Zone Disjoint Multipath Routing Protocol

M. Arvind
Department of Computer Science and Engineering
Pondicherry Engineering College
Pondicherry - 605014

M. Sugumaran
Department of Computer Science and Engineering
Pondicherry Engineering College
Pondicherry - 605014

ABSTRACT

An ad-hoc network is the co-operative engagement of a collection of mobile nodes without the required intervention of any centralised access point or existing infrastructure. Several routing protocols for mobile ad-hoc networks (MANETs) have been proposed. Most of the existing routing protocols are single path routing protocols which establish a single routing path between the source and destination nodes. This results in rapid depletion of battery power of the nodes that comprise the path between the source and destination nodes. This reduces the lifetime of the network. The proposed protocol overcomes these drawbacks by following a hybrid approach to routing of data packets and establishing multiple zone disjoint paths between the source and destination zones. The proposed protocol is based on the Zone based Hierarchical Link State Routing Protocol (ZHLS). The proposed work eliminates the need for the global broadcasting of zone LSP's and the need for the interzone routing tables used in ZHLS. The proposed protocol establishes multiple zone disjoint paths between the source and destination zones. The packets are encrypted by making use of a symmetric cryptosystem. The simulation results show that the proposed work outperforms the existing ZHLS and provides a flexible, efficient and effective approach for routing packets in mobile ad-hoc networks.

General Terms
MANETs, Zone Routing Protocols, Multipath Routing.

Keywords
Zone based Hierarchical Link State routing protocol, Multipath routing protocols, Zone disjoint multipath routing protocols, Hybrid routing protocols.

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are networks comprised of mobile nodes equipped with wireless interfaces and which communicate with each other without relying on any infrastructure. MANETs are ideal for scenarios where network infrastructure is not available or deploying a network infrastructure is impossible, too expensive or not available at that time. MANETs are mostly used in disaster relief operations, battlefields, conferences and other places where infrastructure based network coverage is not available. Nodes in a MANET can act as a client, a server as well as a router. Nodes within the communication range can directly communicate with each other. Nodes which are not in the communication range of one another can communicate with each other in a multihop manner, wherein the data packets are forwarded by the intermediate nodes till the data packets reach the destination node. The intermediate nodes act as routers which route the data packets between the source and the destination nodes. MANETs are characterized by dynamic topology, constraints on bandwidth and energy consumption. Nodes that comprise the MANETs are mobile and hence the topology of the network is subject to frequent change. Thus a path which is effective at a particular point of time may not be so at a later stage of time. The nodes in a MANET operate on limited battery power and hence energy consumption is an important issue in MANETs. If certain nodes in a MANET are extensively used, then their battery power may get depleted and hence these nodes may not be available further. This results in reduction of the lifetime of the network. Establishment of a single path between the source and the destination nodes can result in frequent link breakage due to the mobility of the nodes. Also the nodes in the particular path established between the source and the destination nodes are extensively used and this results in depletion of the battery power of the nodes that comprise the path. Multipath routing establishes multiple paths between the source and the destination nodes. Multipath routing is typically proposed in order to increase the reliability of data transmission and to support load balancing. Multipath routing balances energy utilization of the nodes which results in increase in lifetime of the network. Multipath routing takes network congestion into consideration and reduces the routing delay. Establishment of multiple paths between the source and the destination nodes reduces the frequency of the route discovery process and therefore the latency for discovering another route is reduced when the currently used route is broken. This reduces the overhead associated with the process of finding alternative routes when a currently used active route is broken. Several routing protocols have been proposed for MANETs. These routing protocols can be broadly classified into one of the classes such as proactive, reactive and hybrid. Proactive or table driven routing protocols such as Optimized Link State Routing (OLSR) [1], Destination Sequenced Distance Vector Routing protocol (DSDV) [2] continuously evaluate the routes within the network, so that when a packet needs to be forwarded, the route is already known and can be immediately used. The drawback of the proactive scheme is that the proactive schemes spend a significant amount of scarce wireless resources in keeping the complete routing information current. Reactive routing protocols such as Ad-hoc on demand routing protocol (AODV) [3], Dynamic Source Routing (DSR) [4] maintain routes to the active destinations. A route search is needed for every new destination. Therefore, the communication overhead is reduced at the expense of delay due to route search. Hybrid routing protocols are the new generation of protocols, which are both proactive and reactive in nature. The hybrid routing protocol maintain routes to the nearby nodes proactively and determine routes to distant nodes as and when required by using a route discovery strategy. We propose a hybrid routing protocol called Zone Disjoint Multipath Routing protocol (ZMR) which is based on the hybrid routing protocol Zone based hierarchical link state routing protocol (ZHLS) [5] and incorporates zone disjoint multipath routes between the source and the destination zones.

2. RELATED WORK

2.1. Zone Routing Protocol (ZRP)

Zone Routing Protocol (ZRP) [6][12] is a hybrid routing protocol which exhibits both proactive as well as reactive behavior. ZRP reduces the proactive scope to a zone centered on each node and maintains a reactive approach outside the zone. Zone of a node is nothing but the area of local neighborhood of that node. Size of a zone is given by a radius of length β, where β is the number of hops to the perimeter of the zone. Each node maybe within multiple overlapping zones and each zone may be of a different size. The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius β. The nodes whose minimum distance is less than β are interior nodes. ZRP refers to the locally proactive routing component as the IntrA zone Routing Protocol (IARP) [7]. The globally reactive component is named Inter zone Routing Protocol (IERP) [8]. IARP and IERP are not specific routing protocols. IARP is a family of limited depth proactive routing protocols. IERP is a family of reactive routing protocols. IARP relies on Neighbor Discovery Protocol (NDP) to maintain intrazone routing information. Bordercasting utilizes the topology information provided by IARP to direct query request to the border of the zones. The bordercast packet delivery service is provided by the Bordercast Routing Protocol (BRP). BRP uses a map of an extended routing zone to construct bordercast trees for the query packets. BRP employs query control mechanisms to direct route requests away from the areas of the network that already have been covered. A node that wishes to send data to another node checks if the destination node is present in its zone if so the data packets are routed to the destination node by making use of the intra zone routing table. If the destination node is not present in the same zone as the source node then a route request is sent out to identify the destination node. The route query is routed through the network by making use of the BRP. The node that receives the route request checks its routing zone to see if the destination node is present in its routing zone or if it has a path to the destination node. If the receiver of a route request packet knows the destination it responds by sending a route reply back to the source. The path to the destination node consists of a list of peripheral nodes through which the route request propagated. The route reply traverses the same path as that traversed by the route request. Any change in the peripheral nodes results in a route discovery phase to find out a new route to the destination node. As a result of mobility of the nodes this result in frequent link breakages and frequent route discovery phases and this result in increase in the overhead associated with the protocol.

2.2. Zone-based Hierarchical Link State Routing Protocol (ZHLS)

Zone-based Hierarchical Link State Routing Protocol (ZHLS) [9] is a hybrid routing protocol which incorporates location information into a novel peer-to-peer hierarchical approach. ZHLS maintains routing information proactively within a zone and maintains routing information in a reactive manner outside the zone. The network is divided into non overlapping disjoint zones. Each node in the network is loaded with the zone map before deployment. The zone map has to be worked out at the design stage. Each node by making use of geo-location techniques such as Global Positioning Systems (GPS) is able to map itself onto the zone map and thereby obtain the zone ID of the zone in which it is currently present in. Two types of Link State Packets are used to maintain a two level topology namely the node level Link State Packets (node LSP) and the zone level Link state packets (zone LSP). The node LSP are used to obtain information about the node level topology and the zone LSP's are used to obtain information about the zone level topology. Each node broadcasts a link request and those nodes which are within the communication range of the source node in turn reply with link responses. When all the link responses are received the node generates its node LSP which contains the node ID's of the neighboring nodes and the zone ID's of the neighboring zones. This process is performed by all the nodes in the zone asynchronously. The node LSP's are propagated locally only within a zone. When all the node LSP's of all the nodes in a zone are received the nodes know how the nodes are interconnected to each other in a zone and which zones are connected to their zone. The nodes construct the Intra Zone Routing table by applying the shortest path first algorithm on the received node LSP's. When all the node LSP's are received each node knows to which zones its zone is connected to and by making use of this information generates a zone LSP which is globally flooded throughout the network. When all the zone LSP's are received the nodes know how the zones are connected to each other. The zone LSP's of all the nodes of a particular zone are identical and duplicate zone LSP's are dropped and hence this reduces the overhead associated with the protocol. If the destination is not present in the zone where the source node is present, a location search is used to identify the current zone in which the destination is present. A location request is unicasted to all the zones in the network. The location request is routed to all the zones in the network by making use of the inter zone routing table. Each node receiving the location request checks its intra zone routing table to see if the destination node is present in its zone, if so a location reply is then sent back to the source node. All the nodes in all other zones except the destination node forward the packets by making use of the interzone routing table whereas the nodes in the destination zone route packets by making use of the intra zone routing protocol.

2.3. SPREAD

SPREAD [10] is a multipath routing protocol which aims at transforming a secret message into multiple shares and then delivers the share via multiple paths to the destination so that even if a certain number of message shares are compromised the secret message as a whole is not compromised. The protocol optimally allocates the message shares onto the multiple paths in order to enhance the security of the delivery of the data packets.

The protocol reduces the possibility of an attacker gaining access to the whole message by splitting the data into multiple shares and transmitting these shares over multiple paths established between the source and the destination nodes. The protocol increases the security of data transmission by dividing the data into multiple shares and sending them over multiple paths and thereby forcing an adversary to compromise at least a node in each of the multiple paths to gain access to the message. The SPREAD routing protocol does not establish disjoint paths between the source and the destination. Disjoint paths are essential in order to increase security because if the path is not disjoint then a node maybe part of multiple paths and the compromisation of a single node may compromise multiple paths, Furthermore if interference spreads to a particular area it is essential to have disjoint paths so that interference on a particular area does not affect more than one particular route.

3. PROPOSED WORK

The proposed work is based on the hybrid Zone-based Hierarchical Link State Routing Protocol (ZHLS) [11]. The proposed work incorporates the formation of multiple zone disjoint paths between the source and the destination zones. The major drawback associated with ZHLS is that there are a large number of control packets namely the node Link State Packets (node LSP's) and the zone Link State Packets (zone LSP's) which need to be broadcasted throughout the network. The proposed work reduces the number of control packets namely the zone LSP's that needs to be broadcasted and thereby reduces the overhead associated with the protocol. We establish multiple zone disjoint paths between the source and the destination zones. Zone disjoint paths share no common zones with one another. The construction of zones, the node LSP flooding and routing table construction in ZMR is same as the ZHLS. The detailed working of the proposed Zone disjoint Multipath Routing protocol is given below: The network is divided into non-overlapping disjoint zones. The division of the network into zones is done by geographically partitioning the network into non-overlapping disjoint zones. The nodes in the network make use of geo-location techniques such as Global Positioning Systems (GPS) to identify their current location and map their current position onto the zone map and thereby obtain their current zone ID. If any of the two nodes are within the communication range of one another then a physical link exists between them. If there is a physical link connecting any two zones then a virtual link between the two zones exists. The proposed ZMR protocol makes use of the node level topology to provide information on how the nodes are connected together by the physical links. The node LSP packets are used to maintain the node level topology. The node LSP of a particular node contains the node ID's of the neighbors present in the same zone and the zone ID of the neighboring zones to which it has a direct physical link. The nodes LSP are propagated locally within a zone. The node LSP's of a particular zone are not received by the neighboring zones.

3.1 Node Level Topology

In order to obtain the node level topology of a zone each node of a zone asynchronously broadcasts a link request. Nodes which are within its communication range in turn reply with link responses. When all the link responses are received, the node then generates its node LSP. The node LSP is flooded locally within a zone. When all the node LSP's are received, each node contains all the node LSP's of the nodes in that zone. For e.g. the node level topology of node a is shown in the Fig. 1. The node LSP of node a would contain the node ID of its neighbors which in this case are b, c, d and the zone ID 4 to which the node has a direct physical link to.

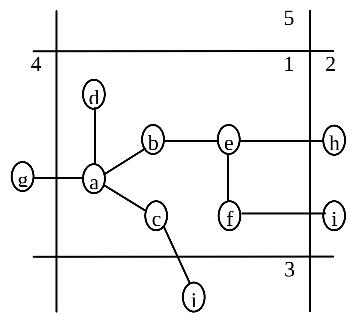
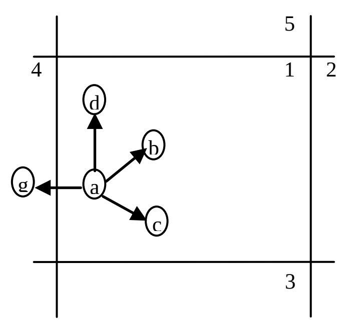
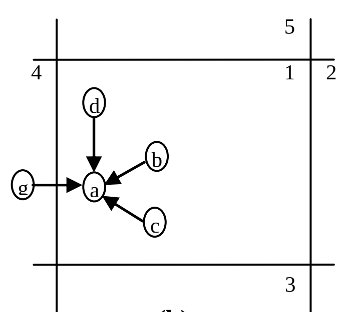


Fig 1: Node Level Topology

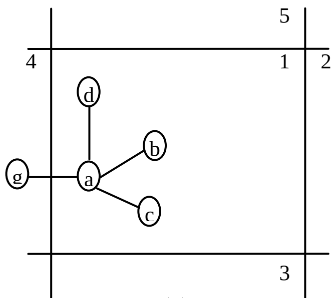
The process of obtaining the node level topology is depicted in the Fig. 2(a)-(d).



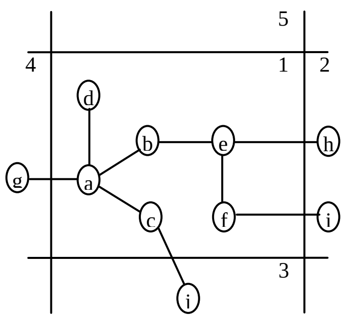
(a)



(b)



(c)



(d)

Fig. 2: Obtaining Node Level Topology (a) Node a broadcasts link request to its neighbors. (b) Node a receives link responses from its neighbors. (c) Node a generates its node LSP which is broadcasted within the zone. (d) All the nodes perform the process asynchronously.

At the end of this process all the nodes in the zone will have all the node LSP's generated by all the nodes in the zone as shown in Table I. All the nodes in a zone are aware of how they are interconnected to each other and to which zones their zones are connected. By applying a variation of the shortest path first algorithm on Table I the nodes can construct their intra zone routing table as shown in Table II. . Due to node mobility the above said procedure has to be performed periodically to maintain information on the connectivity of the network.

Table 1. Node LSP's in Zone 1

Source	Node LSP
a	***b, c, d, 4***
b	***a, e***
c	***a, 3***
d	***a***
e	***b, f, 2***
f	***e, 2***

Table 2. Intra Zone Routing Table of Node *a*

Destination	Next Node
b	***b***
c	***c***
d	***d***
e	***b***
f	***b***
2	***b***
3	***c***
4	***g***

3.2 Location Search & Routing Mechanism

As the nodes in the network are highly mobile, they cannot be associated with a fixed zone ID. Hence a location search mechanism is needed to identify the current zone ID of the destination node . So before sending data to the destination node the source node will check its intra zone routing table for the destination node to see whether it is present in the same zone. If so, then the data will be routed to the destination by making use of the intra zone routing table. If the destination node is not present in the same zone, then the source node initiates a location search and sends out a location request packet to every other zone in the network. The location request packet is given in Fig 3.

Source Node ID	Source Zone ID	Dest. Node ID	Dest. Zone ID	Zone Cache

Fig. 3: Location Request Packet Format

The location request is routed through the network by making use of the intra zone routing table. The location request is routed to the zones to which the source zone is connected to. The gateway node checks if the destination node is present in its zone. If so, then a location reply is unicasted back to the source node. The location reply packet is given in figure 4.

Source Node ID	Source Zone ID	Dest. Node ID	Dest. Zone ID	Zone Cache

Fig 4: Location Reply Packet Format

The zone cache field of the location request and reply packets contain the list of the zones traversed by the packet from the source to the destination zone. The path maintained in the zone cache is used by the intermediate nodes to route the packets between the source and the destination nodes. If the destination node is not present is the zone then the zone ID of the current zone is added the zone cache and the location request is routed to the zones to which the current zone is connected to. For example as show in Fig. 5 if node *a* in zone 1 wants to send data to node *z* in zone 5, the source node *a* checks its intra zone routing table to see if the destination node exists in its zone, as the destination node is in a different zone a location request is sent to every other zone in the network to identify the zone in which the destination node is present. The location request is of the following format < *a*, 1(*a*'s zone ID), *z*, X, 1....> . Each intermediate node routes the location request according to its intra zone routing table. Every gateway node that receives the location request, checks its intra zone routing table to see if the destination node exists in its zone. If so, a location response of the following format is sent back to the source node < *z*, 5(*z*'s zone ID), *a*, 1, 5.....1>. When a location request is received by the destination node, it starts up a Route Request (RREQ) collection timer[13]. As long as the RREQ collection timer is running, the destination node continues to collect RREQ's If the route in the zone cache is different from the previously received RREQ's route then the destination node registers the route

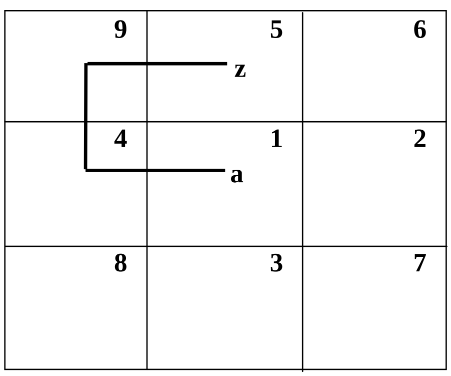


Fig 5: Routing path set up between node *a* in zone 1 and node *z* in zone 5 by using the intra zone routing table.

The only exception is that the source and the destination zones can be identical. After the timer runs out the destination node unicasts a Route Reply (RREP) to the source node. The RREP follows the same path traversed by the RREQ which is maintained in the zone cache. After all the RREP's are received by the source node, the source node transforms the message into multiple shares based on the number of paths formed between the source and the destination nodes. These multiple shares are sent over the multiple paths. Only the destination node can reconstruct the message as per Shamir's (k,n) threshold scheme, wherein only a node which receives k or more shares can reconstruct the message. Knowledge of any k-1 or fewer shares makes it impossible to determine the message. This enhances the secure transmission of data, as the source node divides the message into multiple shares and sends them via multiple independent paths, an adversary must intercept multiple pieces of the message from multiple paths in order to capture the message or he must disable multiple nodes on multiple paths in order to disrupt the delivery service. This technique ensures that the message is less likely to interpreted by adversaries and more likely to reach the destination. Thus the destination node can reconstruct the message sent to it. As only the node ID and zone ID are required for routing, the routes are adaptable to the dynamic topology. This reduces the frequency or the need for discovering new routes frequently and thereby reduces the overhead associated with frequent route discovery.

4. SIMULATION RESULTS

Our simulation has been carried out by making use of the Network Simulator 2.34 (ns 2.34). The simulation has been designed with a network of size 600x600m. The network has been divided into nine non-overlapping disjoint zones each of size 200x200m. The simulation has been designed with a total of 100 nodes distributed over the nine zones. The nodes are mobile and can move from one zone to another. Multiple zone disjoint paths are setup between the source and the destination nodes.

Because the proposed ZMR protocol eliminates the need for the global broadcasting of the zone LSP by all the nodes in the network and also as the data is sent over multiple paths setup between the source and the destination nodes, the nodes in the network consume less amount of energy when compared to the existing ZHLS. This results in an increase in lifetime of the network. Fig 6 shows the comparison of energy consumption between the proposed ZMR and the existing ZHLS.

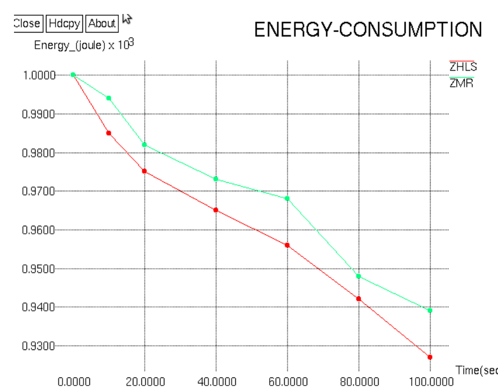


Fig. 6 Comparison of energy consumption between ZHLS and ZMR.

Multiple zone disjoint paths are setup between the source and the destination nodes and the message to be sent is divided into multiple shares and sent across these paths. As zone disjoint paths are setup between the source and the destination the interference affecting one particular route has no effect on any other route and also an adversary wishing to disrupt the data delivery service will have to compromise multiple nodes on multiple paths in-order to be successful.

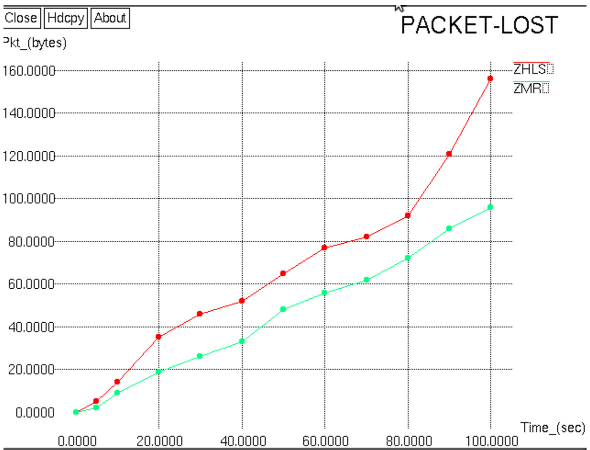


Fig. 7 Comparison of the loss of packets in ZHLS and ZMR.

This greatly reduces the loss of packets in the proposed ZMR when compared to the existing ZHLS as shown in Fig. 7.

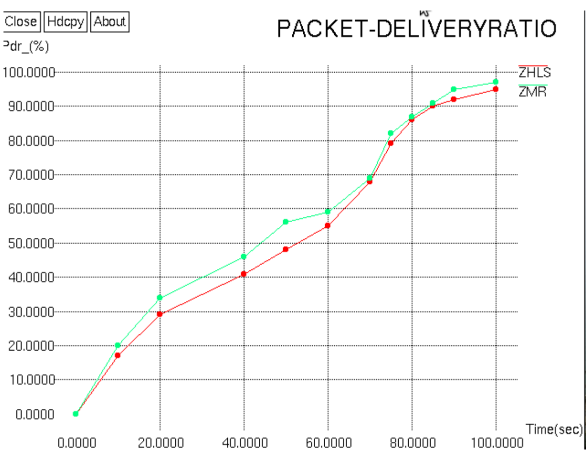


Fig. 8 Comparison of the packet delivery ratio between ZHLS and ZMR.

As the proposed ZMR, eliminates the need for the global broadcasting of zone LSP packets and also the need for the inter zone routing table, the nodes make use of only the intra zone routing table to route the packets and also as the load is balanced through the multiple paths set up between the source and the destination nodes the packet delivery ratio is much higher in the proposed ZMR when compared to the existing ZHLS as shown in Fig. 8.

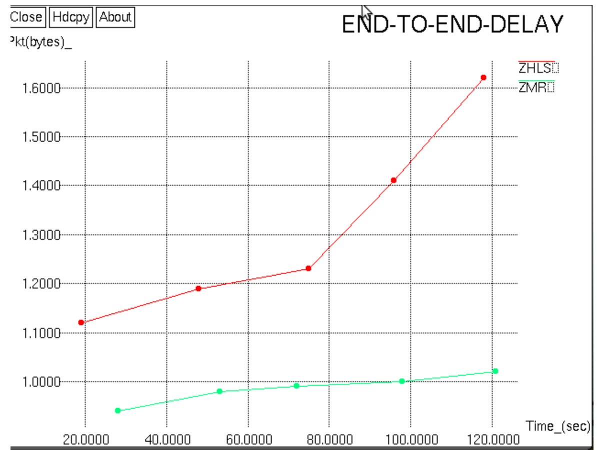


Fig. 9 Comparison of the end-to-end delay between ZHLS and ZMR.

As the proposed ZMR protocol eliminates the need for the global broadcasting of the zone LSP packets and also the need for the interzone routing table and also as the data is split into multiple shares and routed through the multiple paths setup between the source and the destination nodes the end-to-end delay assocaited with the proposed ZMR protocol is very less when compared to the existing ZHLS protocol as shown in Fig. 9.

5. CONCLUSION

In this paper, we have proposed ZMR, a zone disjoint multipath routing protocol. It is a hybrid routing protocol, which establishes multiple zone disjoint paths between the source and the destination. The establishment of multiple zone disjoint paths helps in load balancing thereby increasing the lifetime of the network, reducing congestion and also in decreasing the end-to-end delay associated with packet delivery. The transmission of the message as multiple shares along the various paths setup also results in secure transmission of the message. The simulation results show that the proposed algorithm is very effective in decreasing routing overhead and also in decreasing the end-to-end delay in MANETS.

6. REFERENCES

[1] P. Jacquet, P. Muhlethaler, A. Qayyum, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manet olsr-00.txt, Nov 1998.

[2] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance- Vector Routing (DSDV) for Mobile Computers", Computer Communications Review, pp. 234–44, Oct 1994.

[3] C. E. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing", in Proceedings of the Second IEEE

Workshop on Mobile Computing Systems and Applications, (New Orleans LA), pp. 90–100, Feb. 1999.

[4] D.B. Johnson, D.A. Maltz, " Dynamic source routing in adhoc wireless networks", in T.Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, pp. 153–181,1994.

[5] M. Joa-Ng and I.-T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 17, pp. 1415– 1425, 1999.

[6] Z. J. Haas, "The zone routing protocol (ZRP) for ad hoc networks", Internet Draft, July 2002

[7] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001.

[8] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-01.txt, June 2001.

[9] Takashi Hamma, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata, "An Efficient ZHLS Routing Protocol for Mobile Ad Hoc Networks",in Porc. of 17th International Conference on Database and Expert Systems Applications (DEXA'06), pp.66-70, 2006.

[10] Siguang Chen and Meng Wu, "Secure Multipath Routing Based On Secret Sharing in Mobile Ad Hoc Networks", in Proc. of IEEE International Conference on Network Infrastructure and Digital Content, pp. 539-542, 2009.

[11] M. Joa-Ng, "Routing protocol and medium access protocol for mobile adhoc networks," Ph.D. dissertation, Dept. Elect. Eng., Polytechnic Univ., Brooklyn, NY, 1999.

[12] Z.J. Haas and M. R. Pearlman "Determining the Optimal Configuration for the Zone Routing Protocol," In IEEE Journal on Selected Areas in Communications, pp. 1395-1414, Aug 1999.

[13] Kentaro Aburada, Naonobu Okazaki and Mirang Park, "Proposal of a zone disjoint multi-path routing for ad hoc networks", in Proc. of 8th Asia Pacific Symposium on Information and Telecommunication technology (APSITT), pp.1-4, 2010.