A Noble Reactive Routing Protocol for Mobile AdHoc Network based on AODV: A Review

Arushi[1] Sarabjeet[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]DVIET , Karnal, Haryana

Abstract— A Mobile Ad hoc Network (MANET) is a kind of wireless ad-hoc network. The infrastructure less and the dynamic nature of Mobile AD-HOC networks demands new set of networking scheme to be executed in order to provide efficient end-to-end communication. Mobile AD-HOC network is a collection of mobile nodes which are arbitrarily and dynamically located. Due to high mobility of nodes the topology of ad-hoc networks become highly dynamic. Efiicient routing protocol can make MANET more reliable. MANET is expected to be very useful for the formation of temporary networks in battlefield and disaster recovery such as fire, safety and rescue operations, meetings in which people likes to quickly share information. The main challenging issue of MANET is that of discovering the routes between the mobile nodes due to the continuously changing topology of ad hoc networks. In this paper we have studied the Ad Hoc On-Demand Distance Vector (AODV) routing protocol which is a reactive routing protocol. In this paper, we provide an overview of recent years enhancements that have been suggested to improve the working of AODV like RAODV, MAODV, etc.

Key words: MANET, AODV, Routing protocol, RREQ, RREP, RERR, wireless ad-hoc networks

I. INTRODUCTION

A MANET is the one consisting of a set of mobile hosts which can communicate with one another and roam around at their will. MANETs (Mobile Ad-hoc Networks) are one of the fastest emerging networks. MANET is an unstructured network in which nodes are mobile and independent. Nodes can act as hosts as well as routers. Each device in a MANET is free to move independently in any direction and will therefore change its links to the other devices frequently. Mobile devices with the wireless network interfaces became an important part of future computing environment consisting of infra-structured and infrastructure-less mobile networks. In wireless local area network based on IEEE 802.11 technology a mobile node always communicates with a fixed base station, and thus a wireless link is limited to one hop between the node and its neighbor base station, where Mobile ad hoc network (MANET) is a multi-hop infrastructure-less network where a node can communicates with other nodes directly or indirectly through intermediate nodes. Each must forward traffic unrelated to its own use, and therefore be a router. Typical MANET nodes are PDAs, Laptops, cellular phones, Pocket PCs, palmtops and Internet Mobile Phones. These devices are lightweight and battery operated Fig. shows an example mobile ad hoc network.

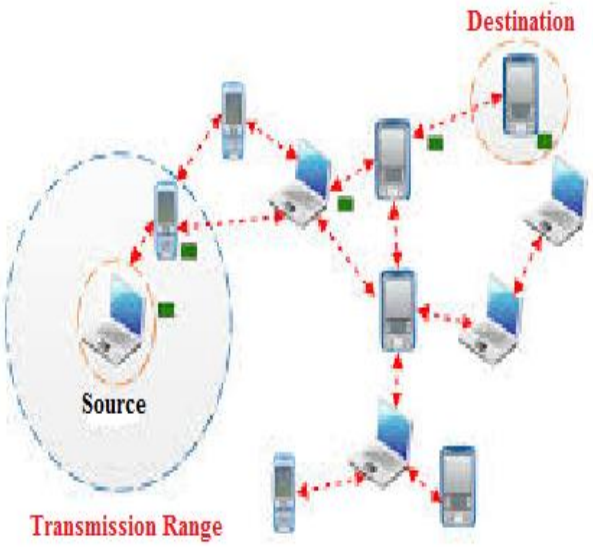

Fig. 1: Mobile Ad Hoc Network

All nodes in a MANET function as routers participating in some routing protocol which are required for creating and then maintaining the routes. Since MANET are infrastructure-less networks, they are highly used for applications such as military operations, special outdoor events, communications in infrastructure-less regions, emergencies and natural disasters. Routes between the nodes of an ad hoc network may include more than a single hop, hence, we call such networks "multi-hop" wireless ad hoc networks.

A. *Characteristics of MANET:*

- Communication via wireless network
- Easy to Deploy
- Dynamic network topology
- Nodes perform roles of both hosts and router
- Flexible
- No infrastructure needed
- Frequent routing updates
- Can be set up anywhere
- Some applications of MANET are
- Defence Development
- Disaster relief operations
- Mine site operations
- Urgent business meetings

II. ROUTING IN MANET

One of the major issues that affects the performance of an ad hoc network is the way routing is implemented in a network. Generally, routing is the process of discovery, selecting, and maintaining paths from a source node to destination node deliver data packets. This is a main challenge in MANET, because the MANET possesses dynamic and random

characteristics. Nodes move in an arbitrarily manner and at changing speed, often resulting in connectivity problems. The high mobility and the arbitrarily movement of nodes in MANET causes links between hosts to break frequently.
Manet Routing Protocols:
The routing of traffic between nodes is performed by a MANET routing protocol. MANET routing protocols can be divided into three categories. In table driven/ proactive routing protocols, nodes periodically exchange routing information and attempt to keep up-to-date routing information. In on-demand/reactive routing protocols, nodes only try to find a route to a destination when it is actually needed for communication. There are a number of proactive routing protocols. They differ in various areas like number of routing table maintained and how the changes are propagated in the network. In the following sections, we first describe the two categories of MANET routing protocols in more details. We then list the challenges faced by MANET routing protocols. The third category is hybrid routing protocols. It is the advanced routing protocol which include both reactive and proactive in nature. Hybrid routing protocols are both proactive and reactive in nature. There protocols work on the merits of these protocols to increase scalability and to decrease the routing overhead .

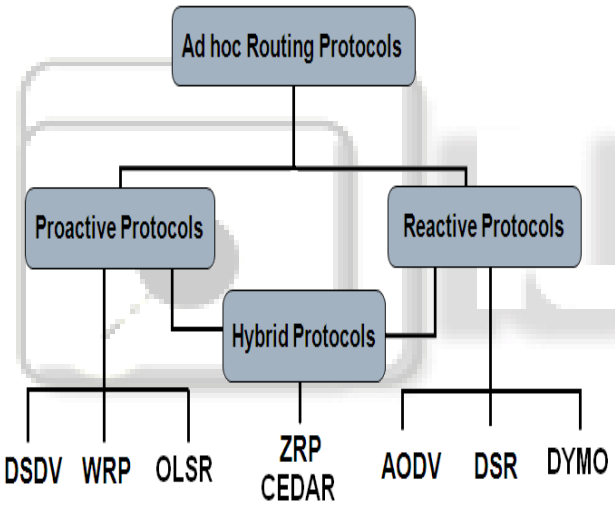

Fig. 2: MANET routing protocols

A. On-Demand Routing Protocols/Reactive Protocols:

On-demand routing protocols only maintain routes that are actually used. On-demand protocols use two different operations to find and maintain routes: the route discovery process operation and the route maintenance operation. When a node wishes to communicate with some other node it tries to find a route to that node, i.e., routing information is acquired on-demand. This is the route discovery operation. Route maintenance is the process of responding to changes in topology that happens after a route has initially been created. The nodes in the network try to detect link breaks on the established routes. Examples of on-demand protocols are DSR, AODV, and DYMO). A disadvantage of the reactive approach is that when the sending node has to discover a route to the destination, the initial delay before data is exchanged between two nodes can be long. It can also results in high rotational latency.

B. Table-Driven Routing Protocols/Proactive Routing Protocols:

Proactive routing protocols maintain routing information continuously. Typically, a node has a table containing information on how to reach every other node (or some subset hereof) and the algorithm tries to keep this table up-to-date. Changes in network topology are propagated throughout the network. Examples of proactive protocols are the Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), Highly Dynamic Destination-Sequenced Distance-Vector Routing, and OLSR.

C. Hybrid Routing:

Hybrid protocols are new generation of protocol. Which are the combination of reactive and proactive and as a result routes are found very fast in routing zone taking advantages both of these protocols e.g. ZRP. These protocols works good for networks which have small no of nodes. Also as the no. of nodes increases then hybrid protocols gives better performance. Reactive routing procedure is to be used at global network level whereas proactive routing procedure is used in a nodes local neighborhood. Hence, hybrid routing is a combination of proactive and reactive routing which performs better.

III. Overview of AODV

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is a reactive protocol. As is the case with all reactive ad hoc routing protocols, AODV consists of two protocol operations:
1) Route discovery
2) Route maintenance.

A. Route Discovery:

Route discovery is the process of creating a route to a destination when a node lacks a route to it. When a node S wishes to communicate with a node T it initiates a Route Request (RREQ) message including the last known sequence number for T and a unique RREQ id that each node maintains and increments upon the sending of an RREQ. The message is flooded throughout the network in a controlled manner, i.e., a node only forwards an RREQ if it has not done so before; the RREQ id is used to detect duplicates. Each node forwarding the RREQ creates a reverse route for itself back to S using the address of the previous hop as the next hop entry for the node originating the RREQ .

When the RREQ reaches a node with a route to T (possibly T itself) a Route Reply (RREP), containing the number of hops to T and the sequence number for that route, is sent back along the reverse path. An intermediate node must only reply if it has a fresh route, i.e., the sequence number for T is greater than or equal to the destination sequence number of the RREQ. Since replies are sent on the reverse path, AODV do not support asymmetric links. Each node receiving this RREP creates a forward route to T in its routing table, and adds the node that transmitted the RREP in precursor list for this entry. The precursor list is a list of nodes that might use these node as next hop towards a destination. Route discovery is illustrated in Fig3, where node 2 wants to communicate with node 9 and floods an RREQ message in the network. Node 9 replies with an RREP. Intermediate

nodes learn routes to both source and destination nodes via the RREQ and RREP packets .

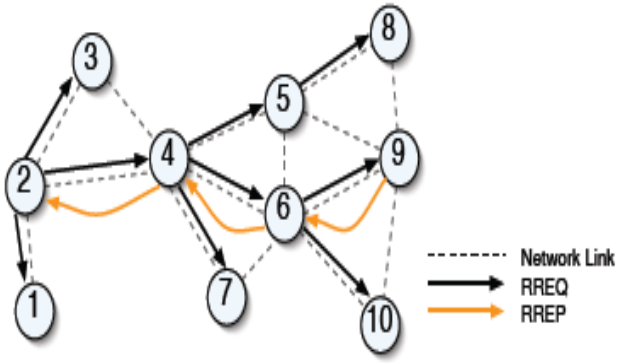

Fig. 3: Route discovery in AODV.

If an intermediate node has a route to a requested destination and sends back an RREP, it must discard the RREQ. Furthermore, it may send a gratuitous RREP to the destination node containing address and sequence number for the node originating the RREQ. Gratuitous RREPs are sent to alleviate any route discovery initiated by the destination node. It might not have received any RREQs and has not learned a route to the originator of the RREQ .

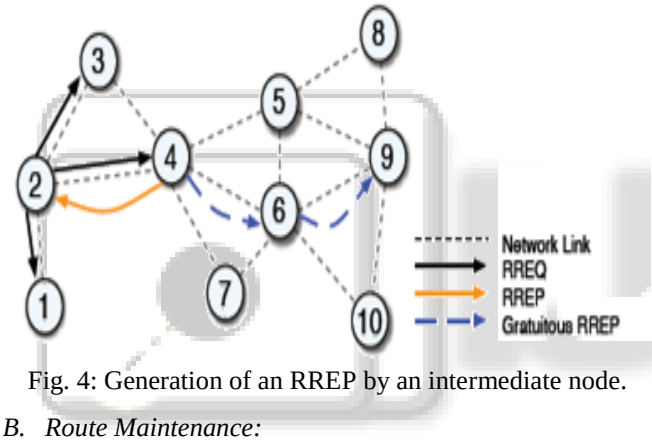

Fig. 4: Generation of an RREP by an intermediate node.

B. Route Maintenance:

Route maintenance is the process of responding to changes in topology. To maintain paths, nodes continuously try to detect link failures (when a neighbour go out of range, the node itself moves, or some other event limiting the communication on the link). Nodes listen to RREQ and RREP messages to do this. Furthermore, each node promises to send a message every n seconds. If no RREQ or RREP is sent during that period, a Hello message is sent to indicate that the node is still present. Alternately, a link layer mechanism can be used to detect link failures. Beside the observation of a link failure, a node must also respond when it receives a data packet it does not have a route for .

When a node detects a link break or it receives a data packet it does not have a route for, it creates and sends a Route Error (RERR) packet to inform other nodes about the error. The RERR contains a list of the unreachable destinations.

If a link break occurs, the node adds the unreachable neighbor to the list. If a node receives a packet it does not have a route for, the node adds the unreachable destination to the list. In both cases, all entries in the routing table that make use of the route through the unreachable destination are added to the list.

The list is pruned, as destinations with empty precursor lists, i.e., destinations that no neighbors currently make use of, are removed. The RERR message is either unicasted (in case of a single recipient) or broadcasted to all neighbors having a route to the destinations in the generated list. This specific set of neighbors is obtained from the precursor lists of the routing table entries for the included destinations in the RERR list .

When a node receives an RERR, it compares the destinations found in the RERR with the local routing table and any entries that have the transmitter of the RERR as the next hop, remains in the list of unreachable nodes. The RERR is then either broadcasted or unicasted as described above. The intention is to inform all nodes using a link when a failure occurs. For example, in Fig5, shows the generation of route error message (RERR). The fig. shows that link between the node is broken and when the link is broken then it generate the route error for the neighboring nodes .In fig the link between node 6 and node 9 has broken and node 6 receives a data packet for node 9. Node 6 generates a RERR message, which is propagated backwards toward node 2. To find a new route, the source node can initiate a route discovery for the unreachable destination, or the node upstream of the break may locally try to repair the route, in either cases by sending an RREQ with the sequence number for the destination increased by one .

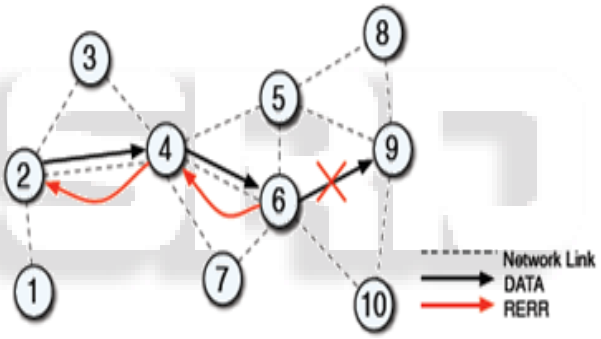

Fig. 5: Generation of RERR messages.

IV. LITERATURE REVIEW

Mustsfa Bani Khalaf, Ahmed Y.Al-Dubai [1]:Mobile ad hoc networks (MANETs) have been gaining tremendous attention owing to the advances in wireless technologies accompanied by many applications and implementations. However, there are still a number of issues in MANETs which require further investigations and efficient solutions. Out of these issues, broadcasting in MANETs has been a major problem for both industry and the research community. The broadcast communication is usually required to disseminate a message to all the nodes of a network. This operation is highly required in MANETs to distribute necessary information and ensure efficient control and coordination over the network nodes. However, broadcasting in MANETs is usually susceptible to several challenging communication issues, including, flooding, packets contentions and collisions, i.e., these problems all together are called the Broadcast Storm Problem (BSP). Despite a number of suggested solutions for BSP, the probabilistic scheme is considered the most promising solution due to its simplicity and suitability for MANETs. Under the umbrella of this scheme, many dynamic probabilistic broadcasting algorithms have been proposed in the literature to solve the

BSP. However, most of them are not suitable for many applications including those real life scenarios as there are many limitations such as the probability of rebroadcasting operation and thresholds rebroadcasting permission, which is caused by collecting local neighbourhoods' connectivity by broadcasting HELLO packets. In an attempt to enhance and promote the quality of the probabilistic scheme, this paper proposes a new probabilistic approach to overcome these limitations. Our proposed approach is augmented with a well-know ad hoc routing protocols including Ad hoc On demand Distance Victor protocol (AODV). We have conducted intensive simulation experiments under different operating condition. The simulation results show that our proposed approach outperforms its counterparts including the well known blind flooding, fixed probabilistic and traditional dynamic probabilistic approaches.

Kulvir Kaur, Sonia Goyal[2]:With the advancement in wireless communications, more and more wireless networks appear, e.g., Mobile Ad Hoc Network (MANET), Wireless Sensor Network (WSN), etc. Shortest path routing is very efficient as it saves time and economically beneficial in terms of cost. One of the most important characteristics in mobile wireless networks is the topology dynamics, that is, the network topology changes over time due to energy conservation or node mobility. In recent years, the routing problem has been well addressed using intelligent optimization techniques, e.g., Artificial Neural Networks (ANNs), Genetic Algorithms (GAs), Particle Swarm Optimization (PSO), etc. In this paper we will discuss these algorithms on various wireless networks.

Anumeha ,Bhawna Mallick[3]:An ad-hoc network is a multi-hop wireless network system where all the nodes cooperatively maintain the network connectivity without any centralized infrastructure. If these nodes in the network cannot remain in their same positions means position various dynamically, that is called a mobile ad-hoc network (MANET) system. Efficient protocols are used here to forward data packets with very low packet loss.In this paper, .an adaptive routing algorithm is proposed in MANET using modified AODV by calculating the loads on different routes using given parameters like aggregate interface queue length and nodes remaining energy. An Adhoc on Demand Distance Vector Protocol (AODV) for routing is one among the effective Reactive Routing Protocols in MANET. The objective of this paper is to basically enhance the AODV network performance, when frequent link failures in network due to mobility of the nodes. The simulations and performance analysis are carried out to evaluate the network performance using Network Simulator tool (NS-2), based on the quantitative metrics packet delivery ratio and average end to end delay. The achieved simulated result helps to understand the precise behaviour of the AODV in the distributed network environment. This paper proposed a new protocol E-AODV (Enhanced AODV) which is a modified AODV with Enhanced packet delivery ratios and minimized end to end packet delay.

Vijaya Singh, Megha Jain [4]:Mobile Adhoc Networks are type of wireless network which are infrastructure less, self organizing, highly mobile and quickly deployable. There is no central authority, the communication occur hop by hop based on cooperation among the nodes. Thus, secure routing protocols are needed which are robust and ensure that the nodes in the network behave in trustworthy manner otherwise detect and eliminate the untrustworthy nodes which degrade the overall network performance. There are several trust based AODV routing protocols given in the past. In this paper, we have given a survey of trust based AODV, in which concept of TRUST is used to ensure secure routing and improved network performance.

P.Samundiswary,P.Dananjayan[5]:Recent advances in wireless networks have prompted much research attention in the area of wireless sensor network (WSN). Sensor network consists of hundreds to thousands of low power multifunctioning sensor nodes operating in hostile environment with limited computational and sensing capabilities. These sensor devices are susceptible to various attacks such as selective forwarding or sinkhole attacks when operated in a wireless medium. Reactive routing protocols such as ad-hoc on demand distance vector routing (AODV) of sensor networks have been developed without considering security aspects against these attacks. In this paper, a secure routing protocol named secured ad hoc on demand distance vector routing (S-AODV) is proposed for mobile sensor networks by incorporating trust based mechanism in the existing AODV. Zigbee hardware prototype is also implemented and tested by increasing the sizes of data and distances in indoor and outdoor environment. Simulation results prove that S-AODV outperforms the AODV by reducing the overhead and improving the delivery ratio of the networks.

V. CONCLUSION

In this Paper, we have study different papers on reactive routing protocol in MANET, to find out the route which make a reduction in end to end delay, overhead and energy consumption. The biggest challenge in designing wireless ad hoc network is routing and limited availability of energy resources. To overcome these problems a lot of routing protocols exist there. Performance alters continuously according to variation in network properties and network parameters . So we will design the protocol in such a way that which performs best.. All these protocols proved that they perform better than the original AODV.

REFERENCES

[1] Khalaf, Mustsfa Bani, Ahmed Y. Al-Dubai, and William Buchanan. "A new adaptive broadcasting approach for mobile ad hoc networks." Wireless Advanced (WiAD), 2010 6th Conference on. IEEE, 2010.
[2] Kulvir Kaur, Sonia Goyal, "Optimized Routing in Wireless Ad Hoc Networks" international journal of communication engineering and technology (IJCET) , Issue No. 1, Vol. 2, Page No.69-74, March 2011
[3] Mallick, Bhawna. "Introducing Efficient AODV Routing Protocol for MANET."International Journal of Computer Applications 124.3 (2015).
[4] Singh, Vijaya, and Megha Jain. "A Survey of Trust Based AODV Routing Protocols in MANETS."
[5] Samundiswary, P., and P. Dananjayan. "Performance Analysis of Trust Based AODV for Wireless Sensor Networks." International Journal of Computer Applications 4.12 (2010): 6-13.

