A Noble Reactive Routing Protocol for Mobile Ad-Hoc Network Based on AODV

Arushi Sharma[1] Sarabjeet[2]
[1]M Tech Scholar [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]DIET, Karnal, Haryana

Abstract— A Mobile Ad-hoc networks formed by a collection of mobile nodes that are connected dynamically, in which each node act as router to all other nodes. Because of the absence of centralized administration this network is self-organising. Efficient 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. Mobile nodes in such network communicate with each other via wireless links because the nodes are moving, routing in such setup is always a challenge. In MANET, we are using Trust based QOS aware routing protocol i.e. TAODV for identifying the nodes in the network. Since, trust is mandatory in routing for transmission of data securely. We purpose a trust based routing protocol for mobile adhoc network known as TAODV. This paper presents a comprehensive study about the working of AODV protocol and for improvement /enhancement in AODV, a new protocol TAODV is purposed to improve the end to end delay, Packet delivery ratio, Throughput, Energy consumption, Network routing load and also discusses its comparison with AODV, MAODV, and RAODV protocol.

Key words: MANET, AODV, Routing Protocol, RREQ, RREP, RERR, Wireless Ad-Hoc Networks

I. INTRODUCTION

MANET: 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 neighbour 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. 1 shows an example mobile ad hoc network.

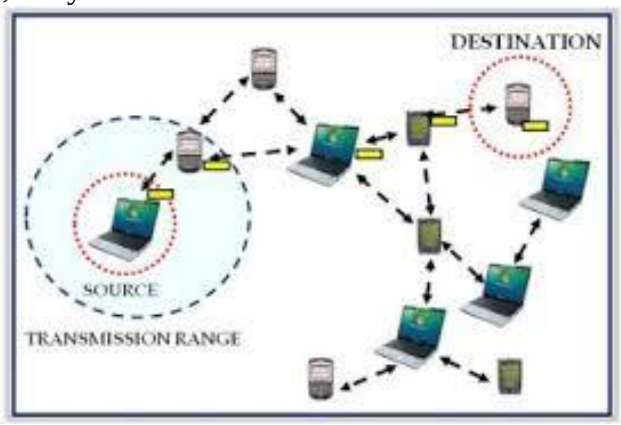

Fig. 1: Mobile Adhoc Network

All nodes in a MANET function as routers by participating in some routing protocol which are required for creating and then maintaining the routes. Since MANET are infrastructure-less networks, they are highly useful for applications such as military operations, communications in infrastructure-less regions, special outdoor events, 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 and Advantages of MANET

In general MANET is having the same characteristics of wireless network, and additional Characteristics those are is specific to the Ad Hoc Networking:

1) Wireless: Each node communicates through wireless media and shares the same media (radio, infra-red, etc.).
2) Ad-hoc-based: MANET is a collection of nodes which is dynamically formed a temporary network in an arbitrary manner as need arises.
3) Infrastructure-less and Autonomous: MANET does not depend on centralized administration or any established infrastructure. Each node in MANET acts as a router, and generates independent data.
4) Multi-hop routing: 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.
5) Mobility: while communicating with other nodes each node is free to move. Topology of an ad hoc network is dynamic in nature due to constant movement of the nodes, causing the communication patterns among nodes to change frequently.

The advantages of mobile adhoc networks are following:

1) Accessibility: Regardless of geographic position MANET provides access to information and services.
2) Deployment: The networks can be set up easily at any place and time.

3) Infrastructure-less: MANET is an infrastructure-less network. This allows people and devices to interwork in areas with no supporting infrastructure.
4) Dynamic: MANET can freely and dynamically self-organize into arbitrary and temporary network topologies.

B. MANET Applications

Ad hoc networks can be set up anywhere at any time Because they are flexible, infrastructure-less, including administration or pre-configuration, because of these simplicity people realizes the commercial potential that mobile ad hoc networking can bring.

This section describes some of the applications of ad hoc networks. The lack of infrastructure and self-configuring nature make them highly appealing for many applications. The lack of infrastructure is good for low-cost commercial systems, since it require a large investment to get the network up and running. Lack of infrastructure is also good for military systems, where communication networks must be configured as quickly as possible, often in remote areas. Other advantages include low maintenance cost and ease of network reconfiguration.

1) Search and Rescue Operations.
2) Sensor Network.
3) Military Networking.
4) Personal Area Network.

C. Design Issues and Challenges

Ad hoc wireless networks have the traditional problems of wireless communications, such as power control, bandwidth optimization, and enhancing the quality of transmission, while, in addition, multi-hop nature, their mobility, and the lack of infrastructure causes a number of complexities and design constraints.

1) Quality of Service: For the successful communication of nodes in the network Quality of Service (QoS) guarantee is very much essential. The different QoS metrics includes packet loss, throughput, jitter, delay, and error rate.
2) Network Security: Mobile networks are more vulnerable to security threats than fixed-wired networks. Mobile networks are more vulnerable to security threats because it uses open and shared broadcast wireless channels means nodes with inadequate physical protection. In addition, because a mobile ad hoc network is a infrastructure-less network, since there is no centralized security control MANET mainly relies on individual security solution from each mobile node.
3) Robustness and Reliability: MANET is multi-hop network, so network connectivity is obtained by forwarding and routing among multiple nodes. Although MANET comes with the advantage of infrastructure-less, it also causes design challenges. Due to various types of failed links, a node may fail to forward the packet, like overload or acting selfishly. Unreliable links misbehaving nodes and can have a severe impact on overall performance of the network. Such types of misbehaviours cannot be find and isolated quickly because of the lack of centralized monitoring and management mechanisms. This increases the design complexity significantly.
4) Energy Constrained Operation: Each node in MANET is battery powered which cannot be recharged. So if a node runs out of the energy then this may cause partitioning of network. Since each node has limited power, energy becomes main threats to the network lifetime. Additional energy is required to forward packets because each node is acting as both a router and an end system at the same time.
5) Limited Link Bandwidth and Quality: Since the mobile nodes communicate to each other via wireless links it cause bandwidth-constrained, error-prone, variable capacity, since wireless links have significantly lower capacity than wired links and, hence, it causes network congestion.
6) Dynamic Topology: The dynamically nature of ad hoc network causes to the formation of an unpredicted topology. This topology change causes dropping of packets, partitioning of the network and frequent changes in route.
7) Infrastructure-less network: The key aspect of an ad hoc network is its lack of infrastructure, and most design issues and challenges come from this characteristic. Also, it brings added difficulty in fault detection and correction because of lack of centralized mechanism.

D. 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.

E. 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.

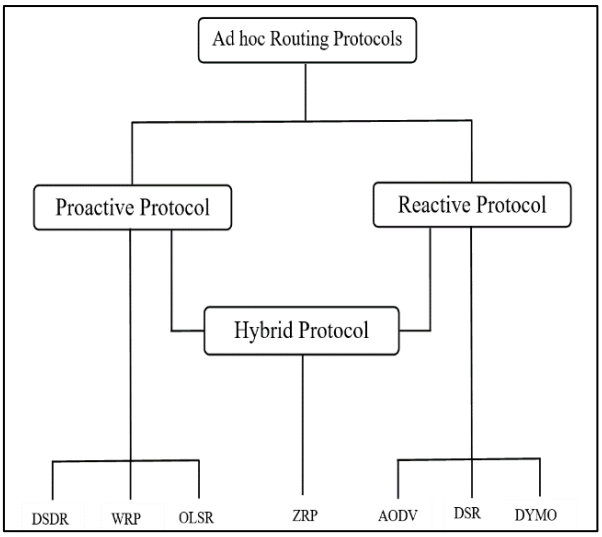

Fig. 2: MANET routing protocols

1) 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.

2) 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.

F. Manet Routing Protocol Challenges

MANET routing protocols face some challenges to be able to work in the envisioned application areas as described earlier.

1) Dynamic topology: Nodes can appear and disappear at random. Nodes can move continuously or be powered off when entering sleep mode. This means that, for example, the routing protocols cannot assume that once information is gained about the topology, it remains fixed and must consider the cost of constantly updating routing information.
2) Resource constraints: Nodes can have limited resources with respect to computational power, e.g., RAM and CPU power available, power supply, and cost of communication. In addition, there are constraints with regard to bandwidth on the wireless link, the effects of multiple access, fading, noise, and interference conditions may severely limit the transmission rate or even prevent link establishment.
3) Heterogeneity: Nodes can have varying characteristics with respect to the resource constraints specified above and be more or less willing to participate in routing.

G. The Aodv Routing Protocol

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.

1) 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 this node as next hop towards a destination.

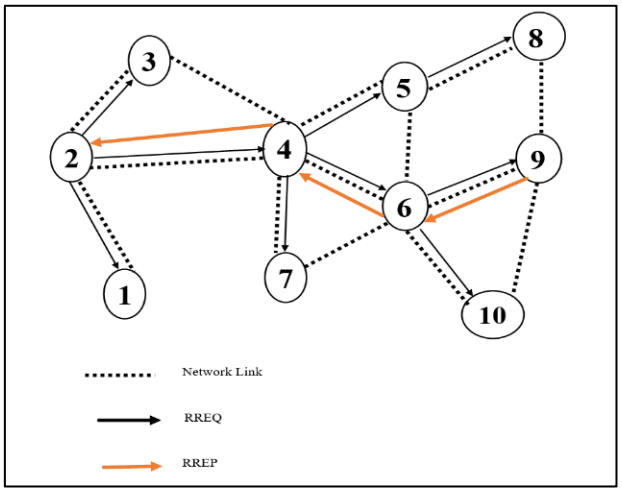

Fig. 3: Route discovery in AODV.

Route discovery is illustrated in Fig.3, 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.

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.

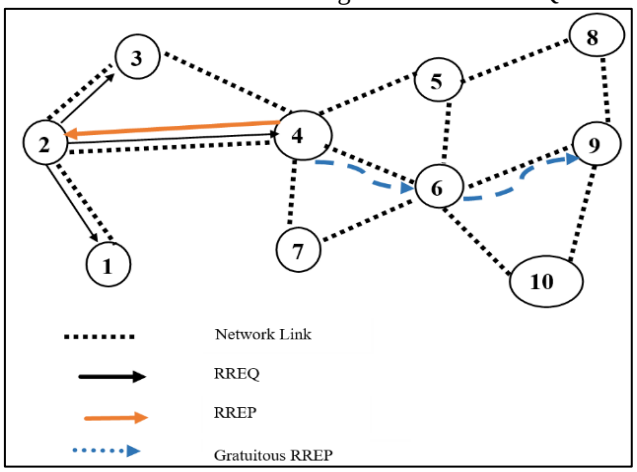

Fig. 4: Generation of an RREP by an intermediate node

2) 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 neighbour 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 neighbours currently make use of, are removed. The RERR message is either unicasted (in case of a single recipient) or broadcasted to all neighbours having a route to the destinations in the generated list. This specific set of neighbours 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.

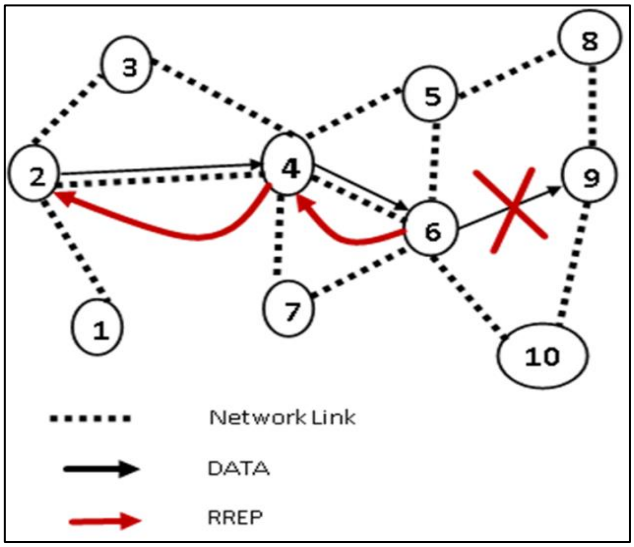

Fig. 5: Generation of RERR messages

For example, in Fig.5, shows the generation of route error message (RERR). The fig. shows that link between the nodes is broken and when the link is broken then it generate the route error for the neighbouring 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.

II. LITERATURE REVIEW

Shobha Tyagi, et al. (2016) [1] Proposed that the basic framework of MANETs relies on best effort delivery of data and does not make any promises regarding assuring Reliability or Quality of Services. Seeing today's demand of multimedia applications and need of being always connected with or without internet is constantly attracting the researchers to evolve the MANETs (Mobile Ad hoc Networks) in order to assure the guarantee of services in terms of quality. In this paper the authors have critically examined the basic AODV a reactive routing protocol of MANET, with all its positive and negative characteristics. AODV (Ad hoc On Demand Distance Vector) is also examined for Quality of Service (QoS) provisioning. In this paper to support QoS, a Reliability aware variant of AODV is proposed. This reliability aware variant of AODV (RA-AODV) is based on conferring stability to routes. The chosen routes are constrained with End-to-End Delay and Bandwidth parameters to provide quality services to application layer. After that to enhance the reliability speed of intermediate nodes is taken into account. If node moves with slow speed stability of route is not hampered but if not, high speed node has to adjust some of its neighbouring node which can act on its behalf as a part of ongoing route part. An extensive simulation performed on basic AODV, MAODV (Modified-AODV constrained with EED and Bandwidth only, no speed parameter considers) and RA-AODV (Reliability Assured AODV) is tabulated and

presented graphically in terms of PDR (Packet Delivery Ratio) , Throughput and EED (End-to-End Delay) based on Mobility .

Hosny M. Ibrahim ,et al.(2015) [2] Presents that the Mobile ad hoc network (MANET) has a distributed and uncontrolled nature in which all nodes are considered trusted and contribute in the route discovery process. Accordingly, MANET is vulnerable to many types of routing attacks. One of the most popular MANET routing protocol that is vulnerable to different attacks is ad hoc on demand distance vector (AODV) routing protocol. In this paper, a mobile backbone network of trusted nodes is proposed to enhance AODV security with minimum overhead. The proposed backbone network does not violate the MANET mobility characteristic. It is constructed from randomly moving regular MANET nodes based on their trust value, location, and power. The backbone network monitors regular nodes as well as each other to periodically estimate monitoring trust values which represent the reliability of each node in the network. The simulation results show that the backbone network is trustable, has dynamic behavior, and has good coverage.

V.L. Pavani, et al. (2015) [3] Suggested that the improvisation version of traditional wireless networks provide mobile ad hoc network (MANET), which is highly suitable for emergency needs. But, at the same time, due to its infrastructure less and resources limitation create many challenges in its performance. Mainly due to its dynamic behaviour it prones to high security concern, as the complete communication cycle depends on the independent nodes which voluntary join and leave. Several security studies reveal that trust management systems can be effective and attained low overhead. But, most of these studies used an automated decision algorithms based on some predefined trust scheme. This kind of scheme unable to distinguish the node intentional and unintentional errors at runtime, which impact the selected paths for the communication. So, it is very important to identify node behaviour and also provide node recovery scheme. In this paper, we propose a novel trust management system based on node behaviour predication algorithm to preserve high network stability and security for the reliable data delivery. The algorithm will predict and identify the node behaviour and distinguish between unintentional temporary errors and intentional malicious behaviour and compute a node overall trust. Experimental results show that, node behavior prediction and trust management system improvise the throughput ratio and network stability.

Sebastian Schellenberg, et al. (2014) [4] proposed that in disaster scenarios, a stable and reliable communication is essential for coordinating rescue operations. As the communication infrastructure could be hit, e.g. by earthquakes or hurricanes, mobile ad hoc networks (MANETs) can be used for connection establishment. As such networks should be decentralized to increase robustness, some usual services are no longer available. In our previous publications, we presented our name resolution framework based on an adaptive routing system. In this paper, we show a service discovery mechanism based on this system. We show, how this mechanism can easily be improved with the use of location information, which is an important issue for service availability.

Tanmoy Kanti Hadler, et al. (2014) [5] proposed that the Computation and routing in Mobile Ad hoc Network (MANET) is strongly co-related with power resource. Recent trend is to minimize the power consumption and maximize the computation without hampering the quality of service in MANET. To increase durability, battery resource of a node that has more power than its neighbor nodes could be used for routing and computation. In this paper a power aware routing scheme based on AODV protocol is presented. The protocol focuses on increasing network lifetime by taking into account residual capacity of the nodes with respect to its neighbors, its internal load as well as no. of message transfers. The protocol finds durable routes having nodes with more residual energy. The results achieved demonstrate the robustness of the proposed algorithm.

Arvind Kumar Shukla Banasthal, et al. (2013) [6] Presents that the Wireless communication system is gaining to much attention for reliable communication. One of modern communication system is Mobile Ad-Hoc Networks (MANET) and it has several routing protocols for communication. The AODV is the one of efficient protocol for the MANET. In this paper we are proposing a novel technique for modeling for AODV routing protocol. The proposed technique is based on the Markov random walk model. Here we calculate the probability distribution for the several operations for efficient communication. This analysis is helpful to understand the dependency of the various factor over the AODV and it impact on QoS. Its effectiveness and efficiency has been checked by various parameters and further analysed for the reliability and scalability.

III. PROBLEM FORMULATION

The Ad Hoc On-Demand Distance Vector routing protocol (AODV) is an improvement of the Destination-Sequenced Distance Vector routing protocol (DSDV). It is based on distance vector and also uses the destination sequence numbers to determine the freshness of the routes. It operates on the On-demand fashion. AODV requires hosts to maintain only active routes. The advantage of AODV is that it tries to minimize the number of required broadcasts. It creates the routes on an on-demand basis, as opposed to maintain a complete list of routes for each destination. Therefore, the literature on AODV classifies it as a pure on demand route acquisition system. The usage of the AODV protocol for mobile ad hoc networking applications provided consistent results for large scale scenarios. It has been observed from the literature that in the existing routing protocol they do not evaluate the reliability of node on the bases of their current health that they have done so far just make the prediction on the bases of the position of the node.In our proposed work we do consider node position and node speed and node energy for the better efficiency.

IV. OBJECTIVES

Aim of our study is to identify which Topology based routing protocol has better performance in MANET. The main purpose of our thesis is to study different routing

protocols of MANET and to find protocols that more suitable in various scenarios (City & Highway). We will use these parameters i.e. Throughput, packet delivery ratio, end-to-end delay, energy and network routing load for comparison with already implemented protocol in MANET. To achieve this we have set the following objectives:

- Analysis the various routing protocol used in MANET.
- Propose the new routing protocol or may be modify the existing routing protocol.
- First objective is to make patch of AODV Routing protocols in NS2.
- To build TCL scripts for different no of nodes with speed.
- To improve the AODV routing protocol AND Comparing performance results of the proposed MANET protocols with the other traditional protocol based on parameters like end to end delay, packet delivery ratio, throughput, energy and network routing load.
- Implement result of routing protocol on network simulator tool.

V. METHODOLOGY

We design a routing protocol for MANET and name given is T-AODV (Trust based ADHOC on demand distance vector).

Flow Chart for Proposed Scheme

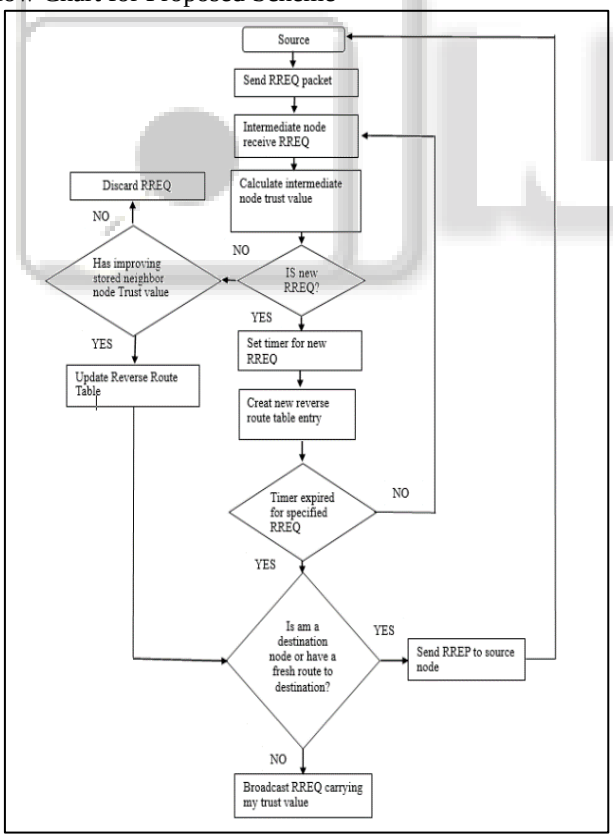

Fig. 6: Flow Chart for Proposed Scheme

A. Control Messages in AODV

Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR) and HELLO Messages are the control messages used for the discovery and breakage of route. The control packets are used to discover routes and then Discovered routes are used to send data packet.

B. Route Discovery and Route Maintenance

AODV has two basic operations: route discovery and route maintenance

Step 1: Whenever there is a need to establish connection source node looks for the route to destination in the routing table. But if there is no path or the path is invalid, then the source node broadcast the ROUTE REQUEST PACKET (RREQ) to the neighbouring nodes targeting the destination and waiting for route reply.

The RREQ packet contains – source node's IP address, source node's current sequence number, destination IP address, destination sequence number

Step 2: Intermediate node receive the route request packet if one of the neighbour node is the destination node then it sends the route reply packet (RREP) otherwise it forward the RREQ to its neighbour nodes.

Step 3: calculate intermediate node trust value. Trust value is defined as it is the combination of node speed, node energy and node position.

Trust value = Node Speed + Node Energy + Node Position

Step 4: If any particular node or any intermediate route node receive RREQ from two or more node, but does not forward it again, because that node has already forwarded RREQ once. Sequence numbers help to avoid the possibility of forwarding the same packet more than once.

If the trust value of the stored neighbouring node is improved or increased then that node update its reverse route table. After updating the route table node checks for itself is am a destination node or have a fresh route to destination if yes then send route reply (RREP) to source node.

Unless the trust value does not improved the RREQ packet is discard.

Step 5: Set timer for each new route request message arrive. For example timer is set for 1second for each new arrival of route request message. After that limited time interval time expired for specified route request packet.

Step 6: Each node maintain an additional data table called route table.

Once an intermediate node receives a RREQ, the node sets up a reverse route entry for the source node in its route table. Reverse route entry consists of Source IP address, Source seq. number, number of hops to source node, IP address of node from which RREQ was received.

Each route table entry for a given destination store all the route from that node to destination. Using the reverse route a node can send a RREP to the source.

Step 7: A RREQ message is initiated with small time to live (TTL) and a specified number of hops by the source. If the TTL values in the RREQ have reached a certain threshold and still no RREP messages have been received, then the destination assumed to be unreachable and the messages queued for this destination are discarded.

Step 8 : Now, the current route node who receive the RREQ check itself weather it's the intended destination or have a fresh route to destination.

Each destination node maintains a monotonically increasing sequence number and the protocol ensures that

nodes only update routes with fresher/ newer ones by using sequence numbers.

If decision is positive/yes then the intended node respond to RREQ by sending RREP to the source node using reverse route table. Forward links are setup when RREP travels along the reverse path.

If decision is negative/no then the node rebroadcast the RREQ packet to its neighbouring node carrying my trust value.

Step 9 : If the TTL values in the RREQ have reached a certain threshold and still no RREP messages have been received, then the destination assumed to be unreachable and the messages queued for this destination are discarded. And send the route error packet (RERR) to the source node.

When the source node receive the rout error packet it can reinitiate the route discovery process.

For route maintenance each node periodically sends HELLO messages to its precursors where a precursor list is a set of nodes that route through the given nodes. Similarly, each node expects to periodically receive messages from each of its outgoing nodes. Outgoing nodes list is the set of next-hops that a node routes through. The node is presumed to be no longer reachable, if a node has received no message from some outgoing nodes for a specified period of time and it removes all affected route entries and generate a route error (RERR) message. A node only forwards a RERR message if at least one route has been removed and route repair process will start. The RERR message contains a list of all destinations that have become unreachable as a result of broken link. The node sends the RERR to each of its precursors. These precursors update their routing tables and forward the RERR to their precursor and so on. When the source node receive the rout error packet it can reinitiate the route discovery process.

VI. RESULTS

We want to evaluate the performance of purposed protocol T-AODV using NS-2. In our model, a network with 50 mobile node which are randomly and uniformly distributed in a rectangular region of 500x500 unit square. We simulate our proposed T-AODV protocol by with other AODV (original-AODV) protocols.

The simulation parameter or specifications are summarised below:

Simulator	NS-2.34
Area	500m x 500m
Routing Protocol	AODV
Simulation time	300s
Number of Nodes	50
Packet Size	512Mac
Protocol	Mac/802.11
Transmission rate	4 Packets /s
Maximum speed	0,10, 20, 30, 40,50, 60 m/s
No of Connections	5 Movement Model Random Waypoint

Table 1: Simulation parameter

A. *Packet Delivery Ratio*

Mobility	AODV	MAODV	RA-AODV	Purposed
5	0.5	0.72	0.97	0.99
10	0.53	0.73	0.98	1
15	0.57	0.73	0.99	0.99
20	0.6	0.83	1	1
25	0.62	0.87	1	1
30	0.63	0.9	1	1

Table 2: Comparison of the QOS parameters as PDR on the basis of Mobility of 50 nodes for AODV, MAODV, RA-AODV and purposed (T-AODV)

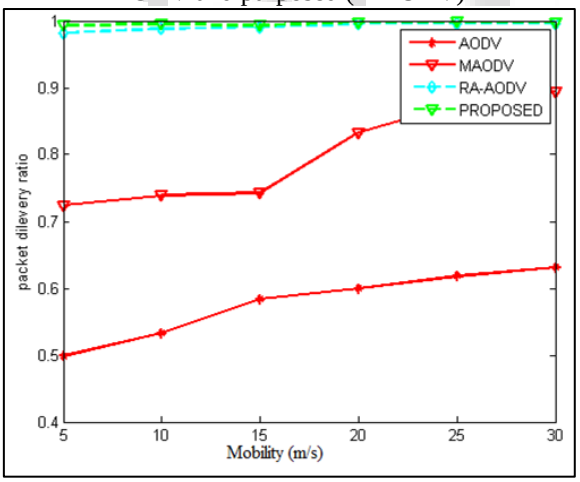

Fig. 7: Comparison of Packet delivery ratio verses Mobility for AODV, MAODV, RA-AODV and proposed (T-AODV) for 50 nodes

B. *End-To-End Delay*

Mobility	AODV	MAODV	RA-AODV	Purposed
5	900	380	50	30
10	850	250	50	30
15	800	150	50	30
20	799	100	50	30
25	455	100	50	30
30	450	100	50	30

Table 3: Comparison of the QOS parameters as EED on the basis of Mobility of 50 nodes for AODV, MAODV, RA-AODV and purposed (T-AODV)

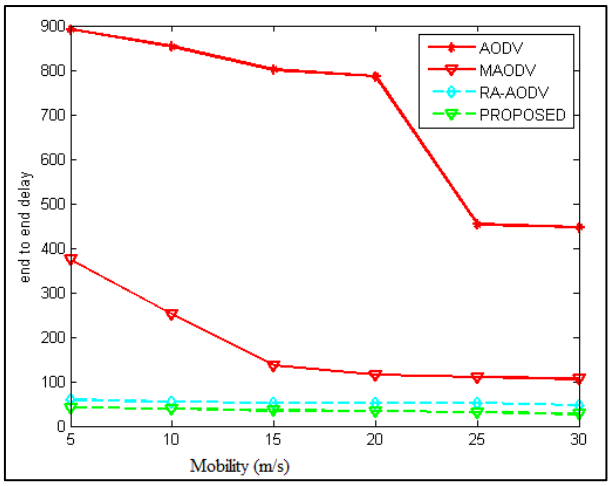

Fig. 8: Comparison of End to End delay verses Mobility for AODV, MAODV, RA-AODV and proposed (T-AODV) for 50 nodes

C. *Throughput*

Mobility	AODV	MAODV	RA-AODV	Purposed
5	650	740	850	1220
10	690	850	970	1220
15	700	880	970	1350
20	750	890	980	1360
25	800	900	990	1400
30	820	920	990	1480

Table 4: Comparison of the QOS parameters as Throughput on the basis of Mobility of 50 nodes for AODV, MAODV, RA-AODV and purposed (T-AODV)

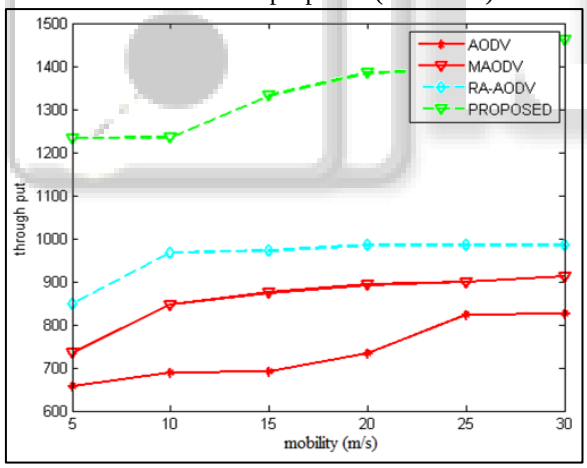

Fig. 9: Comparison of Throughput verses Mobility for AODV, MAODV, RA-AODV and proposed (T-AODV) for 50 nodes

D. *Energy Consumption*

Mobility	AODV	MAODV	RA-AODV	Purposed
5	148	132	104	65
10	150	140	110	70
15	168	148	118	90
20	180	150	106	92
25	183	164	130	110
30	184	176	136	116

Table 5: Comparison of the QOS parameters as Energy Consumption on the basis of Mobility of 50 nodes for AODV, MAODV, RA-AODV and purposed (T-AODV)

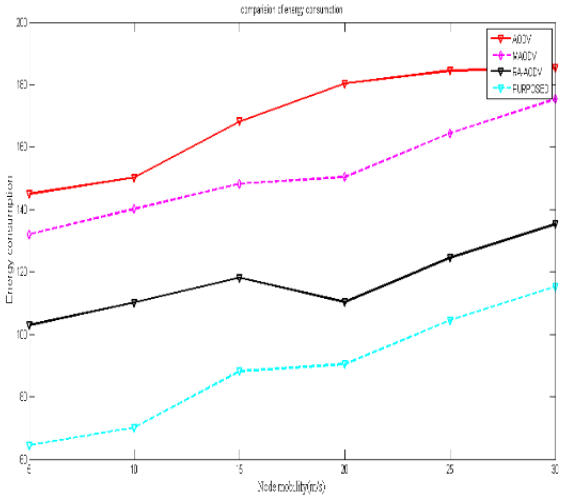

Fig. 10: Comparison of Energy consumption verses Mobility for AODV, MAODV, RA-AODV and proposed (T-AODV) for 50 nodes

E. *Network Routing Load*

Mobility	AODV	MAODV	RA-AODV	Purposed
5	1	0.9	0.5	0.1
10	1.2	0.8	0.3	0.15
15	1.25	0.9	0.5	0.13
20	1.3	0.8	0.7	0.1
25	1.4	0.8	0.6	0.1
30	1.5	0.9	0.9	0.1

Table 6: Comparison of the QOS parameters as NRL on the basis of Mobility of 50 nodes for AODV, MAODV, RA-AODV and purposed (T-AODV)

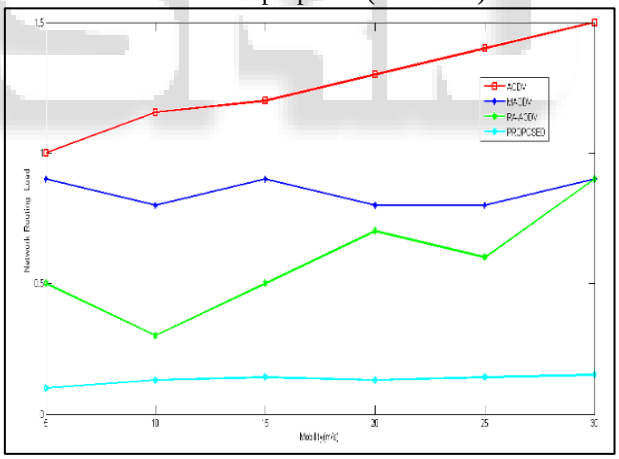

Fig. 11: Comparison of Network routing load verses Node mobility for AODV, MAODV, RA-AODV and proposed (T-AODV) for 50 nodes

VII. CONCLUSION

In this thesis, our focus is on increasing the QOS parameter in purposed method. The T-AODV assures trust by ensuring quality in terms of End to End delay, Throughput, Energy consumption, packet delivery ratio, Network routing load. In route discovery process the route is established by checking the trust value of intermediate nodes which node has the high trust value is selected for the route. In this way, the stability of the selected route is promised. Our proposed T-AODV protocol shows that it is more effective for data transmission in comparison of other traditional routing protocol in MANET.

FUTURE SCOPE

However, further work needs to be done as how to improve the route discovery when the network is sparse with many nodes moving out of the subnet.

As a future work, we would like to modify it further to improve Packet Delivery Ratio Throughput, energy consumption, network routing load and end to end delay. If needed, we will do further modification to improve its performance.

REFERENCES

[1] Tyagi, Shobha, Subhranil Som, and Q. P. Rana. "A Reliability based Variant of AODV in MANETs: Proposal, Analysis and Comparison." Procedia Computer Science 79 (2016): 903-911.
[2] Ibrahim, Hosny M., Nagwa M. Omar, and Ebram K. William. "A secure technique for construction and maintenance of a trusted mobile backbone network in MANET." Networking, Sensing and Control (ICNSC), 2015 IEEE 12th International Conference on. IEEE, 2015.
[3] Pavani, V. L., and B. Sathyanarayana. "A reliable data delivery using trust management system based on node behaviour predication in MANET." 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE, 2015.
[4] Schellenberg, Sebastian, et al. "Routing-based and location-aware service discovery in Mobile Ad-hoc Networks." The International Conference on Information Networking 2014 (ICOIN2014). IEEE, 2014.
[5] Halder, Tanmoy Kanti, Chandreyee Chowdhury, and Sarmistha Neogy. "Power Aware AODV Routing Protocol for MANET." Advances in Computing and Communications (ICACC), 2014 Fourth International Conference on. IEEE, 2014.
[6] Shukla, Arvind Kumar, et al. "The analysis of AODV, based on mobility model." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

