Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

Asian Journal of Scientific Research 7 (4): 472-481, 2014
ISSN 1992-1454 / DOI: 10.3923/ajsr.2014.472.481

RECT Zone based Location-aided Routing for Mobile *Ad hoc* and Sensor Networks

[1]Anna Saro Vijendran and [2]J. Viji Gripsy
[1]Department of MCA, S.N.R. Sons College, Coimbatore, India
[2]Department of Computer Science, PSGR Krishnammal College, Coimbatore, India

Corresponding Author: J. Viji Gripsy, Department of Computer Science, PSGR Krishnammal College, Coimbatore, India

ABSTRACT

In recent decades, routing in Mobile *ad hoc* Sensor Network (MASNet) have become an active research area due to its impact in various science and engineering applications. The increased demand for energy has become a great concern in industrial market which in turn has led to the development of various energy efficient sensor networks. This research study mainly focuses on secure and energy efficient routing in MASNet. A secure multipath algorithm has been presented in this study which facilitates the nodes in MASNet to carry out on-demand discovery and forming set of paths while identifying a disjointness threshold, denoting the maximal number of nodes shared between any two paths in the set of the k established paths. The proposed Rectangular Zone based Location Specific Routing (RZLSR) approach is energy efficient, adaptive, secure and uses labels to carry the disjointness-threshold between nodes during the route discovery which improves the quality of services. The broadcasting scheme used in this approach is based on RECT which forms an efficient framework for routing data between source and destination. A set of security mechanisms, based on the use of Watchdog and digital signature, are used to protect the route discovery process. The simulation results indicate that the proposed approach provides significant performance with lesser overhead, energy efficient and better network lifetime.

Key words: GPS, location aided, rectangular zone, k-x-connectivity, multipath routing, watchdog, threshold signature, mobile *ad hoc*, sensor networks

INTRODUCTION

Mobile *ad hoc* Sensor Networks (MASNets) have been extensively used in several applications. Routing in MASNetis a challenging taskas it has several factors to be taken into consideration. In MASNet, packets would be influenced by several signal deterioration such as shadowing, fast/slow fading, etc (AlOtaibi and Soliman, 2010). Packet losses are built-in and it cannot be completed eliminated in the wireless link. Mobility of the nodes assures frequent topology alterations and links breakages. In an *ad-hoc* network, there is no centralized structure that controls the traffic among the mobile nodes and authenticates supplicant nodes. In sensor networks, sensor nodes have restricted power, processing ability, short transmission range and limited storage space. Thus, a routing approach should consider these essential aspects to guarantee high network throughput, minimal bandwidth usage and low energy consumption.

A number of research studies in routing protocols are available in the literature for MASNETs (Perkins *et al*., 2003; Johnson and Maltz, 1999). But the existing algorithms have the limitations

such as route maintenance overhead, lesser energy efficient, etc. Route maintenance approaches necessitates additional control packets to be transmitted with any alteration in the topology. But, it would result in more energy consumption and higher bandwidth utilization. This would result in higher failure rate among sensor nodes.

In order to eliminate the route maintenance issues, several studies (Alshanyour and Baroudi, 2008; Soliman and AlOtaibi, 2009) have been presented to minimize the number of transmitted control packets, with minimized energy and bandwidth utilization. In such approaches, every node gathers data about its neighbors by exchanging the control packets. These details would be is used to reroute data packets in scenarios like link failures or dynamic topology alterations. The conventional approaches do not offer significant and reliable results due to high speed mobility and frequent topology changes which in turn results in high communication overhead, higher bandwidth utilization and higher energy consumption.

In the last decades, various multipath routing approaches were proposed. Multipath On-Demand Routing Algorithm (MDR) (Dulman *et al*., 2003) guarantees the establishment of disjoint paths between the source and the destination. It partitions the original data packet into 'n' segments and sends these new sub-packets across the suitable paths. The destination will only be conscious of the presence of a path. It returns a route reply comprising of an additional field that shows the number of hops it traversed in a particular time. The hop count of the message would be incremented when node gets a route reply and then forwards the data to the neighbor from which it attains the original route request. This process causes lot of overhead in the network. In Dynamic Multi-Path Source Routing (DMSR) (Yang and Huang, 2008), each node must enclose the details of bandwidth into forwarded packets in order to identify the optimal paths based on the available bandwidth. Best Effort Geographical Routing Protocol (BEGHR) makes use of the position of nodes to forward data and also makes use of the Global Position Systems (GPS). But, the demands for resources at the different nodes are quite high which affect network lifetime to a great extent. Label-based Multipath Routing (LMR) (Hou *et al*., 2004) broadcasts a message to the entire network for attaining a probable alternative path. It defines a lexicographic total order on the label for each node. In this approach, the number of routing paths can be two or more but with relatively higher end to end transmission delay which is a biggest challenge.

In MASNets, the mobility of nodes could, not only affect the maximal number of paths that could be established between any source and destination nodes but also the extent to which these paths are disjoint. The sensitivity of the used applications and the variation of the nodes density from a network location to another, makes it important to extend the multipath routing algorithms so that a new parameter, called disjointness threshold (represent the maximal number of nodes shared between any two paths in the set of the k established paths), will be specified and exploited during the routes discovery to create a trade-off between fault-tolerance and performance.

In this study, improve Location-Aided Routing (LAR) which is one of the most famous location based routing methods based on rectangular zone type (Jain and Chadda, 2013). This kind of technique uses information about the location of mobile node through GPS technique. Our new protocol considers both areas of routing and find path between source and destination by using rectangular zone. At first, we propose a more efficient routing method which improves the quality of services. Secondly, we proposed method that uses a technique to find path between sources to destination.

LITERATURE SURVEY

Razak *et al.* (2004) introduced reputation management systems forassistance enforcement solution in *ad hoc* networks. Sequential Probability Ratio Test (SPRT) is employed to differentiate between cooperative and malicious neighbors. The node behavior may changes from one node to another and from time to time owing to changes in local and network-wide conditions, disturbing the ability of the reputation management mechanism to differentiate between a node's determined decision not to forward packets and its incapability to do so owed to adverse network conditions.

Wang *et al.* (2007) plays an important role in examining the irregular events in MANET. ADRS investigating the MANET anomalies resulted by both the attacks. Each Anomaly Detector (AD) in an ADRS monitors the performance and traffic of the adjacent nodes and distributes the information among the other AD's. The overhead is insignificant owing to light weight of AD's. The behavior of the node is firmed by the packet forwarding ratio. The most important parameter for an ADRS detecting the node behavior is based on a threshold value which measures the distance between the regularity of monitored events and that of normal profiles.

Ko and Vaidya (2000) a Location-Aided Routing (LAR) is proposed in MANETs. In LAR, a source node search for and achieves destination node's location and average speed information. Then it utilizes this information to form a rectangle zone shaped region with the purpose of links the source and the destination nodes. In this case, LAR functions as a conventional flooding mechanism. If the source node does not know the location information and average speed of the destination, LAR organize the conventional flooding mechanism.

Shih and Yen (2008) introduced a location-aware routing through dynamic adaptation of request zone for MANETs. This algorithm is alike to LAR in request and expected zones. Though, it employs a triangular rather than a rectangle-shaped request zone like in LAR. Furthermore, it utilizes an accurate technique than LAR to measure the expected zone. All nodes within the request zone recommunicate the packets generated by the source node to form the triangle-shaped zone. The triangle shape area rises until it covers the entire network if it fails to reach a destination.

Oberg and Xu (2007) a received signal strength-aided flooding (RAF) protocol is introduced. This protocol minimizes the number of rebroadcasts needed to cover the entire network, with all destination nodes. It uses a dynamic delay function to reduce nodes rebroadcast, energy consumption and finds the arrangement of their rebroadcast. By the side of any intermediate node, receipt of a recently broadcasted message will start a countdown timer and the message is rebroadcasted upon its end. For duplicate messages with signal strength over a definite threshold, an additional delay is added to their counters; or else, they will be dropped.

PROPOSED ROUTING PROTOCOL ALGORITHM

This protocol is use to improve the packet delivery ratio from source to destination because it provide the optimal path in terms of bandwidth, automatically due to this the quality of service, throughput and its related parameters of this protocol may enhanced further. This approach provides solution of flooding and reduces the power consumption.

Basics of LAR routing: LAR is an on-demand routing protocol whose function is analogous to Dynamic Source Routing (DSR) (Soliman and AlOtaibi, 2009). Quite the oppositeof DSR, LAR protocol makes use of geological location information to restrict the area for finding a new route to a smaller request zone. In its place of flooding the route requests interested in the whole network, only those nodes in the request zone will forward them.

To find out the request zone, there are two schemes. In the initial one, the source calculates a circular area (expected zone) in which the destination is predictable to be found at the current time. The position and the size of the circle are estimated based on the location information of the preceding destination, the time on the spot associated with the previous location record and the average speed of the destination as seen in Fig. 1: Standard LAR scheme 1. The request zone is a smallest rectangular region that comprises of the expected zone and the source. The coordinates of the four corners are incorporated in the route request packet at what time commencing the route discovery process. RREQ broadcast is limited to this request zone. Therefore, when a node in the request zone receives RREQ, it forwards the packet in general. But when a node which is not in the request zone receives an RREQ, it drops the packet. For instance, in (Fig. 1), if node I receives the route request from some another node, the node I forwards the request to its neighbors node, because I, decide that it is surrounded by the rectangular request zone. Despite the fact that, when node J receives the route request, it rejects the request, as node J is not inside the request zone.

If source node S knows a previous location of destination node D at time t_0, if it also knows its average speed v and the current time t_1, then the expected zone at time t_1 is a circle around P with radius $R = v\times(t_1-t_0)$.

Once the destination D receives the route request packet, it sends back a route reply packet as in the flooding algorithms. Its reply differs by containing its current position, the actual time and its average speed. Source node S is available to make use of this information for a route discovery in the future. In the second scheme, the source calculates the distance to the destination based on the location of the destination. This distance, is integrated in the route request message and sent to neighbors. When an intermediate node receives the request, it calculates its distance to the destination. It will relay the request only if its distance to the destination is less than the distance included in the request message.

Proposed routing algorithm: A middle node will forward a route request packet, merely if it fit in to the request zone. The request zone is supposed tohave the expected zone to reach the destination node D. In normal LAR scheme 1, the sides of the rectangle are always parallel to the X and Y axes.

The rectangular shaped request zone only implemented. On the other hand, further definitions may be used. For example, it is feasible to remove the available restriction when defining the rectangular region: One side of the rectangle may be made parallel to the line connecting the location of source node S to the previous location of D. The proposed LAR scheme is presented in Fig. 2.

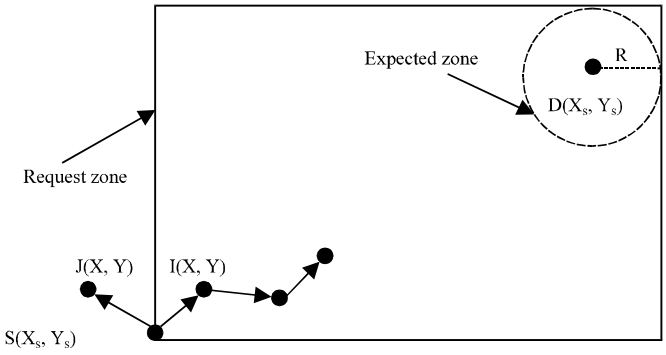

Fig. 1: Standard LAR scheme 1

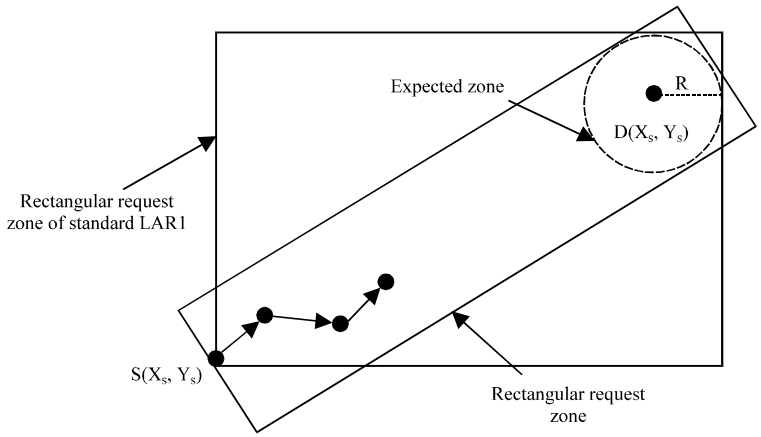

Fig. 2: Alternative definitions of request zone: Tilted rectangular shaped

In this scheme, the source node S finds out the coordinates of the four request zone vertices. These coordinates are comparative to the plane where the node S is the origin and the x-axis is parallel to the line between S and D. After that, the source translates these coordinates (for the four vertices) to the real coordinates by means of this equation:

$$x = x_1 \times \frac{y_D - y_S}{1} + y_1 \times \frac{x_D - x_S}{1} + x_S$$

$$y = x_1 \times \frac{x_S - x_d}{1} + y_1 \times \frac{y_D - y_S}{1} + y_S$$

where, (x_1, y_1) are the coordinates of the vertex in the initial plane and I is the distance between the source node S and the destination node D. Therefore, the coordinates of the four vertices area measured. These coordinates are integrated in the route request packet when commencing the route discovery process. RREQ broadcast is limited to this rectangular request zone. Thus, a node, $I(x_1, y_1)$ forwards the RREQ packet barely when it is in the request zone:

$$\begin{cases} x_1 \geq \text{RequestZone.top Left.x} \\ x_1 \leq \text{RequestZone.bottom Right.x} \\ y_1 \geq \text{RequestZone.bottom Left.x} \\ y_1 \leq \text{RequestZone.top Right.x} \end{cases}$$

Therefore in RECT method called (tilted rectangular shaped) where the source node S includes the coordinates of the vertices of the request zone within the route request message.

SECURITY CONSIDERATIONS

To endow with a secure routing algorithm, adjacent to a set of attacks which plan for the study, were three main properties should be satisfied. Initially, nodes should be able to validate each other through the process of routes establishment. Datagrams generated with forged information should

be redundant before reaching the destination mobile node called as MD. Secondly, every node should not be in position of generating and forwarding datagrams to MD but also of controlling the behavior of its neighbors. Also, the watchdog method is used to identify nodes that do not forward the datagrams as estimated. A node which makes use of watchdog technique is able to decide whether its neighbor nodes are forwarding the datagram they receive or not. If the packet is not forwarded within a definite period, this neighbor is measured as malicious (Jain and Chadda, 2013). Every node should sustain two lists: a list of one-hop neighbors and a list of two hop neighbors.

The two lists are fashioned by hiring every node periodically perform a two-hop broadcast of a Hello Message (i.e., by setting the TTL equal to 2). A node, stateas n1 which receives a generated Hello message by a node, say n0, with a TTL equal to 2, add the identity of n0 to its list of neighbors, appends it own identity (i.e., n1), decreases by one the TTL and forwards the packet. A node, say n2 which receives a datagram with a TTL equal to 1 from the neighbor node n1, adds the identity of the sender (i.e., n0) to its list of two hop neighbors and marks this node as life form reachable in the course of the immediate sender n1. Third, when a node detects a malicious neighbor, both the source and the destination nodes should be well-versed.

To protect the routing algorithm adjacent to forgery of false routing information, a signature based scheme is employed to authenticate nodes and guarantee the integrity of the information they exchange. Suppose, in case of WSN, every node joining the network is authenticated by the BS. Intermediate verification of packets signature permits to remove compromised packets before they reach the destination nodes which optimizes the used energy and communication resources and reduces the overhead of the signature verification process performed by the destination node. For the period of the routes establishment, every node generates or forwards the RReq and adds its identity, the identity of the next receiving nodes and sur-signs record the route. A node which may receiving the forwarded message confirm whether the final appended signature is correct or not, may checks if it is assumed destination, determines the immediate sender (the neighbor node from which the packet is being forwarded) of that datagram and makes sure that it is a neighbor. In case, it adds its identity, the identity of the feasible next hops and sur-signs the datagram. As an alternative of WSN, signature is performed by means of elliptic threshold signature algorithm provided by (Razak *et al*., 2004) is used. It allows to generate a public key kpub, n associated with secret keys kpr1,..., kprn. Every signature produced by a private keys called as kpri, can be checked bykpub. Every node uses its own private key for signature, whereas the same public key is employed by all the other nodes for the purpose of signature verification. In general types of *ad hoc* networks, where nodes can enter and leave the network at any time perfid and no resource limitsmay exist, normal signature can be used. Every node should contain its own private and public keys, where a certificate, containing this public key, is delivered by a certification authority. Mobiles nodes will employ the certificates of the senders to make sure the integrity of the signed datagrams. Assume that each mobile node has the capacity to make contact with a certification authority depository to download the certificate of any node in the network. These techniques increase the flexibility to nodes compromise, particularly in the circumstance of WSN they protect against nodes confine.The protection is done by (a) With digital signature to authenticate packet content and removalof invalid datagrams, (b) With the identification of captured node based on applied watchdog mechanism and intermediate signature and (c) Authorizing x shared nodes in

order to be liberal to discard of compromised paths involving captured node which assures that, even when part of the nodes have been captured, the rest of the network remains secure.

In the context of WSN, where threshold signature is used, if a node is duplicated and its key is used via a malicious node, MD will observe the attack by detecting that the same key was used by several nodes. To carry outthe process MD checks whether two nodes having the same identities have participated in forwarding the RReq. If it is not, for each signature adds to the RReq, the MD finds the identity of the signer node and verifies whether it could really create this signature if its private key was used (in the case of WSNs the MD which is the base station, is assumed to know all the mobile nodes private keys). Note that the use of the public key is not enough to validate the nodes, because it does not permit to detect whether the same private key was used several times to generate the sur-signed RReq. When the BS detects that a node has used the private key of another node or a node has participated numerous times in the similar RReq, it forwards an alert containing the identity of the compromised nodes, requesting for the remaining nodes in the network to reject any packet sent from that node in the future. When a node receives a second copy of the RReq, it signs and stores the received path in the RP list, where each identity, in the received path, is signed by intermediate nodes. If a malicious node wants to modify the RP list, it must use the signatures of all nodes involved in the modified path to re-sign each identity which is impossible. In addition, when an intermediate node eliminates a received RP list instead of forwarding it, the watchdog mechanism used by neighbor nodes will detect such behavior.

PERFORMANCE ANALYSIS

In order to evaluate the proposed protocol, the simulation is carried out using simulator version 2 (NS-2). NS-2 is a famous network simulation tool. Number of nodes in the network is selected to be 20, 30 and 50 for different simulation runs. The nodes are limited in a 1000×1000 m^2 area. Their primary locations are attained by means of a uniform distribution. Individual nodes move about next in a random way point mobility representation as there in (AlOtaibi and Soliman, 2010), eachnode moves incessantly, without pausing at any location.

The performance evaluation is measured by the graphs:

- **Packet delivery ratio (PDR):** PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This metric shows the reliability of data packet delivery. In Fig. 3, PDR is plotted against the number of nodes

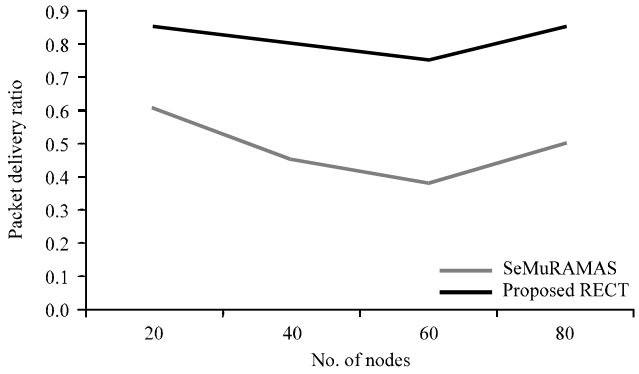

Fig. 3: Packet delivery vs. No. of nodes

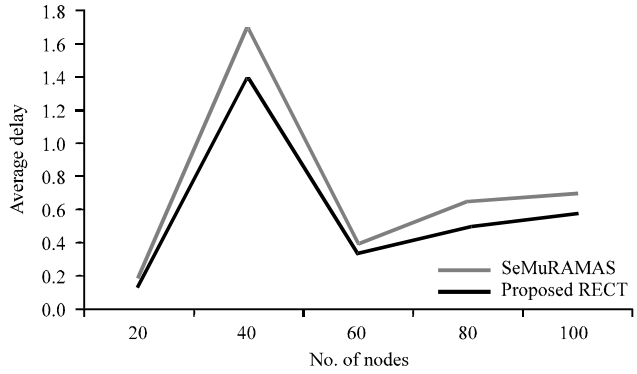

Fig. 4: Average delay vs. No. of nodes

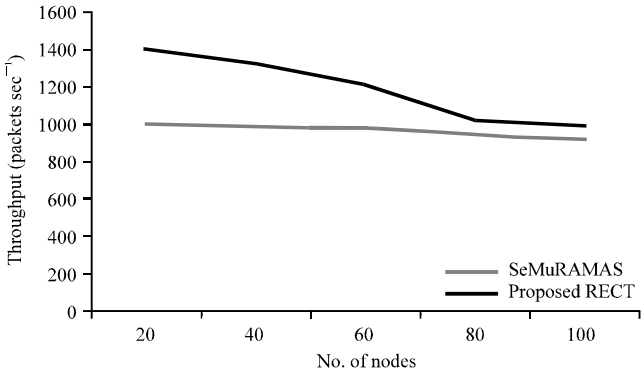

Fig. 5: Throughput vs. No. of nodes

- **Packet overhead:** The number of transmitted routing packets. For example, a HELLO or TC message sent over four hops would be counted as four packets in this metric. In Fig. 4, average delay has been ploted against number of nodes
- **Average delay:** This metric represents average end-to-end and indicates how long it took for a packets to travel from the source to the application layer of the destination. It is measured in seconds
- **Throughput:** This metrics represents the total number of bits forwarded to higher layers per second. It is measured in bps. It can also be defined as the total amount of data a receiver actually receiver to obtain the last packet

Figure 3 is drawn for the packet delivery vs. No. of nodes. From the figure the proposed RECT system which as high packet delivery ratio when compared with the existing techniques like SeMuRAMAS technique.

Figure 4 is drawn for average delay vs. No. of nodes. From the figure the proposed RECT system which as low average delay when compared with the existing techniques like SeMuRAMAS.

Figure 5 is drawn for the throughput vs. No. of nodes. From the figure the proposed RECT system which as high Throughput value when compared with the existing techniques like SeMuRAMAS.

Figure 6 is drawn for the routing overhead vs. No. of nodes. From the figure the proposed RECT system which as low routing overhead value when compared with the existing techniques like SeMuRAMAS.

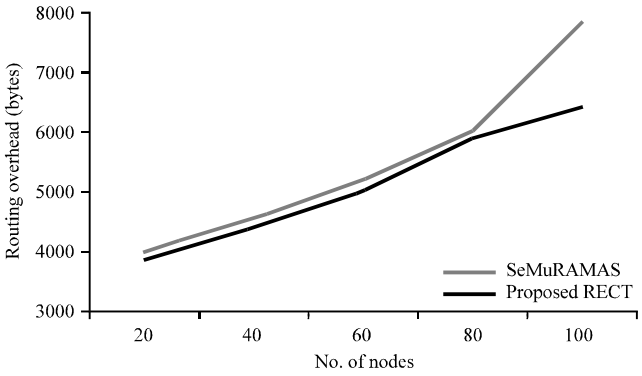

Fig. 6: Routing overhead vs. No. of nodes

Table 1: Results obtained by existing SeMuRAMAS approach

	No. of nodes		
Existing SeMuRAMAS	50	100	150
Generated packets	132	71	91
Received packets	120	51	81
Ratio	90.9	71.83	89.01
Dropped packets	12	20	10
Routing load	0.53	2.8	2.01
CBR bytes	18224	88540	81228
Route bytes	5252	12828	14816
Route costs	0.2	0.1	0.18

Table 2: Results obtained by proposed RECT approach

	No. of nodes		
Rectangle RECT	50	100	150
Generated packets	182	78	122
Received packets	171	72	115
Ratio	93.95	92.3	94.26
Dropped packets	11	6	7
Routing load	0.22	0.38	0.32
CBR bytes	7076	8480	11144
Route bytes	3624	3008	3696
Route costs	0.5	0.3	0.3

By considering both the Table 1 and 2, the proposed RECT based approach shows better results when compared with the existing technique.

CONCLUSION

In wireless *ad hoc* networks, there are several features different with wired networks. The differences are varying of network structure with limited resources such as bandwidth and energy and so on. LAR (Location-Aided Routing) which is one of the good numbersof locations based routing methods that uses information about the location of mobile node through GPS technique. The proposed new protocol is Rectangular Zone based Location Specific Routing (RZLSR) approach

considers both areas of routing and bandwidth. At first, propose a more efficient routing method which improves the quality of services in terms of routing overhead. Secondly, it combines two concept of location specific routing to improve the root discovery process. Those provide solution of the problem if there is any node not present in the area of requested zone.

REFERENCES

AlOtaibi, M. and H. Soliman, 2010. Routeless routing protocols over MASNETS: More energy saving approaches. Int. J. Wireless Mobile Networks, 2: 179-194.

Alshanyour, A.M. and U. Baroudi, 2008. Bypass AODV: Improving performance of *ad hoc* On-Demand Distance Vector (AODV) routing protocol in wireless *ad hoc* networks. Proceedings of the 1st International Conference on Ambient Media and Systems, February 11-14, 2008, Quebec, Canada.

Dulman, S., J. Wu and P. Havinga, 2003. An energy efficient multipath routing algorithm for wireless sensor networks. Proceedings of the IEEE International Symposium on Autonomous Decentralized Systems, April 9-11, 2003, Pisa, Italy.

Hou, X., D. Tipper and J. Kabara, 2004. Label-based multipath routing in wireless sensor routing. Proceedings 6th International Symposium on Advanced Radio Technologies, March 2-4, 2004, Boulder, CO.

Jain, S. and P.D. Chadda, 2013. A dynamic approach of location based routing in mobile *ad-hoc* network. Int. J. Latest Res. Sci. Technol., 2: 23-26.

Johnson, D.B. and D.A. Maltz, 1999. The dynamic source routing protocol for mobile *ad hoc* networks. Internet Draft, IETF MANET Working Group, October, 1999.

Ko, Y.B. and N.H. Vaidya, 2000. Location-Aided Routing (LAR) in mobile *ad hoc* networks. Wireless Networks, 6: 307 -321.

Oberg, L. and Y. Xu, 2007. Prioritizing bad links for fast and efficient flooding in wireless sensor networks. Proceeding of the International Conference on Sensor Technologies and Applications, October 14-20, 2007, Valencia, Spain, pp: 118-126.

Perkins, C.E., E.M. Royer and S. Das, 2003. *Ad-hoc* on-demand distance vector routing. Internet Draft, February, 2003.

Razak, S.A., S.M. Furnell and P.J. Brooke, 2004. Attacks against mobile *ad hoc* networks routing protocols. Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, June 28-29, 2004, World Scientific and Engineering Academy and Society, USA., pp: 147-152.

Shih, T.F. and H.C. Yen, 2008. Location-aware routing protocol with dynamic adaptation of request zone for mobile *ad hoc* networks. J. Wireless Networls, 14: 321-333.

Soliman, H. and M. AlOtaibi, 2009. An efficient routing approach over mobile wireless *ad-hoc* sensor networks. Proceeding of the 6th Consumer Communications and Networking Conference, January 10-13, 2009, Las Vegas, NV., USA, pp: 1-5.

Wang, S.H., C.H. Tseng, K. Levitt and M. Bishop, 2007. Cost-sensitive intrusion responses for mobile *ad hoc* networks. Recent Adv. Intrusion Detect., 4637: 127-145.

Yang, P. and B. Huang, 2008. Multi-path routing protocol for mobile *ad hoc* network. Proceedings of the International Conference on Computer Science and Software Engineering, December 12-14, 2008, Wuhan, Hubei, pp: 1024-1027.