Modified Ad Hoc On-Demand Distance Vector Routing Protocols

Virendra Singh
Department of CSE,
Govt. Engineering College Bikaner India,

Dhanroop Mal Nagar
Department of CSE,
Govt. Engineering College Bikaner

ABSTRACT
Ad Hoc network is a network without physical structure and is established with mobile nodes using wireless connections. Ad Hoc network is highly flexible and supports dynamic network topology. Thus, the efficiency of the routing protocol will affect the overall network performance. Mobile ad hoc networks carriage several kinds of security problems, initiated by their open systems and nature of collaborative by limited accessibility of resources. In this paper we study and analyses various attacks that can be possible on AODV. My planned work is an extension of AODV to the secure AODV protocol extension, which contains tuning policies aimed at improving routing performance. Proposed an extension to Adaptive-SAODV of the secure AODV protocol extension. In our thesis we goals s Developed a routing protocol algorithm to solve the problem of efficiency transmission in Mobile Ad Hoc networks. So that work we divided the process into two parts.

In M-AODV an intermediate node create an adaptive reply decision for an incoming demand that helps to stabile its security and efficiency of incoming messages. I.e. we propose a modification to adaptive mechanism that adjusts M-AODV behaviour.

In the AODV protocol, a backup route will be began to transfer data when the original route is broken. However, a backup method affects the overall network performance such as pdr, end-to-end delay, etc. To solve this problem, the method developed in this research is used to reroute the data traffic and improve the performance of AODV protocol by via ACK reply path as a backup way whenever there is a route failure. The proposed method, called Modified AODV protocol (M-AODV), is developed by modifying the AODV protocol.

The method creates new flags in the routing message, so that as long as the source node can still receive ACK reply from the destination node when an original route is broken, it uses the forwarding path of ACK as a backup route to transfer the rest of the data packets. M-AODV also incorporates features of the M-TCP scheme to solve unnecessary resending of lost data packets. The both algorithm uses only connectivity information to look for illegal structures in the connectivity graph. The algorithm is independent of wireless communication models. We have analysis that our proposed algorithm improve the performance in M-AODV and also compared its performance like the throughput, end-to-end delay and packet delivery ratio with existing mechanisms using EXATA simulation.

Keywords
MANET, Routing Protocols, ad-Hoc networks, Mobility, backup path.

1. INTRODUCTION
Mobile Ad-hoc Networks are wireless networks scenario which are deployed without a predefine Structure, which are Usually collected on a temporary basis to serve a specific deployment purposes like in emergencies such as natural hazards rescue or battlefield communication[1]. It provides a consistent communication in situations where the deployments of infrastructure based system is Unfeasible.

This research to develop of a routing protocol algorithm to solve the problem of secure and efficiency connection establishment in Mobile Ad Hoc networks. As an On-Demand routing protocol establishes routes only when the source node is going to send data packets to a destination node. This saves a lot of resources, power supply and bandwidth while maintaining stability in routing in a network where the topology frequently changes.

A number of routing protocols have been established for mobile Ad Hoc networks. These include: On-Demand routing protocol, Table-Driven routing protocol and Hybrid routing protocol. On-Demand routing protocol builds routes only when the source node is going to send data packets to a destination node. In the Table-Driven routing protocol, all mobile node keeps one or more tables to store routing information, which is updated when the topology of the Ad Hoc network changes. The Hybrid routing protocol combines features of the Table-Driven protocol and the On-Demand protocol into one protocol.

The goal of these routing protocols is to establish a stable and high quality route in a frequently-changing topology in an Ad Hoc network. On-Demand routing protocol has less overhead over the Table-Driven routing protocol. the characteristics of network topology change frequently. To reduce unnecessary power consumption, the On-Demand routing protocols use Dynamic Source Routing Algorithm Ad Hoc On-Demand Distance Vector etc.

1.1 Wireless Network Attacks
The Ad Hoc network equipment are usually carried around as small battery-powered devices or placed inside mobile units like cars. This makes them even more attractive for attackers since they are often easier to get and also easier to carry away from the crime scene. Another point is that it can be quite hard to intercept wired media without getting noticed both because the media itself might be hard to get to and to intercept the cables often will need cutting the cables for a while. In the wireless medium it is as easy as just putting up an antenna, usually small enough not to be noticed.

Also, since many users of the Ad Hoc networks will be using it in public places the threat of unintentionally revealing secrets are large. This can be in the form of a conversation being held so that someone can overhear secret information or shoulder surfing, that is keyboard from behind while entering

passwords. The human nature of bad memory can also be of some help for the attacker. The retrieval of this kind of information can help attackers to guess the correct passwords to system resources.

1.2 Our Contributions

The main contribution of this work is to find routes between a given source-destination pair that are reliable and stable enough to efficiently transmit data traffic in moderate mobility and congestion scenarios. In this paper, we propose and implement a routing protocol algorithm to solve the problem of secure and efficiency connection establishment in Mobile Ad Hoc networks. As an On-Demand routing protocol establishes routes only when the source node is going to send data packets to a destination node. In the AODV protocol, a backup route will be began to transfer data when the primary route is broken. However, a backup route affects the whole network performance such as pdr ,throughput and end-to-end delay, etc.

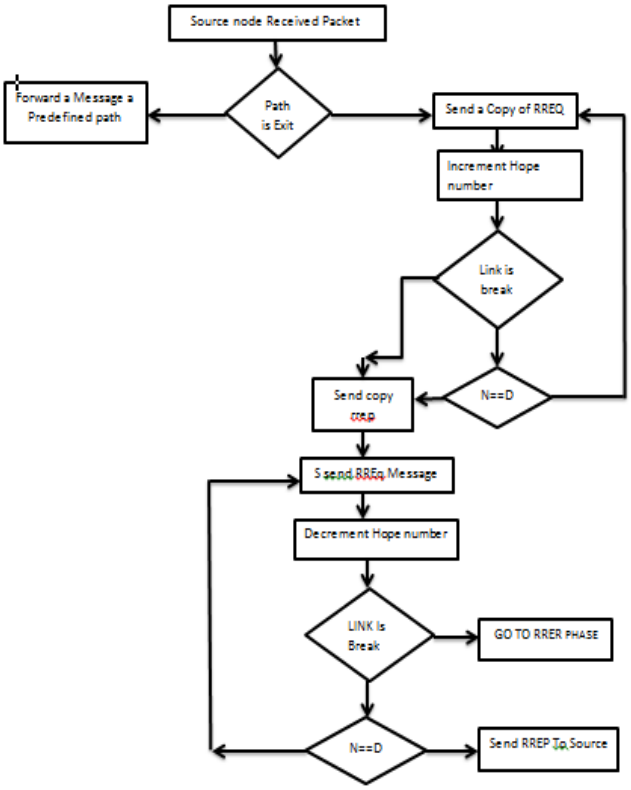

Fig 1: Design Of The Proposed Secure AODV Approach

The system developed in this research is used to reroute the data traffic and improve the performance of AODV protocol by using ACK reply path as a backup route whenever there is a route failure. The proposed method, called Modified AODV protocol (M-AODV), is developed by modifying the AODV protocol. The method creates new flags in the routing message, it uses the forwarding path of ACK as a backup route to transfer the rest of the data packets. To make sure that the routes discovered during the route discovery process are of good quality and secure. M-AODV also incorporates features of the M-TCP system to resolve unnecessary resending of lost data packets.

2. PROPOSED SECURE AODV APPROACH

Figure 1 shows the overall design of the proposed Secure AODV Approach. In the existing routing methodology the routes are selected based upon the shortest route between the source and destination which is not an efficient way to select the routes because of the possibility that the selected route may be unreliable in terms of stability, security & efficiency. if the network is loaded with heavy traffic. Mobility may also high in such random selected routes.

Therefore, to keep this in mind we have developed a new routing protocol that uses the hope count information with npre-msg of a link to decide whether to include or not the current link in the route discovery process. The results obtained from various simulations shows the effectiveness of our proposed approach.

The functionality of our suggested design AODV is divided in two main stages. One for security enmeshment And other for efficiency improvement. So That we first study the security mechanism. In our suggested work, when an middle node that receives RREQ, finds that it has a fresh route to the destination and it is allowed to reply if it has them same, first it checks time to leave (TTL) field of the packet, if its below some predefined time to leave threshold then the packet is simply forwarded to its neighbor nodes assuming that either the packet is going to be dropped after TTL hops or the packet going reach its destination with in this number of hops. When the above condition is not true then the node follows the steps of M-AODV i.e. if the node has fresh route to destination, the node generates a RREP on behalf of destination node.

1) Route Request propagation Phase : In this , we try to discover route for a given destination in such a way that the exposed route is consists of the links that has highest security. To achieve this we use a M-AODV route discovery process as described in the algorithm and the flowchart. In this phase, a route from the destination to the source is created upon which the route reply message will travel from destination to source.

Each ROUTE REQUEST message contains a “hop limit” that may be used to limit the number of intermediate nodes allowed to forward that copy of the ROUTE REQUEST.

As the non-propagating (npre-msg) REQUEST is forwarded, this limit is incremented, and the REQUEST packet is forwarded towards neighbor node before finding the target node.

We currently use this mechanism to send a non-propagating(npre-msg) ROUTE REQUEST (i.e., with hop limit 0) as an inexpensive method of determining if the target is currently a neighbor of the initiator or if a neighbor node has a route to the target cached. The above first phase is completed once the RREQ message is received by the destination node. When destination nodes receives several non-propagating (npre-msg) ROUTE REQUEST messages for the same communication flow. It uses one link to reply with the RREP message. We make sure that the RREP message sent by the destination node will flow the reverse route that is created during the RREQ propagation phase. As the ROUTE REQUEST is forwarded, this hope count value is decremented, and the REQUEST packet is discarded if the value reaches zero before finding the target. This mechanism is use to send a ROUTE REQUEST to determining if a neighbor node has a route to the target.

2)Route Reply propagation phase: The above first phase is completed once the ROUTE REQUEST message is received by the destination node. When destination nodes receives several ROUTE REQUEST messages for the same communication flow. It uses one link to reply with the RREP message. That one link is again chosen as described in the algorithm and the flowchart. We make sure that the RREP message sent by the destination node will flow the reverse route that is created during the RREQ propagation phase. When the RREP is received by the source node we have a good quality forward route from the source node to the destination node.

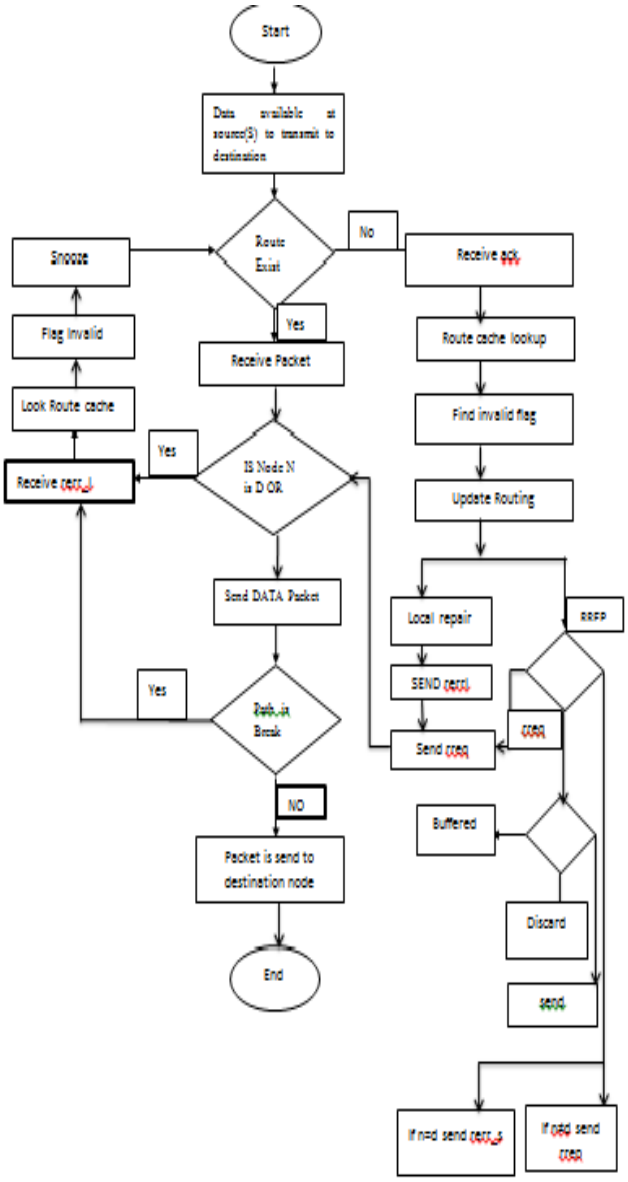

Fig 2: Design Of Proposed Mechanism

Now we proposed a mechanism to improvement efficient M-AODV routing protocol which was developed by modifying the AODV protocol. M-AODV uses the ACK reply path as the backup route to transfer data packets when an original route fails. In addition The source node monitors if it can still receive an ACK reply or not from a destination node when a data transmission route fails. Additionally, all the intermediate nodes which have received an RERR message will not discard but buffer the transferred data packets, and record the sequence number for each data packet.

The source node sends data packets by using the ACK path before the original route is repaired or a new optimum path is established. When the original route has been successfully repaired or re-established, the source node will use the route again to send the remaining data packets. In addition, the buffered data packets will be sent by the intermediate nodes to the destination node.

The operation of M-AODV involves connection processing, which aims at monitoring ACK reply and using the ACK path to transfer data. Then it is the buffering and sending processes, which solve the problem of resending unnecessary data packets by using the M-Tcp scheme. In this research, the situation of the ACK path is considered to be different from the data delivery route. The process flow of the proposed mechanism is shown in Figure 3.3.

Modification was made to the AODV protocol by adding two caches to the RERR (route error) message. Additionally, an MAODV Agent was added to the AODV protocol to monitor the ACK reply information and update the routing table. Furthermore, the M-TCP was used to modify TCP protocol by adding a Tcp Agent to process the information from AODV.

2.1 Modified part of AODV

The RERR (Route Error) message of AODV was modified by adding two new flags - L and S. The “Option Type” and “Opt Data Len” columns are used to show “This is a route error message” and its length is a 8-bit unsigned integer. The type of error encountered is shown by a value in the column “Error Type”, for example, 1 means “node unreachable”, 2 means “flow state not supported”, and so on. “Reserved” means reserved, which is sent as 0, and reserved for future use. In the research, two bits space was divided from “Reserved” and used for flags L and S. The flag L is used to indicate whether the Local Repair mechanism is initiated by the intermediate node when it detects a route failure, whereas, the flag S is used to show whether the local repair is successful or not.

If the flag L is set to 1, it means that this route error message is RERR_L. When an intermediate node detects that a route is broken, it sends the RERR_L message to the source node and initiates

Local Repair-The other intermediate nodes which have transferred the RERR_L to the source node will buffer the data packet which they are forwarding. If the flag L is set to 0, it means that the Local Repair mechanism is not initiated and the intermediate nodes will drop the data packet which they are forwarding. If flag S is set to 1, it means that this route error message is RERR_S. The intermediate nodes will start to send the data packets, which were buffered before they are sent to the destination node, when they receive the RERR_S. On the other hand, if flag S is set to 0, it means that the Local Repair has failed or timed out, in which case, the intermediate nodes will drop the data packets, which were buffered previously, and the source node will reselect a route to transfer the data packets. In the event a source node receives a message indicating route failure, it will start to monitor whether an ACK (from the destination node) can still be received or not. If the ACK can be received by the source node, it means that a path is still available from the source node to the destination nodes. Thus, the data packets can be transferred along the ACK path to the destination node.

3. EXPERIMENTAL RESULTS

We present the performance analysis and impact analysis of our implemented M-aodv protocol on different scenarios over MANETs. To perform all the simulations, we created the scenarios using well knows network simulator called EXata. The results obtained on various scenarios when aodv routing protocol and our proposed efficiency based aodv routing (M-aodv) protocol is compared with each other on three different network layer metrics.

3.1 Simulation Model

In our simulation process we uses the mobility model used in infrastructure-less mobile networks known as Random way point mobility model. In this model, the speed of a node is randomly chosen before moving to the target point is between 0 m/s to 25 m/s. The pause time is set to 10 seconds. We use a terrain with dimensions 1200m x 1200m to randomly deploy 50 nodes in it. The nodes in the network are configured with 802.11a/g MAC specification and their transmission power is 250 meters which is calculated using a nodes transmitting power. All the source-destination pairs are selected randomly in from the network[7]. To model the source nodes as a data generating nodes we configure each source node in the network using the constant bit rate (CBR) application. The CBR generates data according the following given parameters:

i Inter-packet time : 45 milliseconds.
ii Packet size : 1024 bytes.
iii Intervals : the starting and stopping time of the CBR sessions.

Each node stores the received data packets into its output buffers during its wait for a route for destination node. All packets (either data packets or control messages) sent by the routing layer are stored in the packet queue which is implemented as a buffer until they are extracted from the buffer by MAC layer to transmit them to the physical layer. Routing packets are given higher priority than data packets in the buffer. All the simulations performed in this paper run for a time period equal to 400 simulated seconds. Each data point shown in the graphs and tables are represent an average of three runs with similar traffic models, but different randomly generated mobility scenarios by using different seed values.

3.2 Performance metrics

The following metrics are used in varying scenarios to evaluate the three different protocols :

1) Throughput it is measured by the total amount of packets which is received by a destination node. It is measured by byte/sec or bit/sec. High throughput is always expected for any routing protocol[8].

2) Average end-to-end delay of data packets: This metric is calculated by the destination node whenever it receives a data packet. The destination node will calculate the delay of each received data packet by using its send timestamp and its received timestamp at the destination. At the end of the simulation the total time of the data packets received at the destination is divided to the total number of received data packets. We calculate average end-to-end delay for packets received by each destination node as follows:

$$EED = \frac{Accumulative\ sum\ of\ delay\ of\ each\ packet\ receivedal}{PcoTotal\ No.\ Packets\ Received\ by\ Destination}$$

3) First Packet Received :- FPR denotes the time of first packet received by destination node in bit/sec submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network[9].

3.3 Simulation Results

In order to compare and evaluate performances of the aodv and M-aodv protocols in different network conditions, two parameters are varied in the simulations: Maximum mobility of the nodes and Number of data sessions.

At first, simulations are carried out by keeping the number of sources constant in our case we fix it to 6 source destination pairs and varying the mobility in the network. 6 sources are modeled respectively to study the effect of varying mobility in network. In the other scenario, the number of sources is varied from 3 to 15. When varying the number of sources, node's mobility is kept random which falls between the range of 0 to 10 m/s and pause time is set to 30 seconds. The effects of change in network mobility are analyzed on traditional aodv protocols and our proposed efficiency based secure aodv routing (ES-aodv) protocol[10]. The mobility of the nodes is changed by increasing the range by 5 m/s in each simulation.

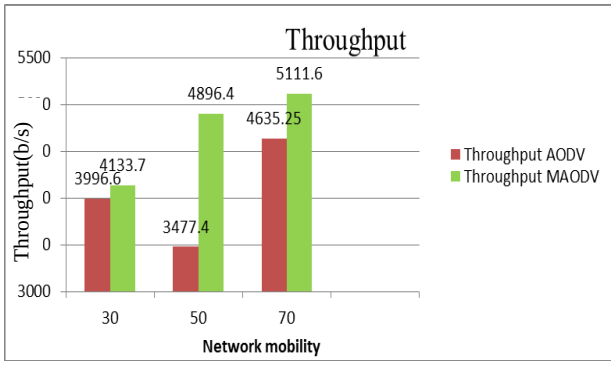

Fig 3: Throughput Of M-Aodv And Aodv With Attack For 30,50,70 Node

In figure 3 we had plotted Average Throughput with increment in network mobility, the Throughput of the network decreases with the increment in the network mobility. This is due to the increment in the route breaks during the communication process the number of packets that are on an active route, which is broken and lost. As it can be saw from the figure 3 that the throughput of my proposed M-aodvis much higher as compared to the traditional aodv routing protocol because of the lower number of re-routing processes caused due to the selection of high quality route selection process that i have implemented in suggested M-aodvrouting protocol.

In figure 4 we had plotted Average End-to-End Delay with increase in network mobility, the end-to-end delay of the data sessions are fluctuating at some mobility points and the general trade shows that the end-to-end delay increasing with the increases in the network mobility because as the mobility. This is because as the mobility increases the number of routes that are broken during the communication process also increases which increase the network mobility.

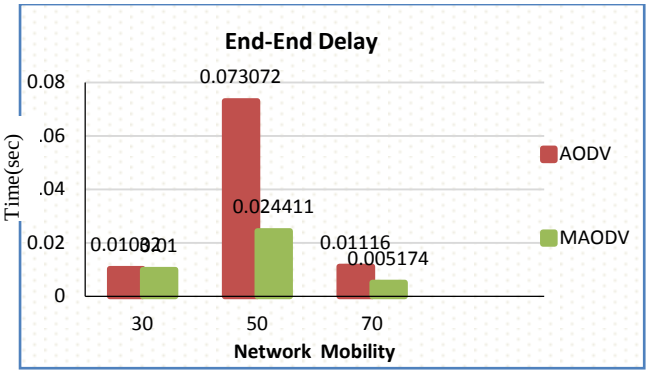

Fig 4: End-to-end delay of M-AODV and AODV for 30,50,70 nodes

In figure 4 i had plotted Average End-to-End Delay (EED) with increment in network mobility, the end-to-end delay of the data sessions are fluctuating at some mobility points and the general trade shows that the end-to-end delay increasing with the increment in the network mobility because as the mobility. This is because as the mobility increases, the number of routes that are broken during the communication process also increases, which increase the network mobility. This is Fig. 4: Average End-to-End Delay (EED) with increase in network mobility due to the fact that increment in the mobility means that the intermediate nodes on an active route can move from the routes which cause the route breaks.

As it can be observed that from the figure 4 that the end-to-end delay of my proposed protocol is lower at low and moderate mobility networks because of the selection of routes that are consists with the links that has high lifetime this decreases the number of route breaks during the communication, which decreases the eed[11].

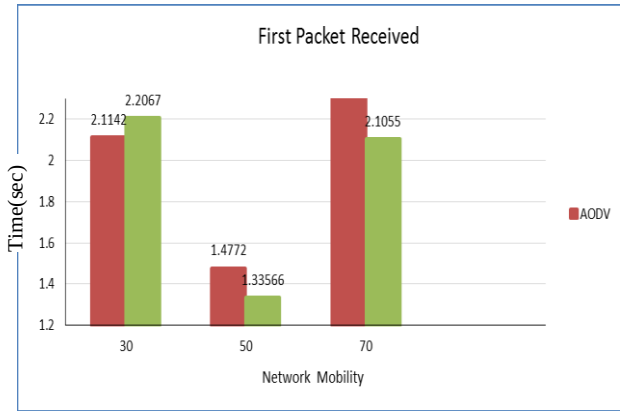

Fig 5: first packet received of M-AODV and AODV with attack at 30,50,70 nodes.

In figure 5 I have plotted first packet received with increment in network mobility which highlights the effect on routing time for aodv and M-aodv protocols with the increase in network mobility. As it can be observed from the figure 5 that the first packet received increases with the increment in the network mobility. As it can also be observed from the figure 5 that the first packet received of my proposed M-aodv is lower than the aodv protocol because of the same reason i have given for the throughput increment that the M-aodv has lower number of re-routings due to its link-quality based route selection process.

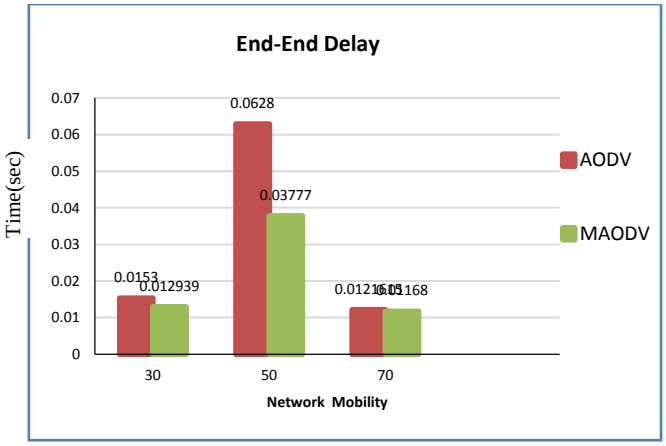

Fig 6 : avg end to end delay with n/w load

In Figure 6 i have plotted the Average End-to-End Delay with increment in network load, the end-to-end delay increases with increment in network load for both the comparing protocols. This is because as the network load increases the congestion in the network increases with these two things happens[12] Firstly, it increases the number of route failures in a data communication session. Secondly, the time taken to transmit a data packet to next hop could increment due to increase in the number of re-transmissions required at the MAC layer due to the congestion or contention on the transmitting link. Although, the end-to-end delay of the proposed M-aodvis not as high as the aodv because it selects routes which has higher received signal power which makes the selected link more reliable as compared to the links that are selected if aodv routing protocol is used for route discovery.

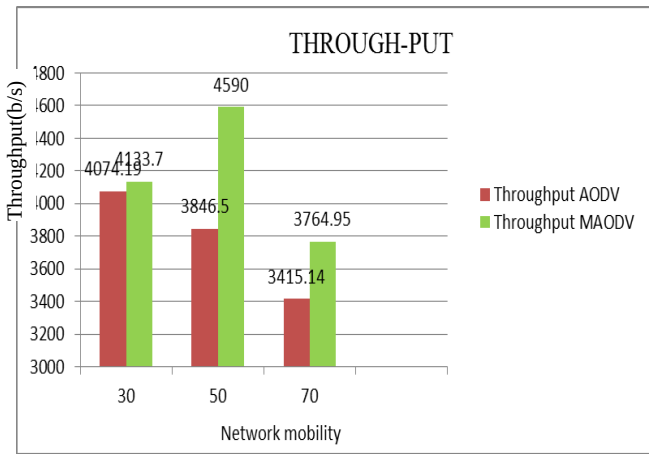

Fig 7: AODV vs. M-AODV throughput For 30,50,70 Node with network load in 30 s Pause Time

In Figure 7 i had plotted the throughput with increment in network load, the throughput of the network decreases with the increment in network load because the increment in network load increases the contention and congestion in the selected routes[13]. Due to this, the active communication routes breaks during the data communication and the data packets on these routes are dropped during the route discovery process. Fig. 7 throughput with increment in network load in network traffic because the newly added flow might use a common link for routing. Although, the throughput of my proposed M-aodvis high even in high load networks because it avoids the use of highly loaded links

during its route discovery process by not selecting the links with high interference [14].

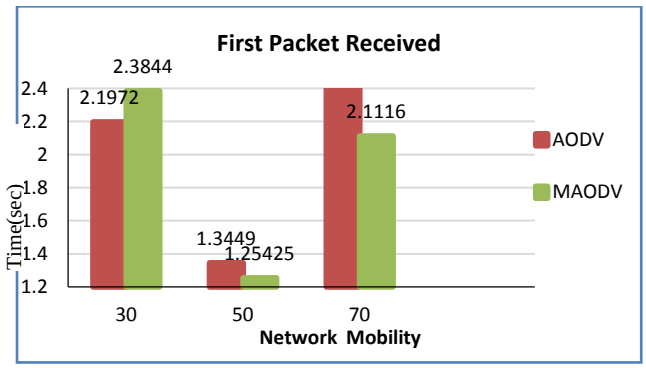

Fig 8 :Average first packet received in 30 s Pause Time

The first packet received of the network with the increment in network load for aodv and M-aodv protocols is shown in Figure 8. It can be observed from the Figure that the routing overhead of our proposed M-aodv is much better than the FPR of the traditional aodv protocol. On the other hand, the first packet received in the aodv routing protocol increases rapidly with the increment in network load because of the same comments and reasons that are provided above to support the increment in network EED with the increased network load [15].

4. CONCLUSION

In this paper, we have proposed an efficient and secure route discovery process that uses the link quality under consideration at each step during its reactive route discovery process. Our proposed M-aodv protocol shows that it is more effective for data transmission in moderate mobility and congested network than the traditional routing protocols in MANETs. Our proposed efficiency based aodv routing protocol uses the received signal power, interfering signal power and noise over a link to identify whether it is a stable radio link or not during the route discovery process.

We have analyzed our proposed work with the help of simulation results that are generated using the network simulator called Exata. The results are generated on large number of scenarios with various parameter values to show its effectiveness in all kinds of situations. Therefore at the end the path which is selected for the data transmission is the one which consists of radio links that has lower interference and low noise in conjunction to high received signal strength.

5. REFERENCES

[1] H. vijayvergia; A. chaudhary; G. Singh; R. S. Shekhawat; ”bit-error rate based adaptive Routing Protocol for Reliable Datatranmission on manet”ieee international conference on signal propagation and computer and technology,(IEEE_ICSPT 2014).

[2] Hamad, Sofian, Hadi Noureddine, and Hamed Al-Raweshidy. "LSEA: Link stability and energy aware for efficient routing in mobile ad hoc network." Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on. IEEE, 2011.

[3] Yang, Peng, and Biao Huang. "QoS routing protocol based on link stability with dynamic delay prediction in MANET." Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on. Vol. 1. IEEE, 2008.

[4] Wang, Wen-Fong, and Po-Hun Shih. "Study on an enhanced link-stability based routing scheme for mobile ad hoc networks." Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on. Vol. 3. IEEE, 2006.

[5] Zhang, Hui, and Yu-ning Dong. "Mobility prediction model based link stability metric for wireless ad hoc networks." Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on. IEEE, 2006.

[6] Yafeng Zhou; Sang-Hwa Chung; Lihua Yang; "A Link-Quality Aware Routing Metric for Multi-hop Wireless Network," International Conference on Communication Software and Networks, 2009(ICCSN’09)., pp.390-394, 27-28 Feb. 2009.

[7] Jenn-Hwan Tarng; Bing-Wen Chuang; Fang-Jing Wu, "A Radio-LinkStability-based Routing Protocol for Mobile Ad Hoc Networks," IEEE International Conference on Systems, Man and Cybernetics,2006(SMC’06). , vol.5, pp.3697-3701, 8-11 Oct. 2006.

[8] Effatparvar, M.R.; Yazdani, N.; Lahooti, F.; EffatParvar, M., "Link Stability Approach and Scalability Method on ODMRP in Ad Hoc Networks," Communication Networks and Services Research Conference, 2009(NSR ’09)., pp.416-421, 11-13 May 2009.

[9] LiminMeng; Wanxia Wu, "Dynamic Source Routing Protocol Basedon Link Stability Arithmetic,"International Symposium on Information Science and Engineering, 2008(ISISE ’08), vol.2, pp.730,733, 20-22 Dec. 2008.

[10] Wu, C.; K.; Kato,"AMANET protocol considering link stability and bandwidth efficiency", International Conference on Ultra-Modern Telecommunications & Workshops, 2009(ICUMT ’09), pp.18, 12-14 Oct. 2009.