ISSN: 0976-3104
SPECIAL ISSUE: Computer Science

ARTICLE

COMPARATIVE STUDY OF ROUTING PROTOCOLS IN WIRELESS MESH NETWORKS

B Sathyasri[1*], EN Ganesh[2], P Senthil Kumar[3]

[1]*Department of Electronic and Communications Engineering, VEL TECH, Chennai, INDIA*
[2] *Department of Electronic and Communications Engineering, Saveetha Engineering College, Chennai*
[3]*Department of Computer Science and Engineering, S.K.R Engineering College, Chennai, INDIA*

ABSTRACT

Fixed and mobile wireless devices are provided reliable access through wireless mesh networks. Traffic between mesh nodes and internet is a challenging task and is routed over mesh gateways. Path from mesh node to internet node is called forward path and mesh node has to be provided with route information of only one destination (i.e. gateway). Whereas on backward path, internet to mesh node, an individual route for every mesh node is necessary. Therefore in this project, we investigate protocols for backward path routing. The three protocols for backward path routing, AODV- a reactive routing protocol, FBR - a proactive routing protocol and GSR- source routing protocol are compared. Our results indicate that FBR has highest packet delivery ratio but is not scalable to network size. Extended AODV seems to be neither scalable nor does it achieve a high packet delivery ratio. The efficient protocol GSR is most scalable to network size and also achieves a high packet delivery ratio.

KEY WORDS
ACK, Ad- hoc on demand Distance Vector, FBR, Gateway Source Routing, RREP, RREQ, RERR, Wireless Mesh Network

INTRODUCTION

A wireless mesh network (WMN) is a telecommunications system built up of radio nodes standardized in a mesh topology. Wireless mesh networks regularly subsist of mesh clients, mesh routers and portal. The mesh clients are orderly laptops, cell phones and alternate wireless devices although the mesh routers progressive traffic to and from the portal which may, but need not, connect to the internet. The scope area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is inferior on the radio nodes working in harmony with each other to conceive a radio network. A mesh network is dependable and offers redundancy. When one node can no longer complete, the rest of the nodes can still interact with each other, directly or through one or more transitional nodes.

A wireless mesh network can be seen as a particular type of wireless ad-hoc network. A wireless mesh network usually has a more prepared composition, and may be expanded to contribute dynamic and cost effective connectedness over a certain geographic area. An ad-hoc network, on the alternate hand, is formed ad-hoc when wireless devices come within intercommunication specifies of each alternate. The mesh routers may be mobile, and be moved according to specific interests arising in the network. Regularly the mesh routers are not specified in terms of resources related to alternate nodes in the network and thus can be overworked to fulfill more resource intensive functions.

Received: 24 October 2016
Accepted: 20 December 2016
Published: 15 February 2017

The characteristics of WMNs are explained as follows

Multi-hop wireless network

A detached to establish WMNs is to line-of-sight (NLOS) connectedness among the end users without direct line-of-sight (LOS) association. To meet these demands, the mesh-style multi-hopping is fundamental, which accomplish higher throughput without endure effective radio range via shorter link distances, less interference between the nodes, and more efficient frequency reiterate.

Hold for ad-hoc networking, and potential of self-forming, self-healing, and self-organization

WMN's strengthen network performance, because of tensile network architecture, easy distribution and configuration, fault tolerance, and mesh connectedness, i.e., multipoint-to-multipoint communications. Due to these features, WMN's have low upfront investment requirement, and the network can grow gradual as needed.

Mobility dependency on the type of mesh nodes: Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes.

Various types of network approach

In WMNs, to get data from an end user to a node in a major network such as the Internet access to the internet and end-to-end communications are guided. In addition, the synthesis of WMNs with other wireless

***Corresponding Author**
B Sathyasri, Department of Electronic and Communications Engineering, VEL TECH, Chennai, INDIA

networks and afford services to end-users of these networks can be adept through WMNs. Dependence of power-consumption motive on the type of mesh nodes. Mesh routers usually do not have strict motive on power consumption. However, mesh clients may desire power active protocols.

Congeniality and interoperability with current wireless networks

For example, WMNs built based on IEEE 802.11 technologies must be suitable with IEEE 802.11 standards in the impression of supporting both mesh capable and conventional Wi-Fi clients. Such WMNs also need to be inter-operable with other wireless networks such as Wi-MAX, Zig-Bee, and cellular networks. Based on their quality, WMNs are generally investigated as a type of ad-hoc networks due to the lack of wired infrastructure that remain in cellular or Wi-Fi networks through distribution of base stations or access points. While ad-hoc networking techniques are enforced by WMNs, the additional effectiveness require more sophisticated algorithms and design principles for the recognition of WMNs. More specifically, rather of being a type of ad-hoc networking, WMNs aim to diversify the capabilities of ad-hoc networks. Therefore, ad-hoc networks can absolutely be considered as a subset of WMNs. To illustrate this point, the inequality between WMNs and ad-hoc networks are zoned below. In this comparison, the hybrid architecture is considered, since it comprises all the advantages of WMNs.

Wireless framework/resolution

WMNs subsist of a wireless backbone with mesh routers. The wireless backbone provides large scope, connectedness, and robustness in the wireless domain. However, the connectedness in ad-hoc networks depends on the individual subscriptions of end-users which may not be stable

Combination

WMNs hold current clients that use the same radio technologies as a maze router. This is adept through a host-routing function applicable in mesh routers. WMNs also facilitate integration of various existing networks such as Wi-Fi, the internet, the cellular and sensor networks through gateway/bridge functionalities in the mesh routers. Therefore, users in one network are sustaining with services in other networks, over the use of the wireless frame work. The combined wireless networks over WMNs relate the internet backbone, seeing that the physical location of network nodes becomes limited than the capacity and network topology.

Adherence routing and frame work

In ad-hoc networks, ultimate consumer devices also achieve routing and structural functionalities for all other nodes. However, WMNs contain maze routers for these functionalities. Hence, the load on end-user devices is extremely decreased, which provides lower energy utilization and high-end application capabilities to possibly mobile and energy strained end-users. Moreover, the end-user requirements are confined which decreases the cost of devices that can be used in WMNs.

Collective radios

Mesh routers can be implemented with collective radios to perform routing and access functionalities. This provides the segregation of two main types of traffic in the wireless domain. While routing and frame work are expanse between maze routers, the access to the network by end users can be carried out on a different radio. This extremely improves the expanse of the network. On the other hand, in ad-hoc networks, these functionalities are achieved in the same channel, and as a result, the execution decreases.

Portability

A foundational problem of multi-hop wireless networks is the confined scalability and reduction of completion with expanding path lengths, i.e. number of hops. This constrain is mainly due to co-channel interference as well as the certainty that IEEE 802.11 interfaces do not hold full-duplex application, i.e. synchronous transmission and reception of data. One access to run over this problem is to use multi-homed (multi-radio) nodes, with radio transceivers tuned to orthogonal channels. Multi-homed nodes have extremely increased capacity, due to decomposition interference and the ability to perform full-duplex communication, which is not sustained by single radio nodes. In addition to degradation interference via increased channel diversity, these appended interfaces can be used to create multiple synchronous links.

Ad-hoc On Demand Distance Vector Routing (AODV) is a peculiar algorithm for the performance of ad-hoc networks. Each Mobile Host enforce as a specialized router and routes are received as required (i.e. on demand), with little or no reliance on cyclic advertisements. This routing algorithm is quite useful for a dynamic self-starting network as required by users desiring to take advantage of ad-hoc networks. AODV provides circumference free routes even while retrieve broken links. Here, this algorithm scales to enormous populations of mobile nodes desiring to form ad-hoc networks. As compared to DSDV and other algorithms which reserve moderately amend routes to all target in the ad-hoc network, this algorithm has quick

response to link breakage in active routes and also reduces memory requirements and causeless reproduction.

ROUTING PROTOCOL

A routing protocol establishes how routers communicate with each other, propagating information that qualify them to prefer routes between any two nodes on a computer network. Routing algorithms induce the specific choice of route. Each router has a preceding knowledge only of networks attached to it without deviation. A routing protocol claim this information first among extant neighbours, and then every place the network. This way, routers benefits attainments of the topology of the network .Routing protocols were conceive for routers. These protocols have been accomplished to allow the replacement of routing tables, or known networks, surrounded by routers. There are a lot of different routing protocols, each one designed for particular network sizes.

Types of Routing

The router learns about remote networks from neighbour routers or from an controller. The router then constitute a routing table that express how to asset the remote networks. If the network is straightly connected then the router at present knows how to asset to the network. If the networks are not appended, the router must learn how to get to the remote network with one of two static routing (controller not automatically enters the routes in the router's table) or dynamic routing (happens consequently using routing protocols).The routers then restore each other about all the system of connection. If a break occurs e.g. a router decreases, the dynamic routing protocols consequently inform all routers about the break. If static routing is used, then the commander has to restore all changes into all routers and therefore no routing protocol is worn.

Only dynamic routing worn routing protocols, which implement routers to:

- Dynamically determine and control routes.
- Multiply routes.
- Dispose routing to restore other routers.
- Reach accord with other routers about the mesh topology.

Statically programmed routers are not able to determine routes, or circulate routing information to other routers. They circulate data by routes defined by the network commander. A root network is so called because it is a obstacle in the network. There is one route inside of the mesh and another one route is in out of the mesh and, because of this, they can be attained using static routing, hence retaining valuable bandwidth.

Routing protocols is a definite of rules or establish that terminate how routers on a network connect and interchange information with each other, allowing them to select outstanding routes to a outlying network, each router has precedence knowledge only of networks attached to it without deviation. Routers moving routing protocol segment this information first, among instant neighbours, then over the entire network. This way, routers share vision knowledge of the topology of the mesh.

Routing protocols perform several activities, including:

- Network detection.
- Renovate and protect routing tables.

The router which settle at the bottom of a network protect a routing table, which is a ballot of networks and dependent routes known by the router. The routing table carry network addresses for its particular interfaces, which are the straightly connected networks, and also network addresses for remote networks. A distant network is a mesh that can be attained by promoting the packet to a router. Distant networks are combined to the routing table in two ways:

i. By the mesh commander not automatically configure the static routes.
ii. By achieving a dynamic routing protocol.

Dynamic routing protocols are worn by routers to measure information about the reachable of the routers and status of distant networks.

IP ROUTING PROTOCOL

There are various aggressive routing protocols for IP. Here are some of the further common aggressive routing protocols for routing IP packets:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)

- IS-IS (Intermediate System-to-Intermediate System)
- BGP (Border Gateway Protocol)

Advantages of aggressive routing protocol

i. Aggressive routing protocols bring up to date and protect the networks in their routing tables.

ii. Aggressive routing protocols not only arrange a greatest path determination to more networks, they will also induce a new greatest path if the initial path becomes unavailable or there is a change in the topology.

AD-HOC ON-DEMAND LAPSE VECTOR ROUTING PROTOCOL

In November 2001 the MANET (Mobile Ad-hoc Networks) in process cluster for routing of the IEFT community has pronounced the first form of the AODV Routing Protocol (Ad-hoc On Demand Distance Vector). AODV is connected with to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its next node and the line to reach them. A node sustain its own routing table, reserve all nodes in the network, the lapse and the nearest hop to them. If a node is not reachable the lapse to it is set to infinity. Every node sends its near by node regularly its whole routing table. So they can check if there is a helpful route to one more node using this nearest as next hop. When a link split a count-to- infinity could happen.

AODV is an 'on demand routing protocol' with slight delay. That means that routes are only entrenched when needed to diminish traffic on high. AODV holds Unicast, Broadcast and Multicast without any extra protocols. The count-to-infinity and loop problem is determined with continuance numbers and the enrolling of the costs. In AODV every hop has the steady cost of one. The routes age very apace in order to receive the movement of the mobile nodes. Link breakages can locally be replaced very productively. AODV uses IP in a proper way. It pleasures an IP address just as a separate identifier. This can easily be done with mounting the subnet mask to 255.255.255.255. But also accumulate networks are sustained. They are appliance as subnets. Only one router in specific node is important to progress the AODV for the inclusive subnet and provide as a offense gateway. It has to sustain continuance number for the whole subnet and to progressive every package.

In AODV the routing table is explicated by a continuance number to every destination and by time to vital for every passage. It is also explicated by routing flags, the intrusion and a list of vanguard and for antiquated routes the final hop count is reserved.

AODV PROPERTIES

1. AODV detect routes as and when necessary. Does not sustain routes from every one node to every other node.
2. Routes are sustained just as long as specified.
3. Every node sustained its monotonically expanding continuous number, expands every time the node notices change in the next topology.
4. AODV use routing tables to reserve routing information. A Routing table for only single routes .A Routing table for many routes .
5. The route table reserve destination adder, next-hop adder, destination continuous number, life time.
6. For each destination, a node sustained a list of vanguard nodes , to route complete them vanguard nodes help in route preservation.
7. Life-time renovate every time the route is worn .If route not worn within its life time, it elapses.

GATEWAY SOURCE ROUTING PROTOCOL

A source routing protocol re-uses the forward paths that are certified by data packets and reserved on the gateways. These paths are then worn for source routing on the regressive path. With gateway source routing (GSR), the progressive path information from the packets that appear at the gateways is repeated. In the routing header of whole packet, the intermediate hops from the maze node to the gateway are certified. These paths are then reserved in the gateways. To route packets to a maze node, the maze gateway inverts the certified. Progressive path and replica it to the packet header. The gateway then express the packet to the opening node of the recursive path. Each and every node restore the path in the headerby eliminate its entry and progressive the packet to the given next neighbour hop since the packet reaches the terminal. By design, this approach is scalable to the representation of mesh nodes as it establishes no beyond that depends on this number. Only the gateways have to sustained up-to-date routes to single mesh nodes. Also, this path does not upgrade the number of control packets returned between the mesh nodes, and thus decreases the chance of collisions. Surely, GSR depend upon that a packet towards a host in the internet is first sent by a maze node in order to originate the recursive path. HIP and most other addressing mechanisms contain cyclic registration messages from the maze node towards a gateway. Those fluctuating registration messages serve also to induct and sustain the path at the gateway.

In wired networks, the worn has to escort access to wired cables so as to drip transmission. In adverse, the attacker only rights a deserved transceiver to receive wireless signal without being exposed. In wired networks, devices like desktops are constantly static and do not change from one place to another. Hence in wired networks there is no essential to protect users' mobility mode or move pattern, while this delicate information should be kept separate from match in wireless environments. Variously, an match is able to profile users according to their change, and expose or misuse worn based on such information. Finally, providing separate protection for ad-hoc networks with less-power wireless devices and lower-bandwidth network connection is a very difficult task. The tonicity property of the determined path weight is worn to establish a routing protocol that can notify the maximum bandwidth path from each every node to each other destination.

A wireless network may have a lot of dependent routing attacks, in which dropping a malicious conduct of nodes is, current anonymous routing protocols essentially concede anonymity and sectional unlink ability, most of them stroke unbalanced feature of public key crypto systems to attain their goals. Complete unlink ability and un observability are not approved due to short content preservation. Current schemes decline to sustain all content of packets from mugger, so that the mugger can obtain information like packet type and continuous number etc. This information can be worn to express two packets, which split unlink ability and may point to source tread back attacks. Concurrently, powerless packet type and continuous number also make current schemes visible to the adversary. Here, distinct from gateway source routing, an address privacy-maintain routing mechanism is involved that accomplish content observability by exploit anonymous key entrenched based on group signature. The setup of this appliance is simple. Each and every node only has to achieve a cluster signature conform key and an ID-based special key from an offline key server or by a key authority scheme. The gradual routing protocol is then completed in two phases. First, an anonymous key formulation process is performed to compose secret huddle keys. Then an gradual route discovery process is completed to find a route to the destination. This is to maintain all parts of a packet's content, and it is reliant of solutions on transit pattern observability, which thereby add excellent results to the dynamic performance of GSR.

RESULTS AND DISCUSSION

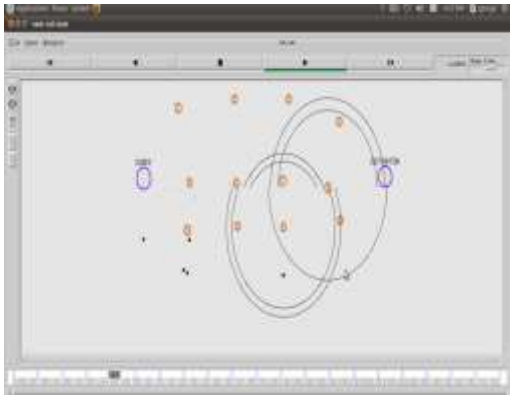


Fig. 1(5): AODV Loss of packets due to link failure or contention

When there is any contention or link failure in the network, there loss of packets occurs thereby reducing the efficiency of the routing protocol. The fig shows the packet loss in the network.

Fig. 1(6): Field Based Routing Protocol Node 8 transmitting packets to the intended destination.

The process of transmission continues till the node having the highest potential is identified, this node is the destination. [Fig. 1(6)] shows the destination receiving packets from node 8.

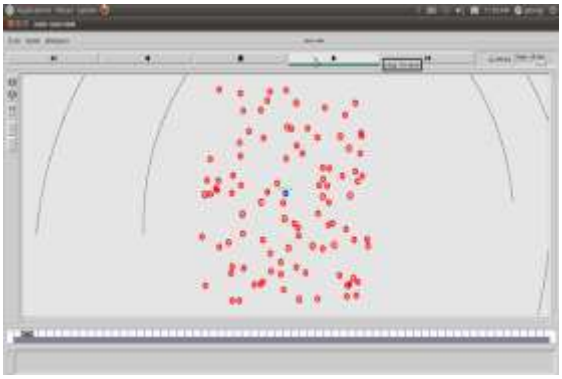


Fig. 1(7): Gateway transmitting packets to the intended destination (node).

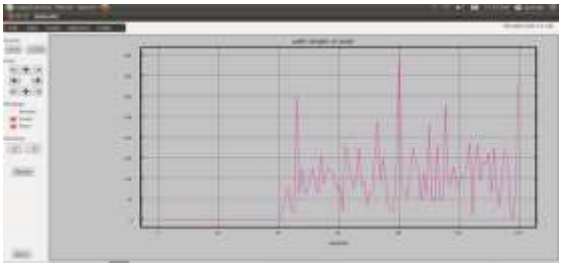


Fig. 1(8): Path length of AODV vs. no. of Packets

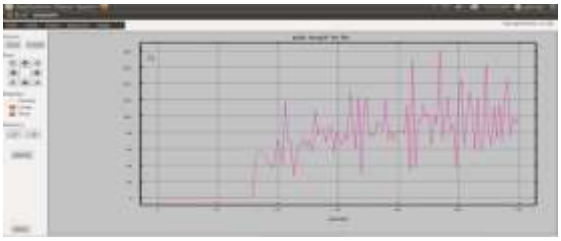


Fig. 1(9): Path length of FBR vs. No. of Packets

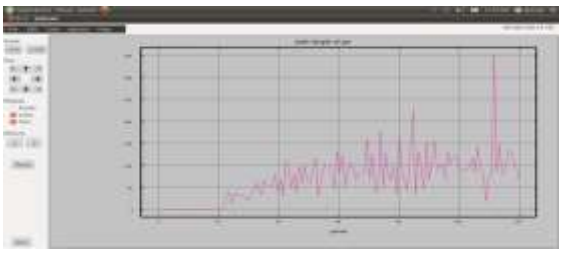


Fig. 1(10): Path length of GSR vs. No. of Packets

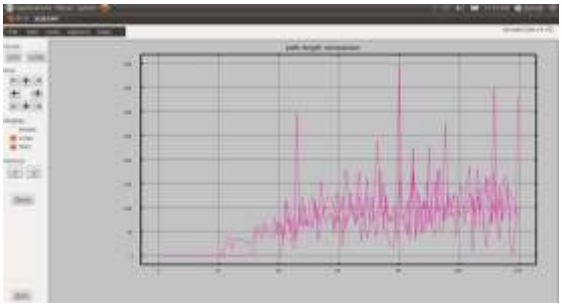


Fig. 1(11): Path length comparison

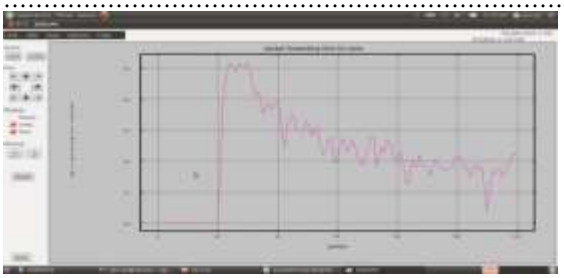


Fig. 1(12): Packet forwarding time of AODV vs. no. of packets

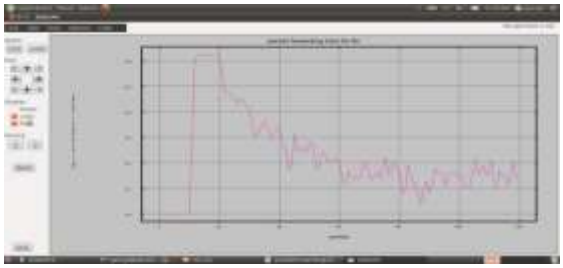


Fig. 1(13): Packet forwarding time of FBR vs. no. of packets

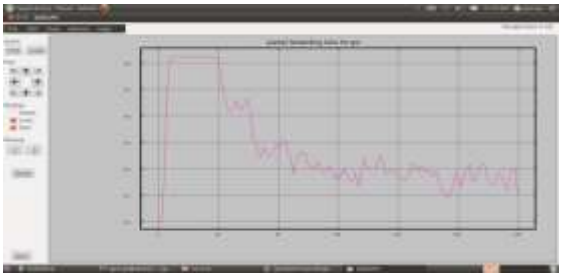


Fig. 1(14): Packet forwarding time of GSR vs. no. of packets

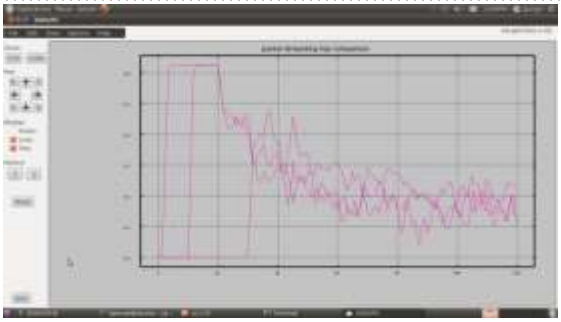
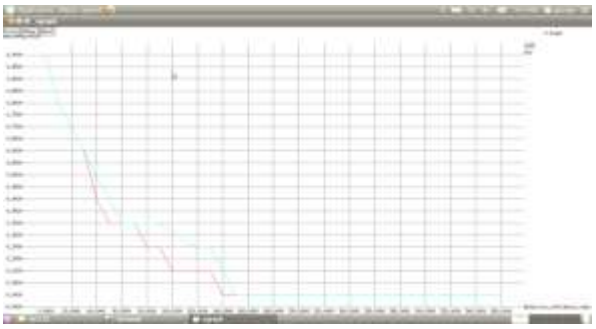


Fig. 1(15): Packet forwarding time comparison

Table 1(1): Representation of protocols



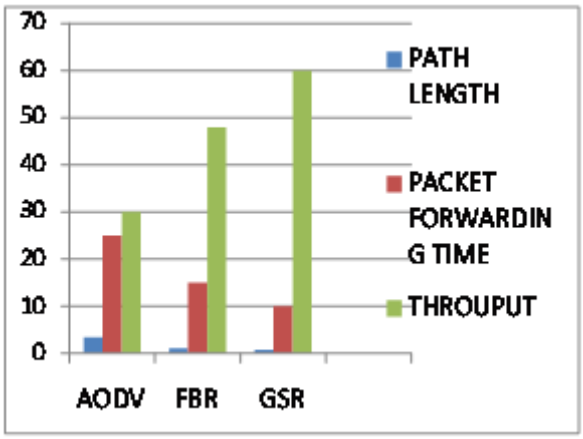


Fig. 1(16): Packet delivery ratio comparison

PROTOCOLS	PATH LENGTH	PACKET FORWARDING TIME	THROUPUT
AODV	3.4	25	30
FBR	1	15	48
GSR	0.75	10	60

Fig 1.17: Comparison for protocol Parameter

CONCLUSION

The main aim of work is increase the overall efficiency of the network. For this purpose we have implemented a protocol called gateway source routing in wireless mesh networks and simulated in NS2 (Network Simulator 2). In this simulation we have created different mesh networks and have transmitted packets using different protocols. The protocols used are, Ad-hoc On demand Distance Vector routing (AODV), Field Based Routing (FBR), Gateway Source Routing (GSR). Hence we analyzed a base paper and found out the best method with which we can improve the efficiency of the network called Gateway Source Routing and have executed the same along with the comparison results of the above mentioned two protocols used for the transmission of the same. This concludes that the gateway acting as the source transmits data efficiently to the intended node using the Gateway Source Routing protocol. The same protocol AODV, FBR and GSR can be implemented in mobile pattern of nodes and the parameters: packet forwarding time, path length and throughput can be simulated using NS2.

CONFLICT OF INTEREST
There is no conflict of interest.

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None.

REFERENCES

[1] C Perkins, E Belding-Royer and S Das [2003] Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561 (Experimental).
[2] T Clausen and P Jacquet [2003] Optimized Link State Routing Protocol.
[3] Vincent Lenders and Martin May and Bernhard Plattner [2006], Density-based vs. Proximity-based Anycast Routing in proceedings of the IEEE Infocom, Barcelona, Spain.
[4] Multi-Linked AODV Routing Protocol for Wireless Mesh Networks Asad Amir Pirzada and Ryan Wishart,[?] Queensland Research Laboratory, Marius Portmann, School of Information Technology and Electrical Engineering, The University of Queensland, Australia.
[5] Vincent Lenders and Martin May and Bernhard Plattner, [2005] "Service Discovery in Mobile Ad Hoc Networks: A Field Theoretic Approach," in Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Taormina, Italy.