QoS Assertion in MANET Routing Based on Trusted AODV (ST-AODV)

Sridhar Subramanian[1] and Baskaran Ramachandran[2]

[1]Department of Computer Applications, S.A.Engineering College, Chennai, India.
ssridharmca@yahoo.co.in
[2]Department of Computer Science & Engineering, CEG, Guindy, Anna University, Chennai, India.
baskaran.ramachandran@gmail.com

Abstract

Mobile ad hoc network is a standalone network capable of autonomous operation where nodes communicate with each other without the need of any existing infrastructure. They are self configuring, autonomous, quickly deployable and operate without infrastructure. Mobile ad hoc networks consist of nodes that cooperate to provide connectivity and are free to move and organize randomly. Every node is router or an end host, in general autonomous and should be capable of routing traffic as destination nodes sometimes might be out of range. Nodes are mobile since topology is very dynamic and they have limited energy and computing resources. These nodes are often vulnerable to failure thus making mobile ad hoc networks open to threats and attacks. Communication in MANET relies on mutual trust between the participating nodes but the features of MANET make this hard. Nodes sometimes fail to transmit and start dropping packets during the transmission. Such nodes are responsible for untrustworthy routing. A trust based scheme can be used to track these untrustworthy nodes and isolate them from routing, thus provide trustworthiness. In this paper a trusted AODV (ST-AODV) protocol is presented which assigns a trust value for each node. Nodes are allowed to participate in routing based on their trust values. A threshold value is assigned and if the nodes trust value is greater than this value its marked as trustworthy node and allowed to participate in routing else the node is marked untrustworthy. The ST-AODV increases PDR and decreases delay thereby enhancing the QoS metrics and trustworthiness in AODV based MANET routing. The work is implemented and simulated on NS-2. The simulation result shows the proposed ST-AODV provides more trustworthy routing compared with general AODV in presence of packet dropping nodes in MANET.

Keywords

Ad-hoc, MANET, AODV, ST-AODV, Trust, Qos

1. Introduction

A MANET is an extremely testing lively network. Mobile Ad-Hoc network [1] is a system of wireless mobile nodes that self-organizes itself in dynamic and temporary network topologies. Nodes can connect and depart the network at anytime and should be in position to relay traffic. The primary goal of MANET is to find an end to end path or route, minimizing overhead, loop free and route maintenance. A few challenges faced in mobile ad hoc networks are mobility, variable link quality, energy constrained nodes, heterogeneity and flat addressing.

Most traditional mobile ad hoc network routing protocols were designed focusing on the efficiency and performance of the network [2]. These protocols should meet some basic requirements like self starting, self organizing, loop free paths, dynamic topology maintenance, minimal traffic overhead etc to deal with the challenges involved in routing. Existing MANET routing protocols can be classified into mainly two types- proactive routing protocols and reactive routing protocols. Table driven (proactive) routing protocols such as dynamic

DOI : 10.5121/ijasuc.2012.3310

Optimized Link State Routing (OLSR), Destination-Sequenced Distance-Vector routing (DSDV), Topology Broadcast based on Reverse Path Forwarding (TBRPF) and On-demand (reactive) routing protocols such as Ad hoc On demand Distance Vector (AODV), Signal Stability-based Adaptive routing (SSA), Dynamic Source Routing (DSR). Other categories are flooding based, cluster based, geographic and application specific. Proactive protocols are table driven protocols much similar to conventional routing, have little delay in route discovery and routing overhead is high. On-demand routing protocols are reactive protocols which obtain route information only when needed and the overhead is low since there is no periodic update of tables.

AODV is a reactive protocol where route discovery initiated when required only using route request (RREQ) and route reply (RREP) packets and stores only active routes in routing table. Explicit route error notification is done by using route error (RERR). Ad-hoc on demand Distance Vector (AODV) routing protocol [3] is an on demand routing protocol that focuses on discovering the shortest path between two nodes with no consideration of the reliability of a node. By broadcasting HELLO packets in a regular interval, local connectivity information is maintained by each node. However, the traditional AODV protocol seems less than satisfactory in terms of delivery reliability there by affecting quality of service.

Due to the dynamic nature of Mobile Ad-Hoc Networks, there are many issues which need to be tackled and one of the areas for improvement is Quality of Service (QoS) routing. When it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met [4]. A few challenges faced in providing Qos are persistently changing environment, unrestricted mobility which causes recurrent path breaks and also make the link-specific and state-specific information in the nodes to be inaccurate.

This ST-AODV protocol is to perform its task based on the trust based scheme where trust values calculated for each node and to decide whether the node can take part or to be isolated from routing. If nodes trust value is less than the threshold then the node is declared to be untrustworthy node and an alternate path is chosen. This trust based routing scheme facilitates in identifying and isolating untrustworthy nodes thus providing trustworthy routing in MANET and also improves the performance Qos parameters like PDR and delay.

2. LITERATURE SURVEY

Mobile ad hoc network is capable of autonomous operation , operates without base station infrastructure , nodes cooperate to provide connectivity and operates without centralized administration. MANETs have put on more significance in recent applications areas like security, routing, resource management, quality of service etc. The significance of routing protocols in MANETs has anticipated for a lot of competent and inventive routing protocols. Continuous evaluation of node's performance and collection of neighbour node's opinion value about the node are used to calculate the trust relationship of this node with other nodes [5]. In this paper, existing AODV routing protocol has been modified in order to adapt the trust based communication feature and the proposed trust based routing protocol equally concentrates both in node trust and route trust.

RAODV (Reliant Ad hoc On demand Distance Vector Routing) [6] is a security-enhanced AODV routing protocol that uses a modified scheme called direct and recommendations trust model and then incorporating it inside AODV. This scheme assures that packets are not handed over to malicious nodes. Based on this trust value a node is selected to perform packet transfer. This protocol results in higher percentage of successful data delivery compared to AODV. A routing algorithm is proposed that adds a field in request packet which stores trust value indicating node trust on neighbor [7]. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all that results not only in saving the node's power but also in terms of bandwidth. A trusted path irrespective of shortest or longest path is used communication in the network.

A routing protocol [8], that adds a field in request packet and also stores trust value indicating node trust on neighbour based on level of trust factor. This scheme avoids unnecessary transmit of control information thus efficiently utilizing channels and also saves nodes power. Route trust value is calculated based on the complete reply path, which can be utilized by source node for next forthcoming communication in the network that results in improvement in security level and also malicious node attacks are prevented. A trust based packet forwarding scheme [9] for detecting and isolating the malicious nodes using the routing layer information that uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node will be punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.

A framework [10] for estimating the trust between nodes in an ad hoc network based on quality of service parameters is proposed based on Probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays. It has been shown that only two end nodes need to be involved and thereby achieve reduced overhead. A Node-based Trust Management (NTM) scheme in MANET [11] is introduced based on the assumption that individual nodes are themselves responsible for their own trust level. Mathematical framework of trust in NTM is developed along with some new algorithms for trust formation in MANETs based on experience characteristics offered by nodes. The above listed works are spotlighting on reliability that is provided to the mobile ad hoc network by using trust schemes.

3. PROPOSED WORK

In MANET, providing reliable routing is difficult because of its dynamic nature that keeps nodes moving and not stable. In spite of this nature nodes communicate with each other and exchange data among the nodes that are in its range on the network. But still there are nodes in the MANET which take part in routing but drop packets while transmitting packets which affects the performance of the protocol. Thus trusted ST-AODV is introduced which checks each node before involving it in the routing process. The design of the proposed work is presented in Fig. 1.

In the MANET an observation is made on all nodes that transmit packets. The total packets they transmit, packets they receive and the packets they drop are taken in to account. Once a particular transmission is to be made the protocol decides the route and the nodes which are going to participate in routing are checked against their trust values which are calculated based on the total packets handled by each node. Based on this trust value a node is located if it is about to drop packets. Thus these packet dropping nodes are spotted and removed from the routing path and the protocol again checks for an alternate node for proceeding the routing. Thus an alternate path is identified based on the trust values of the node that is to be included recently in the routing path to carry on the routing effectively. Thus trusted ST-AODV removes packet dropping nodes in the routing path which causes the performance of the network to decline and resulting in lower QoS values. These packet dropping nodes may result in reducing trust values of nodes by indirectly affecting them in the network.

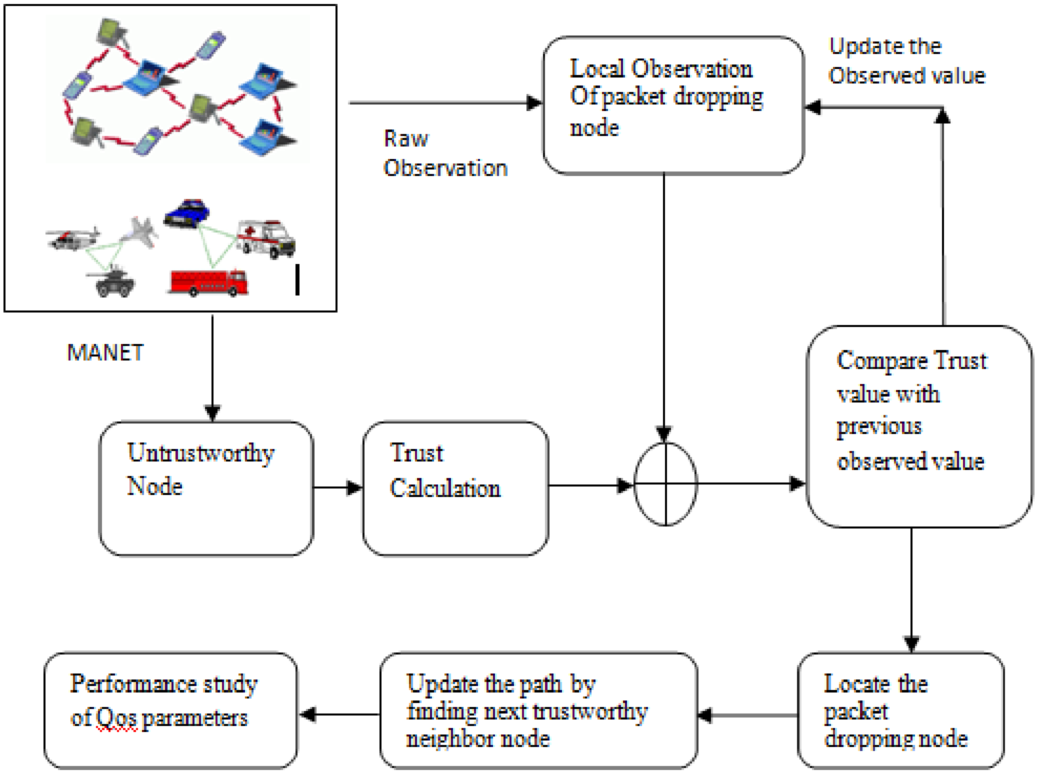
Raw Observation
Local Observation Of packet dropping node
Update the Observed value
MANET
Untrustworthy Node
Trust Calculation
Compare Trust value with previous observed value
Performance study of Qos parameters
Update the path by finding next trustworthy neighbor node
Locate the packet dropping node

Figure. 1. Architecture of Trusted ST-AODV routing in MANET

The trust level value calculation [12] is based on the parameters shown in the table 1. The count field describes about two criteria success and failure which describes whether the transmission was a successful transmission or a failure.

Table 1. Node Trust calculation parameters

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

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 nodes. The parameter qrs is defined as the query request success rate which is calculated based on number of neighbouring 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 neighbouring 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 neighbouring nodes which have not sent the replies for the query request received. 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. However, it is known that for every network there will be minimum data loss due to various constraints

$$Qr = \frac{q_{rs} - q_{rf}}{q_{rs} + q_{rf}} \qquad (1)$$

$$Qp = \frac{q_{ps} - q_{pf}}{q_{ps} + q_{pf}} \qquad (2)$$

$$Qd = \frac{q_{ds} - q_{df}}{q_{ds} + q_{df}} \qquad (3)$$

Where Qr, Qp and Qd are intermediate values that are used to calculate the nodes Request rate, Reply rate and Data transmission rate. The values of Qr, Qp, and Qd are normalized to fall in range of -1 to +1. If the values fall beyond the normalized range then it clearly shows that the failure rate of the node is high and denotes that the corresponding node may not be suitable for routing.

$$TL = T(RREQ) * Qr + T(RREP) * Qp + T(DATA) * Q_d \qquad (4)$$

Where, TL is the trust level value and T(RREQ), T(RREP) and T(DATA) are time factorial at which route request , route reply and data are sent by the node respectively. Apart from the above mentioned normalised range, using the above formula the trust level value (TL) is calculated for each node during routing and is checked against the threshold value (assumed to be as 5). If lesser than threshold then there is a possibility for this node to drop packets for the current transmission and will not be suitable for routing and an alternate path is selected for routing. However, this node may be the best node for some other transmission between some other source and destination in the same network at different time interval. Therefore based on the above calculation the following two cases are derived based on the threshold value that is assumed to be 5. Case 1: The nodes trust value is checked with the threshold value and if the value is greater than the threshold value then the node is defined a trustworthy node and are allowed to participate in routing thereby assuring a trustworthy routing in MANET. Case 2: If the nodes trust value is less than or equal to threshold value then the node in defines as untrustworthy node which cannot be allowed to participate in routing which causes packet dropping. In both cases the trust calculation is performed regularly to check the nodes performance and help it to be marked trustworthy or not. The trust calculation is done for all nodes in the routing path to monitor nodes reliability. If the failure rate increases it automatically affects the Qr, Qp and Qd values thus making them fall beyond the normalized values thus resulting in trust value less than the threshold.

4. EVALUATION RESULTS

The proposed ST-AODV protocol's performance is analyzed using NS-2 simulator. The network is planned and implemented using network simulator with maximum of 50 nodes and other parameters based on which the network is shaped are given in Table2. The simulator is applied with traditional AODV and with proposed trust based ST-AODV and results are obtained for assessment. The proposed trust based ST-AODV protocol has shown good progress over the Qos parameters like PDR & Delay. PDR is increased and delay is reduced compared to the traditional AODV and throughput is maintained in both cases. However there is a fraction of difference in throughput between general and proposed protocol which is rounded off as a whole value in result table. The performance of the proposed protocol is also represented graphically where it clearly shows the betterment of the Qos parameters.

Table 2. Simulation Parameter Values

Parameter	Value
Network size	1600 x 1600
Number of nodes	50
Movement speed	100 kbps
Transmission range	250 meters.
Packet size	5000
Traffic type	CBR
Simulation time	30 minutes.
Maximum speed	100 kbps
MAC layer protocol	IEEE 802.11
Time interval	0.01 sec.
Protocol	AODV
NS2 version	2.34

The values obtained using traditional AODV and proposed trust based ST-AODV at different node sizes are listed in table 3. The traditional AODV doesn't provide reliable routing since the nodes present in the network drop packets while routing which degrades the performance of routing and results in reduced packet delivery ratio and increased delay.

Table 3**.** Result comparison with different node sizes

Node Size	GENERAL AODV			PROPOSED TRUSTED ST-AODV		
	PDR	*Delay*	*Throughput*	*PDR*	*Delay*	*Throughput*
25	46.10	0.44306	757771.43	69.15	0.29538	757771.43
50	62.25	0.26151	120032.60	80.04	0.20340	120032.60
100	70.59	0.18225	115783.25	87.25	0.15595	115783.25
200	79.35	0.15584	113259.53	91.53	0.13759	113259.53
300	81.73	0.12635	110935.75	93.75	0.11925	110935.75

The Qos parameter values are showing better improvement when the routing takes place with the proposed ST-AODV protocol which works using trust values that identifies untrustworthy nodes in the route and immediately take an alternate path to provide trustworthy and successfully routing. The results shown in the following table clearly shows the PDR and delay of the proposed ST-AODV protocol are superior compared to traditional AODV protocol at different node sizes.

Figure 2 specifies the increase in PDR by implementing the proposed trust based ST-AODV protocol compared to the traditional AODV protocol. Figure 3 specifies the decrease in delay while using the proposed trust based ST-AODV compared to traditional AODV.

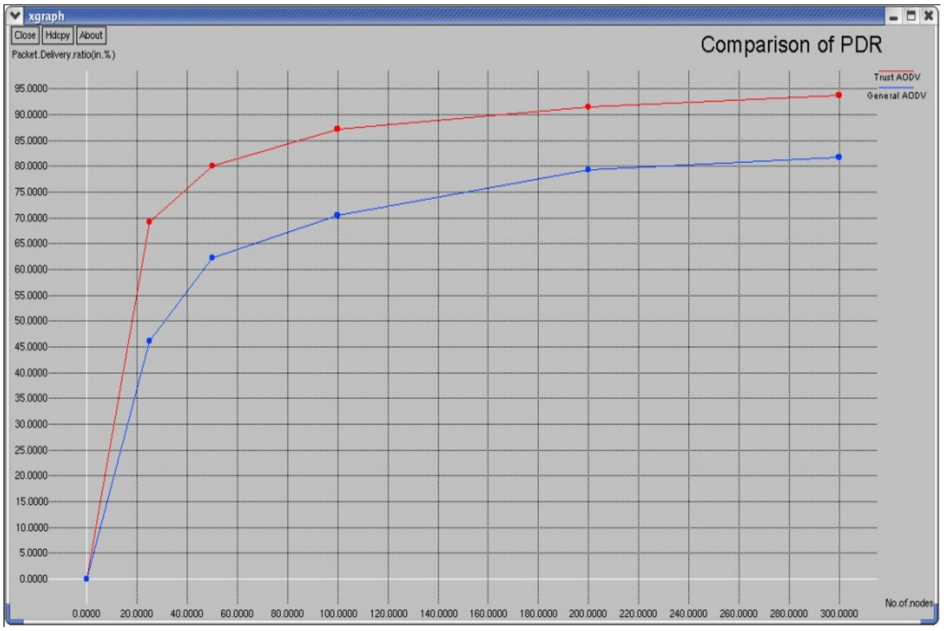

Figure 2. Comparison of general AODV PDR and Trusted ST-AODV PDR

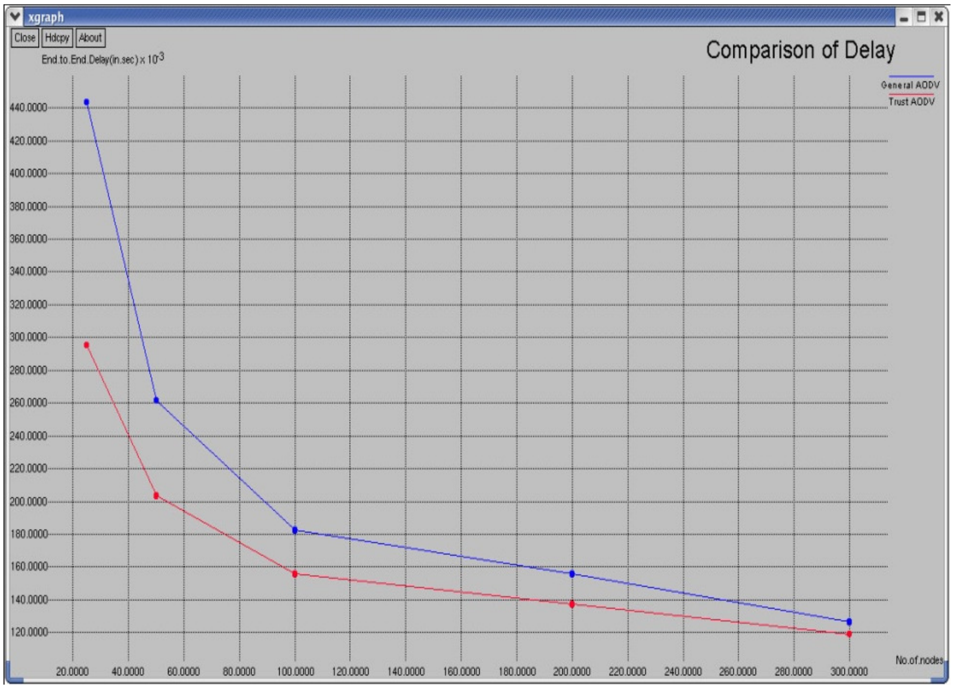

Figure 3. Comparison of general AODV Delay and Trusted ST-AODV Delay

5 Conclusion and future enhancements

In this paper a trusted ST-AODV protocol is proposed that identifies the nodes that drop packets during data transmission. Trust value for each node is calculated to spot the untrustworthy nodes in the path during routing. A node is declared as a trustworthy node if its trust value is greater than the threshold value thus resulting in a trustworthy MANET routing. This proposed scheme has shown a good development over Qos parameters like PDR and delay and has also provided trustworthy routing. The same scheme can also be implemented on other MANET routing protocols and check the performance with respect to Qos parameters. The future work may provide an encryption scheme for secured packet transmission and also to consider energy levels of the nodes participating in the routing to enhance reliability in MANET routing.

References

1. Kortuem.G., Schneider. J., Preuitt.D, Thompson .T.G.C, F'ickas.S. Segall.Z.: When Peer to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks. 1st International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001)
2. P Narayan, V R. Syrotiuk.: Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool. In: the proceeding of ADHOC-NOW in the year of 2004.
3. Charles E. Perkins, Elizabeth M. Belding Royer and Samir R. Das.: Ad-hoc On-Demand
   Distance Vector (AODV) Routing. Mobile Adhoc Networking Working Group, Internet
   Draft, February 2003
4. 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.
5. Pushpa, A.M.: Trust based secure routing in AODV routing protocol. In: IEEE International Conference (2009)
6. Hothefa Sh.Jassim, Salman Yussof.: A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network. In: IEEE 9th Malaysia International Conference on Communications (2009)
7. Mangrulkar, R.S.; Atique, M.: Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network. In: Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), 2010 .
8. R. S. Mangrulkar, Dr. Mohammad Atique.: Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network. 2010
9. Sharma, S.; Mishra, R.; Kaur, I.: New trust based security approach for ad-hoc networks. In: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.
10. Umuhoza, D, Agbinya, J.I, Omlin, C.W.: Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007.
11. Ferdous, R., Muthukkumarasamy, V., Sattar, A.: Trust Management Scheme for Mobile Ad-Hoc Networks. In: IEEE 10th International Conference on Computer and Information Technology (CIT), 2010.
12. Sridhar Subramanian, Baskaran Ramachandran: Trusted AODV for Trustworthy Routing in MANET in the Proceedings of the Second International Conference on Computer Science, Engineering and Applications (ICCSEA 2012) published by Springer (Advances in Computer Science, Engineering and Applications Volume 2, May 2012.

Sridhar Subramanian
Received the B.Sc. degree from the University of Madras, Chennai, India, Master of Computer Applications (MCA) degree from University of Madras, Chennai, India, Master of Philosophy (M.Phil.) degree from Periyar University, Salem, Tamil Nadu, India and pursuing Ph.D. (Computer Science) in Barathiyar University, Coimbatore, Tamil Nadu, India. Currently employed in the Department of Computer Applications, S.A. Engineering College, Chennai as Assistant Professor. The area of research is Qos routing in Mobile Ad hoc networks.