International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-6, Issue-4, December 2016

The Novel Approach For Efficient Routing In MANET Using FSR (Fish State Routing) Protocol

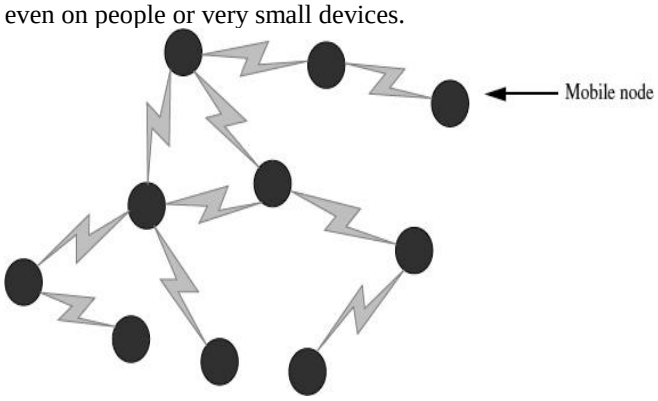
Uma Bharti, Mohit Trehan

***Abstract*— A mobile Adhoc network is an autonomous network that consists of nodes which communicate with each other with wireless channel. Since mobile Adhoc network is dynamic in nature due to which there is loss in data transmission. The routing protocol play important role in transmission in mobile Adhoc network In MANET,A routing protocol shows main role to handle entire network for communication and determines the paths of packets. A node is a part of the defined network for transferring information in form of packets. If all packets transferred from source to destination successfully, it has been assumed that the routing protocol is good. The FSR algorithm is proposed for secure and efficient transmission in network and proposed Algorithm shows efficient transmission result in optimal transmission**

***Index Terms*— MANET, FSR,Routing Protocol**

I. INTRODUCTION

Mobile Ad-Hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. It is the collection of mobile node that dynamically forms of the network without infrastructure. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.



Uma Bharti, M.TECH Scholar, Department of Computer Science GCET, Gurdaspur, India
Mohit Trehan, Assistant Professor, Department of Computer Science GCET, Gurdaspur , India

The difference between ad hoc networks is the lack of a centralized entity within an ad hoc network. There are no base stations or mobile switching centers in an ad hoc network.
Since, there is no fixed infrastructure; a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons.
Ad-hoc networks were mainly used for military applications. Since then, they have become increasingly more popular within the computing industry. Ad-hoc networks can be rapidly deployed because of the lack of infrastructure [1].

II. RELATED WORK

Anumeha, Prof. (Dr.) Bhawna Mallick 2015, Mobile ad hoc networks (MANETs) are becoming more essential to wireless communications due to growing popularity of mobile devices. An ad-hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a mobile ad- hoc network (MANET). Efficient protocols are used to forward data packet without much packet loss.Here.an adaptive routing algorithm is presented in Mobile Ad hoc Networks using modified AODV by calculating the load on different routes using various parameters. The objective of this paper is to enhance the network performance of AODV, when frequent link failure in network due to mobility of the nodes in the network. The performance analysis and simulation are carried out to evaluate network performance using Network Simulator (NS-2), based on the quantitative metrics packet delivery ratio and average end to end delay. The simulated result helps to understand the behavior of the protocol AODV in the distributed network environment. This paper proposed a new protocol Enhanced AODV (E-AODV) which is a modified version of AODV. [2]
Vaibhav Suhane, Mahesh Gour, Sadhna K Mishra 2015,The mobile ad hoc network (MANET) which has no centralized administration and no fix topology without infrastructure. In MANET nodes are communicated with own mutual trust. In MANET there are three types of protocol. These are Reactive, proactive and hybrid protocol .In MANET there are many network attacks like black hole, wormhole, Dos Attack etc. They dispute the network performance. Security is prime concern in MANET.
they proposed new protocol EAODV. Which is an enhanced AODV. Which will detect and prevent the network from wormhole, Black Hole , DOS ,Man in middle, Eavesdropping and data modification. The performance of the EAODV protocol is compared with the existing AODV routing

protocol with variation in Pause time and Node speed.The performances matrices are throughput, End to End delay and total packet loss. [3]

Jaspreet Singh, Kartik Sharma 2015, Mobile ad-hoc networks are infrastructure-less networks used for communication between two or more nodes without a common access point. It is a collection of nodes that is connected through a wireless medium forming changing topologies. In mobile ad-hoc networks all the nodes are mobile in nature and having limited battery charge. Continuous change in position of nodes in the network degrades the battery charge of the nodes therefore it is necessary to save the battery power of those nodes so that the network lifetime can be long lasting. Nodes in the network are working in the presence of limited energy then energy efficient routing is necessary for reducing energy consumption. In this paper we proposed energy efficient AODV routing protocol in which Dijkstra algorithm is enhanced to improve the overall performance of the network. Existing systems are not capable of finding the shortest and energy based path among the nodes in the network if multiple nodes fail simultaneously. Performance parameters are Packet delivery ratio, Throughput, Energy consumption and routing overhead. [4]

Supriya Sawwashere, Ashutosh Lanjewar 2015, AODV (Ad-Hoc On-Demand Distance Vector) is a reactive routing protocol for mobile Ad- Hoc networks (MANETs) and other wireless ad-hoc networks. Reactive means that it establishes a route to a destination only on demand. The cost is one of the most important network performance parameter. Here, the conventional AODV is compared with proposed Improved Cost efficient AODV routing protocol using Euclidean distance. The route with shortest Euclidean distance is selected for communication. The proposed AODV routing protocol thus helps to overcome the factors like End to End Delay, Packet Loss and Network Routing Load which generally occurs in conventional AODV routing protocol due to changing topology of the network. [5]

Arthur Ndlovu 2015, A Mobile adhoc network is a collection of wireless mobile nodes which can provide scalability and independence for mobile topologies. These wireless mobile nodes are battery powered hence the need for energy conservation in order to allow an increase in network lifetime. Energy conservation is very important in applications such as Military operations and Emergency Rescue operations where network infrastructure is not readily available. In this research we developed an improved energy efficient algorithm which uses K- means algorithm as the Clusterhead head selection method that is aimed at improving the network performance of AODV routing protocol. The improved energy idea uses the concept of drain count in sensor nodes which works as follows: Each node is set with an initial energy value which basically determines how long it's going to last in a network and to make sure our network has the highest lifetime possible we set up a threshold energy value. If a particular path has a single node with its energy lesser than that of the set threshold, then the drain count of that particular path is incremented by a factor of one . The drain count will serve as the parameter on which we can choose the path that is most likely to prolong the network lifetime. The path with the least drain count will be the one that is chosen because it has few nodes with energy below the energy threshold. We then introduce K-means algorithm in the energy efficient system for the formation of clusters in our system and again this will help in shortening the transmission path. The proposed strategy is compared with the traditional AODV routing protocol and performance evaluations are done with respect to network lifetime, throughput, end-to-end delay, packet delivery ratio. [6]

Miral V. Vora, Prof. Jignesh H. Joshi 2015, MANETs are a collection of unstructured wireless mobile nodes which provides independence and scalability for mobile networks. It is composed of moving mobile nodes that are battery operated. In AODV routing protocol, first of all broadcast the hello message to discover the Neighbor node and then source node broadcast RREQ (Route Request) packet to Neighbor node for finding path to the destination node. If The Neighbor node having less energy, as well broadcast RREQ and it lifetime expires after some certain time (i.e. node goes down), it cannot forward RREP (Route Reply) on reverse path and also cannot carry the data from the source node that's why source node has to rebroadcast RREQ that results is overhead of the RREQ message, less packet delivery ratio and throughput and more energy consumed. These problem have to be solved so here can proposed energy efficient AODV algorithm based routing protocol. In this paper proposed, source node does not send any data packet; until no enough energy (battery life time) of intermediate node and received RREP of its neighbouring exceeds a particular threshold. In this paper also suggested two approaches for making energy efficient algorithm. The performance of the proposed protocol will simulate with the help of NS-2.34 simulator for various scenario using different parameter, also survey on energy efficient algorithm. At last finally we concluded that the proposed protocol improves energy efficiency, network throughput and network lifetimes. [7]

Madhvi Saxena, Neha Jain 2015, Mobile Ad-Hoc Network (MANET) is a collection of mobile nodes which design a temporary network. In single path routing many times conjunction are in the higher level so multiple routing protocols is design for these conditions, to find shortest and optimized path from a source to destination. Due to dynamic nature, connections in the network can change frequently and nodes can be added and removed at any time. There are various types of limitations; the biggest restriction is the limited energy of the batteries. AODV is one of famous on-demand routing protocols in MANET, which uses the RDP (route discovery process) is triggered to find a new route. In this paper, we propose that the enhanced AODV (Ad-hoc On-demand Distance Vector) routing protocol which is modified to improve the networks lifetime in MANET. Keyword: Mobile ad hoc network (MANET), Ad hoc on demand distance vector routing (AODV), Multipath, Route discovery process (RDP), network lifetime. [8]

M.Sc.Ali Abdulrahman Mahmood, An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Designing a foolproof security protocol for ad hoc network is a challenging task due to its unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources. There are a lot of routing protocol for Ad-hoc network such as OLSR, AODV and ZRP; AODV (Ad Hoc On-Demand Distance Vector) is one of such protocols that help to create and maintain routes in spite of the dynamic network topology. This protocol is vulnerable to a number of security threats that

come from internal malicious nodes which have authorization credentials to participate in the network. Malicious nodes deliberately drop data packets and disrupt the correct operation of the routing protocol. This paper propose a security technique to detect and isolate the malicious node in the AODV routing protocol that cause black hole attack. [9]
Shruti Bhalodiya, Krunal Vaghela 2015, Mobile ad-hoc network (MANET) is a self-deliberate data network, where all nodes behave like host or router. MANET is a collection of number of mobile nodes or devices that randomly generate a temporary network. Security is the fundamental requirement in MANET due to its behavior of changing topology, open medium and lack of centralized authentication. This leads to various security attacks in mobile ad hoc network and violate the criteria of routing mechanism. Mobile Ad-hoc network doesn't need backbone infrastructure support and it is very reliable and also contains the routable networking environment. In this paper, the effect of flooding attack in AODV based network is explained. The network parameters like Throughput, Packet Delivery Fraction (PDF) and End to End Delay are compared with normal network (without flooding attack) and a network with one or more flooder nodes. The performance of network parameters is compared in all the three scenarios. They have proposed a scheme which is finds single or number of malicious nodes in the network and drops fake packets. [10]
Nitesh Funde, P.R. Pardhi 2015," Mobile Ad Hoc Networks (MANETs) consist of wireless mobile nodes which coordinate with each other to form temporary network without its pre-existing infrastructure. AODV is popular Ad-hoc distance vector routing reactive protocol which is used to find correct & shortest route to destination. Due to openness, dynamic, infrastructure-less nature, MANET are vulnerable to various attacks. One of these possible attacks is a Black Hole Attack in which a mobile node falsely replies to the source node that it is having a shortest path to the destination without checking its routing table. Therefore source node send all of its data to the black hole node and it deprives all the traffic of the source node. In this paper, they are proposing a technique to detect and prevent the multiple black hole nodes from MANET so that source to destination communication can be made easily.They also analysed the performance of the network in terms of number of packets sent, received, throughput, energy of network before attack and after detection & prevention of Attack. From these analysis, they can conclude that performance decreased due to attack can be improved after detection & prevention black hole attack in MANET. [11]

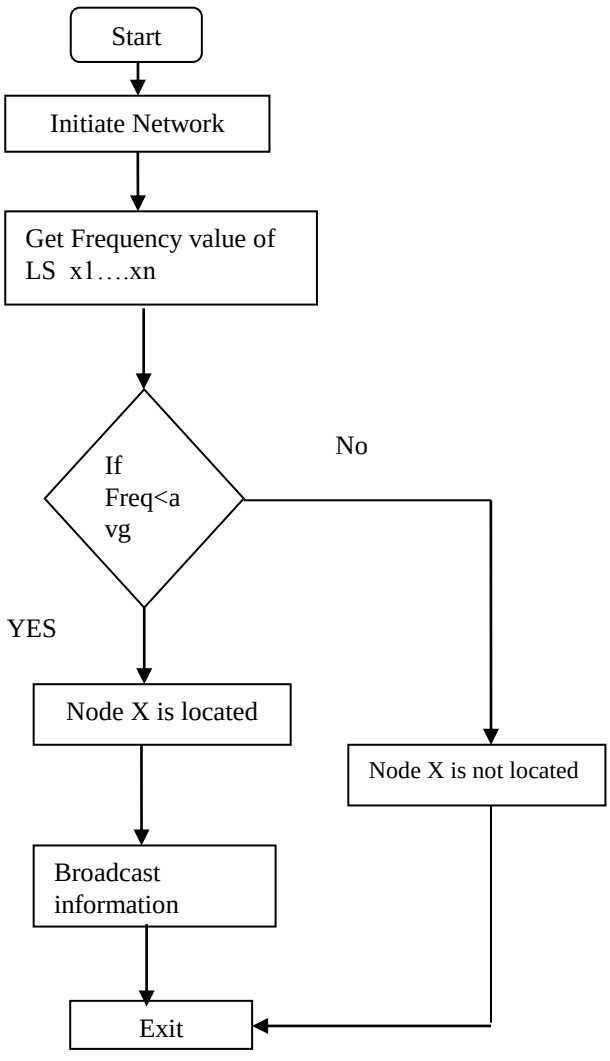
III. PROPOSED METHODOLOGY

The traditional AODV protocol which use blind flooding during rout discovery, has been modified by replaced the blind flooding with new adjusted probabilistic scheme The aim is to reduce the flooding of RREQ packets during the rout discovery operation, and as a result reduces the broadcast storm problem. The net effect is that overall network improved by reduced the average end-to-end delay and also routing overhead. Since the decisions of the nodes are independent, the total number of possible rebroadcasts of an RREQ packet N using the FSR (Fisheye State Routing) algorithm

Routing Table Calculation: The routing table of FSR provides the next hop information to forward the packets for the other destinations in the network. Whenever there are changes detected in the topology table of the node the routing table is updated. Based on the latest topology table algorithm is performed to find the shortest path from the current node to all the destinations those are in the topology table. The old routing table is replaced with the newly calculated routing table. The routing table has the following fields: Destination Address ,Next hop address Distance
In the FSR algorithm the weight or the link cost between two nodes has been taken as 1 and the weight function can be changed depending upon the requirement of functionality
.**Algorithm optimal path in MANET's**

N_{RREP} :RREP from an intermediate node

1. Begin
2. For (source node)
3. {
4. Broadcast RREP packet to every neighbor node
5. Receive RREP
6. RREP Send LS with Each Node
7. Process RREP
8. }
9. Collect nodes based on the of LS
   Near from the distance of LS
10. Broad cast information
11. }



IV. EXPERIMENTAL SETUP

The proposed Algorithm FSR is used for finding optimal Route Path .the NS2.35 simulator is used for finding results of proposed algorithm and to compare the result with previous technique

S. No.	Parameter	Value(s)
1	Simulator used	NS 2.35
2	Simulation Time	10 Secs
3	Simulation Area	800 X 1000
4	MAC	802.11
5	Number of nodes	45
6	Mobility Model	Random Waypoint

V. RESULT AND ANALYSIS

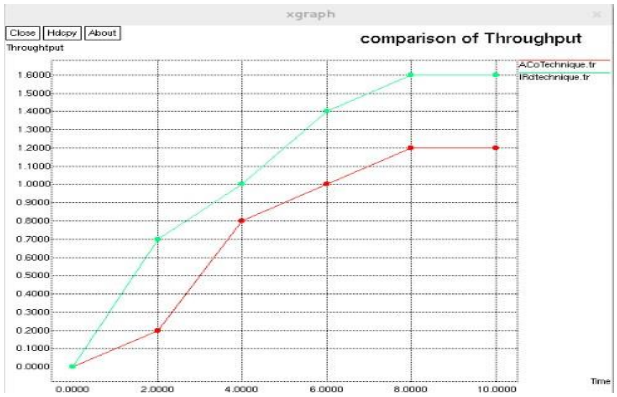


Fig1comparison of Throughput

	Throughput	
Time	ACO	FACO
0	0	0
2	0.2	0.7
4	0.8	1.0
6	1.0	1.4
8	1.2	1.5
10	1.2	1.6

Table 1 Throughput Comparison

The analysis of Throughput with FSR and Previous technique is shown in Fig 1 and Table 1 The results derived from prosed technique are better as compare to previous technique

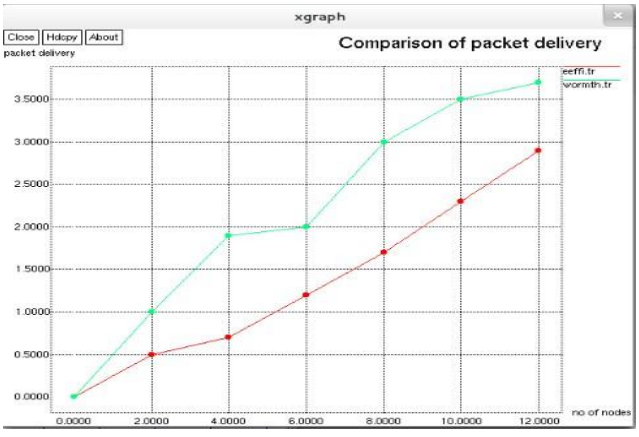


Fig 2 Comparison of packet Delivery ratio

	Packet Delivery ratio	
Time	ACO	FACO
0	0	0
2	0.5	1.0
4	0.8	1.9
6	1.5	3.0
8	2.6	3.5
10	2.9	3.7

Table 2 packet Delivery Comparison

The analysis of Packet Delivery ratio between FSR and Previous technique for optimal route path the fig 2 and table 2 show proposed technique results better as compared to previous technique

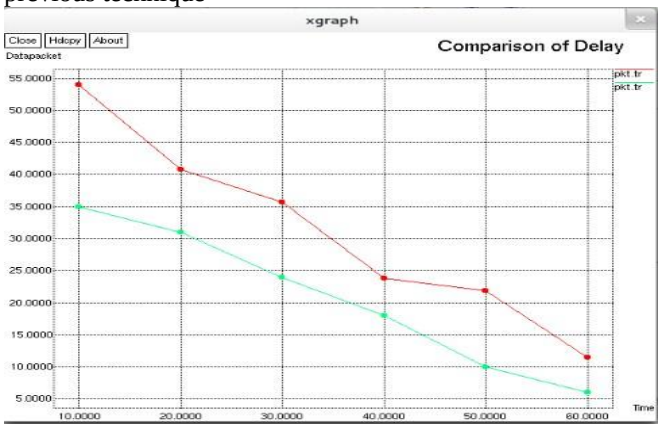


Fig 3 Comparison of End to End Delay

	Packet Delivery Ratio	
No of Nodes	ACO	FACO
10	51000	35000
20	42000	31000
30	36000	24000
40	22000	19000
50	11000	9000

Table 3 End to End Delay Comparison

The analysis of End to End Delay between FSR and Previous technique for optimal route path the fig 3 and table 3 show proposed technique results better as compared to previous technique

VI. CONCLUSION

In this paper, A efficient transmission algorithm has been proposed that can be utilized to identify optimal path in a MANET and thereby identify a efficient routing path from a source node to a destination node avoiding the congestion and delay the proposed scheme ease the optimal transmission . The basic idea of the PPN scheme is that, each node in the network has a specific link state the frequency of link state is used for finding average value with which optimal path between nodes is found for optimal and efficient transmission. The proposed technique shows better result as compare to previous technique

REFERENCES

[1] Krunal N. Chandewar and H.R. Deshmukha, "Mobile Ad-Hoc Wireless Network ", International Journal of Computer Science and Information Technologies, Vol.3,ISSN:0975-9646, 2012, 3782-3786.

[2] Anumeha, Prof. (Dr.) Bhawna Mallick 2015, "Introducing efficient & improved.AODV routing protocol for manet", IJSTM, vol-no.4, pp.36-44.
[3] Vaibhav Suhane, Mahesh Gour, Sadhna K Mishra 2015, "Detection and Prevention of Network from Networks Attacks using EAODV", IJARCSEE, vol-4, pp.80-9.
[4] Jaspreet Singh, Kartik Sharma 2015, "Energy Efficient AODV Routing Protocol for Mobile Ad-hoc Networks", IJARCCE, vol-4, pp.121-124.
[5] Supriya Sawwashere, Ashutosh Lanjewar 2015, "Improved Cost Efficient AODV Routing Protocol", IJERGS, vol-3, pp.65-70.
[6] Arthur Ndlovu 2015, "Improved Energy Efficient AODV Routing using K-means Algorithm for Cluster Head Selection", IJCSME, vol-4, pp.177-187.
[7] Miral V. Vora, Prof. Jignesh H. Joshi 2015, "A Novel Approach on Energy Efficient AODV Algorithm for MANETs", IJIRCCE, vol-3, pp.1071-1077.
[8] Madhvi Saxena, Neha Jain2015, "Network Lifetime Improvement Using Energy Efficient Multipath ad hoc on demand distance vector routing", IJET, vol-4, pp.69-73.
[9]M.Sc.Ali Abdulrahman Mahmood, Dr. Taha Mohammed Hasan, M.Sc.Dhiyab Salman Ibrahim2015, "Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET", IJARCSSE, vol-5, pp.173-178.
[10] Shruti Bhalodiya,Krunal Vaghela 2015, "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol", IJCA, vol.125-no.4, pp.10-15.
[11] Nitesh Funde, P. R. Pardhi 2015, "Analysis of Possible Attack on AODV Protocol in MANET", IJETT, vol-11, pp.306-309.