An Enhanced Secured Dynamic Source Routing Protocol for MANETS

G. Lavanya, A. Ebenezer Jeyakumar

Abstract— Mobile Ad hoc Networks are established for extemporaneous services customized to application. These networks exist for limited period of time based on demands. This infrastructure less networks support data networking services using routing protocols. Reactive routing protocols serve the issue over proactive routing protocols [7]. As the communication is through multiple intermediate nodes, circumstances lead for the attacks lacking security [12]. Existing proactive routing protocols does not endow with security aspects within [1]. In this paper, we introduce an enhanced secured routing protocol and its performance is compared with the existing protocols namely, Ad hoc On demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) & Zone Routing Protocol (ZRP) in terms of delay, jitter and throughput using Qualnet simulation software.

Index Terms— Ad hoc networks, jitter, routing protocols, secured routing

I. INTRODUCTION

Wireless communication and network systems facilitate communication between computers using standard networks without network cabling. Wireless Networks are classified into two types, viz, Access point networks and Ad-hoc networks. In access point networks, nodes use an access point or base station, which acts as a hub providing connectivity between two different nodes, wired and wireless LAN, a node and wireless LAN, etc., In Ad-hoc networks, direct communication between nodes is possible without any access points. Ad hoc networks serve the issue of mobile nodes, due to its inherent properties such as self-organizing, self-healing, multi-hopping, dynamic nature, etc., [6]. Because of its infrastructure less feature, ad hoc wireless networks provide the facility for the user to use the network services while continually moving. The application scenario for the mobile ad hoc networks is emerging in recent years.

Main issues of ad hoc networks are routing, security, service location, energy consumption, etc. [4]. Routing the information using the intermediate nodes in ad hoc networks becomes the major issue due to its dynamic characteristics. Each move of the mobile nodes change the topology of the network in the transmission route which sometime leads to the disconnection of link. Since the communication is through radio waves, when there is a poor environment and the distance between the nodes is large, disconnection may occur [10]. It is necessary that the routing protocols should also provide good route maintenance after the route discovery. The distinctive feature of these networks is that the network nodes need to collaborate with their peers in supporting the network functionality [5]. More probability exists for a malicious or selfish node to disrupt or even deny the communication potentially of any node within the ad hoc networking domain. Every node in the network is required to assist in the network establishment, network maintenance and network operation [4].

Generally, routing protocols are categorized as table driven and on demand. Table driven routing protocol maintain consistent and up to date routing information among the nodes in a routing table. On demand routing protocols discover a new route, when a route is required from the source to the destination node. It serves the user's issue in Ad hoc mobile networks [6]. Later, combinations of the features of above two types turn out hybrid routing protocol. Although few routing protocols provide good performance, they lack in security. Hence, establishing secured data transmission through secured routes becomes a predominant issue.

The security techniques employed in paper [18] increases the routing overhead in transmission. All the secured routing protocols mentioned in survey paper [1] face the same issue by using key exchanges and key generations.

This paper introduces a secured dynamic source routing (SDSR) which includes security aspects in DSR which does not employ any key exchange mechanisms to reduce the routing overhead. This paper also shows the comparative analysis of three existing and well known routing protocol AODV, DSR & ZRP protocols with enhanced secured DSR protocol. The following sections provide the overview of all the above mentioned protocols and new enhanced secured DSR protocol. Final section discusses the performance of new protocol over the existing protocol.

II. ADHOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for Ad hoc mobile networks. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the source. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and sets up backward pointers to the source node in the route tables.

Manuscript received May 30, 2011.

G. Lavanya, Assistant Professor, Department of Information Technology, KTVR Knowledge Park for Engineering & Technology, Coimbatore, India, (e-mail: lavanya_joyce@yahool.co.in).

Dr. A. Ebenezer jeyakumar, Director (Academics), Sri Ramakrishna Engineering College, Coimbatore, India,(e-mail:ebeyjkumar@rediffmail.com).

In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it [16].

As the RREP propagates back to the source node, it sets up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained [17]. A route is considered active as long as there are data packets periodically traveling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform about the unreachable destination. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery process.

The absence of source routing and promiscuous listening allows AODV to gather only a very limited amount of routing information with each route discovery [14]. Single route discovery causes large retransmission delay in case of link failure[10].

III. DYNAMIC SOURCE ROUTING PROTOCOL

The Dynamic Source Routing (DSR) is a reactive unicast routing protocol that utilizes source routing algorithm [11]. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt.

There are two major phases in DSR, the route discovery phase and the route maintenance phase. When a source node wants to send a packet, it initially consults its route cache. If the required route is available, the source node includes the routing information inside the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting route request packets. A route request packet contains addresses of both the source and the destination and a unique number to identify the request. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors. To limit the communication overhead of route request packets, a node processes route request packets that both it has not seen before and its address is not presented in the route record field. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache.

After being created, either by the destination or an intermediate node, a route reply packet needs a route back to the source. There are three possibilities to get a backward route. The first one is that the node already has a route to the source. The second possibility is that the network has symmetric (bi-directional) links. The route reply packet is sent using the collected routing information in the route record field, but in a reverse order. In the last case, there exists asymmetric (unidirectional) links and a new route discovery procedure is initiated to the source. The discovered route is piggybacked in the route request packet [12].

In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source.

DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance. The network is assumed not be too big, for example, the diameter could be 5-10 nodes [13]. DSR is only applicable to a relatively small amount of nodes, less than 100. Otherwise, managing the source routes to every node may become problematic.

IV. ZONE ROUTING PROTOCOL

The Zone Routing Protocol (ZRP) is hybrid routing protocol for mobile ad- hoc networks. The hybrid protocols are proposed to reduce the control overhead of proactive routing approaches and decrease the latency caused by route search operations in reactive routing approaches[6].

In ZRP, the network is divided into routing zones according to distances between mobile nodes. Given a hop distance *d* and a node N, all nodes within hop distance at most *d* from N belong to the routing zone of N. Peripheral nodes of N are N's neighboring nodes in its routing zone which are exactly *d* hops away from N.

In ZRP, different routing approaches are exploited for inter-zone and intra-zone packets. The proactive routing approach, i.e., the Intra-zone Routing protocol (IARP), is used inside routing zones and the reactive Inter-zone Routing Protocol (IERP) is used between routing zones, respectively. The IARP maintains link state information for nodes within specified distance *d*. Therefore, if the source and destination nodes are in the same routing zone, a route can be available immediately. Most of the existing proactive routing schemes can be used as the IARP for ZRP. The IERP reactively initiates a route discovery when the source node and the destination are residing in different zones [8]. The route discovery in IERP is similar to DSR with the exception that route requests are propagated via peripheral nodes.

The main limitation of ZRP design assumes a uniform traffic distribution and then optimizes the overall overhead [15]. When the traffic is non-uniform, these protocols may not actually be efficient [9].

V. SECURED DYNAMIC SOURCE ROUTING PROTOCOL

Proposed secured dynamic source routing (SDSR) protocol solves the issue of secured transmission in DSR.

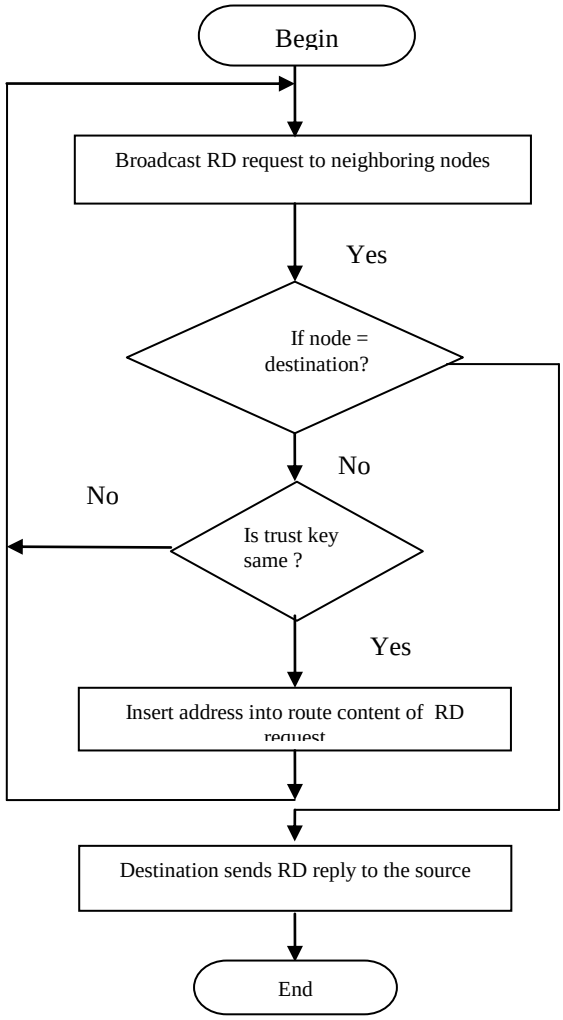

Fig.1 Route Request process

A common trust key is generated by all the group nodes. Any node that has the identical generated trust key can participate in routing. Therefore, the key is generated by each node by installing a common algorithm. Generated trust key is purely based on the synchronized system time in seconds. The trust key is added as an additional field in the route request packet for identifying the secured route. The route request packet size is increased in the proposed routing protocol. The trust key in all the nodes vary for every short time period 'Td' to ensure security, it should not be too small, so that the route request packet trust key should match with the intermediate node and destination node's trust key shown in the Fig.1. Td should not be too large, because the hackers might try to find the trust key to participate in routing. The trust key has to be moderate in order to provide secured routing process. This secured trust key is generated by all the nodes in the personal group. Hence, only group nodes participate in the routing process.

Secured DSR consists of two phases, secured route discovery and route maintenance. When source node S requires the route to destination D, S enters the secured route discovery phase and checks whether adequate fresh routes to D are already available in the Fresh_route cache. If some fresh routes to D in Fresh_route cache are found, S runs Route confirm process.

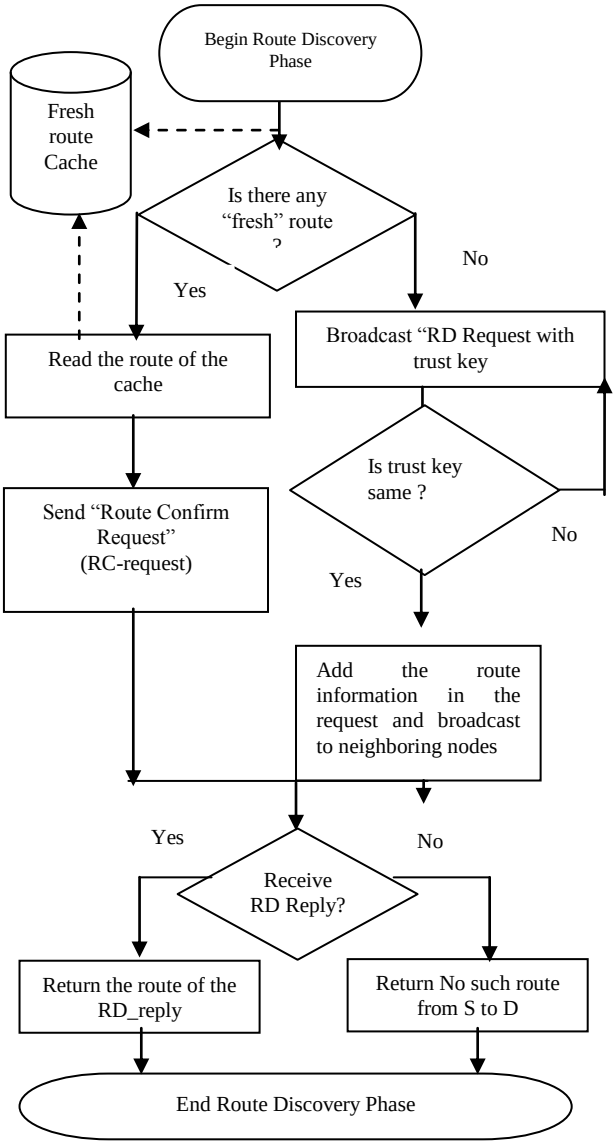

Fig. 2 Secured Route Discovery Phase

Otherwise, S runs new secured route discovery process to find a secured new route to the destination node as shown in Fig. 2.

A. New Secured Route discovery process

Source node S broadcasts Route Discovery (RD) request packet to nearby nodes; RD request includes a sequence number field to distinguish the route discovery process from others, the trust key of the source and the route content field for node address along the path from S to D. After the intermediate node receives RD request from an upstream node X, it inserts its address into the route content field of the RD request only if it is in the same trust key of the source and then sends this modified RD request to its neighboring nodes (excluding the upstream node X).

The RD request cache of the intermediate node also records the information, including the sequence number of the RD request and which neighboring nodes are sent only if the request is not duplicated. Otherwise, the duplicated request is discarded.

B. Route Maintenance phase

When a link failure occurs during the data transmission, route error message is forwarded to the source and source initiates new rout discovery process. This phase is as same as DSR explained in section III.

VI. SIMULATION RESULTS

This section describes briefly the results that are examined in simulating the routing protocols AODV, DSR, ZRP & SDSR. Simulation is carried out using Qualnet software. The routes identified by the new secured route discovery process is among the group nodes was ensured. The identified routes are found to be long, secured and lingered route. The following table below (Table. 1) shows the simulation parameters that are considered. Performance metrics such as average jitter, throughput and end to end delay [13] are analyzed by simulating for node variation between 10 and 50.

PARAMETERS	VALUE
Simulation Time	700s
Mobility	15m/s
Dimension	1500 x1500
Pause time	10s
No. of buffer size	64
Traffic Type	CBR
Packet Size	512 bytes
Zone radius	2
Time Delay 'Td'	5 s

Table 1. Simulation environment

A. Impact on Average Jitter

- AODV has higher jitter than the other routing protocols
- ZRP has an inconsistent jitter
- DSR and SDSR has the same level of jitter, which ensures that by adding trust key does not affects the variation in average jitter as shown in Fig.3.

B. Impact on Throughput

Fig.4 shows the throughput variation for different scale networks.

- AODV has high throughput for more nodes with less reliability.
- ZRP leads to more variation in throughput.
- SDSR provides slightly higher throughput than the DSR, hence including the security aspect in route discovery process does not affect the throughput.

C. Impact on end to end delay

Fig .5 shows the end to end delay variation for different scale networks.

- Delay is higher for less number of nodes in AODV protocol.
- DSR too has a tolerable delay for less number of nodes.
- ZRP protocol has tolerable delay for more number of nodes
- SDSR has consistently less delay irrespective of the number of nodes.

D. Impact on Route Request Packet Time

Deviation in time taken by the source initiated route request packet to reach the destination is shown in Fig.6

- SDSR shows the longer time to forward the route request packet than DSR.
- ZRP takes intolerable time to do the same .
- Though SDSR seizes a sufficient delay in discovering a route, offer a secured route.

Simulation results expose that the enhanced secured dynamic source routing provides security without comprimising the data communication performance. It delivers information as equivalent to the DSR performane.There is no key exchange mechanism employed in the protocol in order to resist the increase of routing overhead.

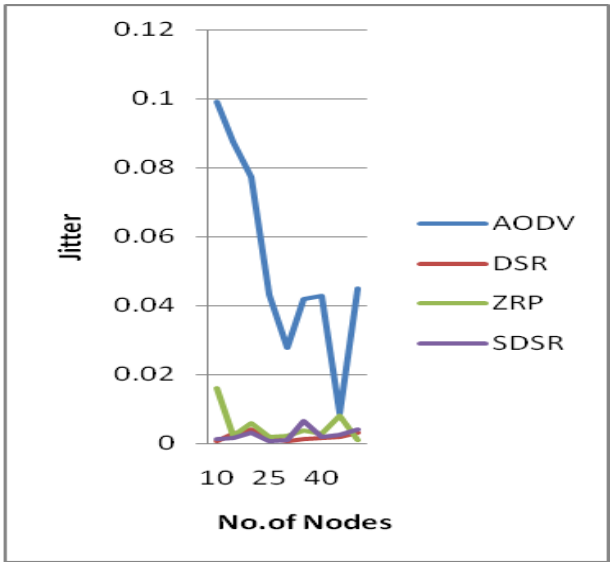

Fig.3 Average Jitter Vs Nodes

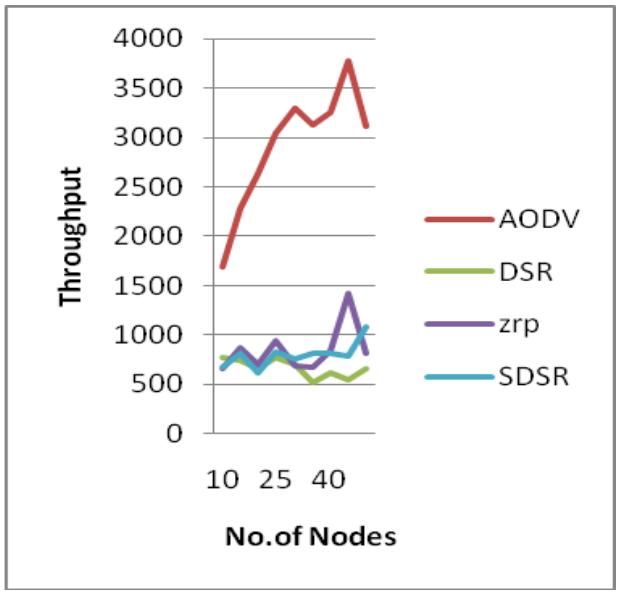

Fig. 4 Throughput Vs Nodes

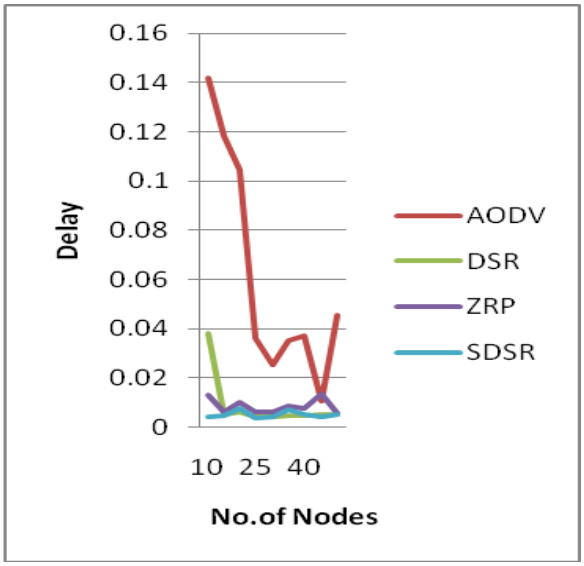

Fig. 5 Delay Vs Nodes

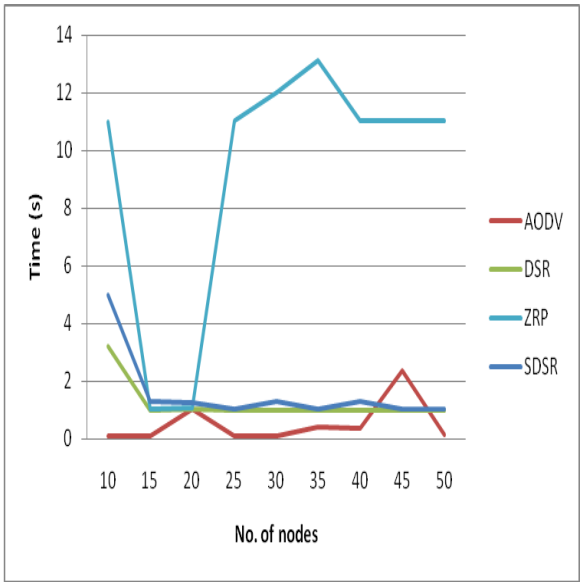

Fig. 6 Route Request time Vs Nodes

VII. CONCLUSION

In this paper, we have investigated SDSR protocol whose novelty is the trust key based on time as the additional security aspect of transferring data through trusted group nodes. Comparative analysis was done to evaluate the routing performance of new proposed routing protocol SDSR with existing routing protocols namely, AODV, DSR, ZRP based on CBR traffic in terms of measuring average jitter, throughput & delay by varying the density of the network, i.e the number of nodes. The results show that the proposed SDSR protocol affords almost equivalent performance as DSR with the secured way of transferring data through the trusted nodes. The overall performance of SDSR is better than all the other three on demand routing protocols. Future work is devised to study the performance based on TCP traffic and compare SDSR with the prevailing secured routing protocols.

REFERENCES

1. L. Abusalah, A. Khokhar, M. Guizani, "A survey of secure mobile Ad Hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78-93, 2008
2. G. Acs, L. Buttyan, I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.
3. Broch J., Maltz D. A., Johnson D. B., Hu Y. C., and Jetcheva J., "A performance comparison of multi-hop wireless ad hoc network routing protocols," *,ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'98)*, October 1998, pp. 85–97.
4. Chakrabarthi S., Mishra A., "QoS issues in ad hoc wireless networks", *communications magzine*, IEEE, volume 39, issue 2, Feb 2001, pp.142-148
5. Das S. R., Perkins C. E., Royer E. M. and Marina M. K., "Performance comparison of two on demand routing protocols for ad hoc networks," *IEEE Personal Communications Magazine, special issue on Mobile Ad Hoc Networks*, vol. 8, no. 1, pp. 16–29, February 2001.
6. S. R. Das, R. Castaneda, and J. Yan. "Simulation-based Performance Evaluation of Routing Protocols for Mobile Ad hoc Networks", *ACM/Baltzer Mobile Networks and Applications (MONET)*, 5(3): 179–189, 2000.
7. Elizabath.M.Royer and Chai-Keong Toh, "A review of current routing protocols for AdHoc mobile networks", *IEEE personal communications*, Volume 6, April 1999,pp-46 –55.
8. Z.J. Hass, R. Pearlman, "Zone routing protocol for ad-hoc networks", *Internet Draft, draft-ietf-manet-zrp-02.*ttxt, work in progress, 1999.
9. Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol", *IEEE/ACM Transactions on Networking*,9(4):427–38, 2001.
10. Huang R., Zhuang Y., Cao Q., "Simulation and Analysis of Protocols in Ad Hoc Network", 2009 *International Conference on Electronic Computer Technology © 2009 IEEE.*
11. D. Johnson, D. Maltz, J. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks", *InternetDraft, draft-ietf-manet-dsr-07.txt*, 2002.
12. D. B. Johnson, D. A. Maltz, Y. Hu, and J. G. Jetcheva." The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)". *http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt*, Feb 2002. IETF Internet Draft
13. G. Lin, G. Noubir, and R. Rajaraman, "Mobility models for *ad hoc* network simulation," *Proc. IEEE INFOCOM, 2004*, pp. 454–463.
14. D.A.Maltz, J.Broch, J.Jetcheva and D.B.Johnson, "The effects of on-demand behavior in routing protocols for multihop wireless AdHoc networks", *IEEE journal on Selected areas of communication*, Volume 17, 1999, pp-1439–1453.
15. Mehran Abolhasan , Tadeusz Wysocki, Eryk Dutkiewicz , "A review of routing protocols for mobile ad hoc networks", *2004 Elsevier, Adhoc networks*, pp. 1-22.
16. Perkins C. E. and Royer E. M., "Ad-Hoc On-Demand Distance Vector Routing, Mobile Computing Systems and Applications," *Proc. IEEE Workshop Mobile Computing Systems & Applications (WMCSA '99)*, pp. 90-100, 1999.
17. C. E. Perkins, E. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector Routing" http://www.ietf.org/rfc/rfc3561.txt,July 2003. RFC 3561.
18. M. Weeks and G. Altun, "Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks," *Journal of Network and Systems Management*, Vol.14, No. 4, pp. 559- 581, Dec. 2006.

AUTHORS PROFILE

G. Lavanya is working as an Assistant Professor in Department of Information Technology in KTVR Knowledge Park For Engineering and Technology, Coimbatore, India. She received her B.E Degree in Electrical and Electronics Engineering from Bharathiar University, Coimbatore, India in the year 1998 and M.Tech Degree in Information Technology from Anna University of Technology, Coimbatore, India in the year 2009.

She has 11 publications in the field of Adhoc Networks.

Dr. A.Ebenezer Jeyakumar is the Director (Academics) in SNR Sons Charitable Trust, Sri Ramakrishna Engineering College, Coimbatore, India. He received his B.E Degree in Electrical and Electronics Engineering from Annamalai University,Chidambaram, India in the year 1972 and M.E Degree in High Voltage Engineering from University of Madras,Chennai,India in the year 1974.He has completed his Ph.D in Anna University, Chennai, India in the year 1992. He is a member of IEEE, ISTE, and IE. Being an eminent Professor in Anna University, many scholars have registered their Ph.D and MS (by research) under him. His main research interest includes Network Security, Mobile Computing, High Voltage Engineering and other related areas. He has nearly 45 publications in National & International Journals.