Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.452 – 456

SURVEY ARTICLE

A Survey of Routing Protocols AODV in Mobile Ad Hoc Networks

Deepak Goyal[1], Munisha Devi[2]

[1]Assistant Professor, Vaish College of Engineering, MDU, Rohtak, Haryana (India)

[2]M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)

manishabnwl@gmail.com

Abstract

The Mobile Ad-hoc Networks (MANETs) is an network without any pre-existing infrastructure or the aid of any centralized administration. The topology of this network keeps on changing as the nodes move randomly. There are so many protocols used for such networks. One protocol is Adhoc On Demand Distance Vector (AODV) routing protocol. AODV decrease the routing overhead and hence enhancing the performance of the network. Routing in MANET is a critical task due to extremely dynamic environment. Several routing protocols have been proposed for ad hoc networks and best among them are DSR, AODV. Mobile nodes can establish network connections anytime. Routing protocols are needed for communication in Ad hoc networks, where it targets for efficient and timely delivery of the messages. The main goal of such type of network is to provide rapid communication, computing and deployment. Each mobile node in Ad Hoc network is capable of routing packets and assists surrounding nodes to do so. In this dynamically changing topology environment the role of routing protocols are very important. This paper provides an overview of AODV protocol by presenting their characteristics, functionality, benefits and limitations and then analyzes security requirements for ad hoc routing protocols.

Index Terms – MANET, Security, DSR, AODV

1. INTRODUCTION

Mobile ad hoc network is a group of wireless mobile, dynamic nodes in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks don't require any fixed network infrastructure such as base stations.

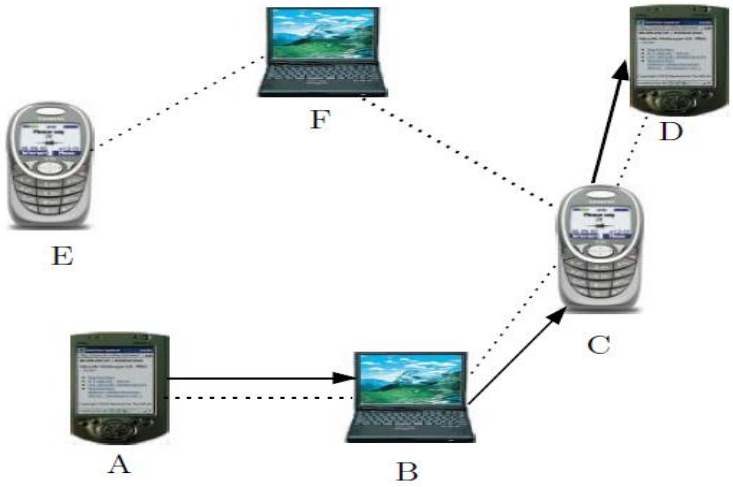

Figure 1. An Ad hoc Network

The nodes are mobile hence the network topology may vary rapidly and unpredictably over time. Mobile Ad-Hoc Network (MANET) is a kind of wireless ad-hoc network and it is a self-configuring network of mobile nodes connected by wireless links. The participating nodes act as router, are free to move randomly and dynamically & thus, the network's wireless topology may change rapidly and unpredictably.
Applications of MANETs include Personal area Networking cell phone, laptop, ear phone, wrist watch, Emergency operations search-and-rescue (earthquakes, boats, airplanes…) as well as civilian applications like an outdoor meeting, or an ad-hoc classroom. The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: *firstly*, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; *secondly*, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; *thirdly*, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; *fourthly*, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks.

Some of the major characteristics of mobile ad hoc routing protocols are:

Dynamic Network topology: The topology may change rapidly in this network and the connectivity within the network varies with time as the nodes move.
Limited Bandwidth: The bandwidth [5] available is limited than that of wired networks. The power is limited and the computation should be energy efficient.
Security: The wireless links lack protect against threats. Various attacks such as denial of services, eavesdropping, replay attacks are possible. MANETs are resource constrained, bandwidth constrained and as the nodes are mobile, the network topology changes dynamically effectively. Therefore routing is to be done and hence the requirement of efficient and good routing protocols.

2. LITERATURE REVIEW

A Several researchers have done the qualitative and quantitative analysis of Ad Hoc Routing Protocols by means of different performance metrics. They have used different simulators for this purpose. *S. Gowrishanker et al* [8] performed the Analysis of AODV and OLSR by using NS-2 simulator, the simulation period for each scenario was 900 seconds and the simulated mobility network area was 800 m x 500 m rectangle. In each simulation scenario, the nodes were initially located at the centre of the simulation region. The nodes start moving after the first 10 seconds of simulated time. The application used to generate is CBR traffic and IP is used as Network layer protocol. Vetrivelan & Dr. A V Reddy [7] analyzed the performance differentials using varying network size and simulation times. They performed two simulation experiments for 10 & 25 nodes for simulation time up

to 100 sec *Arunkumar B R et al.* in this paper they present their observations regarding the performance comparison of the routing protocols for variable bit rate (VBR) in mobile ad hoc networks (MANETs). They perform extensive simulations, using NS-2 simulator . Their studies have shown that reactive protocols perform better than proactive protocols. *S. P. Setty et.al.*[9] evaluated the performance of existing wireless routing protocol AODV in various nodes placement models like Grid, Random and Uniform using QualNet 5.0. *Khan et al*. [10] studied and compared the performance of routing protocols by using NCTUns 4.0 network simulator. In this paper, performance of routing protocols was evaluated by varying number of nodes in multiples of 5 in the ad hoc network. *Jorg D.O*. [11] studied the behaviour of different routing protocols on network topology changes resulting from link breaks, node movement, etc. In his paper performance of routing protocols was evaluated by varying number of nodes etc. But he did not investigate the performance of protocols under heavy loads (high mobility +large number of traffic sources+ larger number of nodes in the network), which may lead to congestion situations. *J Broch et al.* [12] performed experiments for performance comparison of both proactive and reactive routing protocols. In their Ns-2 simulation, a network size of 50 nodes with varying pause times and various movement patterns were chosen.

3. AODV (AD HOC ON DEMAND DISTANCE VECTOR)

Routing protocols in mobile networks are subdivided into two basic classes:
• Proactive routing protocols
• Reactive routing protocols

Routing protocols for ad hoc networks can be classified into two major types: *proactive* and *on-demand*. Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad-hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California. It is an on-demand and distance-vector routing protocol, means a route is established by AODV from a destination only when it is required or on demand. AODV is for both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. AODV also creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by ad-hoc on demand distance vector routing protocol to ensure the freshness of routes. It is loop-free, self-initiating, and scales to large numbers of mobile nodes. AODV defines three types of control messages for route maintenance: RREQ- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Each RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_ id. The RREQ contains the following fields Source, Address, broadcast ID, source Sequence no. , Destination address, destination Sequence no. Hop Count. The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast id is incremented whenever the source issues a new RREQ. RREP- A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator. RERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. The main benefit of AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. It provides loop-free routing. One of drawback of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route-Reply packets in response to a single Route-Request packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption. One disadvantage is that intermediate nodes can lead to inconsistent routes if the

source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route Request packets in response to a single Route Request packet can lead to heavy control overhead. The AODV routing protocol does not need any central administrative system to control the routing process. Reactive protocols like AODV tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. AODV reacts relatively fast to the topological changes in the network and updates only the nodes affected by these changes. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. The AODV routing protocol saves storage place as well as energy. The destination node replies only once to the first request and ignores the rest. The routing table maintains at most one entry per destination. If a node has to choose between two routes, the up-to-date route with a greater destination sequence number is always chosen. If routing table entry is not used recently, the entry is expired. A not valid route is deleted: the error packets reach all nodes using a failed link on its route to any destination. It is possible that a valid route is expired. Determining of a reasonable expiry time is difficult because the nodes are mobile, and sources' sending rates may differ widely and can change dynamically from node to node. Moreover, AODV can gather only a very limited amount of routing information route learning is limited only to the source of any routing packets being forwarded. This causes AODV to rely on a route discovery flood more often, which may carry significant network overhead. Uncontrolled flooding generates many redundant transmissions which may cause so-called broadcast storm problem.

4. PERFORMANCE METRICS

There are number of metrics that can be used to compare reactive routing protocols. Most of the existing routing protocols ensure the qualitative metrics. Therefore, the following different quantitative metrics have been considered to make the comparative study of these routing protocols through simulation.

1) **Routing overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.

2) **Average Delay:** This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.

3) **Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps. It can also be defined as the total amount of data a receiver actually receives from sender divided by the time taken by the receiver to obtain the last packet.

5) **Path optimality:** This metric can be defined as the difference between the path actually taken and the best possible path for a packet to reach its destination

6) **Packet Delivery Ratio**: The ratio between the amount of incoming data packets and actually received data packets.

5. Security Requirements of Ad hoc Networks

The current proposed routing protocols for ad hoc wireless networks allow for many different type of attacks. Due to their particular architecture, ad-hoc networks are more easily attacked than wired network. We can distinguish two kinds of attack: the passive attacks and the active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Instead, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. A good secure routing algorithm prevents the attacks like passive attack, active attack, black hole, location disclosure, wormhole, denial of service, impersonation etc. It must ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation. The term security protocol refers to authentication protocol, or cryptographic protocols, where the goal is to securely share information between two nodes. A routing protocol is considered to maintain route accuracy.

CONCLUSION

In this paper, an effort has been made to concentrate on the study and analysis of on demand/reactive routing protocol AODV. AODV is better in Route maintenance process. It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized Characteristics, security and power awareness is hard to achieve in mobile ad hoc networks. Hence, security and power awareness

mechanisms should be built-in features for all sorts of applications based on ad hoc network. In this paper we review the security problems of AODV routing protocol also.

REFERENCES

[1]Sunil Taneja and Ashwani Kush "A survey of Routing Protocols in Mobile Ad Hoc Networks" ,International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248

[2] Elizabeth M. Royer, "A Review of current routing protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communication * April 1999

[3] Pore Ghee Lay, John C. McEachen "A Comparison of Optimized Link State Routing with Traditional Ad-hoc Routing Protocols" U.S. Navy Research Paper 2.

[4] Umang Singh "Secure Routing Protocols in Mobile Adhoc Network-A Survey and Taxonomy" International Journal of Reviews in Computing 30th September 2011. Vol. 7

[5] Robinpreet Kaur & Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012

[6] Dr.D.Siva Kumar "Review: Swarm Intelligent based routing Protocols for Mobile Adhoc Networks" International Journal of Engineering Science and Technology Vol.

[7] Communications, Vol. 6, Issue 2, pp. 46-55, April 1999.

[8] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc networks", European Journal of Scientific Research ISSN 1450- 216X Vol.31 No.4 (2009).pp.566-576.

[9] S. Gowrishankar, T.G. Basavaraju, M.Singh, Subir Kumar Sarkar, "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad Hoc Networks", Proceedings of the 24th South East Asia Regional Computer Conference, November 18-19, 2007, Bangkok,Thailand

[10] "Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols" IJCSNS International Journal of Computer Science and Network Security VOL.8 No.6,June 2008

[11] Boukerche A., "Performance comparison and analysis of ad hoc routing algorithms", IEEE International Conference on. Performance, Computing, and Communications, 2001, Apr 2001, pp 171-178.

[12] Saurabh gupta "ANALYSIS OF SIMULATION OF ADHOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL", National Conference on Advanced Computing and Communication.

