AODV

The benefits of AODV protocol are that it favors the least congested route instead of the shortest route and it also supports both uncast and multicast packet transmissions even for nodes in constant movement. It also responds very quickly to the topological changes that affects the active routes. AODV does not put any additional overheads on data packets as it does not make use of source routing. The limitation of AODV protocol is that it expects/requires that the nodes in the broadcast medium can detect each others' broadcasts. It is also possible that a valid route is expired and the determination of a reasonable expiry time is difficult. The reason behind this is that the nodes are mobile and their sending rates may differ widely and can change dynamically from node to node. In addition, as the size of network grows, various performance metrics begin decreasing. AODV is vulnerable to various kinds of attacks as it based on the assumption that all nodes must cooperate and without their cooperation no route can be established.

CONCLUSION

The key steps of algorithm used by AODV for establishment of uncast routes are explained below. When a node wants to send a data packet to a destination node, the entries in route table are checked to ensure whether there is a current route to that destination node or not. If it is there, the data packet is forwarded to the appropriate next hop toward the destination. If it is not there, the route discovery process is initiated. AODV initiates a route discovery process using Route Request (RREQ) and Route Reply (RREP). The source node will create a RREQ packet containing its IP address, its current sequence number, the destination's IP address, the destination's last sequence number and broadcast ID. The broadcast ID is incremented each time the source node initiates RREQ. Basically, the sequence numbers are used to determine the timeliness of each data packet and the broadcast ID & the IP address together form a unique identifier for RREQ so as to uniquely identify each request.

REFERENCES

[1] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pages 46-55. See also http://citeseer.nj.nec.com/royer99review.html

[2] Borko Furht and Mohammad Ilyas. Wireless Internet Handbook: Technologies, Standards, and Applications. Chapter 16. Auerbach Publications, 2003

[3] Dave B. Johnson and David A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, October 1999.

[4] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.

[6] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78-87.

[7] J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

[8] J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

[9] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.

[10] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[11] Y. C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Technical Report TR01-383, Rice University, Dec. 2001.

[12] A. Perrig, R. Canetti, D. Song, and D. Tygar. Efficient and secure source authentication for multicast. In *Network and Distributed System Security Symposium (NDSS'01)*, Feb. 2001.

[13] S. Buchegger, and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)," *Proc. 3rd Symp. Mobile Ad hoc Networking and Computing (MobiHoc 2002)*, ACM Press, 2002, pp. 226-236.

[14] Mobile Ad-hoc Networks (MANET),http://www.ietf.org/html.charters/manetcharter. html. (1998-11-29).

[15] PERKINS, C. E., Ed. *Ad Hoc Networking*. Addison–Wesley Publishing Company, 2001. ISBN: 0-201-30976-9.

[16] SCHILLER, J. *Mobile Communications*. Addison–Wesley Publishing Company, 2000. ISBN: 0-201-39836-2.

[17] E.M. Royer, C-K. Toh, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks, IEEE Personal Communications Magazine, April 1999, pp. 46-55. http://www.cs.ucsb.edu/~eroyer/publications.html

[18] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector

Routing (DSDV) for Mobile Computers," *Comp. Commun. Rev.*, Oct. 1994, pp. 234–44.

[19] L. R. Ford Jr. and D. R. Fulkerson, *Flows in Networks*, Princeton Univ. Press, 1962

[20] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and App. J.*, Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97..

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