International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 3, March 2015, PP 88-90
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Study of Recent Routing Strategies in Mobile Ad Hoc Networks

Srinivas Mudepalli

Research Scholar, Department of Computer Science,
Krishna University, Machilipatnam

Abstract: *Mobile Ad Hoc Network (MANETs) is a Collection of autonomous self organized mobile nodes, connected with wireless links. This network doesn't follow any fixed topology as the nodes of this network are mobile devices. As per the basic rule of networking every node must co-operate with other node to route the packets. As this network doesn't have a fixed topology conventional routing protocols may not suitable to this environment. Many routing algorithms have been proposed for MANETs. It is an important problem to model Quality of Service requirements on these types of algorithms. In This paper I have provided a study of recent routing trends in MANETS.*

Keywords: *Mobile ad hoc, routing protocols, mobile nodes, routing strategy*

1. INTRODUCTION

In Mobile Ad hoc Networks (MANET) [1][2], nodes are self-organized and use wireless links for communication between themselves. They dynamically form a temporary network without using any existing network infrastructure or centralized administration. These are often called infrastructure-less networking since the mobile nodes in the network dynamically establish routing paths between themselves. Examples are conference, battlefield, rescue scenarios, sensor networks placed in an area to monitor the environment, mesh networks for wireless Internet access etc. Routing solutions must address the nature of the network, and aim at minimizing control traffic, to preserve both bandwidth and energy at nodes.

Routing is the process of discovery, selecting and maintaining paths between nodes. By using these routes source node can send a data packet to destination. Performance of any network is influenced by its routing technique. There are many routing protocols were designed for conventional computer networks, but conventional routing strategies are impractical in MANETs because this environment has different characteristics. Nodes move in an arbitrary manner and at changing speed, often resulting in connectivity problems. This mobility causes breakage of links of between hosts frequently. Researchers have proposed many routing protocols for MANETs.

2. SWARM INTELLIGENCE

This routing strategy is developed based on the behavior of bird flocks and insect colonies. The reason is that group is better for each animal for evaluation than single. On the basis of this phenomenon researchers proposed many protocols like ANTNET, ANTHOCNET, ANT-AODV. In the following section we are mentioning recent trends in this Swarm Intelligence protocols.

AntNet RSLR: AntNet protocol with the blocking-expanding Ring Search and Local Retransmission technique (AntNet-RSLR)[4]. According to this scheme the packets used in the network can be divided into two classes – data packets and control packets. Data packets represent the information that the end-users exchange with each other. In ant-routing, data packets use the information stored at routing tables for travelling from the source to the destination node. AntNet-RSLR contains a special routing table, in which each destination is associated to all interfaces and each interface has a certain probability. Forward ant (FANT) and a backward ant (BANT) control packets are used to update the routing tables and distribute information about the traffic load in the network. In addition to the above, the neighbor control packets are used to maintain a list of available nodes to which packets can be forwarded. In this algorithm, in the route discovery phase new routes are created by FANT and BANT. A FANT is a small packet with a unique sequence number establishes the pheromone track to the source node. It gathers information about the state of network. A BANT establishes the pheromone track to the destination node. In route maintenance phase, the routes need to be monitored and strengthened during the communication. Once the FANT and BANT have established the pheromone tracks for the source and destination nodes, subsequent data packets are used to maintain the path. AntNet-RSLR recognizes a route failure through a missing acknowledgement. If a node gets a route error (RERR) message for a certain link, it deactivates this link by setting the pheromone value to 0. Then the node searches for an

alternative link in its routing table. According to this protocol, a group of mobile agents build paths between pair of nodes, exploring the network concurrently and exchanging obtained information to update the routing tables that decreases both of the routing message overhead and the average end to end delay.

ODASARA: A novel On Demand Ant based Security Alert Routing Algorithm (ODASARA) for mobile ad hoc a network in grid environment is proposed in [5]. This protocol combines the Ad Hoc On-Demand Distance Vector (AODV) routing protocol with Ant Colony Optimization mechanism using ant like mobile agents. In ODASARA, a security metric is embedded into the RREQ packet, and forwarding behaviour of the protocol is changed with respect to RREQs. Intermediate nodes receive the RREQ packet with security metric. The Security Alert Routing (SAR) ensures that this node can only process the packet or forward it if the node itself can provide the required security or trust level, otherwise the RREQ is dropped. If an end-to-end path with the required security attributes can be found, a suitably modified RREP is sent from an intermediate node or the eventual destination. The route discovered by ODASARA between two communicating entities may not be the shortest route in terms of hop-count, but with a quantifiable guarantee of security. If one or more routes that satisfy the required security attributes exist, SAR will find the shortest route. If all the nodes on the shortest path between two nodes can satisfy the security requirements, this protocol will find optimal routes. However, if the ad hoc network does not have a path with nodes that meet RREQ‟ s security requirements, SAR may fail to find a route.

There are different techniques to measure or specify the quality of security of a route discovered by SAR protocol. The first technique is the explicit representation of trust levels using a simple hierarchy. ODASARA provides applications the ability to incorporate explicit trust levels into the route discovery process. Another alternative is to use what we call the QoP (Quality of Protection) bit vector. Threats to information in transit include corruption of information, disclosure of sensitive information, theft of legitimate service from other protocol entities, or denial of network service to protocol entities. In SAR, the messages are protected by the key management infrastructure. ODASARA provides digital signatures and encryption techniques that can be incorporated on a need-to-use basis to prevent modification.

AODV (Ad-hoc On-demand Distance Vector): In AODV, when a source node has data traffic to send to a destination node, it first initiates a route discovery process. In this process, the source node broadcasts a Route Request (RREQ) packet. Neighbor nodes, which do not know an active route for the requested destination node, forward the packet to their neighbors until an active route is found or the maximum number of hops is reached. When an intermediate node knows an active route to the requested destination node, it sends a Route Reply (RREP) packet back to source node in unicast mode. Eventually, the source node receives the RREP packet and opens the route [6].

OLSR (Optimized Link State Routing) : In OLSR, each node periodically constructs and maintains the set of neighbors that can be reached in 1-hop and 2-hops. Based on this, the dedicated MPR algorithm minimizes the number of active relays needed to cover all 2-hops neighbors. Such relays are called Multi-Point Relays (MPR). A node forwards a packet if and only if it has been elected as MPR by the sender node. In order to construct and maintain its routing tables, OLSR periodically transmit link state information over the MPR backbone. Upon convergence, an active route is created at each node to reach any destination node in the network [6].

SRMP (Source Routing-based Multicast Protocol): In SRMP, route selection takes place through establishing a multicast mesh, started at the multicast receivers, for each multicast session. SRMP is classified as a mesh-based protocol. A mesh (an arbitrary subnet) is built to connect multicast group members providing robustness against link failure due to topology changes and channel fading. To minimize the flooding scope, the Forwarding Group (FG) nodes concept is used in SRMP. In fact, a population of appropriate nodes is selected to cooperate to find the best route to deliver the packets to the destination. Four metrics are used in SRMP to select FG nodes: neighborhood association stability, link signal strength, battery life and link availability estimation.

3. CONCLUSION

The goal of this paper is to provide MANET protocol designers with multiple perspective on the concept of routing strategies followed in MANET, by reading this one can understand the routing protocols implemented in MANET.

REFERENCES

[1]. Charles E. Perkins, Ad Hoc Networking, Addison-Wesley, 2001.

[2]. C.K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2001.

[3]. Intelligent Routing Techniques for Mobile Ad hoc Networks using Swarm Intelligence, IJISA-2013

[4]. Ahmed. A. A. Radwan, Tarek. M. Mahmoud, Essam. H. Hussein AntNet-RSLR: A Proposed Ant Routing Protocol for MANETs 2011.

[5]. R.Rameshkumar, Dr. A.Damodaram, ODASARA: A Novel on Demand Ant Based Security Alert Routing Algorithm for MANET in

Grid Environment, IJCSNS International Journal of Computer Science and Network Security, April 2010.

[6]. Jerome Haerri, Fethi Filali, Christian Bonnet, "Performance Comparison of AODV and OLSR in VANETs Urban Environments under Realistic Mobility Patterns" Institute Eurecomz Department of Mobile Communications, 2006.