Mobile Ad-Hoc Networks: AODV Routing Protocol Perspective

Ayaz Ahmad1, Mahfuzul Huda2, Mohd Atif Kaleem3, Rajendra Kr Maurya4

Computer Science and Engineering, Integral University, Lucknow, India1, 2, 3, 4

Abstract: In current years, an enormous research has been observed going on in the research field of Mobile Ad-Hoc Network (MANET). Despite of restricted assets in Mobile Ad Hoc Networks, to structure a proficient and consistent routing protocol is still a tough task. A more intelligent routing approach is required to proficiently use the restricted assets. Moreover the routing algorithms designed for conventional wired networks such as distance vector or link-state, does not level well in without wired situation. Routing approach in Mobile Ad Hoc Networks is a difficult work and has received a great amount of attention from area researchers and quality controller now a day. In this research paper tries to provide a general idea of the existing Mobile Ad Hoc Networks routing protocols their functionality and characteristics. Further, the protocols comparison is given depend upon the MANET routing information and methodologies on the basis of their routing decisions. This research will help the researchers and industry personnel to obtain an overview of the existing routing protocols and propose which one routing protocols could perform improved results with respect to unstable network situation.

Keywords: Mobile ad hoc Networks, AODV, routing protocols, MANET, Protocol comparison.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a host collection of wireless nodes without fixed network infrastructure and centralized administration [1-4]. Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no fixed communication infrastructure. Every wireless node in MANET acts a mobile router that sends data packets to other destination nodes. Consequently selection of suitable, effective, robust, and adaptive routing protocol is of utmost importance [5, 6]. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency [7, 8].

In this paper, Sections 2, 3, and 4 looks at working of routing protocols like, Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm (TORA) and Ad-hoc On Demand Distance Vector (AODV); Section 4 thoroughly explains the exact operation of AODV. Section also discusses some common features of AODV in MANET; further explains the complete operation of AODV; In this section some suggests for solutions to make AODV secure, Section 5 concludes the paper.

II. CLASSIFICATION OF MANET ROUTING PROTOCOLS

In this section will discuss the types of existing MANET Routing Protocols, their features, types and characteristics. The MANET Routing Protocols for Mobile ad hoc without wired environment can be separated into three broad types based on the nature of packets routing information modified method [9-11]. They could be On-demand (Reactive), Table-driven: that constantly update lists of destinations and routes (Proactive) and Combine the features of reactive and proactive protocols (Hybrid protocols). Following figure shows the categories of Mobile Ad-hoc Network Routing Protocols and name of the proposed Protocols under every MANET protocol category shown in Figure-1.

III. ROUTING IN MANETS OF MANET

A Mobile Ad Hoc Network MANET is types of network as it is self-organized, infrastructure less and multi-hop network with quickly changing topologies grounding the mobile nodes to be separated and joined again [12, 13]. In these MANET networks, every communication node must be proficient of acting as a wireless router. At the same time, a result of limited bandwidth of mobile nodes, the source node and destination node may have to establish via middle nodes shown in Figure-2 and Figure-3.

Inheritance Routing Mechanism in Mobile Ad-Hoc Networks MANET has been a field of challenging
research and in MANET environment numbers of protocols has been developed for tackling the problems of MANET routing [14-15]. These routing protocols are divided into three major categories – Reactive Routing Protocol, Proactive Routing Protocol and Hybrid Routing Protocol [16, 17].

III.I Dynamic Source Routing (DSR)

Dynamic Source Routing is a reactive kind of protocol which reacts on-demand. The main feature of DSR is source routing in which the source always knows the complete route from source to destination. It frequently uses source routing and route caching.

Methods

Route Discovery and Route Maintenance are two main methods used in DSR. It is uncomplicated and efficient protocol. It does not depend on timer-based activities. It allows multiple routes to destination node and routing is loop-free here. Any broken link is notified to the source node with an error message. It works well in large networks where routes change quickly and mobility of routes is higher.

Limitations

In DSR, intermediate nodes do not need to preserve the routing information. Instead the packets themselves contain every routing decision. DSR uses a route discovery process to find a route when a node in the network tries to send a data packet to a destination for which the route is unknown [18]. A route is found by flooding the network with route requests. When a node receives this request, it broadcasts it again until it itself is the destination or it has the route to the destination. This node then replies to the request to the original source. The request and response packets are source routed [19]. Request packet creates the path of traversal. Response packet creates the reverse path to the source by traversing backwards.

III.II Temporally-Ordered Routing Algorithm

Temporally-Ordered Routing Algorithm (TORA) is made to find routes on demand. It tries to achieve high scalability. It creates and maintains directed acyclic graph rooted at the destination node. TORA can establish routes rapidly and can provide multiple routes for a single destination. It doesn’t give Shortest-Path Algorithm too much of importance. Instead it uses longer paths to avoid finding of new routes [20]. TORA minimizes communication over as it acts only when needed and doesn’t react to every topological change as well as it localizes scope of failure reactions.

Methods

There are three main phases of the algorithm: Route Creation, Route Maintenance and Route Erasure. In the Route Creation phase, the query packet is flooded all over the network and if routes exist, an update packet is sent back. In the Route Maintenance phase update packets re-orient the route composition. The route erasure phase involves flooding of a broadcast clear packet all over the network to erase invalid routes.

Limitations

To simulate the protocol, size of network, rate of topological change and network connectivity should be kept in mind.

III.III Ad-hoc On Demand Distance Vector

AODV that is Ad-hoc On Demand Distance Vector is a Reactive Routing Protocol that acts in response on demand. It is an advancement of Dynamic Sequence Distance Vector protocol. It facilitates multi-node, dynamic routing and self-starting in MANETs environment [21, 22]. Ad-hoc On Demand Distance Vector never generates close loop in the routing table of any mobile node because of the idea of generated sequence number counter. AODV Sequence numbers provide as time stamps protocol and agree to mobile nodes to compare how new packet information reached to other nodes in the MANET architecture [23].

IV. OPERATIONS IN AODV

Quantification Route discovery process is started by a source node that wants to communicate with a destination node for which there is no routing information in its routing table. Each node broadcasts a HELLO message after a specific interval to keep track of its neighbors. Thus a node keeps track of only its next hop for a route instead of entire route.
When a node wants to communicate with a node that is not its neighbor it broadcasts a route request packet called RREQ which contains Destination IP Address, RREQ ID, Source IP Address, Source Sequence Number, Destination Sequence Number and Hop Count. Destination Sequence Number is the latest destination sequence no. received in the earlier period by the source for any route towards the destination [24].

Source Sequence Number is the latest destination sequence no. to be used in the packets route entry spot towards the source of RREQ. Every route table entry for every node must include the latest sequence number for the nodes in the MANET network [25, 26] shown in Figure-4 and Figure-5.

If not, it increments the hop count value in RREQ by one. The route table entry for the destination will be updated with the new sequence number if:
1. Destination Sequence Number received from RREQ is greater than the existing value in the route table entry.
2. The Sequence numbers are equal, but the incremented hop count is smaller than existing hop count.
3. The Sequence number is unknown.

Soon after this updating valid sequence number field in the route table entry is set to true. The node searches for a reverse route towards the Source IP Address shown in Figure-6. If need be, route is created or updated using the Source Sequence Number shown in Figure-7 [27-29].

When the reverse packets route is developed or modified following events are carried out:
1. If Source Sequence Number received from RREQ is greater than the existing value in the route table entry, it is updated.
2. The valid sequence number field is made factual and given in Critical analysis Table 1.
3. The next sequence hop in the MANET routing table becomes the node (terminal) from which RREQ was received.
4. The value of hop count is copied from RREQ packet.

**V. CONCLUSION**

MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of...
sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. Although fabrication of source routes (cache poisoning) is not possible in AODV while DSR is prone to it. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used. We should keep in mind that some solutions may not work well in the presence of more than one malicious node, while some require special hardware and some solutions are very expensive. So, there is still a lot of room for research in this area to provide a more secured MANET.

REFERENCES


