Secured Distance Vector Routing (SDVR) Protocol for Mobile Ad-hoc Networks

Dr. S. Santhosh Baboo
Reader, PG & Research Dept. of Computer Applications,
D.G.Vaishnav College, Arumbakkam,
Chennai, India

S. Ramesh MCA. M.Phil.,
Research Scholar,
Dravidian University,
Kuppam, Andra Pradesh, India

ABSTRACT

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes dynamically shaping a provisional network devoid of the use of any existing network infrastructure or centralized management. In MANETs, security is the major challenge due to the dynamic topology which is because of the mobility of the nodes. In this paper, we propose to design and develop a secure methodology incorporated with the routing mechanism without having any compromise on the performance metrics viz., throughput, and packet delivery fraction. Not only just improving the throughput and packet delivery fraction it will also reduce the end-to-end delay and MAC overhead along with reduced packet loss. We name it as Secured Distance Vector Routing (SDVR) protocol. It adopts several features of the already existing protocol named Ad-hoc On-demand Distance Vector Routing (AODV). The simulation results prove that our proposed protocol SDVR outperforms AODV in all performance aspects..

1. INTRODUCTION

The alluring infrastructure-less phenomenon of mobile ad hoc networks (MANETs) has received more attention in the research society. With the success of solving the most fundamental but vital issues in all network layers, persons understand there is commercial value in MANETs. The most of the applications that draw attention for utilizing in current wired networks (e.g., video conferencing, on-line live movies, and instant messenger with camera enabled) would attract interest for MANETs. Though, MANETs present distinctive advanced challenges, including the design of protocols for mobility management, effective routing, data transportation, security, power managing, and quality-of-service (QoS). Once these issues are resolved, the use of MANETs will be attainable. Nowadays applications heavily demand the fulfilment of their Quality of Service (QoS) requirements, which in this distributed and particular environment can be difficult to solve. This scenario requires specific proposals adapted to the new problem statements [4, 7, 13]. Trying to solve all these problems and coming out with a single solution would be too complex. To offer bandwidth-guaranteed QoS, the available end-to-end bandwidth along a route from the source to the destination must be known. The end-to-end throughput is a concave parameter [16], which is determined by the bottleneck bandwidth of the intermediate hosts in the route. A survey of several routing protocols and their performance comparisons have been reported in [11]. Hence in this paper, we focus on providing security along with QoS in MANETs.

In order to design good protocols for MANETs, it is important to understand the fundamental properties of these networks.

Dynamicity: Every node in the mobile ad hoc network will change its position on its own. Hence prediction of the topology is difficult, and the network status is not clear and it is vague.

Noncentralization: There is no existence of centralized control in mobile ad hoc network and, hence assigning resources to MANET in advance is not possible.

Radio properties: The medium is wireless, hence results in fading, multipath effects, time variation, etc. With these complications, Hard QoS is not easy to achieve..

2. RELATED WORKS

In [15] Zhao et al have reviewed the existing approaches of available bandwidth estimation. They presented the efforts and challenges in estimation of bandwidth. Also, they proposed a model for finding available bandwidth with improved accuracy of sensing based bandwidth estimation as well as prediction of available bandwidth.

In [1] Gui et al have defined routing optimality with the usage of different metrics like path length, energy consumption and energy aware load balancing within the hosts. Along with they have proposed a methodology for self-healing and optimizing routing (SHORT) technique for MANET. SHORT increases performance with regard to bandwidth and latency. They classified SHORT into two categories such as Path-Aware SHORT and Energy-Aware SHORT.

The QAMNet [3] approach extends existing ODMRP routing by introducing traffic prioritization, distributed resource probing and admission control mechanisms to provide QoS multicasting. For available bandwidth estimation, it used the same method given in SWAN [9] where the threshold rate for real-time flows is computed and the available bandwidth estimated as the deference between the threshold rate of real-time traffic and the current rate of real-time traffic. It is very difficult to estimate the threshold rate accurately because the threshold rate may change dynamically depending on traffic pattern [9]. The value of threshold rate should be chosen in a sensible way: Choosing a value that is too high results in a poor performance of real-time flows, and choosing a value that is too low results in the denial of real-time flows for which the available resource would have sufficed.

The localization methods are also distinguished by their form of computation, “centralized” or “decentralized”. For example, MDS-

MAP [8] is a centralized localization that calculates the relative positions of all the nodes based on connectivity information by Multidimensional Scaling (MDS). Similarly, DWMDS (Dynamic Weighted MDS) [14] uses movement constraints in addition to the connectivity information, and estimates the trajectories of mobile nodes. TRACKIE [2] first estimates mobile nodes that were likely to move between landmarks straight. Based on their estimated trajectories, it estimates the trajectories of the other nodes. Since these centralized algorithms use all the information about connectivity between nodes and compute the trajectories off-line, the estimation accuracy is usually better than decentralized methods.

In decentralized methods, the position of each node is computed by the node itself or cooperation with the other nodes. For example, APIT [17] assumes a set of triangles formed by landmarks, checks whether a node is located inside or outside of each triangle, and estimates its location. Amorphous [6] and REP [5] assume that location information is sent through multi-hop relay from landmarks, and each node estimates its positions based on hop counts from landmarks. In particular, REP first detects holes in an isotropic sensor network, and then estimates the distance between nodes accurately considering the holes. In MCL [16], each mobile node manages its Area of Presence (AoP) and refines its AoP whenever it encounters a landmark. In UPL [10], each mobile node estimates its AoP accurately based on AoP received from its neighboring nodes and obstacle information..

3. PROPOSED WORK

In order to implement QoS, we propose to develop a protocol which guarantees QoS along with secured distance vector routing. In all the available existing protocols with regard to security, QoS requirements were compromised. We aim to develop a security enriched protocol which does not compromise with QoS requirements. For achieving the above goal we design a framework which uses estimation of ‘bandwidth’, estimation of ‘residual energy’, ‘threshold value’.

3.1 Bandwidth Estimation

Please use a 9-point Times Roman font, or other Roman font

The bandwidth can be estimated as follows

Packet Delivery Time $\mathbf{(Ø_d) = Ø_r - Ø_s}$

Where $Ø_r$ is Packet Received Time,

$Ø_s$ is Packet Sent Time

Bandwidth= $D_S / Ø_d$ → (1)

Where D_S is Data Size.

Bandwidth is the ratio between Size of the Data and Actual time taken to deliver the packet.

In following two cases Bandwidth gets reduced.

- When there is more channel contention i.e., Channel sensing busy due to more Request To Send (RTS) / Clear To Send (CTS) , collisions and higher backoffs.
- When there are more channel errors i.e., error bits in RTS/DATA which causes RTS/DATA retransmission.

3.2 Residual Energy

The Residual Energy [10] is calculated as follows:

$RE_{node} = IE_{node} – CE_{node}$ → 2

Where IEnode is the Initial Energy of the node and CEnode is the Consumed Energy of the node. The residual energy of a node is the difference between initial energy and consumed energy.

3.3 SDVR Routing

'Secured Distance Vector Routing' (SDVR) is a routing protocol for MANETs. Our protocol SDVR, uses distinct routing methodology where all the routing information is retained (updated again and again) at nodes. SDVR has two phases. They are Route Discovery and Route Maintenance. To identify source routes need collecting the address of each node from the source node to destination node in the course of route discovery. When the route discovery process is initiated, the two state-of-the art estimations such as bandwidth and residual energy will be calculated using (1) and (2). For making the reliable path, we have fixed the optimum bandwidth value to be 0.5 mbps and the residual energy to be 90J. This optimum value will be suitable for the higher end applications like video-conferencing. The collected path information is cached by nodes which processes the route discovery packets. The path will be identified if the bandwidth is greater than or equal to 0.5 mbps and residual energy greater or equal to 90J so as to have more reliable path which assures QoS. The identified paths are used to route the packets. To achieve secured source routing, the routed packets will have the address of each node the packet will pass through. This may cause high overhead for longer paths in large scale mobile ad hoc network. To eliminate source routing, our SDVR protocol creates a stream id option which allows packets to be delivered based on a hop-by-hop basis.

Route Reply would only be produced when the message has reached the projected destination node. To send back the Route Reply, the destination node should have a route to the source node. The route would be used when the route is in the Destination Node's route cache. Or else, the node will turn round the route based on the route record in the Route Reply message header.

The Route Maintenance Phase will be started when there is an occurrence of incurable communication or when an Intruder node was identified using IDM. During above situation the Route Error packets are started at a node. The mistaken hop will be deleted from the node's route cache; all routes having the hop are terminated at that point. Once more, the Route Discovery Phase is started to find the most viable route.

3.4 Intruder Detection Methodology (IDM)

After calculating the path in which packets are to be routed, the source node will forward certain number packets to the next hop (node). The number of packets thus sent to the first hop will be set as threshold value. Thus obtained threshold value will be verified at every node in the path before despatching the packets. And if any of the node in the path has got different value other than that of threshold value then they are treated as Intruder and the path is rediscovered with the new threshold value and discarding the intruder node. Once again the above process is repeated till such time it reaches the destination node.

When the non-availability of a route to the next node, the node instantly updates the succession count and broadcasts the knowledge to its neighbors. When a node gets routing knowledge then it verifies in its routing table. If it does not have such entry into the routing table then updates the routing table with routing information it has obtained. If the node finds that it has already had an entry into its routing table then it compares the succession count of the received information with the routing table entry and updates the information. If it has succession count that is less than that of the received one then it rejects the information with the least succession count. Suppose both the succession counts are one and the same then the node keeps the information that has the shortest route or the least number of hops to that destination.

4. PERFORMANCE METRICS

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets sent.
Throughput: It is the number of packets received successfully.

Drop: It is the number of packets dropped.

5. RESULTS AND DISCUSSIONS

Figure 1 gives the throughput of both the protocols when the pause time is increased. As we can see from the figure, the throughput is more in the case of SDVR than AODV.

Figure 2 presents the packet delivery ratio of both the protocols. Since the packet drop is less and the throughput is more, SDVR achieves good delivery ratio, compared to AODV.

From Figure 3, we can ensure that the packets dropped are less for SDVR when compared to AODV.

From Figure 4, we can see that the average end-to-end delay of the proposed SDSR protocol is less when compared to the Ad-hoc On-demand Distance Vector (AODV) routing protocol.

From Figure 5, we can conclude that the MAC overhead get reduced well for SDVR than that of AODV.

We have compared the protocol proposed in this paper, SDVR with our previously developed protocols Secured-destination Sequenced Distance Vector (SSDV) routing protocol and Secured Dynamic Source Routing (SDSR) protocols[18]

From Figure 6, we can see that SDVR protocol has gained higher throughput than that of SSDV and SDSR.

Figure 7, we can see that SDVR protocol has gained higher packet delivery ratio than that of SSDV and SDSR.

Figure 8, we can see that SDVR protocol had very less number of packet drops than that of SSDV and SDSR. Similarly it is found in

Figure 9, our SDVR protocol had very little MAC overhead packets than that of SSDV and SDSR.

Figure 10, we can see that our SDVR protocol had very less end-to-end delay than that of SSDV and SDSR.

Figure 11 shows three scenarios of routing packets through the paths. In that the first one was before attack, in which packets received along the path was 465(threshold value) throughout the destination node. In the second scenario, it can be noticed that from one of the intermediate node 590 packets were sent which is different from the earlier threshold value sent. In this situation using IDM method our SDVR will detect the intruder and re-establish the route and start sending the packets which being depicted in Figure 11 as the third scenario where packets are sent to destination with new threshold value of 269 throughout the path.

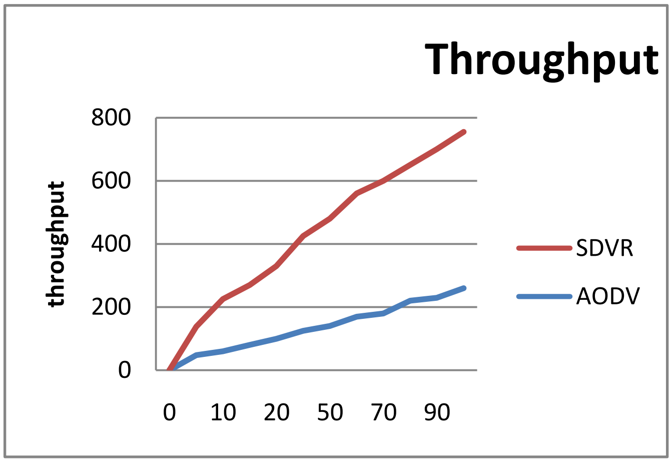

Fig.1. Pausetime Vs Throughput (SDVR Vs AODV)

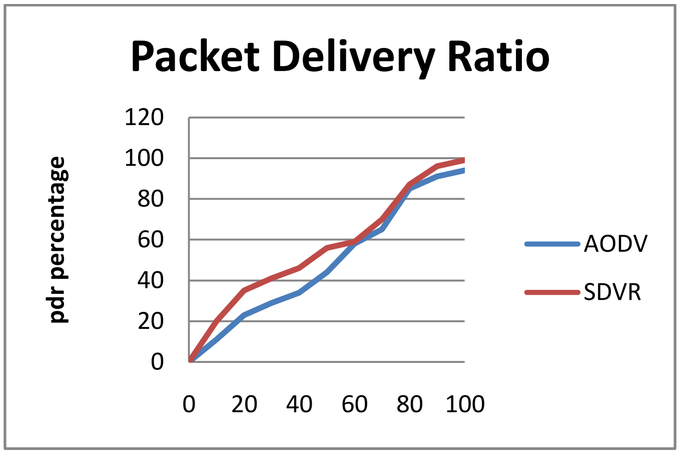

Fig.2. Pausetime Vs Packet Delivery Ratio (SDVR Vs AODV)

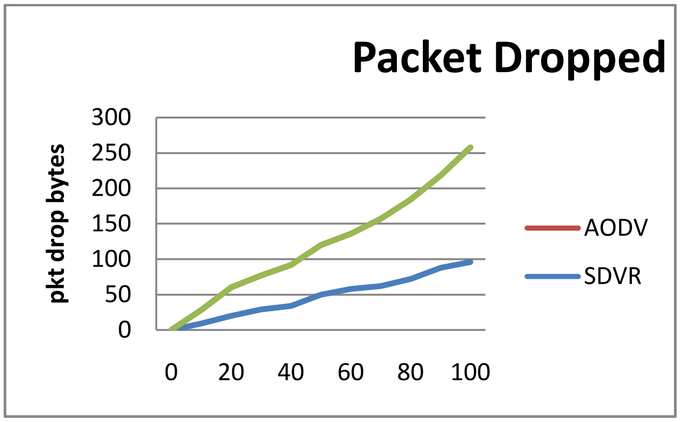

Fig.3. Pausetime Vs Packets Dropped (SDVR Vs AODV)

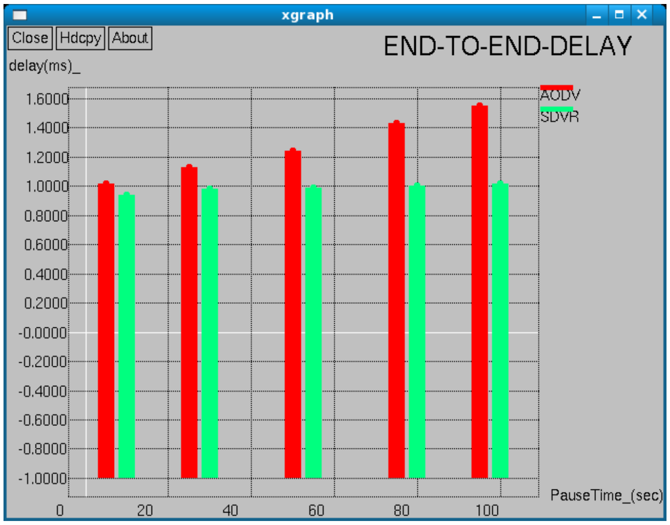

Fig.4. Pausetime Vs End-to-End Delay (SDVR Vs AODV)

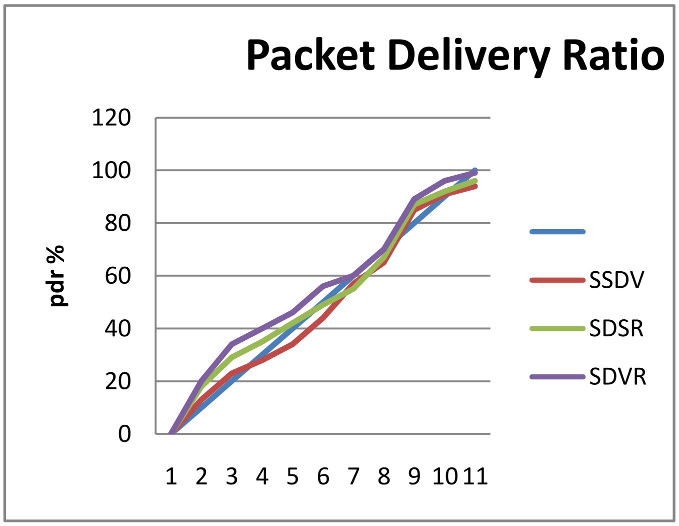

Fig.7. Pausetime Vs Packet Delivery Ratio (SSDV, SDSR, SDVR)

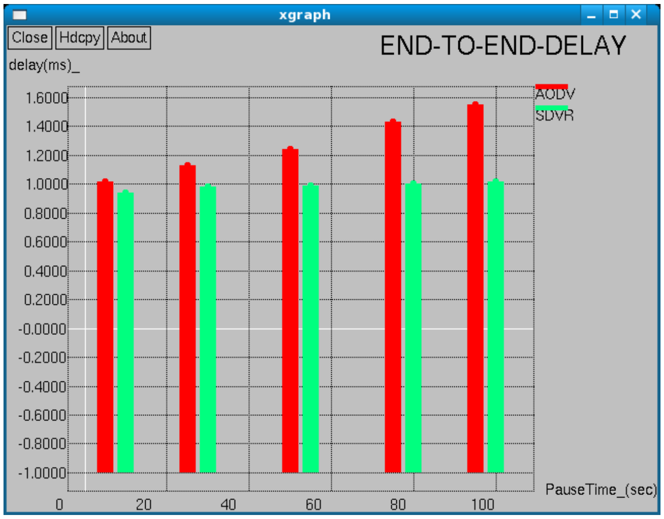

Fig.5. Pausetime Vs MAC Overhead (SDVR Vs AODV)

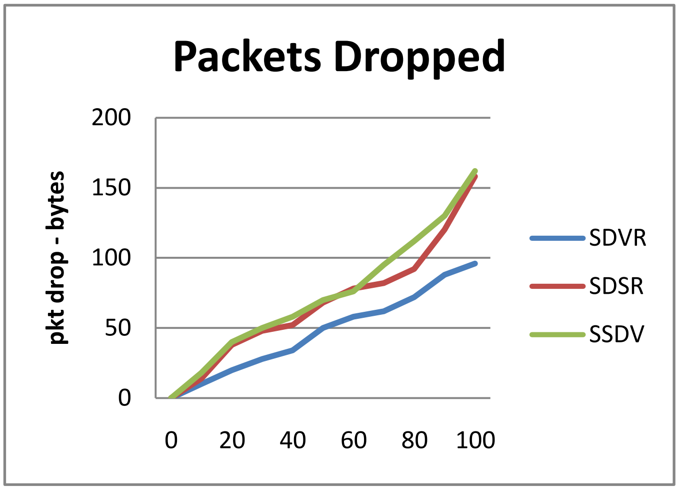

Fig.8. Pausetime Vs No. of Packets Dropped (SSDV, SDSR, SDVR)

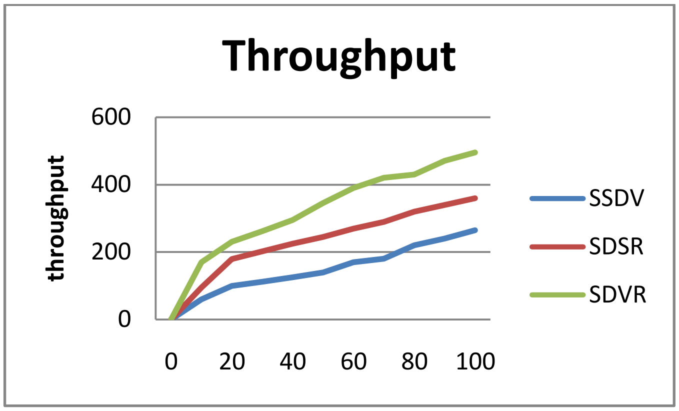

Fig.6. Pausetime Vs Throughput (SSDV, SDSR, SDVR)

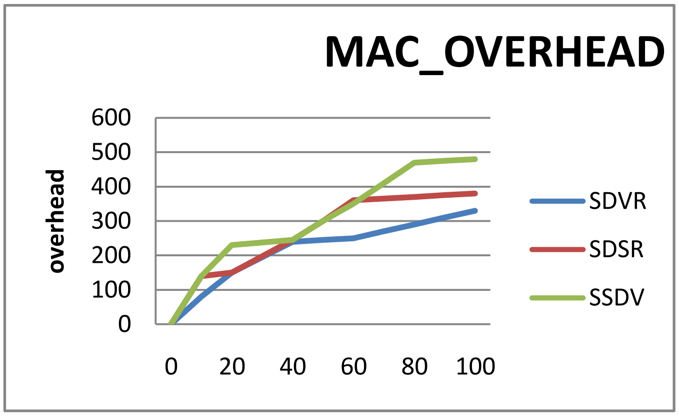

Fig.9. Pausetime Vs MAC Overhead (SSDV, SDSR, SDVR)

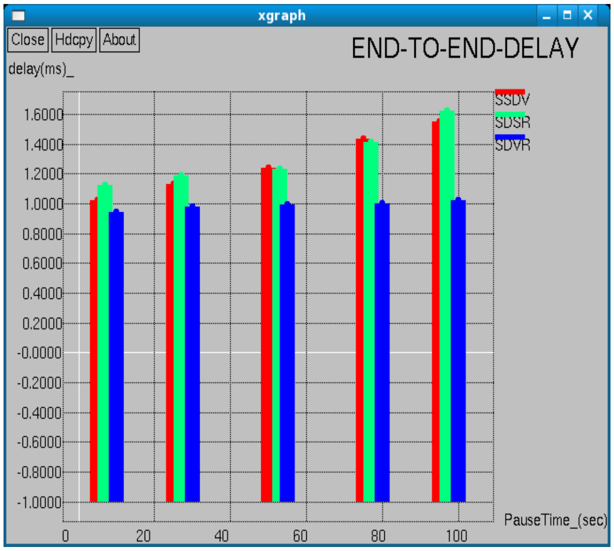

Fig.10. Pausetime Vs End – to – End Delay (SSDV, SDSR, SDVR)

No. Of Packets Received before Attack		
No. Of Packets Received at	20th Node	0
No. Of Packets Received at	22nd Node	465
No. Of Packets Received at	1st Node	465
No. Of Packets Received at	11th Node	465
No. Of Packets Received at	5th Node	465
No. Of Packets Received at	8th Node	465
No. Of Packets Received during Attack		
No. Of Packets Received at	20th Node	0
No. Of Packets Received at	22nd Node	465
No. Of Packets Received at	1st Node	465
No. Of Packets Received at	11th Node	590
No. Of Packets Received at	5th Node	590
No. Of Packets Received at	8th Node	590
No. Of Packets Received after Attack		
No. Of Packets Received at	20th Node	0
No. Of Packets Received at	22nd Node	269
No. Of Packets Received at	1st Node	269
No. Of Packets Received at	11th Node	269
No. Of Packets Received at	5th Node	269
No. Of Packets Received at	8th Node	269

Fig.11. Trace File illustrating route before, during and after attack

6. CONCLUSION AND FUTURE WORKS

In this paper we designed and developed a dynamic source routing named Secured Distance Vector Routing (SDVR) protocol which meets the requirements of QoS such as improved throughput with better packet delivery ratio and reduced end-to-end delay and reduced no of drop in packets. Additionally, we provide a secure route maintenance mechanism by involving threshold in terms of packets. Further we provided security in terms of Advanced Encryption Standard (AES) algorithm using add-round key for data security while transmission of data. The results graph using the performance metrics outperformed when compared with Ad-hoc On-demand Distance Vector (AODV) routing protocol. The framework used in this research would be further incorporated with other distance vector protocols.

7. ACKNOWLEDGMENTS

The first author thanks Dravidian University for having consented to guide PhD. The second author thanks the first author for providing a chance to do PhD under his guidance. The second author also thanks Dravidian University for providing the opportunity to pursue PhD .

8. REFERENCES

[1] Chao Gui & Mohapatra, “A Framework for Self-healing and Optimizing Routing Techniques for Mobile Ad hoc Networks”, Wireless Networks, Vol.14 No.1, pp.29-46, 2008.

[2] S. Fujii, A. Uchiyama, T. Umedu, H. Yamaguchi, and T. Higashino. An off-line algorithm to estimate trajectories of mobile nodes using ad-hoc communication. In Proc. of PerCom 2008, pages 117–124, 2008.

[3] H. Tebbe, and A. Kassler, “QAMNet: Providing Quality of Service to Ad-hoc Multicast Enabled Networks”, 1st International Symposium on Wireless Pervasive Computing (ISWPC), Thailand, 2006.

[4] Reddy T.B, Karthigeyan I, Manoj B. S, & Siva Ram Murthy C, “Quality of service provisioning in ad hoc wireless networks: A survey of issues and solutions”, Ad hoc Networks, Vol. 4 No. 1, pp. 83–124, 2006.

[5] M. Li and Y. Liu. Rendered path: range-free localization in anisotropic sensor networks with holes. In Proc. of MobiCom 2007, pages 51–62, 2007.

[6] R. Nagpal, H. Shrobe, and J. Bachrach. Organizing a global coordinate system from local information on an ad hoc sensor network. In Proc. of IPSN 2003, pages 333–348, 2003.

[7] G. S. Ahn, A. T. Campbell, A. Veres and L.H. Sun, "SWAN: Service Differentiation in Stateless Wireless Ad hoc Networks", In Proc. IEEE INFOCOM, 2002.

[8] Y. Shang, W. Rml, Y. Zhang, and M. Fromherz. Localization from connectivity in sensor networks. IEEE Transaction on Parallel and Distributed Systems, 15(11):961–974, 2004.

[9] Chakrabarti S & Mishr A, “QoS issues in ad hoc wireless networks”, IEEE Communications Magazine, Vol.39 No.2, pp.142–148, 2001.

[10] A. Uchiyama, S. Fujii, K. Maeda, T. Umedu, H. Yamaguchi, and T. Higashino. Ad-hoc localization in urban district. In Proc. of INFOCOM 2007 Mini-Symposium, pages 2306–2310, 2007.

[11] E.M. Royer and C.-K. Toh, "'A review of current routing protocols for ad hoc mobile wireless networks," in: IEEE Personal Communications, (April 1999).

[12] S. Santhosh Baboo, B. Narasimhan, "An Energy-Efficient Congestion-Aware Routing Protocol for Heterogeneous Mobile Ad Hoc Networks," act, pp.344-350, 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009.

[13] Mohapatra & Gui C, "QoS in mobile ad hoc networks", IEEE Wireless Communications, Vol.10 No.3, pp. 44–52, 2003.

[14] J. M. Cabero, F. D. la Torre, A. Sanchez, and I. Arizaga. Indoor people tracking based on dynamic weighted multidimensional scaling. In Proc. of MSWiM 2007, pages 328–335, 2007.

[15] Haitao Zhao, Jibo Wei, Shan Wang and Yong Xi, "Available Bandwidth Estimation and Prediction in Ad hoc Networks", Wireless Networks, Vol.14, pp. 29–46, 2008.

[16] P. Mohapatra, J. Li, and C. Gui, "QoS in mobile ad hoc networks," IEEE Wireless Commun. Mag. (Special Issue on QoS in Next-Generation Wireless Multimedia Communications Systems), pp. 44–52, 2003.

[17] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Range-free localization schemes for large scale sensor networks. In Proc. of MobiCom 2003, pages 81–95, 2003.

[18] Dr.S.Santhosh Baboo & S.Ramesh, "Secured Dynamic Source Routing (SDSR) protocol for Mobile Ad-hoc Networks", International Journal of Computer Science and Information Security, Vol.9 .No.9, Sep 2011.

9. AUTHOR'S PROFILE

Lt. Dr.S.Santhosh Baboo, aged forty, has around Seventeen years of postgraduate teaching experience in Computer Science, which includes Six years of administrative experience. He is a member, board of studies, in several autonomous colleges, and designs the curriculum of undergraduate and postgraduate programmes. He is a consultant for starting new courses, setting up computer labs, and recruiting lecturers for many colleges. Equipped with a Masters degree in Computer Science and a Doctorate in Computer Science, he is a visiting faculty to IT companies. He has been keenly involved in organizing training programmes for students and faculty members.

His good rapport with the IT companies has been instrumental in on/off campus interviews, and has helped the post graduate students to get real time projects. He has also guided many such live projects. Lt.Dr. Santhosh Baboo has authored a commendable number of research papers in international/ national Conference/ journals and also guides research scholars in Computer Science. Currently he is Reader in the Postgraduate and Research department of Computer Applications at Dwaraka Doss Goverdhan Doss Vaishnav College (accredited at 'A' grade by NAAC), one of the premier institutions in Chennai.

Ramesh Sadagoppan conceived his B.Sc.Chemistry and MCA degrees from University of Madras. He got his M.Phil Degree in Computer Science from Annamalai University. He is currently working as a Programmer in Centre for Railway Information Systems under Ministry of Railways in Chennai. He is currently pursuing his PhD Computer Science in Dravidian University under the research supervision of an eminent professor Lt.Dr.S.Santhosh Baboo.