International Journal of Engineering and Technology Vol. 1, No. 2, June, 2009
1793-8236

A Study on Salvaging Route Reply for AODV Protocol in the Presence of Malicious Nodes

Ayyaswamy Kathirvel, Member, ISTE Rengaramanujam Srinivasan, Member, ISTE, FIE

***Abstract*—Mobile ad hoc networks are self-creating, self-administering and self-organizing. A self-motivated set of mobile wireless users dynamically exchange data among themselves in the absence of a predetermined infrastructure and controller. Malicious nodes adversely affect the performance of the network. In this paper, we investigate the effect of salvaging routing reply (SRR) for AODV protocol in presence of malicious nodes. We have conducted extensive simulations using QualNet 4.5 network simulator to evaluate the performance of AODV-SRR. The studies show a significant improvement in performance as compared with that of conventional AODV protocol, with only nominal overheads.**

***Index Terms*— MANET, AODV, AODV-SRR, and malicious nodes**

I. INTRODUCTION

Mobile ad hoc networks (MANET) are self-creating, self-administering and self-organizing. Thus a set of self-motivated mobile wireless users is able to dynamically exchange data among themselves even in the absence of a predetermined infrastructure and controller. Each user of mobile ad hoc network also acts as a router allowing other users to communicate through their mobile communication device. The communication range of each device is limited; therefore, at any given time a user can exchange packets only with any of the other devices in its transmitting or receiving range.

Unlike the conventional cellular networks that rely on extensive infrastructure to support mobility, a MANET does not need expensive base stations and wired infrastructure. These features are important for potential use in a wide variety of disparate situations. Such situations include battlefield communications and disposable sensors, which are dropped from high altitudes and dispersed on the ground for hazardous materials detection. Civilian applications include emergency situations such as responses to hurricane, tsunami, earthquake, and terrorism. Another interesting example is the case, where a set of mobile vehicles on the highway form an ad hoc network of their own in order to provide vehicular traffic management. Security provisioning in wireless ad hoc networks plays an integral part in determining the success of network centric warfare as envisioned for future military operations. Thus, Security is an important issue for these mission-critical applications.

In MANET, a number of prominent routing protocols have been proposed in the literature, to name a few, AODV [3] (Ad hoc On-demand Distance Vector), DSR [6] (Dynamic Source Routing), TORA (Temporarily Ordered Routing Algorithm), WRP (Wireless Routing Protocol) and ZRP (Zone Routing Protocol) [9] [10]. While DSR and AODV share the on-demand behavior in that they initiate routing activities only in the presence of data packets in need of a route, several of their routing mechanics are very different. In particular, DSR uses source routing, whereas AODV uses a table-driven routing framework and destination sequence numbers. DSR does not have any timer-based activities, while AODV has the same to a certain extent. In DSR, several additional optimizations, such as Salvaging, Gratuitous route repair and Promiscuous listening have been proposed and have been found to be very effective.

Our work rests on the fundamentals of an existing system - the SRR (salvaging routing reply) [1], proposed by Mekesh Singhal et al. as an extension to the Ad Hoc On-Demand Distance Vector AODV Protocol. We briefly outline the philosophy of SRR.

The loss of route reply packets causes serious impairment of performance of AODV protocol. This is because route reply packets are obtained after flooding the entire network with RREQs. Mekesh Singhal et al have proposed and implemented the idea of salvaging route reply (SRR) for on demand routing protocols. The basic idea is illustrate in Fig.1. Assume that, initially there exists no active path from source node S to destination node D. Node S is discovering a route to node D. Node D sends a RREP to node S, through intermediate nodes A, B, C and X. Node C cannot send the RREP to node B because B has moved away. Node C becomes the salvor, it saves the RREP message, and then it broadcasts a $RREQ_{SRR}$. Node V receives the $RREQ_{SRR}$ and finds a route to the source node S in its routing table, so V sends a $RREP_{SRR}$ to C. C receives the $RREP_{SRR}$ and successfully salvages the original RREP by sending it along the path discovered by SRR. It can use the new alternative route to send RREP packets to node S, through intermediate nodes A, U, V and C. Then the return path after SRR is D-X-C-V-U-A-S. Route maintenance deals with routing information at nodes, typically involving three possible operations: handling route errors, deleting stale route entries, and learning new routes from the traffic.

With ubiquitous presence of malicious nodes, it is of interest to know how SRR behaves in the presence of malicious nodes. In this paper, we have investigated the effect of salvaging routing reply (SRR) in the presence of malicious nodes. We have conducted extensive simulations to evaluate the performance of SRR. The results show that SRR improves the performance of AODV protocol

Manuscript received March 7, 2009. Manuscript Revised on June 2, 2009. Manuscript accepted June 22, 2009.

Ayyaswamy Kathirvel, Assistant Professor. He is now with the Department of Computer Science and Engineering, B S Abdur Rahman University, Chennai, 600 048, Tamilnadu, India.

Rengaramanujam Srinivasan, Professor. He is now with the Department of Computer Science and Engineering, B S Abdur Rahman University, Chennai, 600 048, Tamilnadu, India.

significantly as compared with that of conventional AODV protocol, with only nominal overheads.

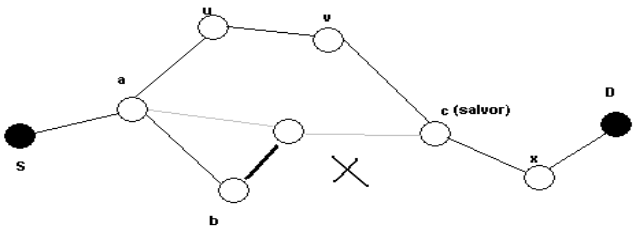

Fig.1. AODV-SRR mechanism: Link broken between B and C. Salvor node is C; intended RREP return path is D-X-C-B-A-S. Actual return path after SRR is D-X-C-V-U-A-S.

The rest of the paper is organized as follows: Section 2 describes the simulation model using QualNet 4.5; Section 3 gives an analysis of results; related work is reviewed in the section 4, while Section 5 draws up conclusions.

II. Simulation Model

We use a simulation model based on QualNet 4.5 in our evaluation [11]. Our performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1500 X 600 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11. The parameter settings are given in Table I.

Before the simulation we randomly selected a certain fraction, ranging from 0 % to 40 % of the network population as malicious nodes. We considered only two types of attacks – modifying the hop count and dropping packets. Each flow did not change its source and destination for the lifetime of a simulation run. For all our studies we had kept the simulation time as 900 s.

We have done three sets of studies using AODV protocol and modified AODV protocol called as AODV-SRR. Set 1 corresponds to routing misbehavior of malicious nodes. In Set 1 malicious nodes give false hop counts. Set 2 corresponds to packet forwarding misbehavior, where malicious nodes deliberately drop data packets and Set 3 simulates a combination of both routing and packet forwarding misbehaviors.

The three performance metrics used by us are as follows:

Packet delivery ratio is the ratio of the data packets successfully, delivered to the destinations to those generated by the CBR sources.

Average end-to-end delay, It is the average time taken for a packet to be transmitted across a network from source to destination. It includes transmission delay, propagation delay and processing delay.

Communication overhead is the total number of control packets sent by routing protocols in order to achieve its goal.

Table I Parameter Settings

Simulation Time	900 seconds
Propagation model	Two-ray Ground Reflection
Transmission range	250 m
Bandwidth	2 Mbps
Movement model	Random way point
Maximum speed	0 – 20 m/s
Pause time	0 seconds
Traffic type	CBR (UDP)
Payload size	512 bytes
Number of flows	10 / 20

III. Analysis of Results

A. Packet Delivery Ratio

In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. We present the packet delivery ratios of plain AODV and AODV-SRR, for malicious node percentages of 0, 10, 20, 30 and 40, with node mobility varying between 0 to 20 m/s. In general, in the absence of malicious nodes both routing protocols (plain AODV and AODV-SRR) have got good packet delivery ratio. In the absence of malicious nodes Set 1, Set 2 and Set 3 have identical results and are presented in Fig. 2.

In the case of plain AODV, with 0% malicious nodes, packet delivery ratio decreases from 98.28 %, when the nodes are stationary to 93.73 %, when the nodes are moving at 20 m/s. corresponding figures AODV-SRR are 99.18 % and 94.98.

From the results of the Set 1 (Fig. 3) the following conclusions can be drawn:

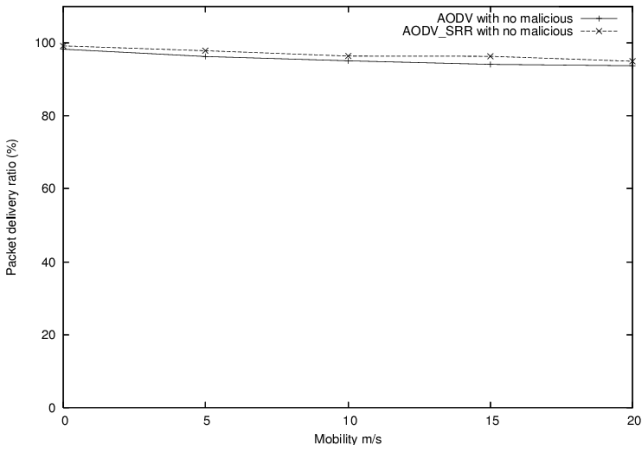

Fig. 2 Packet delivery ratio verses mobility for Set 1, Set 2 and Set 3 of plain AODV and AODV-SRR with 0% malicious node.

1) In general packet delivery ratio decreases as mobility and percentage of malicious nodes increase.
2) In the case of AODV, with 10% malicious nodes, packet delivery ratio decreases from 84.91%, when the nodes are stationary to 64.18%, when the nodes are moving at 20 m/s. Corresponding figures for AODV-SRR are 89.16 % and 68.96 %.
3) With plain AODV, packet delivery ratio has a steep fall from 98.28 (0% malicious nodes, mobility = 0 m/s) to 28.09 (40% malicious nodes, mobility = 20 m/s). Corresponding figures for AODV-SRR are 99.18 % and 30.49 %. Thus throughput is increased nearly by 8.5 %.

From results of Set 2 (see Table II) the following conclusions can be drawn:

We observe that the identical results for both plain AODV

and AODV-SRR this is because the following reason. AODV-SRR takes care of the failure of RREP packets only. Thus SRR mechanism is not be helpful if the data packets are intentionally dropped.

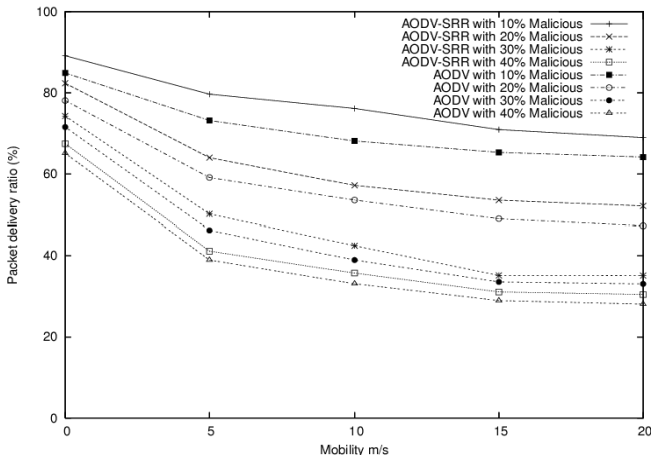

Fig.3 Packet delivery ratio verses mobility for Set 1 of plain AODV and AODV-SRR with 10 % - 40 % malicious nodes

From results of Set 3 (Fig.4) the following conclusions can be drawn:

1) In set 3 simulates misbehavior of malicious nodes in both data forwarding and route reply. Accordingly the performance improvement is lower than that of set 1. The actual performance improvement depends upon ratio of two the types of malicious nodes.

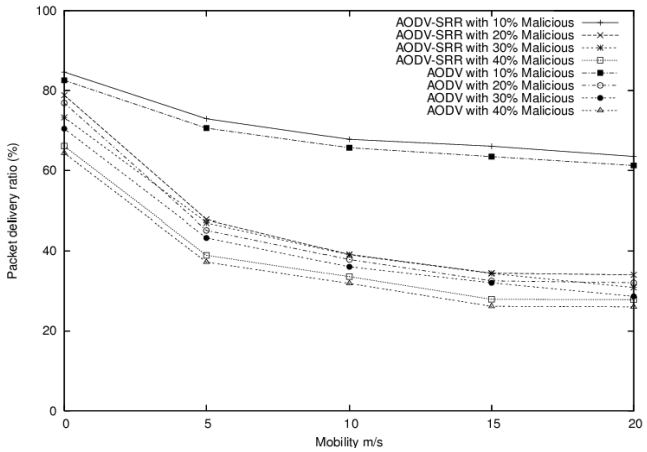

Fig. 4 Packet delivery ratio verses mobility for Set 3 of plain AODV and AODV-SRR with 10 % - 40 % malicious nodes

B. Communication overhead

Communication overhead can be evaluated based on the number of transmissions of control messages like RREQ, RREP, RERR in the case of plain AODV and in addition $RREQ_{SRR}$, $RREP_{SRR}$ in the AODV-SRR. RREQ are to be decimated to the entire network, where as RREP messages are unicasts. We have taken appropriate weights for each message. For example the count of RREP message from destination to source will be k where k is the hop count. We present the communication overhead details for 0% malicious nodes in Fig. 5 of plain AODV and AODV-SRR. Again in the absence of malicious nodes Set 1, Set 2 and Set 3 have got identical communication overhead.

From results of Set 1 (Fig. 6), Set 2 (Table 2) and Set 3 (Fig. 7.) following inferences can be drawn:

1) The communication overhead increases with increasing percentage of malicious nodes.
2) In the case of AODV (Set 1), with 10% malicious nodes, communication overhead increases from 1.11, when the nodes are stationary to 1.32, when the nodes are moving at 20 m/s as shown in the Fig. 6. Whereas AODV-SRR with same percentage malicious nodes, communication overhead has reduced values of 1.02 (0 m/s) and 1.21 (20 m/s).
3) We observe that the identical communication overhead for set 2 of both plain AODV and AODV-SRR as given in the Table 2. The communication overhead has a steep rise from 9046 (0 % malicious nodes, mobility = 0 m/s) to 20732 (40 % malicious nodes, mobility = 20 m/s).
4) For Set 3 of plain AODV, the increases from 1.22 (10% malicious nodes; mobility = 0) to 1.91 (40% malicious nodes and mobility = 20 m/s) as shown in the Fig. 7. The corresponding values for AODV-SRR are 1.08 and 1.69.

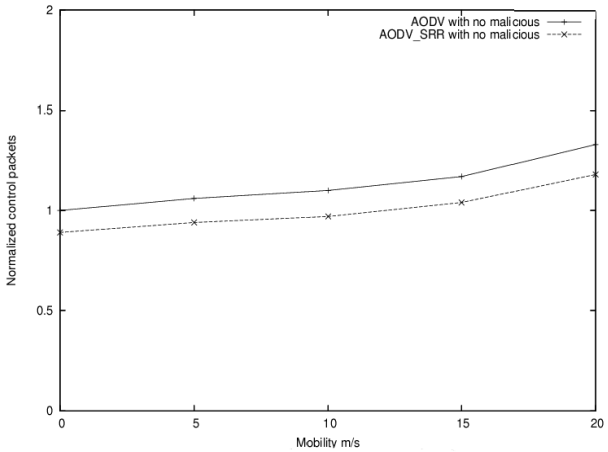

Fig. 5 Communication overhead verses mobility for Set 1, Set 2 and Set 3 of AODV and AODV-SRR with 0% malicious nodes

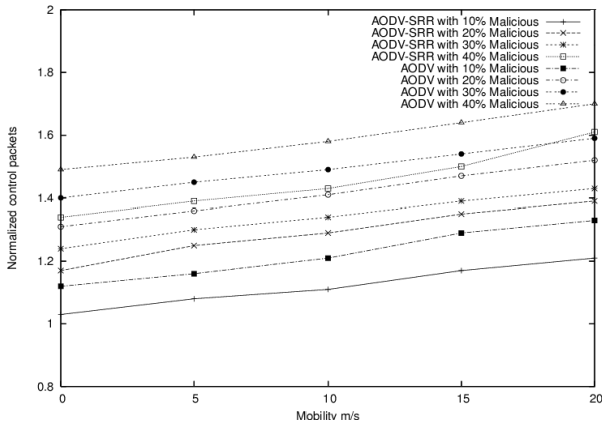

Fig. 6 Communication overhead verses mobility for Set 1 of AODV and AODV-SRR with 10% - 40 % malicious nodes

5) In Set 3 of AODV-SRR with 40% malicious nodes, we find that the decrease in communication overhead is 11 % as compared with plain AODV.
6) Fig. 6, Fig. 7 and Table 2 provides a comparison of increase in communication overheads for plain AODV and AODV-SRR corresponding from 10% to 40% malicious nodes of Set 1, Set 2 and Set 3. We find that there is a reduction in communication overhead with

plain AODV.

7) The communication overhead has a steep rise from 12371 (10 % malicious nodes, mobility = 0 m/s) to 20732 (40 % malicious nodes, mobility = 20 m/s).

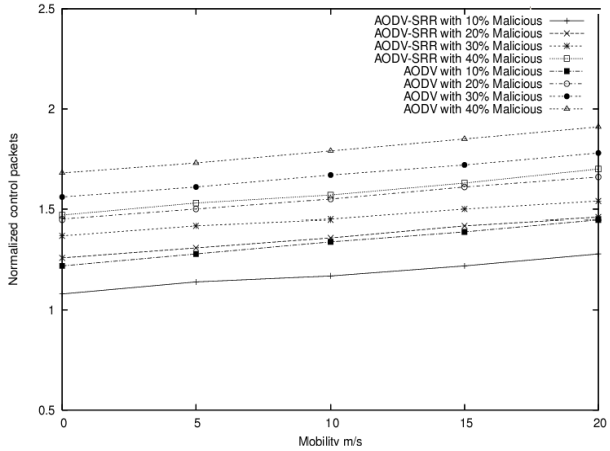

Fig. 7 Communication overhead verses mobility for Set 3 of AODV and AODV-SRR with 10% - 40 % malicious nodes

C. 3.3 End-to-end delay

In absence of malicious nodes with varying speed, both AODV and AODV-SRR protocols in the case of Set 1, Set 2 and Set 3 have got identical end to end delay as shown in the Fig. 8.

1) In the case of plain AODV (Set 1), with 10% malicious nodes, end to end delay increases from 2.64, when the nodes are stationary to 6.93, when the nodes are moving at 20 m/s. Corresponding figures for AODV-SRR are 1.72 and 5.90.
2) We observe that the identical end-to-end delay for set 2 of both plain AODV and AODV-SRR as given in the Table II.

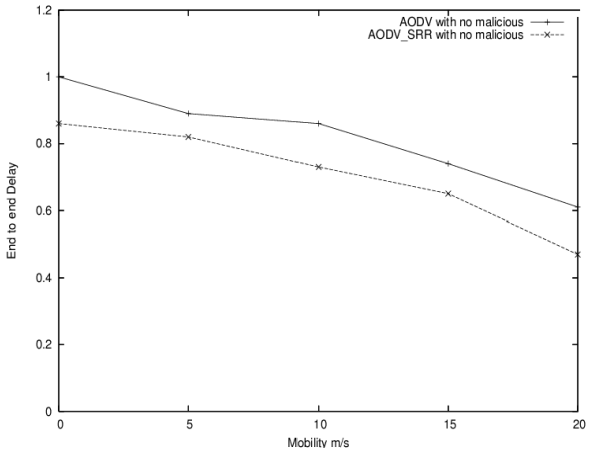

Fig. 8 End-to-end delay verses mobility for Set 1, Set 2 and Set 3 of AODV and AODV-SRR with 0% malicious nodes

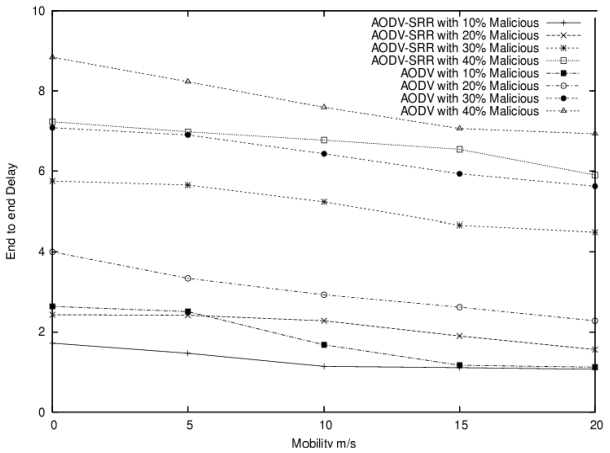

Fig. 9 End-to-end delay verses mobility for Set 1 of AODV and AODV-SRR with 10% - 40 % malicious nodes

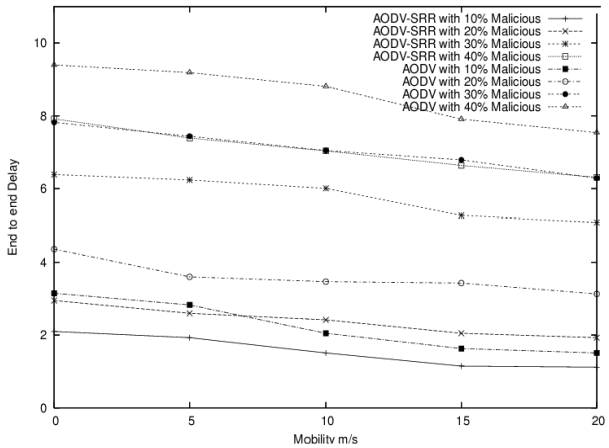

Fig.10 End-to-end delay verses mobility for Set 3 of AODV and AODV-SRR with 10% - 40 % malicious nodes

iii. For Set 3 of plain AODV, the increases from 3.15 (10% malicious nodes; mobility = 0) to 7.54 (40% malicious nodes and mobility = 20 m/s) as shown in the Fig. 10. The corresponding variation for AODV-SRR is from 2.10 to 6.31.

IV. RELATED WORK

Many approaches have been proposed to improve the performance of reactive routing protocols. Some approaches have been beneficial to most of the reactive routing protocols. Expanding ring search optimization has been proposed for AODV protocol [2-5] [8-10]. Since RREQ packets are flooded throughout the network; this algorithm does not scale well to large networks. If the destination node is located relatively near the source, issuing a RREQ packet that potentially pass through every node in the network is wasteful. The source node searches successively larger areas until the destination node is found. This is done by, for every RREQ retransmission until a route is found, incrementing the *time to live* (TTL) value carried in every RREQ packet, thus expanding the ``search ring" in which the source is centered. DSR have three optimization mechanisms (i.e) Salvaging: An intermediated node uses an alternative route from its cache, when a data packet meets a failed link on its source route. Gratuitous Route Repair: A Source node receiving RERR

piggybacks the RERR in the following RREQ, to clean the caches of other nodes that may use the failed link. Promiscuous Listening: When a node overhears a packet not addressed to itself, it checks whether the packet could be routed via itself to gain a shorter route. If so, sends a gratuitous RREP to S with a better new route [6-7].

Path optimizing [12-13] approaches typically require nodes to work in promiscuous mode to find an optimization opportunity. Route caches are used to reduce the overhead of route discovery. DSR uses routing cache aggressively, and maintains multiple routes per destination [9] [10].

Adaptive Hello Rate (AHR), a two-state adaptive mechanism for adjusting HELLO_INTERVAL parameter in AODV. They have used two states: high Hello rate and low Hello rate. They have potential benefit [2][5]. In the paper [14] when a path is likely to be broken, a warning is sent to the source indicating the likelihood of a disconnection.

V. Conclusion

We have conducted simulation studies to evaluate the performance of AODV-SRR in the presence of malicious nodes and have compared it with plain AODV routing protocol. The results show that AODV-SRR significantly improves the performance of AODV in all metrics, namely, packet delivery ratio, control overhead and end-to-end delay. Our future work will focus on studying the design of SRR for other major on-demand routing protocols and studying their respective performance improvements.

ACKNOWLEDGEMENTS

We express our thanks to Dr. P. Kanniappan, the vice chancellor, Prof. V. M. Periasamy, the Registar and Prof. Manu Natarajan, the Head, Department of CSE, B.S.A.Crescent Engineering College Chennai, Tamilnadu, India for the encouraging environment provided.

References

[1] Rendong Bai, and Mekesh Singhal. Salvaging Route Reply for On-Demand Routing Protocols in Mobile Ad-Hoc Networks, in proc. ACM MSWiM 2005.

[2] Gomez C, Catalan m, Mantecon X, Paradells J and Calveras. Evaluating Performance of Real Ad-hoc Networks using AODV with Hello Message Mechanism for maintaining local connectivity. IEEE PIMRC 2005.

[3] C.E.Perkins, E.M. Belding-Royer, and I.D.Chakeres. Ad hoc on demand distance vector (aodv) routing. IETF Internet draft, oct. 2003.

[4] C.E. Perkins and E.M. Royer. Ad hoc on demand distance vector routing. In proceedings of the second IEEE workshop on Mobile Computer Systems and Applications, Feb 1999.

[5] Gomez C, Paradells J and Cuaves A. AHR: A two state adaptive Mechanism for link connectivity maintenance in AODV. ACM REALMAN 2006.

[6] D.B. Johnson, D.A.Maltz, and Y.c.Hu. The dynamic source routing protocol for mobile ad hoc networks (dsr). Internet draft, draft-ietf-manet-dsr-09.txt, apr 2003.

[7] Yih-Chun Hu and David B.Johnson. Implicit Source Routes for On-Demand Ad hoc Network Routing. ACM 2001.

[8] http://folk.uio.no/kenneho/studies/essay/node22.html

[9] S. Das, C. Perkins, and E. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks", in Proc. IEE INFOCOM, 2003, pp. 3-12.

[10] Jochen Schiller, "Mobile Communications", Pearson Education, Second edition, 2007.

[11] C.Siva Ram Murthy, and B.S.Manoj. Ad Hoc Wireless Networks Architectures and Protocols, Pearson Education, 2005.

[12] Scalable Networks Technologies: QualNet simulator 4.5 http://www.scalable-networks.com/

[13] C. Gui and P. Mohapatra. SHORT: Self-Healing and Optimizing Routing Techniques for mobile ad hoc networks. ACM MobiHoc 2003.

[14] V. C. Giruka, M. Singhal and S. P. Yarravarapu. A path compression technique for on-demand ad hoc routing protocols. ACM MASS 2004.

[15] Tom Goff, Nael B. Abu-Ghazaleh, Phatak and Ridvan Kahvecioglu. Preemptive Routing in Ad Hoc Networks. ACM SIGMOBILE 2001.

*[16]*W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135..

A.Kathirvel - born in 1976 in Erode, Tamilnadu, India, received his B.E. degree from the University of Madras, Chennai, in 1998 and M.E. degree from the same University in 2002. He is currently with B.S.A. Crescent Engineering College in the Department of computer science and Engineering and pursing Ph.D. degree with the Anna University, Chennai, India. He is a member of the ISTE. His research interests are protocol development for wireless ad hoc networks, security in ad hoc networks.

Rengaramanujam Srinivasan -- born in 1940 in Alwartirunagari, Tamilnadu, India, received B.E. degree from the University of Madras, Chennai, India in 1962, M.E. degree from the Indian Institute of Science, Bangalore, India in 1964 and Ph.D. degree from the Indian Institute of Technology, Kharagpur, India in 1971. He is a member of the ISTE and a Fellow of Institution of Engineers, India. He has over 40 years of experience in teaching and research. He is presently working as a Professor of Computer Science and Engineering at BSA Crescent Engineering College, Chennai, India and is supervising doctoral projects in the areas of data mining, wireless networks, Grid Computing, Information Retrieval and Software Engineering.

Table II Experiment result of Set 2 of AODV-SRR with 10%-40% malicious nodes.

	Packet Delivery Ratio				Communication overhead				End-to-end delay			
	Malicious node				Malicious node				Malicious node			
Mobility	10%	20%	30%	40%	10%	20%	30%	40%	10%	20%	30%	40%
0	80.16	73.16	66.26	59.18	12371	15201	17036	18397	3.5251	4.8898	7.8992	9.4876
5	68.64	54.76	42.53	32.48	12749	15640	17515	19099	3.2158	4.4742	7.5895	8.6454
10	63.49	48.56	35.74	26.51	13234	16180	18001	19639	2.4897	4.0789	6.9868	8.1289
15	60.94	44.16	27.52	21.23	13807	16684	18528	20191	1.9784	3.5872	6.5237	7.7455
20	58.46	42.56	26.44	21.17	14259	17205	19023	20732	1.6781	3.1856	5.9781	7.1471

F. A. Author is Associate Professor and Head of Department, Department of Mechanical Engineering, with Haryana College of Technology and Management, Kaithal–136027 (Haryana), INDIA (Phone:+91 9996021544; fax: +91 1746280711; e-mail: sorabh_gupta123@rediffmail.com)

S. B. Author is with National Institute of Technology, Kurukshetra, Haryana, INDIA (e-mail: pctewari1@rediffmail.com).