Volume: 02, Issue: 03, Pages: 679-685 (2010)

QoS for Real Rime Transmission on MANET

Chandra Mouli Venkata Srinivas Akana
Associate Professor, Department of CSE, AMC Engineering College, Bangalore-83., India.
Email:mouliac@yahoo.co.in
Sundeep Kumar K.
Asst. Professor, Department of ISE, A.M.C Engineering College, Bangalore-83., India.
Dr. C.Divakar
Professor & Principal, Visakha Institute of Technology, Visakhapatnam, AP,India
Phani Sirisha Katikireddy
Asst. Professor, Department of MCA, A.M.C Engineering College, Bangalore-83., India.

ABSTRACT
The Ad hoc network is set up with multiple wireless devices without any infrastructure. Its employment is favored in many environments[7]. Thus, many efforts are put in ad hoc networks at both the MAC and routing layers. Meanwhile, QoS aware issues are considered in both MAC and routing layers for ad hoc networks[3]. This work gives a review of ad hoc networks at both the MAC and routing layers. IEEE 802.11 is discussed and routing protocols widely used in ad hoc networks are analyzed and compared[1]. Solutions for QoS aware routing protocols are summarized. Evaluations are presented by doing simulations with both the QoS AODV and AODV routing protocols[8][10]. Thus, from the simulation results and analysis, it can be seen that adding QoS to routing protocols is meaningful to optimize the performance of traffic on the network especially the real time traffic[9][2].

Key words – AODV, IEEE 802.11, MAC, MANET, QoS

Date of Submission: March 31, 2010 Date of Acceptance: June 09, 2010

1. Introduction

In ad hoc networks, communications are done over wireless media between stations directly in a peer to peer fashion without the help of wired base station or access points. Lots of efforts have been done on ad hoc networks. One of the important and famous groups developing ad hoc networks is Mobile Ad-hoc network Group (MANET)[1]. With the popularity of ad hoc networks, many routing protocols have been designed for route discovery and route maintenance. They are mostly designed for best effort transmission without any guarantee of quality of transmissions. Some of the most famous routing protocols are Dynamic Source Routing (DSR) Ad hoc On Demand Vector (AODV) Optimized Link State Routing protocol (OLSR), and Zone Routing Protocol (ZRP). In MAC layer, one of the most popular solutions is IEEE 802.11.At the same time, Quality of Service (QoS) models in ad hoc networks become more and more required because more and more real time applications are implemented on the network. In MAC layer, IEEE 802.11e is a very popular issue discussed to set the priority to users[11]. In routing layer, QoS are guaranteed in terms of data rate, delay, and jitter and so on.

By considering QoS in terms of data rate and delay will help to ensure the quality of the transmission of real time media. For real time media transmission, if not enough data rate is obtained on the network, only part of the traffic will be transmitted on time[3]. There would be no meaning to receiving the left part at a later time because real time media is sensitive to delay. Data that arrive late can be useless. As a result, it is essential for real time transmission to have a QoS aware routing protocol to ensure QoS of transmissions. In addition, network optimization can also be improved by setting requirements to transmissions. That is to say, prohibit the transmission of data which will be useless when it arrive the destination to the network. From the routing protocol point of view, it should be interpreted as that route which cannot satisfy the QoS requirement should not be considered as the suitable route in order to save the data rate on the network[6][9]. The term bandwidth used by people who discussed the topic in the field of QoS aware routing protocols means data rate but not the physical bandwidth with the unit of Hertz[12]. People always used it not right. In this paper the term bandwidth that people usually misused is modified to data rate with the unit of bits per second.

2. Overview

2.1. History of Mobile Ad Hoc Networks

In early 1970s, the Mobile Ad hoc Network (MANET) was called packet radio network which was sponsored by Defense Advanced Research Projects Agency (DARPA). They had a project named packet radio having several wireless terminals that could communication with each other on battlefields[11]. .It is interesting to note that these early packet radio systems predate the Internet, and indeed were part of the motivation of the original Internet Protocol suite.

2.2. Applications of Mobile Ad Hoc Networks

A MANET is a dynamic multi-hop wireless network that is established by a group of mobile nodes on a shared wireless channel. Mobile ad hoc networks can be in military use, emergency use, wireless sensor networks and also can have mesh wireless network architecture.

2.2.1. Military applications

Use of ad hoc networks in military becomes more and more popular. Using ad hoc networks makes the setting up of communications between soldiers easy. In such applications, the used ad hoc networks need to be reliable and secure. The ability of multi-cast is required when the group leader in the army want to give order to all his soldiers.

2.2.2. Emergency operations

In emergency situation such as earthquakes, the wired networks could be destroyed. There will be a need of wireless network which could be deployed quickly for coordination of rescue[3].

An example is the design for future public safety communications. A European project called Wireless Deployable Network System (WIDENS) concentrated their work on this field. WIDENS have an idea that using ad hoc network to interoperate with existing TETRA network which is used for public safety. The system structure is shown in Fig. 2.1 .

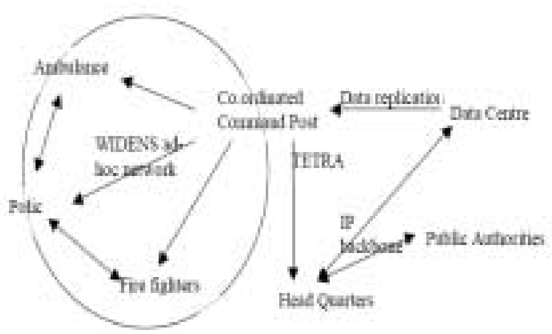


Fig. 2.1 WIDENS system structure

2.2.3. Wireless mesh networks

Wireless mesh networks are ad hoc wireless networks which are formed to provide communication infrastructure using mobile or fixed nodes/users. The mesh topology provides alternative path for data transmission from the source to the destination. It gives quick re-configuration when the firstly chosen path fails. Wireless mesh network should be capable of self-organization and self-maintenance. The main advantages of wireless mesh networks are high speed, low cost, quick deployment, high scalability, and high availability[10]. It works on 2.4 GHz and 5 GHz frequency bands, depending on the physical layer used. For example, if IEEE 802.11a is used, the speed can be up to 54 Mbps.

An application example of wireless mesh network could be a wireless mesh networks in a residential zone, which the radio relay devices are built on top of the rooftops. In this situation, once one of the nodes in this residential area is equipped with the wired link to the internet, this node could be the gateway node. Others could connect to the internet from this node. Other possible deployments are highways, business zones, and university campus.

IEEE 802.11 standard provides physical (PHY) and MAC layer solutions for wireless local area networks. With the popularity of IEEE 802.11 standard family used in laptops, and Personal Digital Assistants (PDAs), this standard is considered to be one of the solutions used in ad hoc networks. Especially in the simulations, IEEE 802.11 standard is used in ad hoc networks by most of the people.

2.3.1. IEEE 802 family

IEEE 802 specifications are focus on the data link layer and physical layer of the Open System Interconnection (OSI) reference model. Some of the main family members of IEEE 802 are listed in Table2.1.

Table 2-1 IEEE 802 Families

IEEE Standard	Network Definition	Known As
802.3	Wired Local Area Network	Ethernet
802.11	Wireless Local Area Network (WLAN)	Wi Fi
802.15.1	Wireless Personal Area Network (WPAN)	Bluetooth
802.15.4	Low Rate-Wireless Personal Area Network (LR-WPAN)	ZigBee
802.16	Wireless metropolitan area network (WMAN)	WiMax
802.20	Mobile Broadband Wireless Access (MBWA)	

3. QoS in different layers

QoS of a network can be considered at different layers. QoS considered in physical layer means the quality in terms of transmission performance. For example, through transmission power control both the stations that are near the sender or far away from the sender could hear the signal clearly with different transmission power. Power control is used both to ensure the quality of reception and to optimize the capacity. QoS implemented in MAC layer is also important. It could provide high probability of access with low delay when stations with higher user priority want to access the wireless medium.

3.1 QoS models

The existing QoS models can be classified into two types based on their fundamental operations. The QoS models are Integrated Service (IntServ) and Differentiated Services (DiffServ)[7]. IntServ is a fine grained approach which provides QoS to individual applications or flows. It uses Resource Reservation Protocol (RSVP) to provide a circuit switched service in packet switched network. IntServ decides whether the desired service could be provided with the current available network resource. Admission control is performed to new flows. The admission of each new flow might cause interference to the already existing flows. One of the responsibilities of admission control is that the interference caused by adding a new flow should not make QoS of old flows get worse than it has required. The drawback of IntServ is the scalability problem. This is caused by the need of storing every flow state in the routes. DiffServ provides QoS to large classes of data or aggregated traffic. It is a coarse grained approach. It maps flows into a set of service levels. In DiffServ, routers are divided into two types: edge routers and core routers. Edge routers are at the boundary of the networks. In edge routers, traffic will be classified, conditioned and assigned to different behavior aggregate when it traverse between different networks. The word different networks means for example networks that belong to different Internet Service Providers (ISP).

Differentiated Services Code Points (DSCP) bits are reformatted which represent the Type of Service (ToS) in Internet Protocol (IP) header. Core routers forward packets based on this ToS field. In addition, core routes also need to follow the per-hope behavior (PHB) which takes charge of scheduling of packets. IntServ eliminated the need of keeping the flow state information somewhere in the network.

4. Data rate calculations

4.1. Transmission range and carrier sensing range

To predict the available data rate at nodes, two ranges in wireless transmission have to be considered firstly. They are transmission range and carrier sensing range. The transmission range refers to the maximum separation between a sender and receiver for successful packet reception. Nodes within the transmission range of senders are called neighbors[4]. The carrier sensing range is a maximum distance between nodes within which nodes share data rate with each other. It means that, when the range between two nodes is over carrier sensing range, the power received by the receiver from the sender is below the threshold of the interference power.

Nodes outside transmission range of one node but within its carrier sensing range cannot successfully decode the packets from the node, whereas can detect them. Nodes inside a carrier sensing range are called carrier sensing neighbors. In wireless MAC protocol based on the CSMA mechanism, e.g. IEEE 802.11, all carrier sensing neighbors are unable to initiate packet when one node is transmitting because of the interference. That is, nodes in the carrier sensing range of sender share the data rate with the sender. The carrier sensing range will affect the reuse of the network resource. As a result, the relationship between carrier sensing range and transmission range affects the scheme of calculating the available data rate.

4.2. Locally available data rate

Locally available data rate is the data rate that a node itself could calculate. It should be the total data rate subtracted from the sum of the data rates used by it and others who are sharing data rate with it. In this part, the calculated available data rate referred is the locally available data rate.

Method 1 :

The first method is shown as follows:

Firstly, the ratio of time when the node is idle is calculated. It is normally calculated as the idle time in window divided by the window duration. Link utilization factor (μ) is the ratio of the busy time divided by the window duration. The window duration is the total time duration that used for observing. As a result (1-μ) is the ratio of time that the node is idle.

$$\mu = \frac{\text{Busy Time}}{\text{Window Duration}} \qquad \ldots(1)$$

When is the node busy? In IEEE 802.11 MAC, physical carrier sense and a virtual carrier sense are used to reserve the channel discussed in 2.3.5. Now these can be used to determine the free and busy times of the channel. If we consider the virtual carrier sensing method, the following conditions should be satisfied to change the mode between busy and idle.

The MAC layer claims that the channel becomes busy from idle when one of following occurs:

- NAV sets a new value
- Receive state changes from idle to any other state
- Send state changes from idle to any other state

The MAC layer detects the channel as idle when all the follows satisfy:

- The value of NAV is less than the current time
- Received state is idle
- Send state is idle

Secondly, the real data rate used for data transmission needs to be calculated, that is the throughput. It is the packet size (in terms of bits) that is going to be

Volume: 02, Issue: 03, Pages: 679-685 (2010)

transmitted divided by the time that is used to transmit these bits. Here, time used to transmit these bits not only include the time when channel is used for transmitting those data bits, but also include the time which is used to ensure the correct and non-collision transmission of theses bits. For example, we need this extra time to compete for the use of the resource when others want to transmit at the same time. They are used as in CSMA/CA and RTS/CTS as told in the previous part. The queuing time is the time the packet is waiting at the node, and if many traffic flows are routed via the same node, queuing time at this node will be relatively long.

The time used for transmitting S bits includes queuing time t_q at layer two of the OSI model, transmission time of S bits t_s, collision avoidance phase time (SIFS, DIFS) t_{CA}, the control overhead time (e.g. RTS, CTS) T-overhead, and back-off time T_B. In addition, R is the retransmission times. The throughput can be calculated from the following formula that is the total bits transmitted divided by the total time used for transmitting these bits.

$$Throughput_{packet} = \frac{S}{t_q + (t_s + t_{CA} + t_{overhead})*R + \sum_{r=1}^{R} B_T} \quad ...(2)$$

Then, the final available data rate for one node is the ratio of time that channel is idle during the last observing time multiply by the throughput as shown in the following formula.

$$Available\ Data\ Rate = (1-\mu)*Throughput_{packet} \quad …(3)$$

In this method, time used for contention by IEEE 802.11 MAC including SIFS, CTS, RTS, ACK are clearly taken into account. By considering these, the real data rate that could be achieved is obtained.

Method 2 :

The assumption for this method is that the transmission range is equal to the carrier sensing range. The available data rate of the node is calculated as the whole data rate minus the sum of data rate used for receiving at this node, transmitting and receiving at its neighbor nodes, showing as in the following formula. It tried to show when the node should be deemed as busy.

$$Available\ Data\ Rate_i = Data\ Rate_i - (\underbrace{Z_i}_{Case1} + \underbrace{\sum_{j\in N_i} Z_j}_{Case2} + \underbrace{\sum_{j\in N_i, k\notin N_i} x_{jk}}_{Case3}) \quad … (4)$$

Definitions of each part in the above equation is as follows:

Available Data Rate i is the total data rate at Node i.

Case 1 calculates the data rate used by Node i for receiving data.

Case 2 is the data rate consumed by neighbors who are receiving. j is the neighbor of Node i. It means when one of neighbors of i is receiving data, this node cannot send to prevent the hidden effect. In RTS/CTS mechanism, a node which receives RTS will reply CTS to the sender as well as all its neighbors in order to tell its neighbors that it will use the channel. It helps to prevent the hidden node effect.

Case 3 is the data rate consumed by neighbors who are sending. To be precise, since Node i can not send when its neighbors are sending traffic. Case 3 sums the data rate used by neighbors of Node i to send traffic. Data rate will not be counted in case 3, if both the transmitter and receiver are the neighbor of the node i, because this data rate consumption has been taken into account in Case2.

4.3. Listen Mode and Hello Mode

In the above three methods, the consumed data rate of one node is always considered to be calculated by the node itself. That is, nodes by listening to the channel judge how much data rate is used by others who are in its interference (carrier sensing) range. Another method is to estimate the residual data rate by getting information from exchanging Hello messages. The current data rate of the sender as well as the current data rate usage of the one-hop neighbors of the sender is piggybacked onto the standard Hello message Through Hello message nodes could know the data rate that is used by its carrier sensing neighbors.

The difference between these two modes can be seen as follows. What the node hears in listen Mode is the packets including RTS, CTS, ACK, retransmissions and routing packets, whereas, hello Mode only counts the transmitted packets. That is the total number of bits what the node hears from the neighbors in Listen Mode is a little bit more than the total number of bits that the node is told by received Hello Messages. This should be paid attention to during the designs of QoS aware routing protocol.

4.4. Real available data rate of one node

No matter which method we use, the calculated available data rate for this node is not the actual available data rate for this node. The available data rate of one node should be the minimum of the available data rate and its carrier sensing neighbors because the available data rate that is allowed to be used for transmission should not deprive the reserved data rate of any existing flows in its carrier sensing range.

4.5. Admission control mechanisms

With the information of the available data rate at the nodes, it is still not simply to compare the available data rate at node and the required data rate for one traffic when deciding the node satisfy the requirement. We have to check if the given flow fits or not into the n-hop route. Here we need the Call Admission Control (CAC) during the path discovery process. The following two methods of admission control mechanisms are designed based on the AODV routing protocol. A different ratio of carrier sensing range to the transmission range leads to the following different methods

Method 1.

The assumption of this method is that the transmission range is equal to the carrier sensing range. This method can be used together with the second method of available data rate calculation. The rule will be firstly stated and then an example will be shown With a N-hop route, the source and destination nodes should satisfy ABi>=2r, the second and N-1 node ABi >=3r and the intermediate nodes ABi >=4r. Here, r is the required data rate requirement and ABi is the available data rate at node i. N-1 node is the node on the path which is next to the destination node.

Example with four hops route (Table 4-1 and Fig. 4.1): with intra flow from Node A to Node E, Node A will first take the role of transmitting, and when Node B is transmitting, Node A which heard the RTS of Node B has to be shut up because they shared channel with each other. As a result, only when Node A has twice of the data rate can this traffic be transmitted according to the required data rate to ensure the continuous transmission. The following table gives an example of the role of each node at each hop. Sender/Receiver means the node is taking the role of sender or receiver at this hop. RTS/CTS means the node is the neighbor of the transmitter or the receiver who receives RTS or CTS when its neighbor is sending or receiving. Finally, total times of the data rate needed for a flow are summed. The result is exactly as the formula shown in the above paragraph.

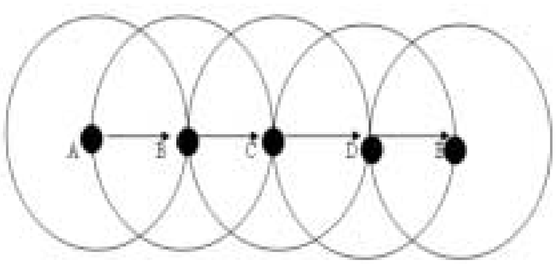


Fig. 4.1 Example of QoS with admission control (1)

Table 4.11 Example of QoS with admission control (1)

	A	B	C	D	E
Hop1	Sender	Receiver	CTS	-	-
Hop2	RTS	Sender	Receiver	CTS	-
Hop3	-	RTS	Sender	Receiver	CTS
Hop4	-	-	RTS	Sender	Receiver
Total	2	3	4	3	2

In this example, to get RREP from Node E to Node A, Node A and Node E which are source and destination node, should have at least twice of the required data rate. Node B and D should have at least 3 times of the required data rate, and Node C should have at least four times of the required data rate.

With this example, the route searching process in QoS based AODV protocol is according to the following steps. If Node A wants to send traffic to Node E, Node A first generates a RREQ, all the neighbor who are in transmission range of Node A will hear it, and since here a simple line structured topology is assumed, only Node B hear this RREQ.
Node B will first check whether it has enough data rate to satisfy requirement of the RREQ, that is, compare available data rate of Node B with required data rate of the RREQ. Only if Node B has enough data rate, it will broadcast RREQ further. The same step is done at Node C and D until the destination of the RREQ: Node E is reached. Node E should know that he is the destination node itself. Then according to the rule of access control, Node E will initiate RREP when it has twice of the required data rate. When RREP arrive Node D, D will check whether it has 3 times of the available data rate. If satisfied, it forwards this RREP further, the same access control mechanism is taken until Node A receive this RREP, then a successful route discovery is finished. How does the node know the position of itself during the flow? During route request and route reply message process, the hop count number should be remembered at each node for every session in order to know the position of each node on the path. That is because this information is needed for the admission control mechanism as it is discussed right in the previous part.

Method 2 :

To provide a good estimation for intra flow contention, a parameter called Contention Count is introduced in this method. The value of this parameter will help to determine the actual required data rate at each node during an intra flow transmission as it is told in method 1.In this method, the carrier sensing range is assumed to be more than twice of the transmission range. It means that the nodes which are one hop or two hops away from the transmitter will get the interference and cannot use the channel. In other word, a node will share channel with others which are one hop and two hops away. Considering one flow which goes through multiple hops, the node has to consider the interference from one hop and two hops upstream and downstream nodes. It is possible that the three hops away node could also gives interference to this node, on the other side, it is also possible that the third hops away nodes have already been out of the carrier sensing range. In this method, people only consider the interference coming from nodes which are one hop and two hops away. It brings some imprecise factors since the nodes which are three hops away could also be in the carrier sensing range. The contention count is calculated as follows

$$\text{If } h_{req} > 2 \rightarrow h_{req} = 2$$
$$\text{If } h_{rep} > 3 \rightarrow h_{rep} = 3$$
$$CC = h_{req} + h_{rep}$$

…(5)

The h_{req} and h_{rep} in the .if. sentence mean the number of the hop count from source node to this node. h_{req} and h_{rep} at the right side of the arrows are the weight of upstream and downstream nodes of interference. An example is showed to explain this idea in a clear way.

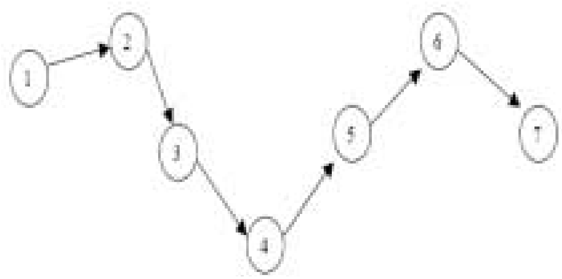


Fig. 4.2 Example of QoS with admission control (2)

There is a flow intended from Node 1 to Node 7. Take Node 4 for example. h_{req} is 3 and h_{rep} is 3. CC = 2 + 3 = 5 according to the formula. Table 4-2 shows how each CC at each node is calculated out by showing the details. CS means that the node is in the carrier sensing range of some other node that is transmitting. For example, at the 3rd hop, Node 3 is transmitting packets to Node 4, Node 1, 2 and 4 will get the interference and the channel for Node 1, 2 and 4 should be set as busy since they share channel with Node 3.

Table 4.2 Example of QoS with admission control (2)

	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7
Hop 1	Sender	Receiver	CS				
Hop 2	CS	Sender	Receiver	CS			
Hop 3	CS	CS	Sender	Receiver	CS		
Hop 4		CS	CS	Sender	Receiver	CS	
Hop 5			CS	CS	Sender	Receiver	CS
Hop 6				CS	CS	Sender	Receiver
	3	4	5	5	4	3	2

The CC value is counted along the way of the RREP message. Only when the available data rate of the node is larger than CC multiplied by the required traffic rate, the RREP will be unchaste further towards the source node. As a result, the RREP which arrive the source node finally has found a route which has enough data rate for the traffic session.

5. Conclusions

Based on the simulation, it is found that packets could get less end to end delay with a QoS aware routing protocol when the traffic on the network is high. This low end to end delay is meaningful for real time transmissions. When the traffic is relatively high on the network, not all the routes that are found by the AODV routing protocol have enough free data rate for sending packets ensuring the low end to end delay of each packet. As a result, the QoS AODV protocol works well and shows its effects when the traffic on the network is relatively high. People who work on the area of ad hoc networks with the aim of improving the QoS for ad hoc networks can get benefit from reading this thesis. For this QoS AODV routing protocol, problems would rise when the node density of the network is high. The reason is that the QoS AODV routing protocol uses the Hello message to exchange information between neighbors. When the node density is too high, the sending of Hello messages will cost much available data rate. As a result, the network will be ruined and traffic will be delayed more since Hello messages have higher priority than data packets. To conclude, it is predicted that the QOS AODV will not work well in high density ad hoc networks.

References

[1] C. Siva Ram Murthy and B.S. Manoj .Ad hoc wireless networks Architectures and Protocols,. Prentice Hall, 2004.

[2] Wireless Deployable Network System: www.widens.org, visited 2007-10-22.

[3] Handouts of Helsinki University of Technology course: Wireless Personal, Local, Metropolitan, and Wide Area Networks
www.comlab.hut.fi/studies/3240/index.html, visited 2007-10-20.

[4] Gu, D; Zhang, J., "QoS Enhancement in IEEE802.11 Wireless Local Area Networks", IEEE Communications Magazine, ISSN: 0163-6804, Vol. 41, Issue 6, pp. 120-124, June 2003.

[5] OSPF relevant lecture slides from Helsinki University of Technology: http://keskus.hut.fi/opetus/s382121/s05/Slides/S2121-04-LS-e.pdf, visited 2007-11-25.

[6] R. Guerin, A. Orda, D. Williams .QoS Routing Mechanisms and OSPF Extensions, August, 1999, Network Working Group, Request for Comments: 2676.

[7] S. R. Das, C. E. Perkins, E. M. Royer, and M. K. Marina. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. INFOCOM

2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume 1, 26-30 March 2000 pp. 3 - 12.

[8] QoS relevant lecture slides from Helsinki University of Technology: http://keskus.hut.fi/opetus/s382121/s05/Slides, visited 2007-10-22

[9] H. Badis and K. Al Agha, Quality of Service for Ad hoc Optimized Link State Routing Protocol (QOLSR) IETF-63 Meeting : Internet Engineering Task Force, draft badis-manet-qolsr-02.txt, Vancouver, Canada, November 2005. Draft IETF

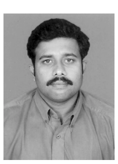
[10] C. E. Perkins, E. M. Royer, S. R. Das, .Quality of Service for Ad hoc On-Demand Distance Vector Routing,. draft-perkins-manet-aodvQoS-02.txt, IETF Internet Draft, work in progress, October 2003.

[11] NS manual http://www.isi.edu/nsnam/ns/ns-documentation.html, visited 2008-01-12

[12] Leiming Xu, Bo Pang, Yao Zhao, .NS and network simulation. POST &TELECOM PRESS, 2003.

Authors Biography

Chandra Mouli Venkata Srinivas Akana received the Masters Degree in Computer Science & Engineering from Guru Jambheshwar University Of Science & Technology, Hisar, Haryana, India. He is currently working as Associative Professor in the Department of Computer Science & Engineering, AMC Engineering College, Bangalore, Karnataka, India. His current research is focused on Software Engineering, Ad-hoc Networks, Network Computing & Security, Data mining & Warehousing and Database Management System. He has published several papers in National & International Journals. He has guided to more than 60 academic projects at Postgraduate & under Graduate level. He is a member of the IEEE, CSI & ISTE.



K Sundeep Kumar received the M.Tech (IT) from Punjabi University in 2004, and ME (CSE) from Anna University in 2009. He is with the department of Information Science & Engineering and as an Asst. Professor, and as a Placement Officer, AMC Engineering College, Banglaore. He presented more than 10 papers in International and national Conferences. His research interests include OOAD, Software Engineering and Data Warehousing. He is a member in ISTE.

Dr. Divakar C. received his Masters Degree as well as Doctorate in Computer Science & Engineering from Andhra University, Visakhaptnam, and Andhra Pradesh, India. He is currently working as Professor & Principal for Visakha Institute of Technology, Visakhapatnam, Andhra Pradesh, India. He is guiding six Ph.D. research Scholars. His current research is focused on Bio-informatics, Software Engineering, Ad-hoc Networks, Network Computing, Image Processing & Database Management System. He has published several papers in National & International Journals. He has guided several academic projects at Postgraduate & under Graduate level.

Phani Sirisha K. received the Masters Degree in Computer Applications from Andhra University, Visakhapatnam, Andhra Pradsh, India. She is currently working as Assistant Professor in the Department of Master of Computer Applications, AMC Engineering College, Bangalore, Karnataka, India. Her current research is focused on Software Engineering, Ad-hoc Networks, Network Computing, Image Processing & Database Management System. She has guided to more than 25 academic projects at Postgraduate level.