Continuous evaluation of node's performance and collection of neighbor node's opinion value about the node are used to calculate the trust relationship of this node with other nodes. A perfect trust model [26] is introduced in the network layer to establish secure route between source and destination without any intruders or malicious nodes. Thus the existing AODV routing protocol has been modified in order to adapt the trust based communication feature. Proposed trust based routing protocol equally concentrates both in node trust and route trust. A routing algorithm [27] which adds a field in request packet which stores trust value indicating node trust on neighbor is proposed. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all. This not only saves the node's power by avoiding unnecessary transmitting control information but also in terms of bandwidth (channel utilization), which is very important in case of MANET. The malicious node can attack on the control packet and misbehave in the network. The malicious node, which may or may not be trusted node. Here, a trusted path irrespective of shortest or longest path which can be used for communication in the network is proposed. Route trust value is calculated on the complete reply path which can be utilized by source node for next forthcoming communication in the network.

A security-enhanced AODV routing protocol [28] called R-AODV (Reliant Ad hoc On-demand Distance Vector Routing) is presented. The implementation is done by a modified trust mechanism known as direct and recommendations trust model and then incorporating it inside AODV which will allow AODV to not just find the shortest path, but instead to find a short path that can be trusted. This enhances security by ensuring that data does not go through malicious nodes that have been known to misbehave. The R-AODV protocol does provide a more reliable data transfer compared to the normal AODV if there are malicious nodes in the MANET.

Two kinds of approaches [29] are applied to a well-known routing protocol called SAODV in order to improve its performance and to offer more resilience to attack from malicious nodes authenticated by the network. A preventive approach based on a cryptographic mechanism and a reactive approach to detect the anomalous and malicious behavior of nodes is considered. An extension of SAODV to offer Intrusion Detection mechanism (IDM) and trust-based mechanism (TBM) to promote the collaboration of the cooperating node and penalize the selfish nodes are proposed. The extended and proposed protocol SAODV-SDO is presented and simulation results performed in order to show the effectiveness of the proposed protocol in comparison with AODV and SAODV.

III. PROPOSED WORK

In Mobile ad hoc network routing is affected due to the dynamic nature of nodes. In spite of this dynamic topology nodes communicate with each other and exchange data on the network. The architecture of the proposed work is shown in Fig. 1. Trust based work [30] designed & implemented and for every run it takes into account the nodes which have good success rate and failure rate. Trust is calculated based on success and failure rate and trust values for nodes are stored

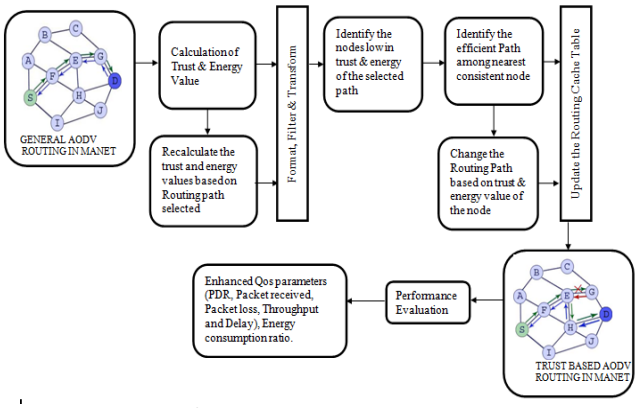

Fig. 1. Architecture of the proposed work

TABLE I
TRUST VALUE CALCULATION PARAMETERS

Count Type	RREQ	RREP	Data
Success	Qrs	Qps	Qds
Failure	Qrf	Qpf	Qdf

separately for each node during simulation. When network starts, the initial trust value is 1 for all nodes. This value either increases or decreases based on nodes success or failure rate. All nodes are trusted nodes initially but trust value changes for every run of simulation. During simulation communication messages (RREQ and RREP) are exchanged between nodes in the network. RREP contains energy values also.

The trust level value calculation is based on the parameters shown in the Table I. The count field describes about two criteria, success rate (packets delivered successfully) and failure rate (packets lost or not delivered). RREQ and RREP are the route request and route reply respectively which are exchanged between nodes in the network. Data refers to the payload transmitted by the node in the routing path.

The parameter Qrs is defined as the query request success rate which is calculated based on number of neighboring nodes who have successfully received (RREQ) from the source node which has broadcasted it, Qrf defined as the query request failure rate which is calculated based on number of neighboring nodes which have not received the query request, Qps is defined as the query reply success rate which is calculated as successful replies (RREP) received by the source node which has sent the RREQ and Qpf is defined as the query reply failure rate which is calculated based on the number of replies not received by the source node for which RREQ was sent. Qds is defined as the data success rate calculated based on successfully transmitted data and Qdf is defined as data failure rate calculated based on data which have failed to reach destination.

A. *Trust calculation Pseudocode*

Step 1: Begin; For nodes i to n do
Step 2: Initialize qrs, qps,qds //Success rate parameters
Step 3: Initialize qrf, qpf, qdf // Failure rate parameters
Step 4: Initialize QR, QP, QD // Intermediate values of request, reply and date respectively.

Step 5: Calculate QR: $QR = \sum_{i}^{n} \frac{qrs - qrf}{qrs + qrf}$

Step 6: Calculate QP: $QP = \sum_{i}^{n} \frac{qps - qpf}{qps + qpf}$

Step 7: Calculate QD: $QD = \sum_{i}^{n} \frac{qds - qdf}{qds + qdf}$

Step 8: Calculate Trust Level Value:

$TL = T(RREQ) * QR + T(RREP) * QP + T(DATA) * QD$

// T is the time factorial of RREQ, RREP, DATA sent respectively

Step 9: For all neighbor nodes j to n do

Step 10 : Calculate Trust-Threshold: $TT = \sum_{i}^{n} \frac{TL}{n}$

Step 11: End

B. Energy calculation procedure:

In MANET, nodes energy also plays a key role. Node is selected for routing only if its energy level is also greater than the threshold value (average of energy values of the nodes). During simulation scenario energy values are displayed on top of each node. For every transmission the transmission power and reception power gets subtracted from its initial value of 100 Joules (initialized during simulation). Energy calculation is based on nodes sending and receiving rate.

Step 1: Do For all intermediate nodes which receive route request from a source node.
Step 2: Introduce energy for all nodes and set initial parameters values as initialenergy = 100, maxenergy=100, nodes=50 and Nodeid (unique id for each node)
Step 3: Calculate Intermedenergy based on event , time where events can be (event = "Tm" || event= "Rm" || event ="Im"|| event="Om") // Transmit mode, Receive mode, Idle mode and Overhear mode.
Step 4: Compute consumed energy for each node;

```
for (i in Intermednergy) {
consumedenergy[i]=initialenergy-Intermedenergy[i]
totalenergy +=consumedenergy[i]
if(maxenergy<consumedenergy[i]){
maxenergy=consumedenergy[i]
nodeid=i }}
```

Step 5: Node which sends route request collects energy value of all nodes which receive the request from source and reply to source along with their energy value (consumed energy).
Step 6: Compute threshold as total energy of nodes replied to node that has sent request by number of nodes replied.

Step 6. a:Calculate Energy-Threshold $ET = \sum_{i}^{n} \frac{ConsumedEnergy}{n}$

Step 7: Next hop node selected based on its energy value which is higher than the threshold.
Step 8: Compute average energy:
Averagenergy = totalenergy/nodes
Step 9: End

Therefore the next hop node is selected based on the trust and energy value. To select the next hop node the trust and energy value of all neighboring nodes from current source node is calculated and finally a node which has highest value than the threshold is selected as next hop node for the current routing. For example, Route starts from node N1 and next hop node N2 is selected. Now to select next hop node for N2 its neighbors are identified and their trust values and energy values are calculated. If N3, N4, N5, N6, N7 are the neighboring nodes of N2 then trust and energy value for all these nodes are collected and an average of this is identified and this value is set as threshold value for selecting the next hop node for N2 only. The node which has the highest trust and energy value than the threshold will be selected as next hop node. Threshold value is calculated dynamically for every next hop node selection in each run. The nodes which are not selected for the current transmission based on their trust and energy value cannot be tagged as unfit node and can serve as best trusted node for another transmission based on the scenario. Thus the consideration of node's trust value and its energy value makes the routing more efficient compared with traditional AODV and DSR.

TABLE II
COMPARISON OF PDR

Node Size	PDR(%)		
	AODV	DSR	Proposed AODV
25	29.99	31.89	35.35
50	31.50	44.64	74.47
100	56.64	54.23	80.25

TABLE III
COMPARISON OF THROUGHPUT

Node Size	Throughput (bits/sec.)		
	AODV	DSR	Proposed AODV
25	40	44	64
50	130	299	367
100	3175	873	8276

TABLE IV
COMPARISON OF DELAY

Node Size	Delay (sec.)		
	AODV	DSR	Proposed AODV
25	0.235	0.375	0.081
50	1.415	2.423	0.806
100	6.799	9.292	3.516

IV. RESULTS

The performance of proposed AODV protocol is analyzed using NS-2 simulator. The network is designed using network simulator with 25, 50 and 100 nodes. General AODV & DSR are simulated initially and its Qos metrics are observed. Proposed AODV is simulated and its results are also

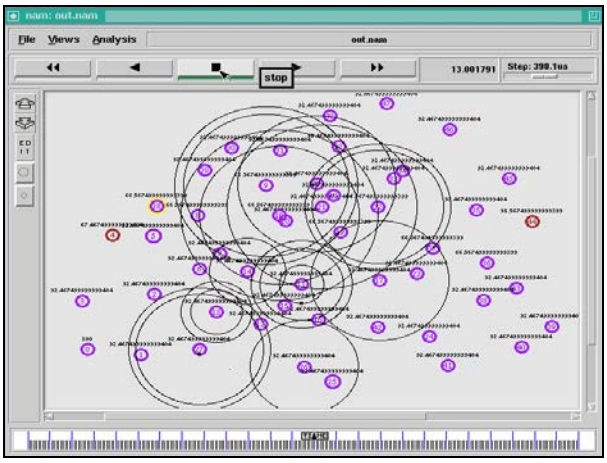

Fig. 2. Snapshot showing source and destination.

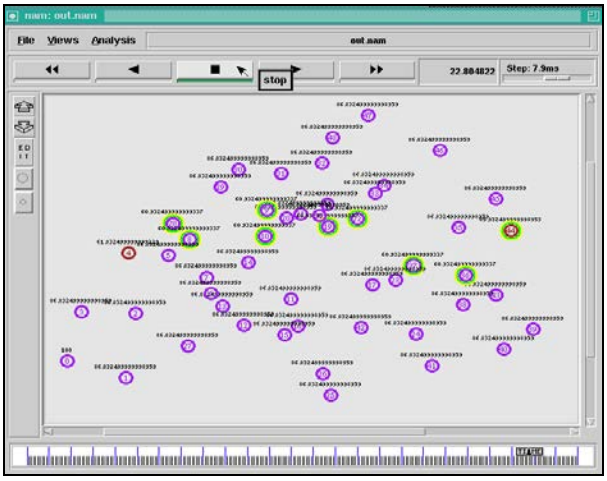

Fig. 3. Snapshot showing the misbehaving nodes.

observed. Results are compared in terms of Packet delivery ratio, Throughput, Delay and Energy consumption ratio. The proposed AODV shows good improvement in Qos metrics. PDR and Throughput are higher, delay is reduced and energy consumption is also less compared with general AODV and DSR as shown in Table II, Table III and Table IV.

Initially when trust model alone was incorporated the PDR was increased by 15%. Now the trust and energy schemes are combined together and implemented in the proposed AODV. On an average of 20% increase is shown in PDR. This increase is because nodes are selected based on their trust and energy value. The next hop node selected to complete the path form source to destination, is based on its trust and energy value. This trust and energy based routing assures an efficient routing and avoids misbehaving nodes in routing path. The proposed AODV has also shown a decreased delay and an increase in throughput. Nodes which are trusted and with high energy levels are only used for routing path which ultimately reduces the time taken to reach the destination. Energy is vital for a node to perform in the network. Nodes with good trust may be selected for routing but inefficient energy may lead to poor performance of the node towards routing. This scheme selects node for only routing which has good energy values. The energy consumption of nodes are reduced so that they maintain good energy levels for future transmission and extend their lifetime in the network. Compared with proposed AODV, DSR and traditional AODV have consumed more energy.

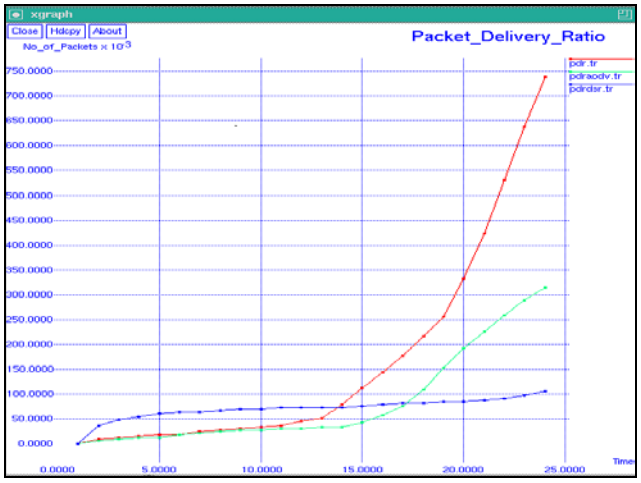

Fig. 4. Comparison of general AODV, DSR and proposed AODV PDR

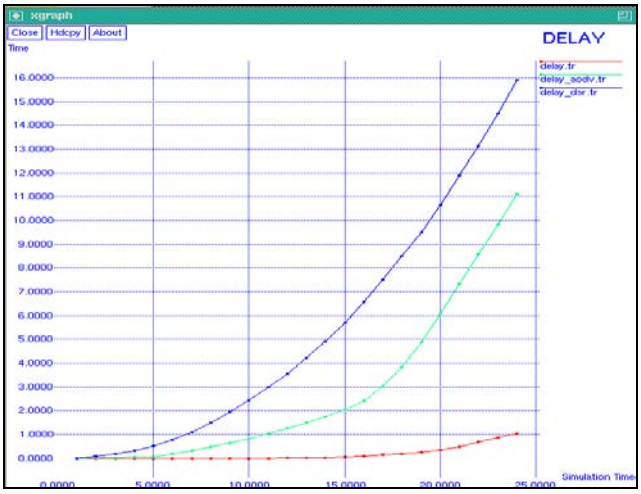

Fig. 5. Comparison of general AODV, DSR and proposed AODV Delay

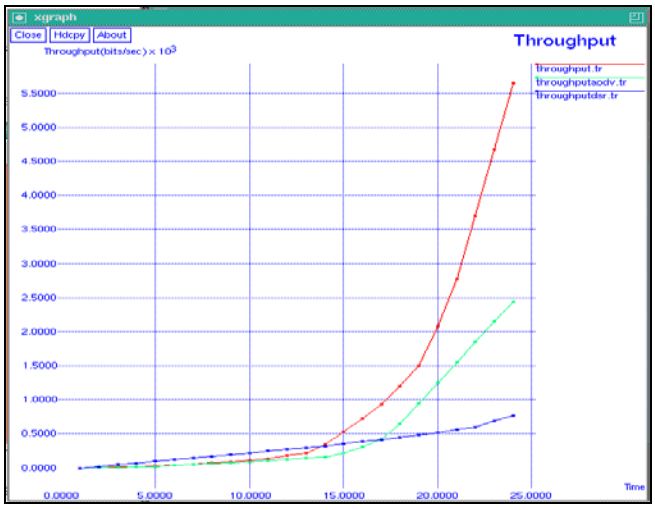

Fig. 6. Comparison of general AODV, DSR and proposed AODV Throughput

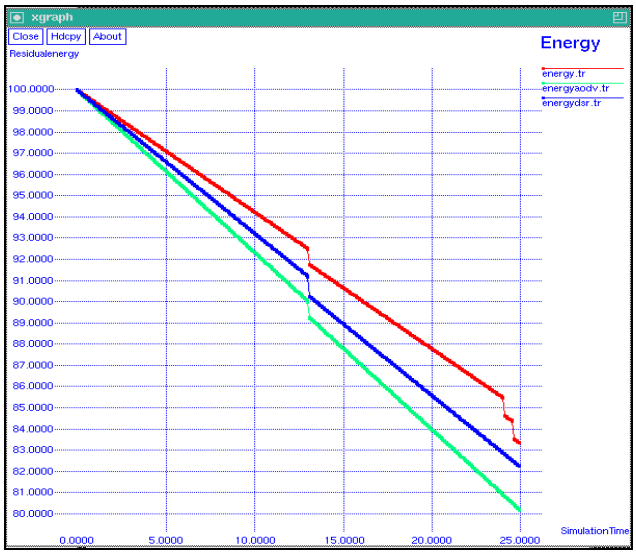

Fig. 7. Comparison of general AODV, DSR and proposed AODV energy consumption

V. CONCLUSION

Nodes in MANET may misbehave or drop nodes during routing which affects the Qos parameters and brings down the performance of the Network. A trust model is proposed which identifies misbehaving nodes the routing path and isolates those nodes from routing and selects an alternate path for efficient routing and also improves the QOs performance. The trust factor is calculated based on the nodes success rate and failure rate of transmission. Though node is trusted if it has not got enough energy in it becomes ineffective for routing. Therefore Energy is also considered for routing where in node should have sufficient energy for taking part in routing. Simulation results show good improvement in Qos metrics. The results of the proposed AODV protocol are compared with traditional AODV and DSR protocol. In proposed AODV protocol, Packet delivery ration is increased, throughput is increased and Delay is reduced. Energy consumption is reduced in proposed protocol. The work can be used in scenarios where transmission needs to be really secured and reliable like any sort of emergency situations, Military fields, etc. The Proposed protocol can be compared with many other Reactive and Proactive protocols and virtual energy concepts can be introduced in future works.

REFERENCES

[1] Remondo, "Tutorial on wireless ad hoc networks", in *proc.*Second International Conference in Performance Modeling and Evaluation of heterogeneous networks, 2004. pp. 216-220.

[2] C.E.Perkins and E.Royer, "Ad-hoc on-demand distance vector routing", in *proc.* Second IEEE Workshop on Mobile Computing Systems and Applications, LA, USA, 1999, pp. 90–100.

[3] D.B.Johnson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Kluwer, 1996, pp. 246-258.

[4] V.Park and M.S.Corson, "A highly adaptive distributed routing Algorithm for mobile wireless networks", in *proc.* IEEE INFOCOM, Kobe, Japan, 1997, pp. 1405–1413.

[5] C.K.Toh, "A novel distributed routing protocol to support ad-hoc mobile computing", in *proc.* fifteenth IEEE Annual International Phoenix Conference on Computers and Communications, 1996, pp. 480–486.

[6] R.Dube, C.D.Rais, K.Y.Wang and S.K.Tripathi. (1997, may). On Signal stability-based adaptive routing (SSA) for ad hoc mobile networks. *IEEE Personal Communications. [online]*. 4(1)), pp. 36–45. Available: http://pdos.csail.mit.edu/decouto/papers/dube97.pdf.

[7] G.Aggelou and R.Tafazolli, "RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks", in *proc.* WoWMoM, 1999, pp. 26–33.

[8] C.E.Perkins and P.Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers", in *proc.* ACM Special Interest Group on Data Communication, London, UK, 1994, pp. 234–244.

[9] S. Murthy and J.J.Garcia-Luna-Aceves, "A routing protocol for packet radio networks", in *proc.* ACM First International Conference on Mobile Computing and Networking, CA, USA, 1995, pp. 86–95.

[10] S. Murthy and J.J.Garcia-Luna-Aceves. (1996, aug). On An efficient routing protocol for wireless networks. *ACM Mobile Networks and Applications, Special Issue on Routing in Mobile Communication Networks.[online]*. 1(2), pp. 183–197. Available: http://. http://link.springer.com/article/10.1007%2FBF01193336

[11] G.Pei, M.Gerla and T.W.Chen, "Fisheye state routing: a routing scheme for ad hoc wireless networks", in *proc.* ICC, LA, 2000, pp. 70–74.

[12] I.Jawhar and J. Wu, "Quality of Service Routing in Mobile Ad Hoc Networks," in M Cardei, I Cardei & DZ Du (eds), Resource Management and Wireless Networking, Kluwer Academic Publishers. 1999, pp 152-168.

[13] T.Beth, M.Borcherding and B.Klein, "Valuation of trust in open networks", *in proc.* ESORICS, 1994.

[14] K. S. Cook, "*Trust in Society,*" *in* Russell Sage Foundation Series on Trust, New York. vol. 2, 2003, pp. 22-30

[15] K.Muthumayil, V.Rajamani and S.Manikandan, "A novel cross layered energy based ad hoc on-demand routing protocol for MANETs", in *proc.* ICoAC, 2011, pp. 276-281.

[16] Arash Dana, Golnoosh Ghalavand, Azadeh Ghalavand and Fardad Farokhi,. (2011, May). On A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic. *International Journal of Computer Science Issues.[online]*. 8(3), pp. 128 – 133. Available: http://ijcsi.org/papers/IJCSI-8-3-1-128-133.pdf.

[17] Yunhuai Liu, Yanmin Zhu, Lionel M. Ni and Guangtao Xue. (2011, Dec). On A Reliability-oriented transmission service in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems.[online]*. 22(12), pp. 2100 – 2107. Available: ieeexplore.ieee.org › ... › Parallel and Distributed Syst

[18] MouZonghua and Meng Xiaojing, "A modified AODV routing protocol based on route stability in MANET", in *proc.* 4th IET International Conference on Wireless, Mobile & Multimedia Networks, 2011, pp. 63 - 67.

[19] A.Bagwari, R.Jee, P. Joshi and S.Bisht, " Performance of AODV Routing Protocol with Increasing the MANET Nodes and Its Effects on QoS of Mobile Ad Hoc Networks", in *proc.* International Conference on Communication Systems and Network Technologies, 2012 , pp. 320-324.

[20] A.Akhter and T.Sanguankotchakorn, " Modified AODV for multi-constrained QoS routing and performance optimization in MANET", in *proc.* International Conference on Electrical Engineering/Electronics Computer Telecommunications and Information Technology, 2010 , pp. 234 – 238.

[21] Chee-Wah Tan and S.K.Bose, "Investigating Power Aware AODV for Efficient Power Routing in MANETs", in *proc.* Fifth International Conference on Information, Communications and Signal Processing, 2005, pp. 584 – 588.

[22] Jin-ManKim and Jong-WookJang, "AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET", in *proc.* International Conference on Internet and Web Applications and Services, 2006, pp. 77.
[23] M.S.Alkatheiri, JianweiLiu and A.R.Sangi, "AODV routing protocol under several routing attacks in MANETs", in *proc.* ICCT, 2011, pp. 614 – 618.
[24] Zhang Jianwu, ZouJingyuan and ZhaoQi, " MANET Routing Protocol for Improving Routing Discovery Based on AODV", in *proc.* International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp.197 - 200.
[25] S.Sarkar and R.Datta, "A trust based protocol for energy-efficient routing in self-organized MANETs", in INDICON, 2012, pp. 1084 – 1089.
[26] A.M.Pushpa, "Trust based secure routing in AODV routing protocol", in *proc.* IMSAA, 2009, pp.1 – 6.
[27] R.S.Mangrulkar and M.Atique, "Trust based secured adhoc On demand Distance VectorRouting protocol for mobile adhoc network ",in *proc.* WCSN, 2010, pp.1 – 4.
[28] H.S.Jassim, S.Yussof, Tiong Sieh Kiong, S.P.Koh and R.A.Ismail, "A routing protocol based on trusted and shortest path selection for mobile ad hoc network", in *proc.* MICC, 2009, pp.547 - 554.
[29] F.De Rango, "Improving SAODV protocol with trust levels management, IDM and incentive cooperation in MANET", in Wireless Telecommunications Symposium, 2009, pp. 1 – 8.
[30] S.Sridhar and R.Baskaran, "Quality of service routing in MANET using trusted AODV (TS-AODV)", in *proc.* ICCCMIT, Chennai, 2014, pp. 58.

S. Sridhar received UG degree, B.Sc. Computer Science from the University of Madras, Chennai, India, in 1998, PG degree, Master of Computer Applications (MCA) from University of Madras, Chennai, India, in 2001 and another PG degree Master of Philosophy (M.Phil.) in Computer Science from Periyar University, Salem, Tamil Nadu, India, in 2007. Currently pursuing the Ph.D. degree in computer science at Barathiyar University, Coimbatore, Tamil Nadu, India. Since 2001 he has been working with Department of Computer Applications (MCA), S.A.Engineering College, Chennia, Tamilnadu and currently heading the department. He has got more than 15 international publications. His research interests include Mobile Adhoc networks, Wireless sensor networks and Adhoc networks. He is an editorial member of 2 International Journals and reviewed many technical papers for conferences and journals.

R. Baskaran obtained M.E. and Ph.D. in the field of Computer Science and Engineering in Anna University at Chennai, India. He is working as Associate professor in Department of computer science, Anna University, Chennai. He is having around a decade of experience as an academician and his research areas include Multimedia and principles, Software quality engineering, Software Agents and Distributed networking.
He has published around 75 research papers in National and International Journals and Conferences. He is a member of various forums. He is the editor and a reviewer of various journals. He is guiding research scholars working in area of software standards for Attributes Specific SDLC Models & Evaluation and Metric Based Efficient Traffic Management.