EVALUATION OF QUALITY OF SERVICE PARAMETERS AND PERFORMANCE OF WIRELESS AD HOC NETWORKS

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

in

PAPER TECHNOLOGY

by

KUMAR MANOJ

DEPARTMENT OF PAPER TECHNOLOGY
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
SAHARANPUR CAMPUS
SAHARANPUR - 247001 (INDIA)

JUNE, 2010

ACKNOWLEDGEMENT

I feel expedient to express my profound indebtedness & deep sense of gratitude and sincere thanks to Dr. S.C. Sharma, Associate Professor, Department of Paper Technology (Indian Institute of Technology-Roorkee), Saharanpur and Dr. S.P. Singh, Associate Professor Department of Paper Technology (Indian Institute of Technology, Roorkee), Saharanpur, for their valuable guidance, inspiration, encouragement and whole hearted co-operation in understanding the relevant field and help in presenting this work. Their keen interest and efforts in planning the work in this form can not be expressed in words, as they devote their valuable time in discussions and in critical analysis of the work. I am highly obliged to them. It is a great opportunity to express my respect and gratitude to Dr. Mohan Lal, Assistant Professor, ICC, IIT Roorkee for all his valuable guidance, inspiring discussions, and overall motivation during my Ph.D. I would also like to thank Dr. S.C. Gupta (Emeritus Professor), for providing me with valuable suggestions and guidance during my study. I am extremely grateful to Dr. Satish Kumar, Professor and Head, DPT, IIT Roorkee, Saharanpur Campus for providing necessary administrative help for carrying the work. The author is also thankful to Prof. J.S. Upadhayaya (Ex-HOD), Prof. M.C. Bansal (Ex-DRC Chairman) and Prof. A.K. Singh, chairman, DRC, DPT, IIT Roorkee, Saharanpur campus whose co-operation and encouragement helped a great deal in this endeavor. I am also thankful to research colleague Dr. S. Quamar, Dr. A. K. Jain, Parmanand, Santosh Kumar, Mussurat Ali, Ms. Leena Arya, Sandip Vijay and Vishal Gupta for providing me necessary help to complete this work. I am also thankful to my colleagues, Ramakrishna & Vrince Vimal for inspiring me and providing necessary support to complete this work.

I would like to express my sincere thanks and regards to Dr. Chhaya Sharma, Asstt.Prof, DPT, IIT Roorkee, Saharanpur campus and her family for giving me morale support and inspiration from time to time.

It is my pleasant duty to acknowledge my thanks to all my well wishers, employees of D.P.T, Saharanpur (Since it is not possible to mention all the names), who support, and inspired me through their love and regards directly or indirectly. I am also thankful to management of College of Engineering Roorkee for proving me necessary help and support to present this work. No words, no language is ever adequate to express my heartfelt veneration for my respected parents Shri B.B. Srivastava, Smt. Gayatri Srivastava, my brother Kumar Santosh, Kumar Prashant, my sister Bharti, Arti and Prapti, my wife Mrs. Vijayanka and my son Mr. Siddha, and all my family members for their cheerful, enthusiastic and dedicated efforts to engage myself in high pursuits.

Above all, I praise the almighty 'God' for his blessings.

Dated: June, 2010 (Kumar Manoj)

ABSTRACT

A wireless Ad-hoc network consists of wireless nodes communicating without the need for a centralized administration, in which all nodes potentially contribute to the routing process. A user can move anytime in an ad-hoc scenario and, as a result, such a network needs to have routing protocols which can adapt dynamically changing topology. To accomplish this, number of ad-hoc routing protocols have been proposed and reported in the literature. The ad-hoc networking has been receiving continuous attention from the wireless research community.

In recent years several routing protocols have been proposed for mobile ad-hoc networks (MANETs), prominent among them are DSDV (destination sequenced distance vector), AODV (ad-hoc on-demand distance vector) and DSR (dynamic source routing) protocols. Considerable amount of simulation work have been reported in the literature to measure the performance of these routing protocols with identical traffic load and mobility patterns. Due to constant changing nature of these protocols, a new performance evaluation for quality of service (QoS) parameters with different traffic load and mobility conditions is essential.

In this work, the performance of commonly used ad-hoc network routing protocols with different traffic load and mobility patterns have been compared using OPNET/ns2 simulators. For validation, the simulated results have been compared with the experimental data available in the literature. The effect of QoS parameters on congestion nodes has been evaluated. To avoid congestion using modification of IEEE 802.11 MAC layer parameters and fuzzy technique have been proposed. The bandwidth control management routing algorithm have been developed and analyzed.

Objective of the Present Work

The objective of the present work is to analyze the performance of various routing protocols in terms of different QoS parameters such as throughput, end-to-end delay, retransmission, control traffic received and sent, data traffic received and sent, no. of loads, mobility, and bandwidth in wireless ad hoc network.

The work carried out is divided into:

- The assessment of impact of varying load on various QoS parameters for different protocols (AODV, DSR & DSDV) in wireless ad-hoc network and comparison of the simulated result with the reported experimental data.
- The assessment of effect of congestion on QoS parameter for routing protocol (AODV) using IEEE 802.11 MAC layer parameter & fuzzy approach.
- Performance analysis of proposed bandwidth control management for wireless ad hoc networks.

The assessment of effect on QoS parameters of static & dynamic networks for different protocols

The protocols reported in literature are constantly being improved by Internet Engineering Task Force (IETF). As a result, a comprehensive performance evaluation of ad-hoc routing protocols essential. In this work, a comparative performance evaluation has been carried out in terms of different QoS parameters for recently reported protocols such as (AODV, DSDV, DSR etc.).

The simulation analysis has been carried out for different protocols in terms of different QoS parameters of wireless ad-hoc networks. The work is extended to see the effect of protocols like DSDV, AODV and DSR with the static nodes, keeping the same scenarios reported by H. Hallani for the analysis of throughput and delay. Further the analysis has been carried out for dynamic behavior of the network (by giving mobility) for AODV protocol. We analyze the effect of throughput for different protocols of different scenario and for validation the results are compared with experimental data of AODV protocol.

The assessment of effect of congestion on QoS parameters for routing protocol (AODV) using IEEE 802.11 MAC layer parameters & fuzzy approach

Congestion is an unwanted situation in networked systems, where the part of the network is being offered more traffic than its rated (desired) capacity. Effects of congestion include drastic drops in network throughput, unacceptable packet delays, session disruptions and other various causes such as uncertainty, randomness and fuzziness. QoS guarantees for real time application or multimedia application require high throughput, low delay and jitter. These QoS guarantees can be achieved by controlling MAC layer parameters.

In the research work, the congestion analyses have been carried out in terms of delay, glob load, throughput, packet drop, media access delay. The performance of the network will be enhanced by modification or variation of MAC layer parameters i.e. DIFS and contention window. Further fuzzy based scheme has been proposed to improve the performance of the network in terms of average throughput, packet delivery ratio and end-to-end delay. The input parameters such as buffer occupancy, data rate and expiry time to find the priority index has been taken for analysis. The performance evaluation has been analysed under different load and mobility conditions using OPNET/ns-2 simulator.

Performance analysis of proposed bandwidth control management for wireless ad-hoc networks

Multimedia communications include video conferencing, video-on-demand, multimedia learning, distant learning programs etc. Each of the services request for different amount of bandwidth based on quality of service requirements. The popularity of wireless ad-hoc networks has made bandwidth a demanding parameter. There is a pressing need to develop efficient bandwidth allocation routing scheme which increases the call acceptance probability, reduces call dropping probability and increases the network bandwidth utilization.

In this work, the routing algorithm has been proposed in BWCM (bandwidth control management) model for bandwidth allocation and reservation of ad-hoc networks for both real and non real time application. The proposed algorithm establish the path between sources to destination and also create standby route during disconnect the primary path. The QoS parameter has been analyzed in terms of end-to-end delay, throughput, rerouting, packet loss, and total number of connection, percentage of different path and probability of enough bandwidth. The performance in various QoS traffic flows have been examined through ns2 simulator under different mobility condition.

CONTENTS

LIST OF ACRONYMS

ACK	Acknowledgment
ALM	Application layer metrics
AODV	Ad hoc On-demand Distance Vector Routing
AP	Access point
ARQ	Automatic repeat request
ATM	Asynchronous Transfer Mode
BB	Black-Burst
BER	Bit error rate
BS	Base station
BSS	Basic Service Set
BWA	Broadband wireless access
BWCM	Bandwidth control management
CBR	Constant bit rate
CBWFQ	Class-based weighted fair queuing
CC	Channel Capacity
CDMA	Code division multiple access
CEDAR	Core-Extraction Distributed Ad hoc Routing
CQ	Custom queuing
CSMA/CA	Carrier sense multiple access/ collision avoidance

CTS	Clear-To-Send
CW	Contention window
DCF	Distributed Coordination Function
DIFS	Differentiation Inter Frame Spacing
DLC	Data link layer
DR	Data rate
DS	Distribution system
DSDV	Destination sequenced distance vector
DSR	Dynamic source routing
DSSS	Direct sequence spread spectrum
ESS	Extended service set
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEC	Forward error correction
FHSS	Frequency hopping spread spectrum
FIFO	First in first out
FQMM	Flexible QoS Model for MANET
GHz	Giga hertz
HCF	Hybrid coordination function
IAPP	Inter access point protocol
IBSS	Independent Basic Service Set

IEEE	Institute of Electrical & Electronics Engineering
IETF	Internet Engineering Task Force
IF	Intermediate frequency
IMP	Inter-modulation products
IP	Internet Protocol
IR	Infra Red
ISM	Industrial, scientific, medical
LAN	Local Area Network
LLC	Logical link control
MAC	Medium Access Control
MACA/PR	Multiple Access Collision Avoidance with Piggyback Reservation
MANET	Mobile ad hoc network
Mbps	Mega bit per second
MHz	Mega hertz
MLM	MAC layer metrics
NLMs	Network layer metrics
NS-2	Network Simulator-2
OFDMA	Orthogonal Frequency Division Multiple Access
OPNET	Optimized Network Engineering Tools
OSI	Open system interconnection
OSI	Open system interconnection

PCF	Optional Point Coordination Function
PDA	Personal digital assistant
PHB	Per-hop forwarding behaviours
PHY	Physical layer
PKT	Packet
PLR	Packet loss ratio
PMP	Point-to-multipoint
PQ	Priority queuing
QoS	Quality of Service
RF	Radio frequency
RREP	Route reply
RREQ	Route request
RSVP	Resource Reservation Protocol
RT	Reservation table
RTP	Real-Time Protocol
RTS	Request-To-Send
SINR	Signal-to-interference plus noise power ratio
SS	Subscriber stations
STA	Stations
TCP	Transfer Control Protocol
TDD	Time Division Duplex

TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
WDS	Wireless Distribution System
WFQ	Weighted fair queuing
Wi-Fi	Wireless-Fidelity
WiMAX	Worldwide interoperability for microwave access
WLAN	Wireless Local Area Network
WRR	Weighted Round-Robin

LIST OF FIGURES

LIST OF TABLES

Packet delivery ratio: Packet delivery ratio is the ratio of the number of data packets actually delivered to the destination to the number of data packets supposed to be received. This number presents the effectiveness of the protocol.

Average end-to-end delay: This indicates the end-to-end delay experienced by packets from source to destination. This includes the route discovery time, the queuing delay at node, the retransmission delay at the MAC layer and the propagation and transfer time in the wireless channel.

Throughput: This is average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per seconds (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Retransmission: It is the resending of packets which have been either damaged or lost. It is a term that refers to one of the basic mechanisms used by protocols operating over a packet switched computer network to provide reliable communication (such as that provided by a reliable byte stream for example TCP)

Delay: It refers to a lapse of time.

Latency: Latency is a measure to time delay experienced in a system, the precise definition of which depends on the system and the time being measured.

Jitter: In computer networking, packet delay variation is the difference in end-to-end delay between selected packets in a flow with any lost packets being ignored. The effect is sometimes, incorrectly, referred to as jitter.

REFERRED INTERNATIONAL/NATIONAL JOURNALS

1. ***Kumar Manoj***, S. C. Sharma & S.P. Singh, "Impact of Throughput in MANET for Static & Dynamic Network For IEEE 802.11" ***IEEE Journal on Selected Area in Communication*** *(Communicated, Jan. 2010)*
2. ***Kumar Manoj***, Parma Nand, S. C. Sharma & Leena Arya " Fuzzy Based QoS Analysis in MANET for DSR Protocol" ***IJCITE - International Journal of Computers, Information Technology and Engineering***, Vol. 3, no.1, pp. 33-38, Jan.-June 2009.
3. ***Kumar Manoj***, S. C. Sharma & Parmanand "Analysis of Bandwidth Control Management in Wireless Ad hoc Network" ***International Transactions on Computer Science and Engineering, USA,*** *Vol.* 53, no. 1, pp. 147-161, April 2009.
4. ***Kumar Manoj***, S. C. Sharma, Parmanand & S.P. Singh "Scheduler Based QoS Analysis in MANET For DSR Protocol" ***International Journal of Recent Trend in Engineering*** (Computer Science)*", Finland,* Vol.1 (2), pp. 100-102, June 2009.
5. S.C. Sharma, ***Kumar Manoj*** & Leena Arya "Performance Analysis of Power in Mobile Ad hoc Network for Different Protocols" ***International Journal of Computing Science & Communication Technologies"*** Vol. 2, no. 1, June 2009.
6. ***Kumar Manoj***, Parma Nand, S. C. Sharma & Leena Arya " Fuzzy Based QoS Analysis in MANET for DSR Protocol" ***International Journal of Computers, Information Technology and Engineering***, Vol. 2, No.1, pp. 33-38, April 2009.
7. ***Kumar Manoj***, S.C. Sharma & Mohan Lal "Performance Analysis of QoS through Fuzzy-Based Scheduler in MANET" ***Icfai Journal of Electrical & Electronics Engineering***, Vol 2, No. 2, pp. 56-66, April 2009.

8. ***Kumar Manoj*** & S.C. Sharma "Trade-off of Various QoS Parameter in Wireless Adhoc Network for Different Protocols" ***International Journal of Information of Computer Application in Engg. Tech. and Sciences*** Vol. 1(1), pp. 83-92, 2008.

9. ***Kumar Manoj*** & S.C. Sharma "Impact on Throughput and Delay Analysis in Wireless Ad-Hoc Network IEEE 802.11b" ***IEC Journal of Annual Review of Communication, International Engineering Consortium, USA***. Volume 61, pp. 317-325, December 2008.

10. A.K. Jain, S.C. Sharma, R. Jha & ***Kumar Manoj*** "Effect of congestion on the performance of IEEE 802.11 network" ***Int. J. Information and Communication Technology, USA,*** Vol. 1(3/4), pp. 318-328, 2008.

11. ***Kumar Manoj***, S. C. Sharma & Parmanand "Design and Analysis of BWCM Model for Wireless Ad-hoc Networks" ***International Journal of Computer science & Network Security,*** *USA,* Vol. 8 No. 11, pp. 416-422, November, 2008.

12. ***Kumar Manoj***, S.C. Sharma & A.K. Jain "Analysis of Impact of Random Loss In Mobile Ad-Hoc Networks" ***International Journal of Hybrid Computational Intelligence*** Vol.1, No.2, pp. 197-203, July-December 2008.

13. ***Kumar Manoj***, S.C. Sharma & A.K. Jain "Effect of QoS Parameter in Wireless Ad-Hoc Network (IEEE 802.11b)" ***International Journal of Hybrid Computational Intelligence,*** Vol. 1, No.2, pp. 197-203, July-December 2008.

14. ***Kumar Manoj***, S.C. Sharma & A.K. Jain, "Analysis and Effect of Delay & Throughput in Mobile Ad-hoc Network (IEEE 802.11b) for AODV Protocol" ***Journal of Cooperation among University, Research and Industrial Enterprises*** *(CURIES),* Vol. 1. No. 2, pp. 16-22, July 2008.

15. ***Kumar Manoj***, S.C. Sharma & A. K. Jain "An Analysis of throughput management in wireless ad hoc network" ***National Journal of IT & Management***, Vol. 2 no. 1 pp. 54-60, Oct. 2008.

INTERNATIONAL/NATIONAL CONFERENCES

1. ***Kumar Manoj***, S.C. Sharma & S.P. Singh, ""Performances Analysis of Tahoe and Reno TCP variant in MANET using Random Noise variable" International Multiconference on Intelligent Systems & Nanotechnology (IISN-2010), pp. 479-483, Feb. 26-28, 2010.
2. ***Kumar Manoj***, S.C. Sharma & S.P. Singh "Dynamic Behavior of Bandwidth Control Management in Mobile Ad-Hoc Network" Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. I, pp. 229-235, WCECS 2009, October 20-22, 2009, ***San Francisco, USA***.
3. ***Kumar Manoj***, Parmanand, S.C. Sharma & S.P. Singh "Performance of QoS Parameter in Wireless Ad hoc Network (IEEE 802.11b)" Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. I, pp. 280-284, WCECS 2009, October 20-22, 2009, ***San Francisco, USA***.
4. ***Kumar Manoj***, S.C. Sharma & Leena Arya "Fuzzy Based QoS Analysis in Wireless Ad hoc Network for DSR Protocol" IEEE International Advance Computing Conference ***(IACC'09)***, Thapar, pp. 3428-3432, 6-7 March 2009.
5. ***Kumar Manoj***, S.C. Sharma & Leena Arya "Effect of Throughput Management in MANET (IEEE-802.11)" 3rd International Conference on Intelligent Systems and Networks *(IISN-2009)*, pp. 346-350, Feb. 14-16, 2009.

HONORS' & BEST PAPER AWARD

2007: [***Kumar Manoj***, S.C. Sharma and Sandip Vijay, "Energy Efficient parameters for controlling physical layer of mobile ad-hoc networks"] National Conference on Emerging Technologies in Computer Science (ETCS-2007) held at MIET, Meerut, Sept. 2007 (AICTE- New Delhi).

2008: [***Kumar Manoj*** & S.C. Sharma, "Simulation-Based Analysis of Impact of Random Loss"] First International Conference on Emerging Trends in Engineering & Technology, July 2008, IEEE Computer Society USA.

2008: [S.C. Sharma, ***Kumar Manoj*** & Leena Arya, "Performance Analysis of Power in Mobile Ad hoc Network for Different Protocols"] 3rd International Conference on Advance Computing & Communication Technology, November 2008, APIIT, Panipat, India.

2010: [***Kumar Manoj,*** Kumari Arti & S. C. Sharma "Simulation Based Analysis of Delay & Throughput in MANET (IEEE 802.11b) for TORA Protocol"] National Conference on Advance in Microwave Communication, Devices & Applications held at JIET, Jaipur, Feb. 16, 2010, IEEE MTT-S INDIA COUNCIL.

15. ***Kumar Manoj***, S.C. Sharma & A. K. Jain "An Analysis of throughput management ir wireless ad hoc network" ***National Journal of IT & Management***, Vol. 2 no. 1 pp. 54-60 Oct. 2008.

INTERNATIONAL/NATIONAL CONFERENCES

1. ***Kumar Manoj***, S.C. Sharma & S.P. Singh, ""Performances Analysis of Tahoe and Renc TCP variant in MANET using Random Noise variable" International Multiconference or Intelligent Systems & Nanotechnology (IISN-2010), pp. 479-483, Feb. 26-28, 2010.
2. ***Kumar Manoj***, S.C. Sharma & S.P. Singh "Dynamic Behavior of Bandwidth Control Management in Mobile Ad-Hoc Network" Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. I, pp. 229-235, WCECS 2009, October 20-22, 2009, ***San Francisco, USA***.
3. ***Kumar Manoj***, Parmanand, S.C. Sharma & S.P. Singh "Performance of QoS Parameter in Wireless Ad hoc Network (IEEE 802.11b)" Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. I, pp. 280-284, WCECS 2009, October 20-22, 2009, ***San Francisco, USA***.
4. ***Kumar Manoj***, S.C. Sharma & Leena Arya "Fuzzy Based QoS Analysis in Wireless Ad hoc Network for DSR Protocol" IEEE International Advance Computing Conference ***(IACC'09)***, Thapar, pp. 3428-3432, 6-7 March 2009.
5. ***Kumar Manoj***, S.C. Sharma & Leena Arya "Effect of Throughput Management in MANET (IEEE-802.11)" 3rd International Conference on Intelligent Systems and Networks *(IISN-2009)*, pp. 346-350, Feb. 14-16, 2009.

6. ***Kumar Manoj***, S.C. Sharma & Leena Arya "Analysis of QoS Parameter in MANET for Different Scenario" International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT 2009) from 14th-16th March 2009.

7. ***Kumar Manoj***, Parmanand, S.C. Sharma & Leena Arya "Simulation Based-Effect & Analysis of Throughput in Wireless Ad-hoc Network" ***Proceedings of the*** INTERNATIONAL CONFERENCE ON VLSI AND COMMUNICATION ENGINEERING *(ICVCom-2009)*, Kottayam, pp. 33-38, 16^{th}-18^{th} April 2009.

8. ***Kumar Manoj***, S. C. Sharma & S.P. Singh "Adaptive Analysis of Throughput in Mobile Ad-hoc Network (IEEE-802.11)" National Conf on Cutting Edge Computer and Electronics Technologies-$(CE)^2T$, Pantnagar, pp. 388-391, 14-16^{th} Feb. 2009.

9. A.K. Jain, S.C. Sharma, ***Kumar Manoj***, R. Jha "Effect of Congestion on the Global Performance of IEEE 802.11 Network" International Conference on "Intelligent Systems and Networks" *(ISN-2008)*, ISTK Haryana, pp. 231-235, 22-24^{th} Feb. 2008.

10. ***Kumar Manoj***, S.C. Sharma, Sandip Vijay and Amit Dixit "Performances Analysis of Wireless Ad-hoc Network Using OPNET Simulator "International Conference on Intelligent Systems and Networks, ISTK Haryana, pp. 267-270, 22-24^{th} Feb. 2008.

11. ***Kumar Manoj*** & S.C. Sharma, "Simulation-Based Analysis of Impact of Random Loss" First International Conference on Emerging Trends in Engg. & Tech. *(ICETET-08)*, Nagpur, IEEE Computer Society Press, pp. 828-833, 16-18^{th}July, 2008.

12. A.K. Jain, ***Kumar Manoj*** & S.C. Sharma, "Simulation Based Analysis of QoS in MANET (IEEE 802.11)" 3^{rd} International Conference on Advance Computing & Communication Technology, Panipat, pp. 354-359, November 08-09, 2008.

13. ***Kumar Manoj***, S.C. Sharma & Leena Arya, "Performance of QoS Parameter in Mobile Ad hoc Network (IEEE 802.11b)" 3^{rd} International Conference on Advance Computing & Communication Technology, Panipat, pp. 378-382. Nov. 08-09, 2008.

14. ***Kumar Manoj***, S.C. Sharma & Leena Arya, "Analysis of QoS through Fuzzy Based i Wireless Ad hoc Networks" 3rd Int. Conf. on Advance Computing & Communicatio Technology (ICACCT-08), Panipat, pp. 461-465. November 08-09, 2008.

15. S.C. Sharma, ***Kumar Manoj*** & Leena Arya, "Performance Analysis of Power in Mobile A hoc Network for Different Protocols" 3rd International Conference on Advance Computing & Communication Technology, Panipat, pp. 373-377, Nov. 08-09th, 2008.

16. ***Kumar Manoj***, S.C. Sharma, Sandip Vijay, S.P.Singh & A.K.Jain "Throughput Analysis i Wireless Ad-hoc Network" A National Level Conf. on "Issues and Challenges in Internet & Mobile Computing", IMR Gaziabad, pp. 283-288, 28th March-2008.

PEER REVIEWED INTERNATIONAL/NATIONAL BOOK CHAPTERS

1. "Energy Efficient Parameters for Controlling Physical Layer of Mobile Ad-hoc Networks" by ***Kumar Manoj,*** Sandip Vijay and S. C. Sharma in *"Information Technology: Emerging Trends"* 1st ed. New Delhi, Vitasta Publishing Pvt. Ltd. 2009. *(ISBN: 8189766406 KK-70675),*

   http://www.kkagencies.com/toc/70675.htm.

2. SVEEN: Loss Rate Measurement in Ad-hoc Wireless Networks by ***Kumar Manoj,*** Sandip Vijay and S. C. Sharma in *"Information Technology: Emerging Trends"* 1st ed. New Delhi, Vitasta Publishing Pvt. Ltd. 2009.

   (ISBN: 8189766406 KK-70675)

   http://www.kkagencies.com/toc/70675.htm.

HONORS' & BEST PAPER AWARD

2007: [***Kumar Manoj***, S.C. Sharma and Sandip Vijay, "Energy Efficient parameters for controlling physical layer of mobile ad-hoc networks"] National Conference on Emerging Technologies in Computer Science (ETCS-2007) held at MIET, Meerut, Sept. 2007 (AICTE- New Delhi).

2008: [***Kumar Manoj*** & S.C. Sharma, "Simulation-Based Analysis of Impact of Random Loss"] First International Conference on Emerging Trends in Engineering & Technology, July 2008, IEEE Computer Society USA.

2008: [S.C. Sharma, ***Kumar Manoj*** & Leena Arya, "Performance Analysis of Power in Mobile Ad hoc Network for Different Protocols"] 3rd International Conference on Advance Computing & Communication Technology, November 2008, APIIT, Panipat, India.

2010: [***Kumar Manoj,*** Kumari Arti & S. C. Sharma "Simulation Based Analysis of Delay & Throughput in MANET (IEEE 802.11b) for TORA Protocol"] National Conference on Advance in Microwave Communication, Devices & Applications held at JIET, Jaipur, Feb. 16, 2010, IEEE MTT-S INDIA COUNCIL.

CHAPTER 1

INTRODUCTION

1.1 Background and Motivation

The growth of wireless communications coupled with high speed broadband technology has led to a new era in telecommunications. In third generation mobile networks, efforts are undertaken to merge many technologies and systems to support a wide range of traffic types with various quality of service requirements. As the use of wireless local area networks (WLAN) based on institute of electronics and electrical engineers 802.11 (IEEE 802.11) increase, the need for quality of service (QoS) becomes more obvious. QoS refers to a set of service requirements that needs to be met by the network, while transporting packets from a source to destination. Informally, it refers to the probability of a packet passing between two points in the network. The network is expected to guarantee a set of measurable pre-specified service attributes to the users in terms of end-to-end performance, such as delay, bandwidth, probability of packet loss, jitter, power consumption etc. The mobile networks can be classified in two main types: infrastructure-based and infrastructure-less mobile networks, the latter are also known as mobile ad-hoc networks (MANET).

Infrastructure Based Networks

The infrastructure based network requires a base station for communication between the sources and the destination in the network. The BSS contains a gateway to the wired network that communicate between a station of the BSS with stations of other BSSs and other local area networks (LANs) as seen in figure 1.1. The gateway is called access point

(AP) in the IEEE 802.11 standard. APs communicate with each other via either cable or radio to interconnect BSSs. The IEEE 802.11 standard specifies a distribution system (DS) to enable roaming between interconnected BSSs and to create connections to wired network resources. The interconnected BSSs and DSs allow extension to an IEEE 802.11 network as large as desired. This is called extended service set (ESS) in IEEE 802.11. There handover support in the medium access control (MAC) layer in order to provide connectivity within the ESS. The DS resides above MAC layer, which makes it homogeneous and can be implemented by any other backbone network such as ethernet, token ring, optical or wireless network. In WLAN, stations maintain their connections during their movement. If station crosses one BSS to another in the same ESS, stations make a decision and change its AP. During this change, the station associates itself with a new AP and the information is sent to DS which notifies the old AP about the new location.

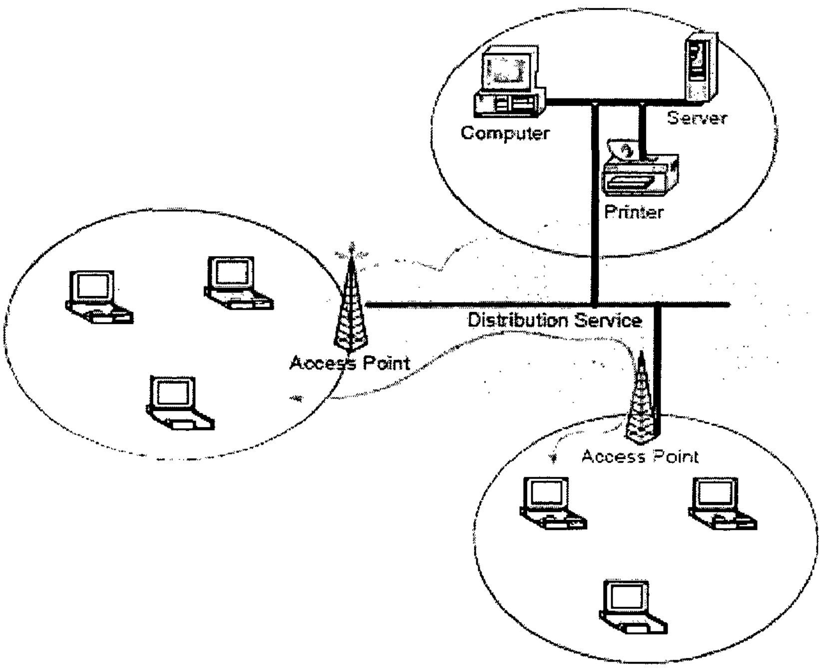


Figure 1.1: Infrastructure Based Network (IEEE 802.11 Network)

Infrastructure less Networks

The infrastructure less or ad hoc wireless networks do not required, any base station or central administration for communication between source to destination [1]. As defined by the Internet Engineering Task Force (IETF), the body responsible for guiding the evolution of the Internet,

"A mobile ad hoc network (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the larger Internet" [2].

Mobile ad hoc networks (MANET) are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using any other network infrastructure or centralized administration. In general, routes between nodes in an ad hoc network may include multiple hops, and hence it is appropriate to call such networks as "multi-hop wireless ad hoc networks". Each node is able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop. The design of network routing for these networks is a complex issue. Irrespective of application, MANET's need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment, where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination is usually the optimal route in a static network, this idea is not easily extendable to MANET's. Factors such as variable wireless link quality, propagation path loss, fading, multi-user interference, QoS, bandwidth, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. MANETs are typically local area networks (LANs) or other small networks in which some of the network devices are part of the network only for the duration of a communication session. No fixed infrastructure is included in the configuration of the networks. Packets are delivered to destination nodes as per the routing protocols [3-12]. MANETs are self-organizing networks built dynamically in the presence of nodes equipped with radio interface devices. The nodes are capable of moving in an arbitrary fashion. The nodes themselves carry out routing and switching function. In fact, each mobile node operates not only as a host but also as a router. Multi hop Scenario is preferred over single hop because of limitations such as radio power limitation, channel utilization, and power saving concerns [13]. The salient characteristics of the MANETs such as dynamic topologies, bandwidth-constrained, variable capacity links, energy-constrained operation and limitation of physical security have been described in [14]. These are focused around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile networks that is both flexible and powerful. Some of the application of the MANET are given below:

- Personal area networking

  cell phone, laptop, ear phone, wrist watch

- Military environments

  soldiers, tanks, planes

- Civilian environments

taxi cab network, meeting rooms, sports stadiums, boats, small aircraft

- Emergency operations

  search-and-rescue, policing and fire fighting

1.2 Issues in Ad hoc Networks

The flexibility and convenience of ad hoc networks come at a price. The multi-hop nature and the lack of fixed infrastructure add the complexities and design constraints in ad hoc networking [15]. Wireless ad hoc networks the following challenges.

- Packet Losses
- Variation in Link
- Energy Constrain
- Network Scalability
- Routing
- Security and Reliability
- Quality of Service (QoS)
- Internetworking
- Power Consumption

Packet Losses

In mobile ad hoc networks, because nodes can move arbitrarily, the network topology, which is typically multi-hop, can change frequently and unpredictably, resulting in route changes, frequent network partitions, and possibly packet losses.

Variation in Link

Each node may be equipped with one or more radio interfaces that have varying transmission/receiving capabilities and operate across different frequency bands [16-17]. This heterogeneity in node radio capabilities can result in possible asymmetric links. In addition, each mobile node might have a different software/hardware configuration resulting in variability in processing capabilities. Designing network protocols and algorithms for this heterogeneous network can be complex, requiring dynamic adaptation to the changing conditions (power and channel conditions, traffic load/distribution variations, congestion, etc.)

Energy Constrained Operation

Each mobile node has to carry that can have limited power supply. This in turn, limits services and applications that can be supported by the nodes. As each node is acting both as an end system and as a router at the same time, additional energy is required to forward packets from other nodes.

Network Scalability

Currently, popular network management algorithms mostly designed to work on fixed or relatively small wireless networks. Many mobile ad hoc networks applications involve large networks with tens of thousands of nodes, as found for example, in sensor networks and tactical networks. Scalability is critical to the successful deployment of these networks. The steps toward a large network consisting of nodes with limited resources are not straight forward, and present many challenges that are still to be solved in areas such as-addressing, routing, location management, mobility management, clustering, mobility management, TCP/ UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance qos/multimedia, inter operability, security, high capacity wireless technologies, etc.

Routing

Since the topology of the networks is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

Security and Reliability

In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics also introduce reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses and data transmission errors.

Quality of Service (QoS)

Providing different quality of service levels in a constantly changing environment is also a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services. The detail of the QoS in MANET has been described in chapter 2.

Internetworking

In addition to the communication within an ad hoc network, networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

Power Consumption

For most of the light-weight nodes, the communication-related functions should be optimized for lean power consumption. Since the nodes communicate over wireless links, they have to contend with the ill effects of radio communication, such as *noise, fading,* and *interference*.

In wireless communication, background acoustic *noise* is the most irritant and abundant in nature. Background acoustic noise may be caused due to mechanical friction, airflow, street noise etc. A single noise source may cause difficulties on both receiving ends of the communications channel.

A signal experiences *fading,* when the interaction of multipath components and time- or frequency-varying channel conditions cause significant fluctuations in its amplitude at a receiver. Fading is endemic in mobile, long-distance, high frequency, and other communication channels as it causes power fluctuations about the local-mean power.

Some possible types of nonlinear *interference* and distortions for wireless communication systems are:

- Spurious radiation of transmitters
- Harmonics and sub-harmonics, inter-modulation products (IMP), noise etc. The inter-modulation radiation can be caused by an external signal (from a nearby transmitter) as well as by several carriers (in CDMA systems, for example) in the transmitter's power amplifier
- Spurious responses of receivers: adjacent, image and intermediate frequency (IF) channels
- Nonlinear behavior of receivers may also cause the system performance degradation (desensitization, IMPs, local oscillator noise and harmonics' conversion etc.)

1.3 Challenges in Mobile Ad hoc Networks

A major challenges encountered in the design of high speed networks, is to handle busty sources that congestion. Congestion is defined as the state, in which the network is not able to meet the negotiated performance objective for the established connection.

To compare with the wired LAN, the main advantages of WLAN including cost effectiveness, ease of set-up/implementation, flexibility, scalability, unlimited access to existing information infrastructures, station mobility etc. But on the other hand, WLAN also exhibit disadvantages in relation to QoS and security issues. In fact, WLANs offer lower quality than the wired LANs, mainly because of the lower bandwidth due to limitations in radio transmission and higher error rates due to interference. In the mean time, using radio waves for data transmission in public environment might cause security concerned.

Ad hoc networks will be formed by different types of terminals, e.g. PDA-like devices, mobile phones, sensors or desktop computers, with different capabilities in terms of maximum transmission power, energy availability, mobility patterns and QoS requirements. Therefore, ad hoc networks, in general, are heterogeneous in terms of terminals and offered services. On the other hand, ad hoc networks connected to external networks such as fixed infrastructures (e.g. the Internet, a company's Intranet or a home network) or cellular systems. The interworking should occur when the opportunity and the need arises. This is closely related to the self-organizing and self-managing properties of ad hoc networks that make these networks blend into the environment of the person they are associated with. A point of attention is the fact that information on the geographical location of (some of) the terminals may be available. This can be a powerful tool for improving network architecture, routing schemes and location-aware services.

Challenges [18] for wireless ad hoc network are---

- Limited wireless transmission range
- Broadcast nature of the wireless medium
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Security and QoS

1.4 Simulation tools for wireless Networks

The simulation tool [19] for global needs must be able to provide

- standard protocol
- model specific protocols and specific applications
- bind these models to standard ones
- timing aspects as accurately as possible for network exchanges
- develop new protocols
- optimize existing protocols
- study the performance of existing protocols in different network topologies during varying traffic loads
- evaluate competing protocols

Optimized Network Engineering Tools (OPNET) meet most of these criteria. OPNET developed by MIL3, Inc., runs on both Unix and Windows NT machines. OPNET can perform modeling, simulation and performance analyzing of communication networks and communications protocols. OPNET models are hierarchical. At the lowest level, a state-transition diagram encodes the behavior of an algorithm or protocol with embedded code based on C language constructs. At the middle level, discrete functions such as buffering, processing, transmitting, and receiving data packets are performed by separate objects, some of which relay on an underlying process model. These objects, called models, are created or modified using the Node Editor and connected to form a higher-level network model. At the highest level, node objects based on underlying node models are deployed and connected by links to form a network model. The network model defines the scope of the simulation, and it is used as a "table of contents" when the simulation is executed, and it is bound together from its discrete components.

OPNET is a sophisticated workstation-based environment for the modeling and performance-evaluation of communication systems, protocols and networks. OPNET features include graphical specification of models; a dynamic, event-scheduled Simulation Kernel; integrated data analysis tools; and hierarchical, object-based modeling.

OPNET comes with a library with ready-made models of the most widely used communications protocols such as Ethernet, IP, UDP, TCP, ATM, FDDI, Frame Relay and CDPD. These models are very detailed and include all features of the mentioned protocols. OPNET also contains models of the most commonly used routers and switches (for example a number of Cisco routers).

When developing an OPNET model the user can either

- Use a ready-made model for the protocol or networks that they wants to model
- Use ready-made models such as Ethernet, IP, and TCP models as a part of their model
- Develop a completely new model from scratch

In the workspace, one can create a network model, collect statistics directly from each network object or from the network as a whole, execute simulations, and view results. For the basic aspects of modeling, several editors are needed to accomplish a simulation project. Basically, they are

- Project Editor
- Node Editor
- Process Model Editor
- Link Model Editor

- Packet Format Editor
- Probe Editor

Analysis Tool

Although simulation results can be viewed in the project editor, the analysis tool has several useful additional features. One can define templates to which he can apply statistical data, and create analysis configurations for application of statistical data, and create analysis configurations that can be saved and viewed later.

Network Characteristics

Attribute selection has to be done for each and every element of the network. Attribute selections are done on the OPNET modeling software by using the attribute menu selector option for each element. This attribute menu can support a sophisticated set of properties or characteristics that allow the model designer to ensure that the end user will know the purpose of an attribute and to prevent that user from assigning invalid attribute values. First we need to define the application and profile definition of the network.

Application Definition Object

It is now necessary to define and configure applications. A user's behavior or "profile" can be described by the applications he or she uses, for how long, and how often these applications are used each day. A number of common network applications such as email for sending and receiving, telnet for remote login, database access for database queries, and http have been selected for this work.

Network Simulator (NS-2)

Network Simulator 2 (NS-2) [20-21] is a simulation tool originated from Lawrence Berkeley National Laboratory. NS-2 provides substantial support for simulation of routing and multicast protocols over wired and wireless networks. NS-2 has an advanced IEEE 802.11 module, which is applied and verified extensively in the network community; hence it's an excellent simulation tool within this research.

Xgraph and Gnuplot

Xgraph [22] and Gnuplot [23] are X-Window applications that include interactive plotting and graphing, and animation and derivatives. For the analysis the programs to create graphic representations of simulation results. Output data from TCL scripts are used as data sets to Xgraph or Gnuplot.

Other tools

Other library tools include AWK, *grep* and Perl scripts; these are mainly used to extract important statistics information from trace files. AWK utility allows us to do simple operations on data files such as averaging the values of a given column, summing or multiplying term by term between several columns. In our work we extensively used this utility to calculate and extract QoS metrics from trace files. The *grep* command in UNIX allows to "filter" a file. This is important because some generated trace files are enormous hence needs to be filtered.

1.5 Objective of the Present Work

The objective of the present work is to analyze the performance of various routing protocols in terms of different QoS parameters such as throughput, end-to-end delay, retransmission, control traffic received and sent; data traffic received and sent no. of loads, mobility, and bandwidth in wireless ad hoc network.

The work carried out is divided into:

- The assessment of impact of varying load on various QoS parameters for different protocols (AODV, DSR & DSDV) in wireless ad-hoc network and comparison of the simulated result with the reported experimental data.
- The assessment of effect of congestion on QoS parameter for routing protocol (AODV) using IEEE 802.11 MAC layer parameter & fuzzy approach.
- Performance analysis of proposed bandwidth control management for wireless ad hoc networks.

1.6 Organization of the Thesis

Chapter 1 introduces of wireless ad hoc network, their challenges and simulator used in brief. A review of the basic concepts of wireless network and quality of service is presented in the chapter 2. In chapter 3, the assessment of effect on QoS parameters of static and dynamic networks for different protocols. Chapter 4, the assessment of effect of congestion on QoS parameter for routing protocol (AODV) using IEEE 802.11 MAC layer parameter & fuzzy approach. Chapter 5, performance analysis of proposed bandwidth control management for wireless ad hoc networks. Finally, we provide the concluding remarks and scope for future work in chapter 6.

CHAPTER 2

OVERVIEW ON IEEE 802.11 AND QUALITY OF SERVICE

2.1 Background and Motivation

In recent years, the continuing advances in communications and networks and the ever-increasing demand for mobility of users, have been fueling the interest in wireless communications. Mobility, installation speed, simplicity, scalability, and less point-of-break problem, make wireless local area networks (WLANs) a better choice than LAN. WLANs have become more prominent with the development of IEEE 802.11 WLAN standard in 1997. IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802.11) in the 5 GHz and 2.4 GHz FCC (Federal Communications Commission) spectrum bands mainly regarding unlicensed transmission.

The IEEE 802.11 WLAN standard as shown in figure 2.1 covers the MAC sub-layer and the physical (PHY) layer. Logical link control (LLC) sub-layer is specified in the IEEE 802.2 standard. This architecture provides a transparent interface to the higher layer users stations (STAs) may move, roam through an 802.11 WLAN and still appear as stationary to 802.2 LLC sub-layer and above. This allows existing TCP/IP protocols to run over IEEE 802.11 WLAN just like wired ethernet deployed.

Characteristics of Wireless LANs (WLAN)

Advantages

- very flexible alternative to wired LANs
- no wiring difficulties

- ad-hoc networks without previous planning possible
- more robust against disasters, e.g. earthquakes, fire, etc.

Disadvantages

- lower bandwidth compared to wired networks
- possible interference may reduce bandwidth
- no guaranteed service due to license-free spectrum
- need to consider security issues
- proprietary solutions, especially for higher bit-rates
- wireless products have to follow many national restrictions
- long time to establish global standards

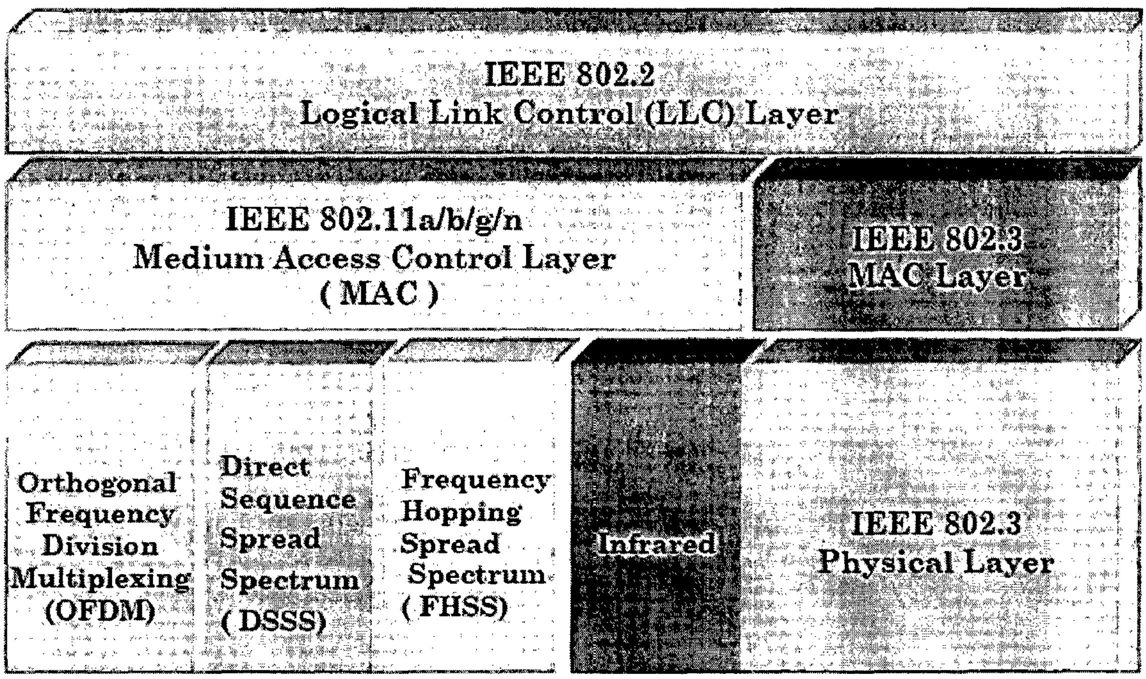


Figure 2.1: Standard Architecture of WLAN

2.2 IEEE 802.11 PHY

In 1997, IEEE provides three kinds of options in the PHY layer of the open system interconnection (OSI) network model, which are

- An Infra Red (IR) base band PHY, and usually provides a speed of 1 to 2 Mbps.
- A frequency hopping spread spectrum (FHSS) radio in 2.4 GHz ISM (Industrial, Scientific and Medical) band.
- A direct sequence spread spectrum (DSSS) radio in 2.4 GHz ISM (Industrial, Scientific and Medical) band. All these options support both 1 Mbps and 2 Mbps PHY rate.

Photonic Wireless Transmission - Diffused Infrared (IR)

The only implementation of these types of LANs uses infrared light transmission. Photonic wireless LANs uses the 850 to 950 Nm band of infrared light with a peak power of 2 watts. The physical layer supports 1 and 2 Mbps data rates. Although photonic wireless systems potentially offer higher transmission rates than RF based systems, they also have some distinct limitations.

- Infrared light like visible light is restricted to line of sight operations. However, the use of diffuse propagation can reduce this restriction by allowing the beam to bounce off passive reflective surfaces.
- Power output (2 watts) is kept low to reduce damage to the human eye, that transmissions are limited to about 25 meters.
- Sensors (receivers) need to be laid out accurately; otherwise the signal may not be picked up. Photonic-based wireless LANs are inherently secure and are immune (as are optical fiber networks) from electromagnetic radiation, which can interfere with cable

and RF, based systems. IR communications are described as both indirect and non-line-of sight. The diffused infrared signal, which is emitted from the transmitter, fills an enclosed area like light and does not require line-of-sight transmission. Changing the location of the receiver does not disrupt the signal. Many diffused infrared products also offer roaming capabilities, which enables you to connect several access points to the network, then connect your mobile computer to any of these access points or move between them without losing your network connection. Usually IR provides a radius of 25 to 35 feet and a speed of 1 to 2Mbps.

Frequency Hopping Spread Spectrum Technology (FHSS)

Frequency Hopping Spread Spectrum (FHSS) is analogous to FM radio transmission as the data signal is superimposed on, or carried by, a narrow band carrier that can change frequency. The IEEE 802.11 standard provides 22 *hop patterns* or frequency shifts to choose from in the 2.4GHz ISM band. Each channel is 1MHz and the signal must shift frequency or *hop* at a fixed hop rate (U.S. minimum is 2.5 hops/sec). This technology modulates a radio signal by shifting it from frequency to frequency at near-random intervals. This modulation protects the signal from interference that concentrates around one frequency. To decode the signal, the receiver must know the rate and the sequence of the frequency shifts, thereby providing added security and encryption. FHSS products can send signals as quickly as 1.2 to 2Mbps and as far as 620 miles. Increasing the bandwidth (up to 24Mbps) can be achieved by installing multiple access points on the network. In FS, the 2.4 GHz band is divided into 75 one-MHz sub-channels. In order to minimize the probability that two senders are going to use the same sub-channel simultaneously, frequency hopping is used to provide a different hopping pattern for every data exchange. The sender and receiver agree on a hopping pattern, and data is sent over a sequence of sub-channels according to the pattern. FCC regulations require bandwidth up to 1 MHz for every sub-channel, which forces the FHSS technique to spread the patterns across the entire 2.4 GHz, resulting in more hops and a high amount of overhead.

Direct Sequence Spread Spectrum (DSSS)

Spread spectrum was first developed by the military as a secure wireless technology. It modulates (changes) a radio signal pseudo-randomly so it is difficult to decode. This modulation provides some security, however, because the signal can be sent great distances, you do risk interception. To provide complete security, most spread spectrum products include encryption. DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the *chipping sequence*. The sequence is also known as the spreading code that is an 11-bit sequence (10110111000). The chipping or spreading code is used to generate a redundant bit pattern to be transmitted, and the resulting signal appears as wide band noise to the unintended receiver. One of the advantages of using spreading codes is even if one or more of the bits in the chip are lost during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. The ratio between the data and width of spreading code is called processing gain.

Table 2.1 Various Categories of IEEE 802.11 Standards, which are Active

Standard	**Responsibility**
IEEE 802.11e MAC enhancement for QoS	Covers issues of MAC enhancements for QoS, such as EDCF service differentiation & hybrid coordination function (HCF).
IEEE 802.11 k	To define radio resource measurement
IEEE 802.11 m	Maintenance of the IEEE 802.11-1999 (reaff. 2003) standard
IEEE 802.11 n	Investigating the possibility of improvements to the 802.11 standard to provide high throughput (>100Mbps)
IEEE 802.11 p	Covers issues of amendment of IEEE 802.11 to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments, and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50ms).
IEEE 802.11 r	Enhancements to the 802.11 medium access control (MAC) layer to minimize or eliminate the amount of time data connectivity between the station (STA) and the distribution system (DS) is absent during a basic service set (BSS) transition, limited to the state necessary for the operation of the MAC.

IEEE 802.11 s	To develop an IEEE 802.11 extended service set (ESS) Mesh with an IEEE 802.11 wireless distribution system (WDS) using the IEEE 802.11 MAC/PHY layers that supports both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies.
IEEE 802.11 t	To provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of 802.11 WLAN devices and networks at the component and application level as a recommended practice.
IEEE 802.11 u	Amend the IEEE 802.11 MAC and PHY to support Inter working with external networks.
IEEE 802.11 v	Amendment to provide wireless network management enhancements to the 802.11 MAC, and PHY, to extend prior work in radio measurement to effect a complete and coherent upper layer interface for managing 802.11 devices in wireless networks.

2.3 IEEE 802.11 MAC

The IEEE 802.11 MAC sub-layer defines two medium access coordination functions, the basic Distributed Coordination Function (DCF) and the optional Point Coordination Function (PCF). It supports two types of transmission asynchronous and synchronous.

Asynchronous transmission is provided by DCF whose implementation is mandatory in all 802.11 (Stations) STAs. Synchronous service is provided by PCF that basically implements a polling based access. The implementation of PCF, however, is not mandatory.

There are two different modes to configure an IEEE 802.11 wireless network ad-hoc mode and infrastructure mode. In ad-hoc mode, the mobile STAs can directly communicate with each other to form an Independent BSS (IBSS) without connectivity to any wired backbone. In infrastructure mode, the mobile STAs can communicate with the wired backbone through the bridge of access point (AP). DCF can be used both in ad-hoc and infrastructure modes, while PCF is only used in infrastructure mode [24]. In 1999, the IEEE defined two high rate extensions IEEE 802.11b to support 5.5/ 11 Mbps in 2.4 GHz ISM band and IEEE 802.11a to support 6, 9, 12, 18, 24, 36, 48, 54 Mbps in 5 GHz Unlicensed National Information Infrastructure (UNII) band [24]. The standards approved so far in recent past are IEEE 802.11 d-Global harmonization (2001); IEEE 802.11 f-inter access point protocol (IAPP) (2003); IEEE 802.11 g (2003); IEEE 802.11 h –dynamic channel selection. (2003); IEEE 802.11i –security (2004) and IEEE 802.11 j (2004) [25]. Table 2.1 show various categories of standards, which are not approved yet and work is still going on towards their standardization.

2.4 IEEE 802.15

The bluetooth technology is a de-facto standard for low-cost, short-range radio links between mobile PCs, mobile phones, and other portable devices [26]. The IEEE 802.15 working group for wireless personal area networks approved its first WPAN standard derived from the bluetooth specification [27]. The IEEE 802.15.1 standard is based on the lower portions of the Bluetooth specification. A bluetooth unit, integrated into a microchip, enables wireless ad hoc communications, of voice and data between portable and/or fixed electronic devices like computers, cellular phones, printers, and digital cameras [28]. The Bluetooth system can manage a small number of low-cost point-to-point, and point to multi-point communication links over a distance of up to 10 m with a transmit power of less than 1mW. It operates in the globally available unlicensed ISM (industrial, scientific, medical) frequency band at 2.4 GHz and applies frequency hopping for transmitting data over the air using a combination of circuit and packet switching. Due to its low-cost target, Bluetooth microchips may become embedded in virtually all consumer electronic devices in the future.

2.5 IEEE 802.16

Over the last few years, Wireless-Fidelity (Wi-Fi) is has been deployed as the last hop of the Internet or telephone network. The advantages that Wi-Fi provides are mobility and coverage. Together, these characteristics provide “any-time”, “any-where” connectivity. Meanwhile, a new standard for broadband wireless connectivity, known as worldwide interoperability for microwave access (WiMAX), is emerging. WiMAX a non-line-of-sight, point-to-multipoint broadband wireless access (BWA) technology, is emerging as a potential competitor to wireline DSL and cable for last-mile access and a strong backhaul option for Wi-Fi. Wi-Fi (up to 100meters) and WiMAX (up to 50 kilometers) are expected to provide new broadband wireless connectivity. Wi-Fi provides service for client-to-access point (AP) communications. WiMAX is for implementations of AP-to-AP and AP-to-service providers that are needed for wireless last-mile [29-30].

Recent developments in this area have given WiMAX-based broadband wireless access (BWA) a new hope for growth in client-to-service providers with IEEE 802.16e standard, which is based on Orthogonal Frequency Division Multiple Access (OFDMA) system, expected to be ratified in early 2005. Industry and research communities are consequently investing considerable effort in the convergence of multimedia services and ubiquitous instant access, which by necessity depends on the use of BWA technologies [31]. Standards for BWA are being developed within IEEE project 802, working group 16, often referred to as 802.16. The current version of the standard was published in 2004 [32], though the standardization process is still ongoing [33]. The 802.16 standard specifies two modes for sharing the wireless medium point-to-multipoint (PMP) and mesh (optional). In the PMP mode, the nodes are organized into a cellular-like structure, where a base station (BS) serves a set of subscriber stations (SSs) within the same antenna sector in a broadcast manner, with all SSs receiving the same transmission from the BS. Transmissions from SSs are directed to and coordinated by the BS. On the other hand, in Mesh mode, the nodes are organized ad hoc and scheduling is distributed among them. In the IEEE 802.16 standard, uplink (from SS to BS) and downlink (from BS to SS) data transmissions are frame-based, i.e., time is partitioned into subframes of fixed duration. Since the transmission is broadcast, all SSs listen to the data transmitted by the BS in the downlink subframe. However, an SS is only required to process data that are directed to itself or that are explicitly intended for all the SSs. In the uplink subframe, on the other hand, the SSs transmit data to the BS in a time division multiple access (TDMA) manner. Downlink and uplink subframes are duplexed using one of the following techniques frequency division duplex (FDD), where downlink and uplink subframes occur simultaneously on separate frequencies, and time division duplex (TDD), where downlink and uplink subframes occur at different times and usually share the same frequency. SSs can be either full duplex, i.e., they can transmit and receive simultaneously, or half-duplex, i.e., they can transmit and receive at non-overlapping time intervals. Since it would not be feasible to address the QoS requirements of all of the applications foreseen for an IEEE 802.16 network, their functionality are grouped by the standard into a small number of classes named scheduling services based on the commonality of their

1) QoS service requirements (e.g., real-time applications with stringent delay requirements, best effort applications with minimum guaranteed bandwidth)
2) Packet arrival pattern (fixed/ variable-size data packets at periodic/aperiodic intervals)
3) Mechanisms to send bandwidth requests to the BS. Thus, each scheduling service is tailored to support a specific class of applications.

2.6 HIPERLAN Standard

HIPERLAN is a European standard developed by ETSI. The ETSI HiPERLAN standard has two sub-standards. HiPERLAN/1 is designed for ad-hoc networks and operates in the 5.1-5.3 GHz bandwidth. The MAC protocol is based on carrier sense multiple access/ collision avoidance (CSMA/CA) scheme. HiPERLAN/1 does not guarantee QoS and considers only best effort service whereas HiPERLAN/2 provides the QoS guarantee and focuses on managed infrastructure and wireless distribution system. It is based on time division multiple access/time division duplexing (TDMA/TDD) protocol. As a result, HiPERLAN/2 schedules the access in a deterministic manner where a time slot is assigned to each station to transmit packets [34]. The HIPERLAN standard defines part of the bottom two layers of the open system interconnection (OSI) model, namely the physical layer (PHY) and the data link layer (DLC). Only the medium access control (MAC) sub-layer within the DLC is specific to HIPERLAN. Two distinct frequency bands are allocated. One is in 5.15 to 5.25 GHz, with potential extensions possible for up to 5.30 GHz, and the other is in 17.1 to 17.3 GHz range.

2.7 Quality of Service

Quality of Service (QoS) refers to a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [35]. Informally, it refers to the probability of a packet passing between two points in the network. The network is expected to guarantee a set of measurable pre-specified service attributes to the users in terms of end-to-end performance, such as delay, bandwidth, probability of packet loss, delay variance (jitter), power consumption etc.

The capability to provide resource assurance in a network is referred to as quality of service (QoS), which is a critical requirement in order that new IP-based applications can operate within well-defined parameters. Especially, QoS is a critical problem in a wireless network. Different users use the more applications and services, the worse the status and quality of wireless network services are. In the point of QoS, it is very difficult to achieve the level of desired quality by both administrators and users.

QoS Issues

QoS is a challenging problem due to following reasons

- network bandwidth is of limited availability
- timely delivery of multimedia data is difficult due to mobility, low power capabilities and service disruption because of link failure and/or security problems
- the wireless channel fading and high bit error rate(BER) directly affect the throughput performance of the network

Most network architectures deal with all packets in the same way, a single level of a service. However, applications have diverse requirements and may be sensitive to packet losses and latency. For example, interactive and real-time applications such as IP telephony and streaming services such as audio, video and interactive services such as web and transaction

Table 2.2 Common Wired-Network Performance Characteristics

Application	**Reliability**	**Delay**	**Jitter**	**Bandwidth**
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Video conferencing	Low	High	High	High

have a different level of requirement to the quality of services such as packet losses and latency. When the latency or packet loss rate exceeds certain levels, some applications and services become unusable. The service currently provided by default is often referred to as best effort. Best-effort service is adequate for some applications as given in table 2.2 that can tolerate large jitter and packet losses; it clearly does not meet the needs of many new time-sensitive multimedia based applications such as IP telephony, videophone and videoconferencing. Resource assurance is critical for many new wireless applications and services. Although the IntServ and DiffServ paradigms figure predominantly as QoS solutions, they focus on the IP layer and it is necessary for the underlying layers to be able to respond to and configure such IP-based services requirement in wireless network.

QoS within a Single Network Element

Congestion management, queue management, link efficiency, and shaping/policing tools provide QoS within a single network element.

- **Congestion Management**

Because of the burst nature of voice/video/data traffic, sometimes the amount of traffic exceeds the speed of a link. At this point, what will the router do? Will it buffer traffic in a single queue and let the first packet in be the first packet out? Or, will it put packets into different queues and service certain queues more often? Congestion management tools address these questions. Tools include priority queuing (PQ), custom queuing (CQ), weighted fair queuing (WFQ), and class-based weighted fair queuing (CBWFQ).

- **Queue Management**

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and will be dropped. This is a tail drop. The issue with tail drops is that the router cannot prevent this packet from being dropped. So, a mechanism is necessary to do two things

1) Make sure that the queue does not fill up, so that there is room for high-priority packets

2) Allow some sort of criteria for dropping lower priority packets before dropping higher-priority packets. Weighted early random detect provides both of these mechanisms.

- **Link Efficiency**

Many times low-speed links present an issue for smaller packets. For example, the serialization delay of a 1500-byte packet on a 56- kbps link is 214 milliseconds. If a voice packet were to get behind this big packet, the delay budget for voice would be exceeded even before the packet left the router. Link fragmentation and interleave allow this large packet to be segmented into smaller packets interleaving the voice packet. Interleaving is as important as the fragmentation. There is no reason to fragment the packet and have the voice packet go behind all the fragmented packets. Another efficiency is the elimination of too many overhead bits. For example, RTP headers have a 40-byte header. With a payload of as little as 20 bytes, the overhead can be twice that of the payload in some cases. RTP header compression (also known as Compressed Real-Time Protocol header) reduces the header to a more manageable size.

- **Traffic Shaping and Policing**

Shaping is used to create a traffic flow that limits the full bandwidth potential of the flow. This is used many times to prevent the overflow problem mentioned in the introduction. For instance, many network topologies use Frame Relay in a hub-and-spoke design. In this case, the central site normally has a high-bandwidth link (say, T1), while remote sites have a low-bandwidth link in comparison (say, 384 Kbps). In this case, it is possible for traffic from the central site to overflow the low bandwidth link at the other end. Shaping is a perfect way to pace traffic closer to 384 Kbps to avoid the overflow of the remote link. Traffic above the configured rate is buffered for transmission later to maintain the rate configured. Policing is similar to shaping, but it differs in one very important way. Traffic that exceeds the configured rate is not buffered.

2.8 Quality of Service in Ad Hoc Networks

A key issue for multimedia applications in any network is QoS support. QoS is the performance level of a service offered by the network to the user. A main concern for researchers is if proposed QoS solutions for wired networks can be transported to MANETs. According to CCITT, QoS is defined as

"The collective effect of service performance which determines the degree of satisfaction of a user of a service"

MANETs characteristics generally lead to the conclusion that they provide weak support to QoS. Wireless links have a variable capacity, and high loss rates. Topologies are highly dynamic with frequent links breakages. Random access-based MAC protocols are commonly used in this environment (e.g., 802.11b), has no QoS support. Finally, MANET link layers typically run in unlicensed spectrum, making it more difficult to provide strong QoS guarantees in spectrum hard to control [36]. This scenario indicates that, not only hard QoS guarantees will be difficult to achieve, but also if the nodes are highly mobile even statistical QoS guarantees may be impossible to attain, due to the lack of sufficiently accurate knowledge (both instantaneous and predictive) of the network states [37]. Furthermore, since the quality of the network (in terms of available resources reside in the wireless medium and in the mobile nodes e.g., buffer and battery state) varies with time, present QoS models for wired networks are insufficient in a self-organizing network, and new MANET QoS model are reported in the literature [38].

The research on QoS support in MANETs include

- QoS models
- QoS signaling
- QoS routing
- QoS Medium Access Control (MAC)

2.9 QoS Models

A QoS model for MANETs specifies an architecture in which some kinds of services could be provided in the network. It is the system goal and will influence the functionality of all other QoS components. The model should first consider the challenges of MANETs, e.g. dynamic topology and time-varying link capacity along with seamless connection to the Internet, as potential commercial applications require the seamless connection to the Internet. So, the existing QoS architectures in the Internet also need to be examined. QoS models for the Internet available in the literature are- IntServ proposed by R. Braden *et al.*

[39] and DiffServ proposed by S. Blake [40]. The basic idea of the IntServ model is that the flow-specific states are kept in every IntServ-enabled router. DiffServ model, the other architecture, is designed to overcome the difficulty of implementing and deploying IntServ and RSVP in the Internet backbone. Both of them require accurate link state (e.g., available bandwidth, packet loss rate delay, etc.) and topology information. For applications with high priority, per-flow QoS guarantees of IntServ and for applications with lower priorities per class differentiation of DiffServ may be used. As FQMM separately applies both IntServ and DiffServ for different priorities, the drawbacks related to IntServ and DiffServ still remain.

2.9.1 Flexible QoS Model for MANET (FQMM)

Flexible QoS Model for MANET (FQMM) proposed by H. Xiao et al. in [41] considers the characteristics of MANETs and tries to take advantage of both the per-flow service granularity in IntServ and the service differentiation in DiffServ. As in DiffServ, three kinds of nodes (ingress, interior, and egress nodes) are defined in FQMM. An ingress node is a mobile node that sends data. Interior nodes are the nodes that forward data for other nodes. An egress node is a destination node. Note that the role of a mobile node is adaptively changing based on its position and the network traffic. The provisioning in FQMM, which is used to determine and allocate the resources at various mobile nodes, is a hybrid scheme of per-flow provisioning as in InterServ and per-class provisioning as in DiffServ. For applications with high priority, per-flow QoS guarantees of IntServ are provided and for applications with lower priorities, per-class differentiation of DiffServ is provided. FQMM tries to preserve the per-flow granularity for a small portion of traffic in MANET, given that a large amount of the traffic belongs to per aggregate of flows, that is, per-class granularity. A traffic conditioner is placed at the ingress nodes where the traffic originates. It is responsible for re-marking the traffic streams, discarding or shaping packets according to the traffic profile, which describes the temporal properties of a traffic stream such as rate and burst size. FQMM is the first attempt at proposing a QoS model for MANETs. However, some problems still need be solved. First, how many sessions could be served by per flow granularity? Without an explicit control on the number of services with per-flow granularity, the scalability problem still exists. Second, just as in DiffServ, the interior nodes forward packets according to a certain PHB that is labeled in the DS field. We argue that it is difficult to code the PHB in the DS field if the PHB includes per-flow granularity considering the DS field is at most 8bits without extension. Finally, making a dynamically negotiated traffic profile is very difficult. In FQMM, both IntServ and DiffServ scheme are separately used for different priority classes. Therefore, the drawbacks related to IntServ and DiffServ remain to be a drawback in FQMM. Moreover, to the best of our knowledge FQMM does not take into account the characteristics of MANET.

2.9.2 Cross Layer QoS Model

A cross-layer QoS model proposed by Navid Nikaein et al. [42-43] separates metrics at the different layers (i.e. application layer metrics, network layer metrics, and MAC layer metrics) and map them accordingly. This is because the quality of service that an application requires depends strictly on the "quality" of the network. As stated earlier, the quality of network should represent the available network resources reside both in the wireless medium and in the mobile nodes as well as the stability of these resources. At the application layer, the QoS requirements has been classified into a set of QoS priority classes (classes, I, II, & III) with their corresponding application layer metrics (ALMs) which can be mapped to appropriate metrics.

- Class I corresponds to applications that have strong delay constraints, such as voice. This class is mapped to the delay metric at ALMs
- Class II is suitable for applications requiring high throughput such as video or transaction-processing applications. Similarly, we map this class to the throughput metric at the ALMs
- Class III has no specific constraints, and it is mapped to best effort at the ALMs

This mapping is shown in figure 2.2. At the network layer, the use of nodes' power state, buffer state, and stability state has been used as network layer metrics (NLMs) that will characterize the quality of network. The power level represents the amount of available battery over time (i.e. energy). The buffer state stands for the available unallocated buffer. The stability means the connectivity variance of a node with respect to its neighboring nodes over time. To compute the quality of a path, concave or /and additive functions have to be used in order to represent the NLMs of a path given the value of these metrics for individual nodes on that path. The network layer metrics of a particular node can also reveal whether the node is forced to be selfish or not. In the selfish mode, a node can cease to be a router and acts only as a host due to its poor quality. At the MAC layer, link signal-to-interference plus noise power ratio (SINR) has been considered as MAC layer metrics (MLM) to estimate the quality of network. Link SINR determines the communication performance of the link, the data rate and associated probability of packet error rate or bit rate (bit error rate BER) that can be supported by the link. Links with low SINR are not typically used due to their poor performance, leading to partial connectivity among all nodes in the network.

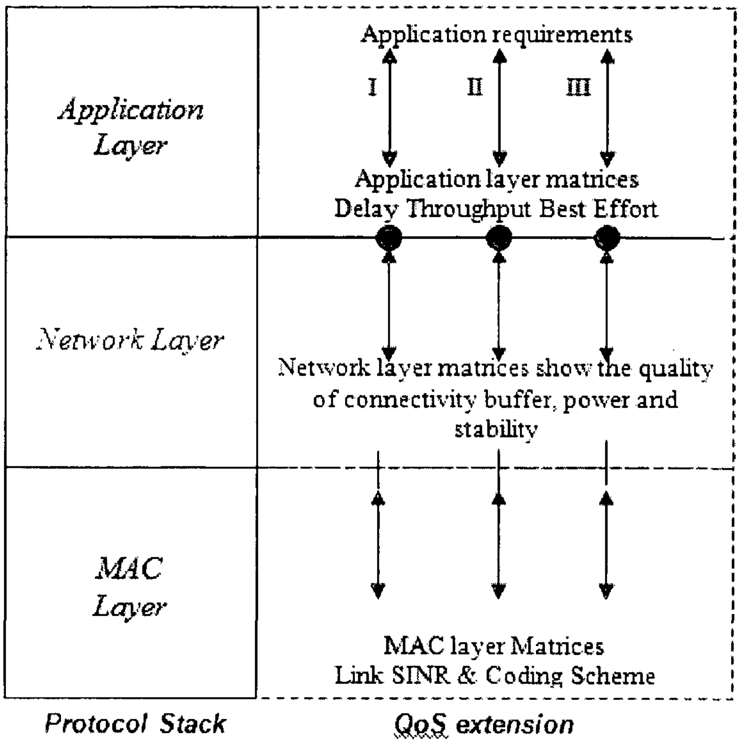


Figure 2.2: Global View of a Cross Layer QoS Model

Moreover, it is essential to minimize the volume of traffic being transmitted over the wireless interface because of the scarce wireless resources. This can be achieved via coding schemes. That is why the author has suggested applying different coding schemes such as FEC and ARQ for different QoS classes. For example, forward error correction (FEC) uses a coding scheme for both error detection and correction, which impose constant overhead over the applied data. This scheme is more appropriate for a high priority class, e.g. class I. On the other hand, *automatic repeat request* (ARQ) only uses an error detecting code;

where in case of error, a packet is retransmitted. ARQ is feasible as long as the channel bit error rate is not too high and retransmission delay is admissible. The ARQ is more suitable for low priority class, e.g. class III. Hybrid ARQ/FEC techniques take the advantage of the two schemes. If the error in a packet cannot be corrected by the error correcting code, a retransmission will be demanded. So, Hybrid ARQ/FEC technique is more suitable for the medium priority class, e.g. class II. However, it is important to keep in mind that the bandwidth savings are a trade-off against the processing requirements on the mobile nodes. Hence the complexity of the coding algorithms must also be considered. Indeed, NLMs and MLM determine the quality of links in order to generate the paths with good quality. They try to evenly distribute the traffic in the network and avoid paths with a low quality regardless of the application. Then, application layer metrics select exactly one path out of the paths with the good quality that is more likely to meet application requirements. This implies that applications may need to adapt to the quality of network. That is why, a cross-layer quality of service model is proposed in order to responds to both network and application requirements. This model does not define specific protocols or implementations. Figure 2.2 shows the defined QoS classes together with their ALMs, NLMs and MLM constraints. Table 2.3 shows the mapping between QoS classes, ALMs, NLMs, and MLM. In this model, class I and II can be mapped to the buffer level and hop count at the NLMs and to link SINR at MLM; and class III to stability level and hop count, and to link SINR at MLM. Hence, MAC layer metrics, network layer metrics and application layer metrics might be used as the additional constraints to the conventional ones to determine paths between a source and a destination.

Table 2.3 QoS Classes & Mapping

Priority Classes	ALMs	NLMs	MLM
Class I	Delay	Buffer & Hop Count	SINR
Class II	Throughput	Buffer & Hop Count	SINR
Class III	Best effort	Stability & Hop Count	SINR

An application can adapt to the corresponding ALM based on following mechanism [44-45]. A node checks the application requirements. If the application is delay sensitive–i.e. class I, then the dropping approach may be used. Although this approach implies an increase of loss rate, the probability of the path failure is reduced as it avoids an extra delay. On the other hand, if the application requires low loss rate- i.e. class II, then the delaying approach might more appropriate when the stability is high and hence the path can support an extra delay caused by this approach. At the network layer, routing protocol must be *adaptive* according to given NLMs of nodes in the path generation process between source node and destination node. The MAC layer, on the other hand, can adapt the coding technique to meet the application requirements given current channel and network conditions.

2.10 QoS Signaling

QoS signaling acts as the control center in QoS support. It coordinates the behaviors of QoS routing, QoS MAC, and other components such as admission control and scheduling. The QoS model determines the functionality of QoS signaling. QoS signaling is used to reserve and release resources, set up, tear down, and renegotiate flows in the networks.

QoS signaling system should have following two distinct mechanisms

i. The QoS signaling information must be reliably carried between the routers
ii. The QoS signaling information must be correctly interpreted and the relative processing should be activated. Based on the first mechanism, the QoS signaling system can be divided into in-band signaling and out-of-band signaling. The in-band signaling refers to the fact that control information is carried along with data packets [46], the out-of-band signaling refers to the approach that uses explicit control packets.

2.10.1 Resource Reservation Protocol (RSVP)

This protocol is adopted as the signaling system in the Internet. RSVP is an out-of-band signaling system.

RSVP has two important characteristics.

i. It is the receiver, instead of the sender, that initiates the resource request. Note that different receivers may have different requirements in the multicast case.
ii. The flow and reservation information is periodically refreshed. This feature is important in case of link failures. Currently, RSVP has been modified and extended to include more mechanisms, for example, resource reservation for aggregation of flows [47].

RSVP is not suitable for MANETs since the signaling overhead of RSVP is heavy for the mobile hosts. The signaling control message will contend with data packets for the channel and cost a large amount of bandwidth. Furthermore, it is not adaptive for the time-varying topology because it has no mechanism to rapidly respond to the topology change in MANETs.

2.10.2 INSIGNIA

INSIGNIA [46][48] is an in-band signaling system that supports QoS in MANETs. It has been claimed as the first signaling system designed solely for MANETs. The signaling control information is carried in the IP option of every IP data packet, which is called the INSIGNIA option. Like RSVP, the service granularity supported by INSIGNIA is per-flow management. Each flow state information is established, restored, adapted and removed over an end-to-end session in response to topology change and end-to-end QoS condition. Figure 2.3 shows the position and the role of INSIGNIA in wireless flow management at a mobile host. The packet-forwarding module classifies the incoming packets and forwards them to the appropriate modules (routing, INSIGNIA, local applications, and packet scheduling modules). If a received IP packet includes an INSIGNIA option, the control information is forwarded to and processed by the INSIGNIA module. In the meantime, the received packet is delivered to a local application or forwarded to the packet-scheduling module according to the destination address in the IP head. If the mobile host is the destination of the packet, the packet is processed by a local application. Otherwise the mobile host will forward the packet to the next hop determined by the MANET routing protocol. Before the packets are sent through the MAC component, a packet-scheduling module is used to schedule the output of the flows in order to fairly allocate the resource to different flows. In INSIGNIA, a weighted round-robin (WRR) discipline that takes location dependent channel conditions into account [49] is implemented. A wide variety of scheduling disciplines could be used to realize the packet scheduling. The INSIGNIA module is responsible for establishing, restoring, adapting and tearing down real-time flows. It includes fast flow reservation, restoration and adaptation algorithms that are

2.10.2 INSIGNIA

INSIGNIA [46][48] is an in-band signaling system that supports QoS in MANETs. It has been claimed as the first signaling system designed solely for MANETs. The signaling control information is carried in the IP option of every IP data packet, which is called the INSIGNIA option. Like RSVP, the service granularity supported by INSIGNIA is per-flow management. Each flow state information is established, restored, adapted and removed over an end-to-end session in response to topology change and end-to-end QoS condition. Figure 2.3 shows the position and the role of INSIGNIA in wireless flow management at a mobile host. The packet-forwarding module classifies the incoming packets and forwards them to the appropriate modules (routing, INSIGNIA, local applications, and packet scheduling modules). If a received IP packet includes an INSIGNIA option, the control information is forwarded to and processed by the INSIGNIA module. In the meantime, the received packet is delivered to a local application or forwarded to the packet-scheduling module according to the destination address in the IP head. If the mobile host is the destination of the packet, the packet is processed by a local application. Otherwise the mobile host will forward the packet to the next hop determined by the MANET routing protocol. Before the packets are sent through the MAC component, a packet-scheduling module is used to schedule the output of the flows in order to fairly allocate the resource to different flows. In INSIGNIA, a weighted round-robin (WRR) discipline that takes location dependent channel conditions into account [49] is implemented. A wide variety of scheduling disciplines could be used to realize the packet scheduling. The INSIGNIA module is responsible for establishing, restoring, adapting and tearing down real-time flows. It includes fast flow reservation, restoration and adaptation algorithms that are specifically designed to deliver adaptive real-time service in MANETs. The flow state information is managed in soft-state method, that is, the flow state information is periodically refreshed by the received signaling information. Coordinating with the admission control module, INSIGNIA allocates bandwidth to the flow if the resource requirement can be satisfied. Otherwise, if the required resource is unavailable, the flow will be degraded to best-effort service. To keep the processing simple and lightweight, INSIGNIA does not send rejection and error messages if the resource request is not satisfied.

For fast responding to the changes in network topology and end-to-end QoS conditions, INSIGNIA uses QoS reports to inform the source node of the status of the real-time flows. The destination node actively monitors the received flows and calculates QoS statistical results such as loss rate, delay, and throughput etc. The QoS reports are periodically sent to the source node. Through this kind of feedback information, the source node can take corresponding actions to adapt the flows to observed network conditions. INSIGNIA is an effective signaling protocol for MANETs. Coordinating with other network components (viz. routing protocol, scheduling, and admission control), INSIGNIA can efficiently deliver adaptive real-time flows in MANETs. However, since the flow state information should be kept in the mobile hosts, the scalability problem may hinder its deployment in the future.

2.10.3 Out-of-band Signaling versus In-band Signaling

Signaling is usually the most complex component in a computer network [50]. This is because signaling must support complex network services and have strict requirements on performance and reliability. For example, in MANETs, the flows should be rapidly established with minimal signaling overhead; active flows should be maintained even if the topology changes and rerouting happens; flow state information should be automatically removed when the session is finished. All of these are non-trivial tasks. In addition, signaling software should be extensible and maintainable because people often want to add new services into the existing network. For example, the mechanism of resource

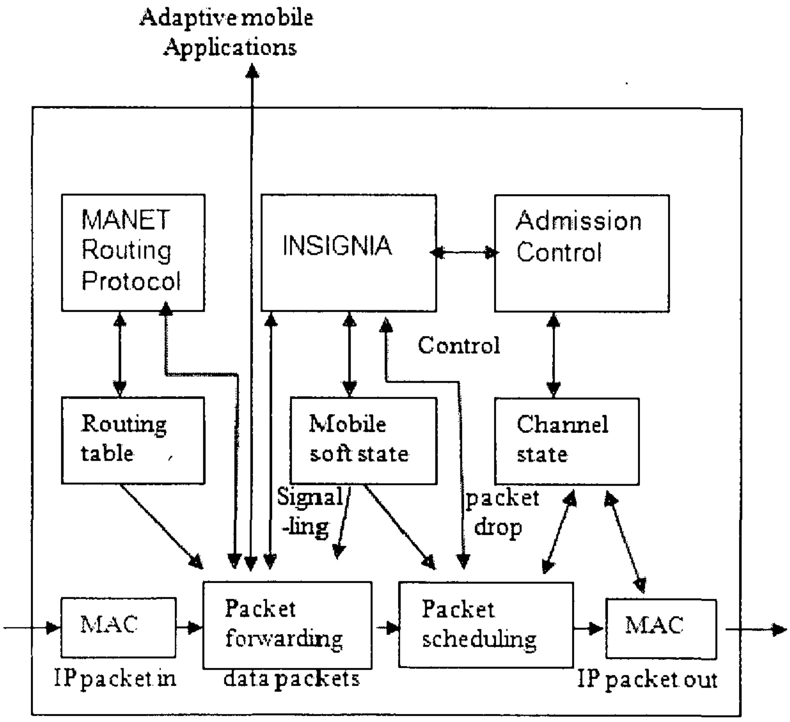


Figure 2.3: Wireless Flow Management Model at a Mobile Host

management for aggregation of flows should be provided if we want to support per-class based service in MANETs. The complexity of the signaling system requires clean solutions to deal with signaling independently. This is the main reason why most signaling systems use explicit out-of-band control messages. Because the control messages do not rely on the transmission of data packets, it is flexible to implement the out-of-band signaling system. Furthermore, the supported services can be rich and powerful. In some cases, it is even impossible to implement some functionality with absolute in-band signaling. For example, in the circumstance that the data flow is totally unidirectional from the source to the destination once it is established, sending a feedback control message back to the source with absolute in-band signaling is impossible during the session of the flow. We use the term absolute in-band signaling to refer the situation where all control information is piggybacked within data packets. Out-of-band signaling, however, consumes more network bandwidth. In wireless networks, it competes for transmission channel with data packets. Since the signaling messages should have higher priority over data packets, a complex out-of-band signaling system will greatly degrade the performance in bandwidth-constrained MANETs. On the other hand, in-band signaling carries the control information in data packets. It is usually lightweight and simple. Although in-band signaling costs some bandwidth more or less, it will not contend for the transmission channel with data packets since it is included in every data packet. This feature is very important in wireless networks, where all neighboring hosts share the transmission channel. Due to bandwidth and power constraints, keeping the signaling lightweight and simple is more important than designing a powerful but complex signaling system. At least at present, this should be one of the main principles of designing signaling system in MANETs.

2.11 QoS Routing

QoS routing searches for a path with enough resources but does not reserve resources. It is the QoS signaling to reserve resources (if necessary in the QoS model) along the path determined by QoS routing or other routing protocols. Hence, QoS routing enhances the chance that enough resources can be guaranteed when QoS signaling wants to reserve resources. Without QoS routing, QoS signaling can still work but the resource reservation may fail because the selected path may not have enough resources. QoS signaling will work better if it coordinates with QoS routing. However, since most QoS routing algorithms are complicated, we must balance the benefits against the cost of QoS routing in the bandwidth constraint MANETs.

2.11.1 Difficulties of QoS Routing

QoS routing protocols search for routes with sufficient resources for QoS requirements. The QoS routing protocols should work together with resource management to establish paths through the network that meet end-to-end QoS requirements, such as delay or delay jitter bounds, bandwidth demand, or multi-metric constraints. The QoS metrics could be concave or addictive. The bandwidth metric is concave, i.e., a certain amount of bandwidth must be required on each link along the path. Delay, delay jitter, and cost are additive. Wang et al. proved that if QoS contains at least two additive metrics, then the QoS routing is an NP-complete problem [51]. Therefore, searching for the shortest path with minimal cost and finding delay-constraint least-cost paths are NP-complete problems. For this reason, we only seek approximated solutions for these problems.

QoS routing is difficult in MANETs because

i. The overhead of QoS routing is too high for the bandwidth limited MANETs because the mobile host should have some mechanisms to store and update link state information. We have to balance the benefit of QoS routing against the bandwidth consumption in MANETs.

ii. Due to the dynamic nature of MANETs, maintaining the precise link state information is very difficult.

iii. The traditional meaning that the required QoS should be ensured once a feasible path is established is no longer true. The reserved resource may not be guaranteed because of the mobility-caused path breakage or power depletion of the mobile hosts. QoS routing should rapidly find a feasible new route to recover the service.

Comparing with the abundant work on QoS routing for fixed wire networks [52], results for QoS routing in MANETs are relatively scarce due to the above difficulties. Even the question of whether to support QoS routing in MANETs is still a hotly debated issue. However, some promising work on QoS routing in MANETs, such as CEDAR [53], ticket-based probing [54], and QoS routing based on bandwidth calculation [55], have been done and show good performance.

2.11.2 Core-Extraction Distributed Ad hoc Routing (CEDAR)

Raghupathy S. et al. [12] proposed a CEDAR algorithm, which can react effectively to the dynamics in MANETs. It includes three main components- core extraction, link state propagation, and route computation.

Core Extraction

The dominating set of a network is a set of hosts, (DS), such that every host in the network is either in DS or a neighbor of a node in DS. The minimum set of the DS is called the minimum dominating set of the network. The purpose of core extraction is to elect a set of hosts to form a core of the network by using only local computation and local state. The core of the network is an approximation of a minimum Dominating Set (DS) of the network. Every host in DS is called a core host. Every host not in DS chooses one of its neighbors who are in DS as its dominator. Note that the dominator of a core host is itself. Two core hosts are called nearby core hosts if the distance between them is no more than 3. A path between two core hosts is called a virtual link. The graph that consists of core nodes and virtual links to connect nearby core hosts is called a core graph. A core path is a path in the core graph. CEDAR presents a distributed algorithm to choose core nodes. When a host loses connectivity with its dominator due to mobility, it either finds a core neighbor as its dominator, or nominates one of its non-core-host neighbors to join the core, or itself joins the core. Since flooding in MANETs causes repeated local broadcasts, it is highly unreliable because of the abundance of hidden and exposed hosts [56]. CEDAR proposes the core broadcast mechanism to ensure that each core host does not transmit a broadcast packet to every nearby core host. The core broadcast approach has very low overhead and adapts easily to topology changes. It also provides an efficient way to update link state information.

Link State Propagation

In order to compute the feasible QoS paths in CEDAR, each core host maintains its local topology as well as the link-state corresponding to stable high-bandwidth links further away. Note that it does not keep the link state information of unstable or low-bandwidth further links, because these links are not useful in searching for the QoS routes. To achieve this goal, CEDAR utilizes the increase/decrease waves. For every link l = (a, b), the host a hosts to form a core of the network by using only local computation and local state. The core of the network is an approximation of a minimum Dominating Set (DS) of the network. Every host in DS is called a core host. Every host not in DS chooses one of its neighbors who are in DS as its dominator. Note that the dominator of a core host is itself. Two core hosts are called nearby core hosts if the distance between them is no more than 3. A path between two core hosts is called a virtual link. The graph that consists of core nodes and virtual links to connect nearby core hosts is called a core graph. A core path is a path in the core graph. CEDAR presents a distributed algorithm to choose core nodes. When a host loses connectivity with its dominator due to mobility, it either finds a core neighbor as its dominator, or nominates one of its non-core-host neighbors to join the core, or itself joins the core. Since flooding in MANETs causes repeated local broadcasts, it is highly unreliable because of the abundance of hidden and exposed hosts [56]. CEDAR proposes the core broadcast mechanism to ensure that each core host does not transmit a broadcast packet to every nearby core host. The core broadcast approach has very low overhead and adapts easily to topology changes. It also provides an efficient way to update link state information.

Link State Propagation

In order to compute the feasible QoS paths in CEDAR, each core host maintains its local topology as well as the link-state corresponding to stable high-bandwidth links further away. Note that it does not keep the link state information of unstable or low-bandwidth further links, because these links are not useful in searching for the QoS routes. To achieve this goal, CEDAR utilizes the increase/decrease waves. For every link l = (a, b), the host a and b are responsible for monitoring the available bandwidth on the link. When the link l comes up or the bandwidth of the link l increases beyond a given threshold value, host a and b will notify their dominators to initialize a core broadcast for an increase wave, which indicates the stable high bandwidth link. On the other hand, if the link l breaks down or the bandwidth of the link l decreases beyond a given threshold value, host a and b inform their dominators to initialize a core broadcast for a decrease wave, which indicates the unstable or low bandwidth link. The increase wave is slow moving, while the decrease wave is fast moving. For the same link state, the fast-moving decrease wave will take over and kill the slow-moving increase wave. Finally, the survivable increase wave will propagate the stable high-bandwidth link state information through the cores. In addition, CEDAR provides a mechanism that keeps the decrease wave from propagating throughout the whole network. So the unstable low-bandwidth link states are kept locally.

Route Computation

The QoS route computation in CEDAR includes three main steps (a) discovering the location of the destination and establishing a core path to the destination, (b) searching for a stable QoS route with the established core path as a directional guideline, and (c) dynamically re-computing QoS routes upon link failures or topology changes. When a source s wants to send messages to a destination d, it first sends a <s, d, b> triple to its dominator, dom(s), where b is the required bandwidth. If dom(s) can calculate a feasible path to d with its local state information, it responds to s immediately. Otherwise, dom(s) discovers the dom(d) if it does not know the location of d, and simultaneously establishes a core path to d. A core path request message is initialized and core-broadcasted by dom(s).

By the virtue of the core broadcast algorithm, the core path request message traverses an implicitly established source routed tree from dom(s), which is typically a breadth-first search tree. Thus the core path is approximately the shortest path in the core graph from dom(s) to dom(d) and provides a good directional guideline for the calculation of QoS routes. Because dom(s) knows the up-to-date local topology and only some possibly out-of-date link state information about remote stable high-bandwidth links, dom(s) may not be able to calculate a possible path to d with enough required bandwidth based on its own link state knowledge. However, as mentioned before, the core path from dom(s) to dom(d) provides a good directional guideline for the possible QoS routes. Based on its own link state information, dom(s) will try to calculate a route with enough bandwidth to meet the bandwidth requirement to the furthest core node, dom(t), which is on the core path from dom(s) to dom(d). Then dom(s) sends dom(t) a message to notify it of continuing the same computation further. If dom(t) can calculate a route with enough bandwidth to d based on its own link state knowledge, then the computation is finished and a feasible path with enough bandwidth from dom(s) to d is found. Otherwise, dom(t) repeats the same operation as dom(s). The computation will continue along the core path from dom(s) to dom(d) step by step. Finally, at a core node tn, a feasible path with enough bandwidth from tn to d is found or no possible path could be produced at tn. In the first case, the whole feasible path is the concatenation of the partial paths computed by the core nodes s, t ... tn. In the latter case, the bandwidth requirement cannot be satisfied and the request is rejected.

CEDAR deals with link failures by two mechanisms

i) Dynamic recomputation of a feasible route at the point of failure.

ii) Notification back to the source to activate re-computation of a feasible route at the source.

iii) The two mechanisms work in concert to respond to topology changes.

The simulation of CEDAR shows that it can compute good admissible routes with high probability and still adapt effectively with low overhead to the dynamics of the network topology. These characteristics are very important to QoS routing in MANETs.

2.11.3 Ticket-Based Probing Algorithm

Ticket-based probing algorithm has been proposed for QoS routing in MANETs. The basic idea is using tickets to limit the number of candidate paths. When a source wants to find QoS paths to a destination, it issues probe messages with some tickets. The number of the tickets is based on the available state information. One ticket corresponds to one path searching; and one probe message should carry at least one ticket. So the tickets bound the maximum number of the searched paths issued from the source. When an intermediate host receives a probe message with n tickets, based on its local state information, it decides whether to and how to split the n tickets and where to forward the probe(s). When the destination host receives a probe message, a possible path from the source to the destination is found. Some questions must be answered in the above route search approach.

First, how many tickets should be issued by the source?

Second, when an intermediate host receives a probe message with n tickets, it must decide

i. Whether and how to split the n tickets?

ii. Where to forward the probe message(s). What are the ticket-splitting and probe-forwarding rules?

iii. How to dynamically maintain the multiple paths?

These questions have been solved in detail [54]. Simply stated, for the first question, more tickets are issued for the connections with tighter or higher requirements. For the second question, the link with larger residual bandwidth gets more tickets. For the third question, the techniques of re-routing, path redundancy, and path repairing are used. Other QoS routing protocols include preemptive routing, multi path routing and power aware routing.

2.12 QoS MAC Protocol

QoS MAC protocol is an essential component in QoS support in MANETs. All upper-layer QoS components (QoS routing and QoS signaling) are dependent on and coordinate with the QoS MAC protocol.

2.12.1 Mechanisms of QoS MAC Protocols

QoS supporting components at upper layers, such as QoS signaling and QoS routing, assume the existence of a MAC protocol, which solves the problems of medium contention, supports reliable unicast communication, and provides resource reservation for real-time traffic in a distributed wireless environment. A lot of MAC protocols [57] have been proposed for wireless networks. Unfortunately, their design goals are usually to solve medium contention and hidden/exposed terminal problems and improve throughput. Most of them do not provide resource reservation and QoS guarantees to real-time traffic. The first problem that a MAC protocol in wireless networks should solve is the hidden/exposed terminal problem. As shown in figure 2.4, host A and host C can not hear each other. When A is transmitting a packet to B, C cannot sense the transmission from A. Thus C may transmit a packet to B and cause a collision at B. This is the "hidden terminal" problem since A is hidden from C. Similarly, when B is transmitting a packet to C, A can not initiate a transmission to D, since this can potentially cause collisions of the control packets at both B and A, thereby disrupting both transmissions. This is the "exposed terminal" problem since A is exposed to B. An RTS-CTS dialogue can be used to solve the hidden/exposed terminal problem. In figure 2.4, when C wants to send a data packet to B, it first sends a Request-To-Send (RTS) message to B. When B receives the RTS, it broadcasts a Clear-To-Send (CTS) message to C and A. When C receives the CTS, it begins to transmit the data packet. Upon receiving the CTS, A will defer its data transmission because it knows B will receive data from C. This method avoids the possible collisions at host B and thus solves the hidden terminal (A is hidden from C) and exposed terminal (A is exposed to B) problems. Another dialogue frequently used in MAC protocols is the PKT-ACK dialogue, which means the sender sends a data packet (PKT) to the receiver and the receiver immediately responds with an acknowledgment packet (ACK) to the sender if the data packet is correctly received.

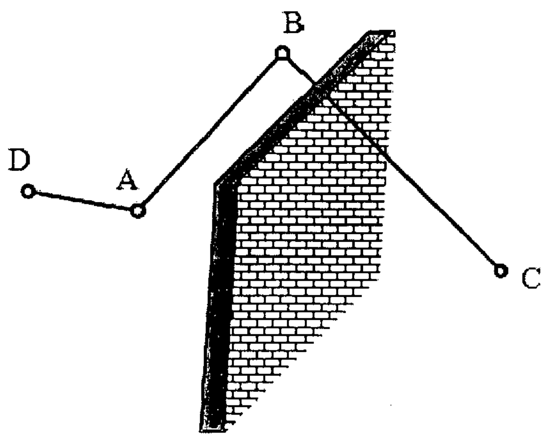


Figure 2.4: Hidden Terminal Problems

Failure to receive the ACK will prompt a retransmission after a short timeout within the link level. Besides dealing with the hidden/exposed terminal problems, a QoS MAC protocol must provide resource reservation and QoS guarantees to real-time traffic. The GAMA/PR protocol [58] and the newly proposed Black-Burst (BB) contention mechanism [59] can provide QoS guarantees to real-time traffic in a distributed wireless environment. However, they are supposed to work in a wireless LAN in which every host can sense each other's transmission, or in a wireless network without hidden hosts.

2.12.2 Multiple Access Collision Avoidance with Piggyback Reservation (MACA/PR)

C.R. Lin and M. Gerla [60] proposed MACA/PR for multihop wireless networks. MACA/PR provides rapid and reliable transmission of non-real-time data grams as well as guaranteed bandwidth support to real-time traffic. For the transmission of non-real-time data grams in MACA/PR, a host with a packet to send must first wait for a free "window" in the reservation table (RT), which records all reserved send and receive windows of any station within the transmission range. It then waits for an additional random time on the order of a single hop round trip delay. If it senses that the channel is free, it proceeds with RTS-CTS-PKT-ACK dialogue for a successful packet transmission. If the channel is busy, it waits until the channel becomes idle and repeats the above procedure. For the transmission of real-time packets, the behavior of MACA/PR is different. In order to transmit the first data packet of a real-time connection, the sender S initiates an RTS-CTS dialogue and then proceeds with PKT-ACK dialogues if the CTS is received. For subsequent data packets (not the first one) of a real-time connection, only PKT-ACK dialogues are needed. Note that if the sender fails to receive several ACKs, it restarts the connection with the RTS-CTS dialogue again. MACA/PR does not retransmit the real-time packets after collision. In order to reserve bandwidth for real-time traffic, the real-time scheduling information is carried in the headers of PKTs and ACKs. The sender S piggybacks the reservation information for its next data packet transmission on the current data packet (PKT). The intended receiver D inserts the reservation in its reservation table (RT) and confirms it with the ACK to the sender. The neighbors of the receiver D will defer their transmission once receiving the ACK. In addition, from the ACK, they also know the next scheduled receiving time of D and avoid transmission at the time when D is scheduled to receive the next data packet from S. The real-time packets are protected from hidden hosts by the propagation and maintenance of reservation tables (RT) among neighbors, not by the RTS-CTS dialogues. Thus, through the piggybacked reservation information and the maintenance of the reservation tables, the bandwidth is reserved and guaranteed for the real-time traffic.

CHAPTER 3

THE ASSESSMENT OF EFFECT ON QOS PARAMETERS OF STATIC & DYNAMIC NETWORKS FOR DIFFERENT PROTOCOLS

3.1 Background & Motivation

Ad-hoc networking is a concept in computer communications, which means that users wanting to communicate with each other form a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore is willing to forward packets for other nodes. For this purpose, a routing protocol is needed. Although considerable amount of simulation work [61-66] has been done to measure the performance of ad-hoc routing protocols, due to the constant changing nature of these protocols, a new performance evaluation is essential.

In recent years several routing protocols and new standards have been reported to enhance the capabilities of ad hoc routing protocols such as Ad-hoc On-demand Distance Vector Routing (AODV), Destination sequenced distance vector (DSDV) and Dynamic source routing (DSR). A very little performance evaluation and comparison between them is available in literature. So a continuous updating of performance evaluation is essential.

In this work, a comparative performance evaluation has been carried out for all available metrics for recently reported protocols such as (AODV, DSDV, DSR, etc.). All these protocols are constantly being improved by IETF. As a result, a comprehensive performance evaluation is essential of ad-hoc routing protocols. Since these protocols have different characteristics, the comparison of all performance differentials is not always possible.

The simulation analysis has been carried out for different protocols for different parameters of wireless ad hoc networks. The performances of networks are evaluated in terms of number of retransmission attempts, control traffic sent and received, data traffic sent and received, throughput, routing traffic sent and received and delay with the help of OPNET/ns2 simulator. The work presents the results of a packet or bit-level simulation.

3.2 Related Work

Many routing protocols for wireless ad hoc network have been reported in the literature [3-12] [67]. Performance evaluation results for some ad hoc network protocols were previously reported in [68] which primarily covered the impact of the throughput, end-to-end delay, and no. of hopes. A performance comparison of multi-hop ad hoc wireless network routing protocols are reported in [69-72]. The very few comparative analysis of different QoS parameter between the different protocols has been reported. Recently H. Hallani et al. [73] has reported the experimental setup for ad hoc network and calculated the performance of throughput having five and twenty nodes using AODV protocol. In his analysis he has consider all the nodes are static. In this work, initially we have compared the various QoS parameters (such as control traffic received and sent, data traffic received, throughput, retransmission attempts, routing traffic sent and received) of recently reported protocols using OPNET/ns-2.

The work is extended to see the effect of protocols like DSDV, AODV and DSR when the node are static, keeping the same scenarios reported by Hallani for the analysis of throughput and delay. Further the analysis has been carried out for dynamic behavior of the network (by giving mobility) for AODV protocol. We analyze the effect of throughput for different protocol of different scenario and for validation the results are compared with experimental data of AODV protocol.

3.3 Simulation Environment

Simulation environment consists of 20 wireless nodes forming an ad hoc network, moving about over a 100 m x 100 m flat space. Each run of the simulator accepts as input a scenario file that describes the exact motion of each node and the exact sequence of packets originated by each node, together with the exact time at which each change in motion or packet origination is to occur. The simulation parameters are given in table 3.1. Figure 3.1 is a snapshot of the network model considers for simulation. For evaluating the effect of variation on different protocols- routing traffic received and sent, data traffic received & sent, control traffic received & sent, throughput, retransmission attempts and delay. Protocol evaluations are based on the simulation using OPNET/ns2 simulator.

Table 3.1 Simulation Environment

Area (m)	100 x 100
Physical Characteristics	DSSS
Packet Reception Power Threshold	5.33 E-14
Mobility Model	random waypoint
Node Placement	random uniform
Buffer Size	128000
Fragmentation Threshold	512
Data Rate (Mbps)	11
No. of Nodes	20

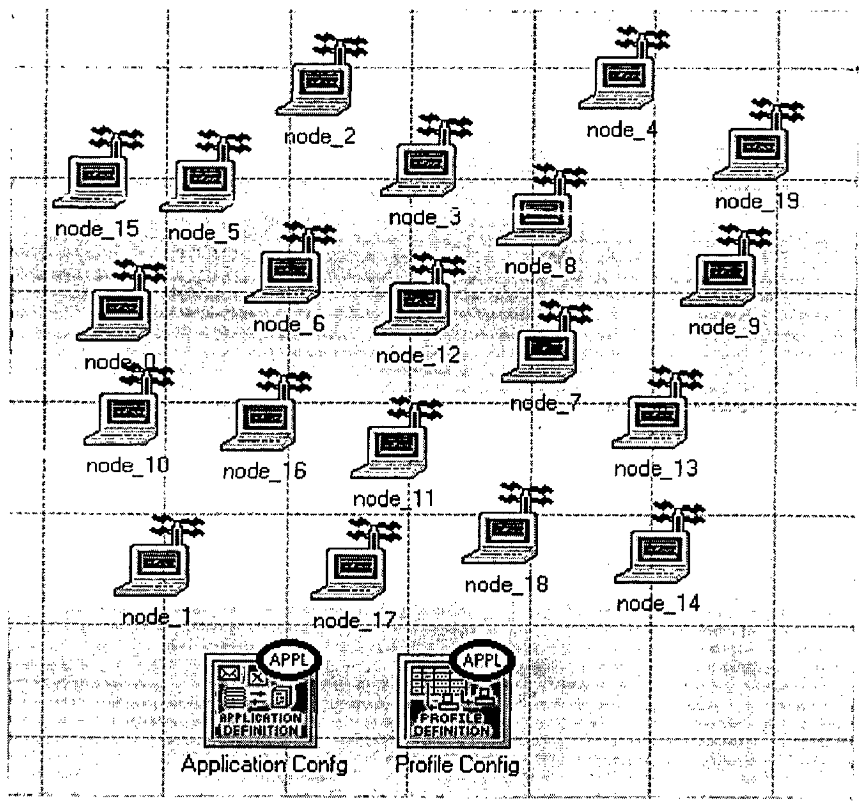


Figure 3.1: Ad-hoc Network Model

3.4 Simulation Results & Analysis

We compare the different QoS parameters with different protocols for static and dynamic networks and for validation the results are compared with experimental data. We have considered the four different cases for analysis.

Case 1: Analysis of different QoS parameters for different protocols such as AODV, DSDV and DSR of static network.

Case 2: Analyze the Qos parameters for different protocol with varying the load.

Case 3: Impact of delay and throughput analysis for different scenario and compare the results with experimental data for validation of results.

Case 4: Impact of throughput with mobility for AODV protocol.

Case 5: Impact of throughput for different scenario for DSDV, AODV and DSR protocols.

Case 1: Analysis of different QoS parameters for different protocols such as AODV, DSDV and DSR of static network

Figure 3.2 shows the control traffic sent in bits/sec. It is obvious that AODV performs better than DSDV and DSR. Although DSDV and DSR have shown an average performance throughout the entire simulation time, they show better performance compared to AODV at the start and end of the simulation time. AODV uses a HELLO message, which is critical for AODV's better performance. Figure 3.3 shows the control traffic received in bits/s for AODV, DSDV and DSR protocols for a wireless application. It is observed from the simulation results that the AODV protocol performs better than the other two (DSDV and DSR). Although DSDV does not perform well at the beginning, later it performs better. DSR's performance remains average during the entire evaluation time. Both DSDV and DSR have to go through route creation using RREQ and RREP messages. Once the routes are created, DSDV and DSR tend to do better than AODV. It is observed from the simulation results as shown in figures 3.2 and 3.3 that, near the end of simulation time, both DSDV and DSR show better performance than AODV.

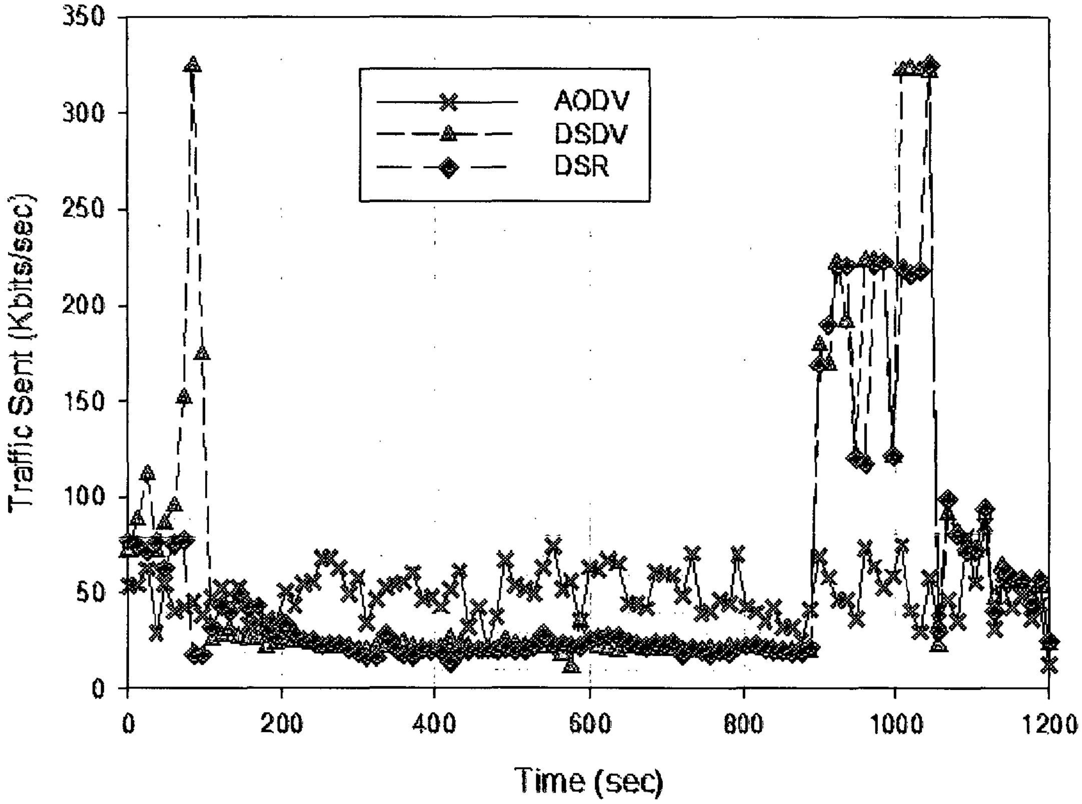


Figure 3.2: Control traffic sent for different protocols

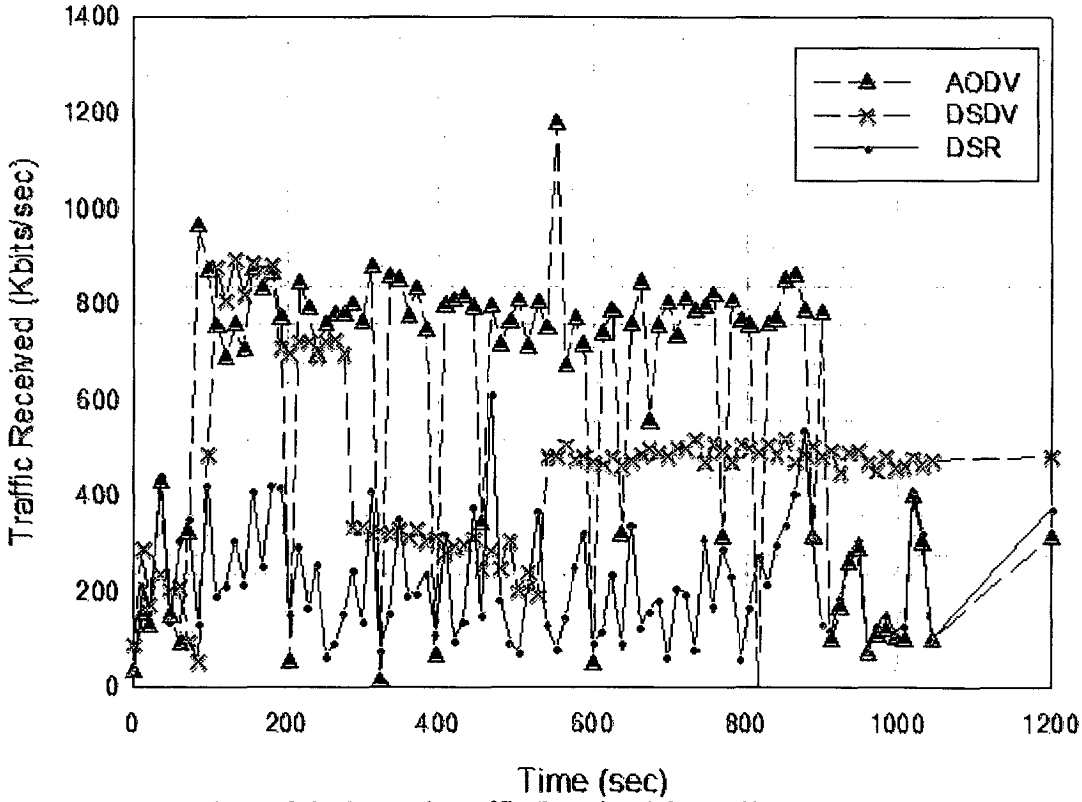


Figure 3.3: Control Traffic Received for Different Protocols

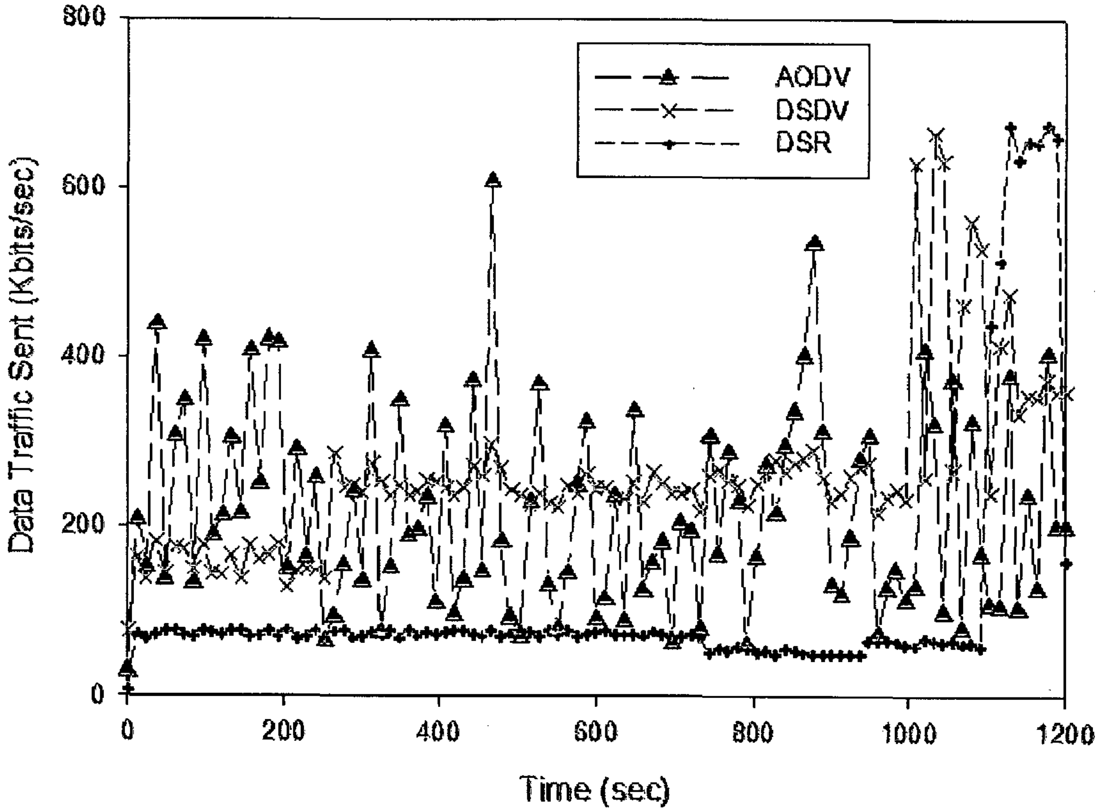


Figure 3.4: Data Traffic Sent for Different Protocols

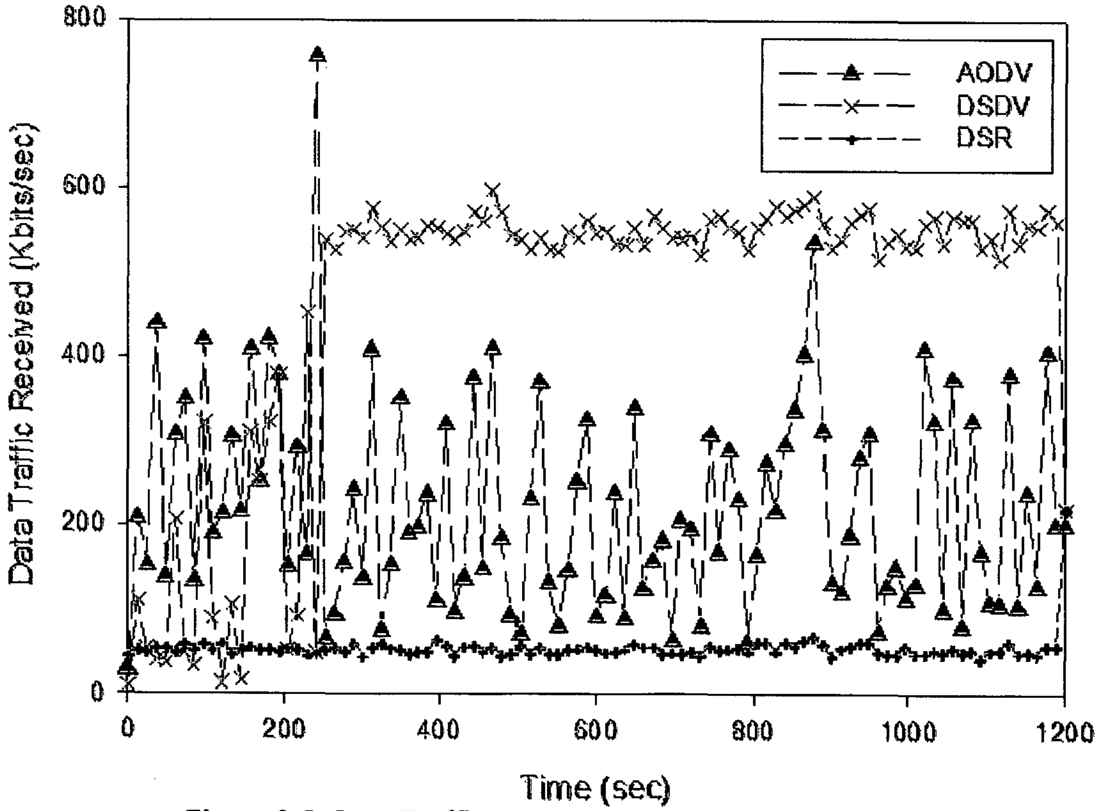


Figure 3.5: Data Traffic Received for Different Protocols

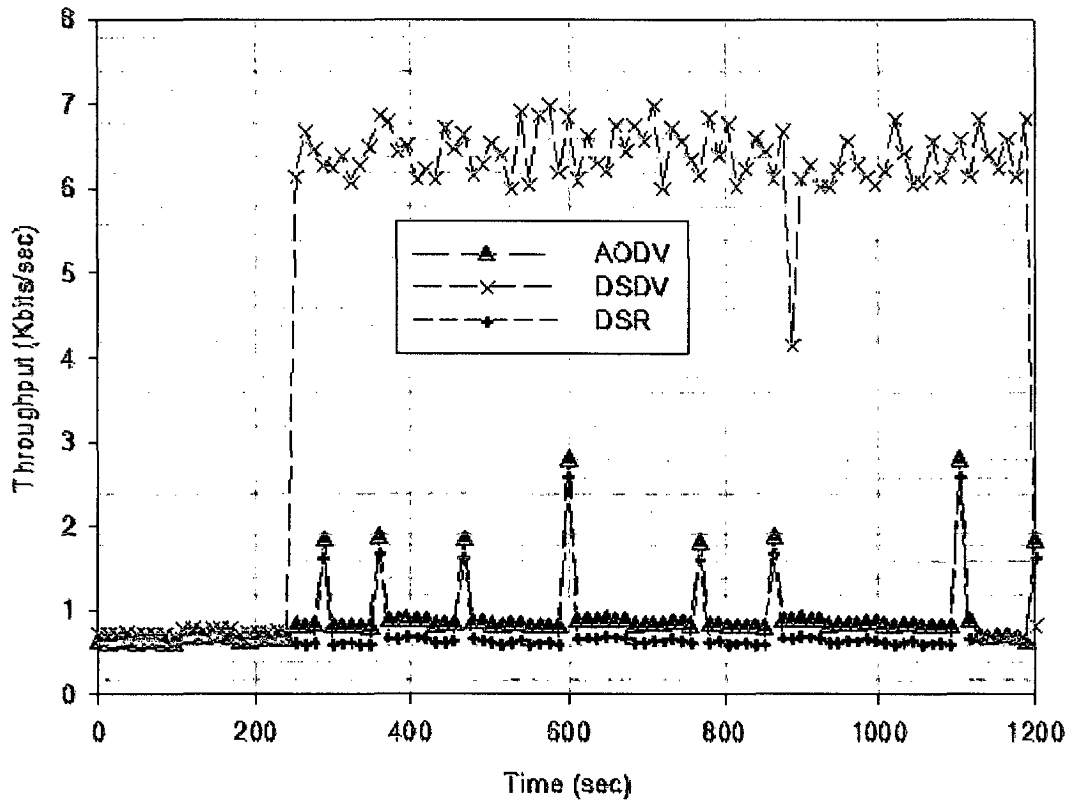


Figure 3.6: Throughput Comparison of Different Protocols

In figure 3.4, it is observed that AODV performs well during most of the simulation time. DSDV shows consistent performance and peaks at the end of the simulation. DSR does not show any positive traffic except for the last few seconds of the simulation. From figure 3.5, it is evident that, at the beginning of the simulation AODV appears to dominate over DSDV and DSR, but at the most of the simulation time, DSDV yields the best result. DSR shows poor performance and the traffic remains always at the lower level, whereas DSDV performs well most of the time. Figure 3.6 shows the throughput in bits/sec for AODV, DSDV and DSR protocols, where DSDV shows significantly better performance than the other two (AODV and DSR), and AODV performs slightly better than DSR.

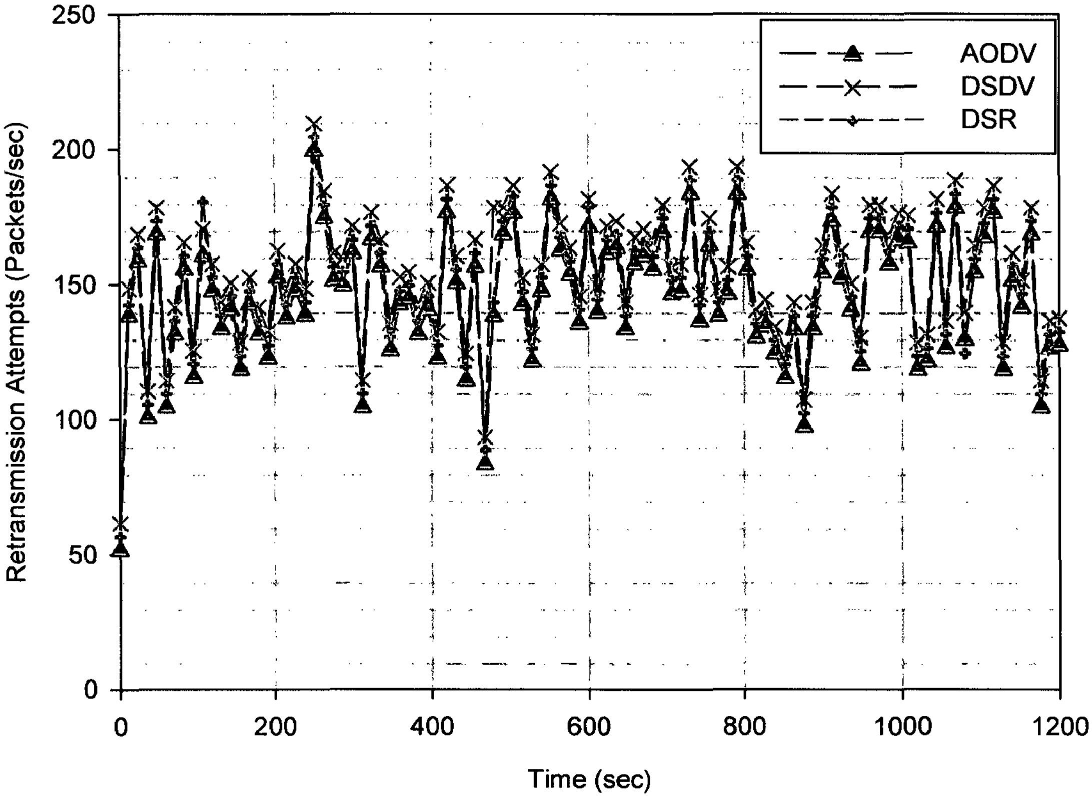


Figure 3.7: Retransmission Attempts for Different Protocols

Figure 3.7 shows the retransmission attempts in packets as a function of time for wireless network involving different protocols. It is evident from figure 3.7 that AODV requires a lot of retransmission attempts before it can successfully transmit data due to the fact that only AODV uses HELLO message. When a node first gets a RREQ message for a destination, if it does not have a route for the requested destination, it broadcasts a RREP message for source. In this way, it tries to transmit the HELLO message until it gets the destination node. DSDV and DSR have almost the same logic to find a route and show almost similar performance near the end of the simulation time.

Case 2: Analyze the QoS parameters for different protocol with varying the load

We investigated the effect of different loads (30, 50 and 70 nodes) on AODV protocol performance. Figures 3.8 and 3.9 show AODV performance of routing traffic sent and routing traffic received, for different loads, respectively. We observe that the number of packets received and sent per second increases with incremental load increase. This is due to the route cache AODV uses for creating and maintaining routes. AODV keeps a large amount of data in routing cache, which increases with the increase in the number of nodes in a network. To analyse the effect of different load, there are various node are used to evaluate the performance of the different protocols (AODV, DSDV, DSR).

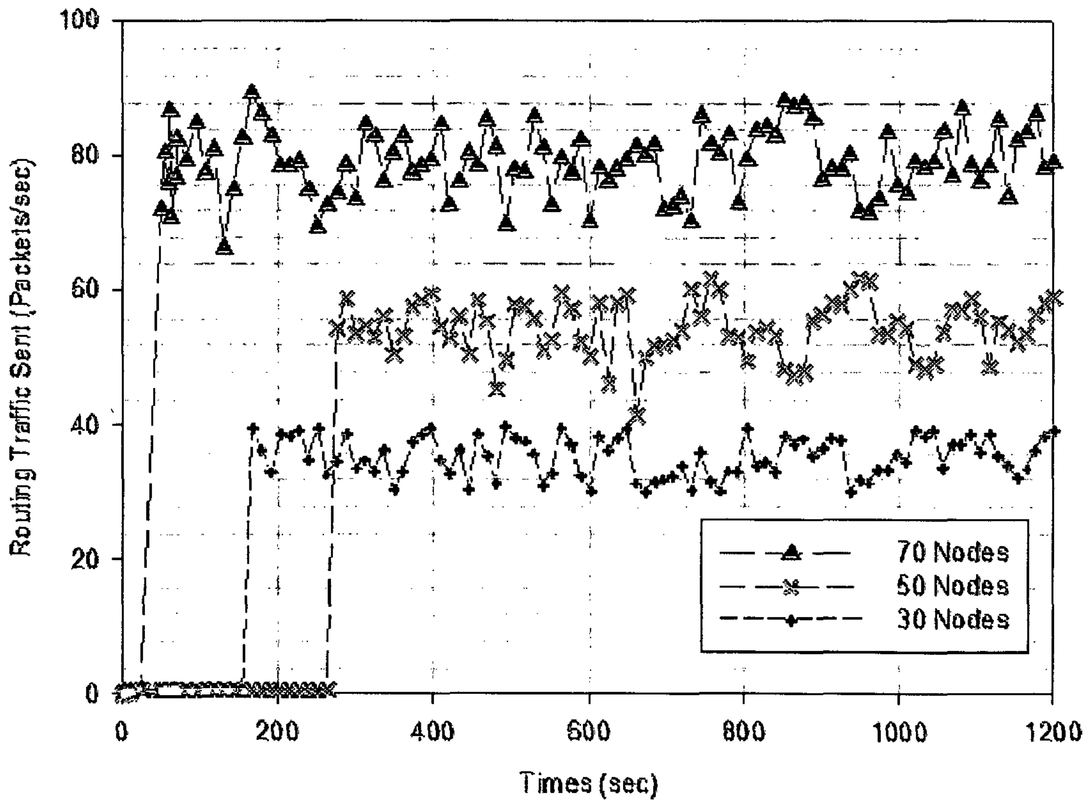


Figure 3.8: Routing traffic sent for AODV protocols under various loads

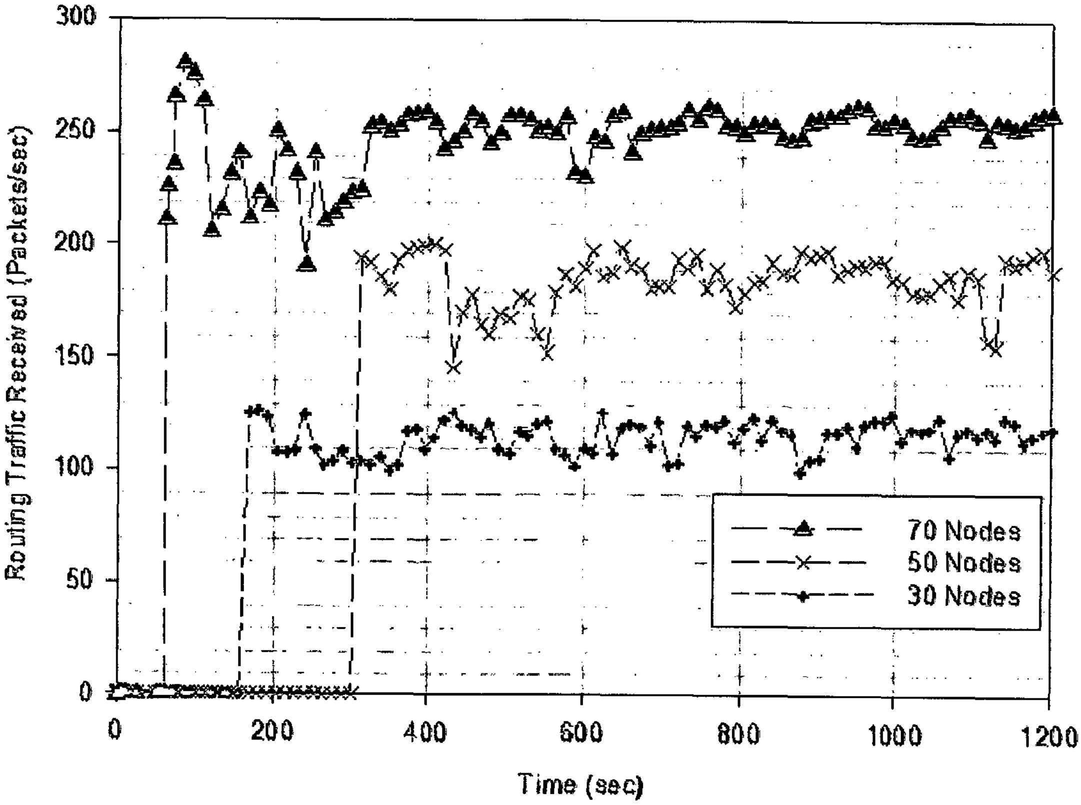


Figure 3.9: Routing traffic received for AODV protocol under various loads

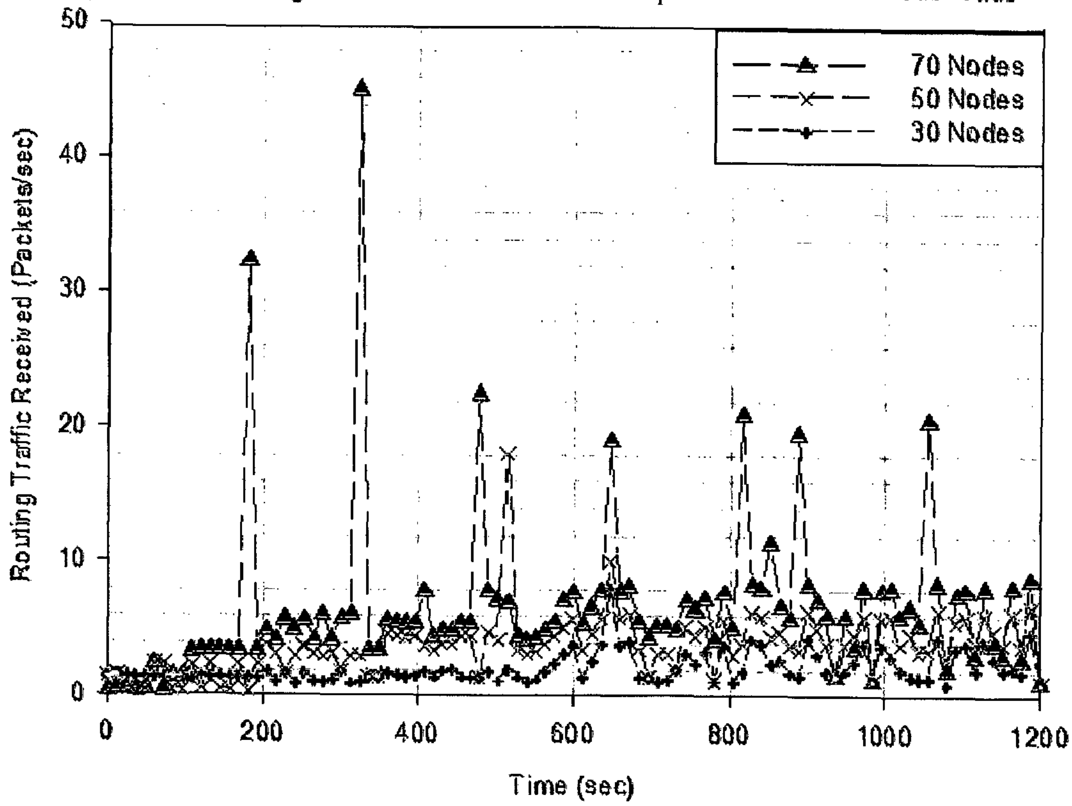


Figure 3.10: Routing traffic received for DSDV protocol under various loads

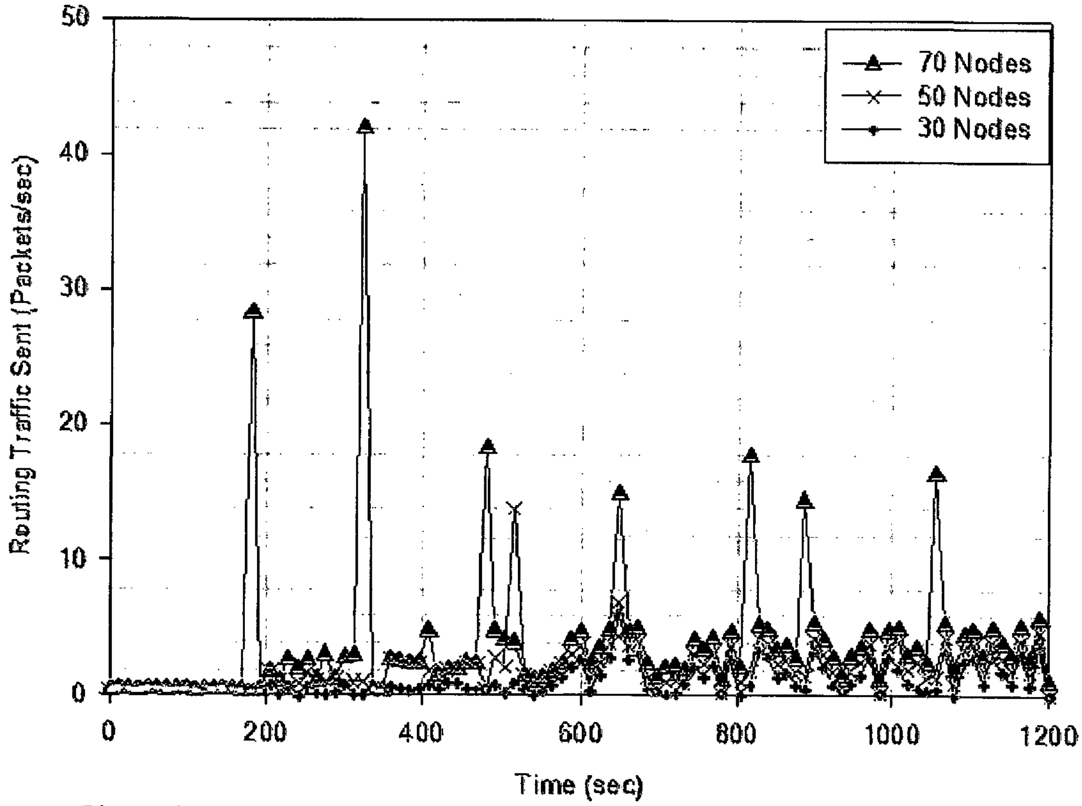


Figure 3.11: Routing traffic sent for DSDV protocol under various loads

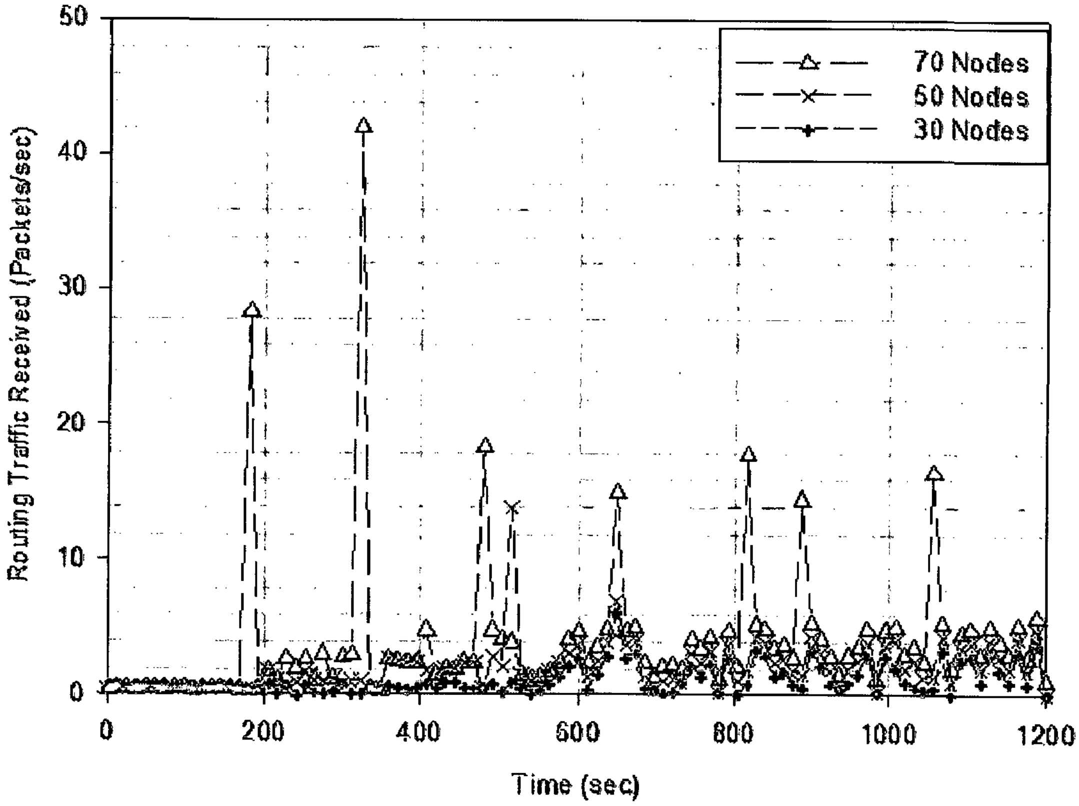


Figure 3.12: Routing traffic received for DSR protocol under various loads

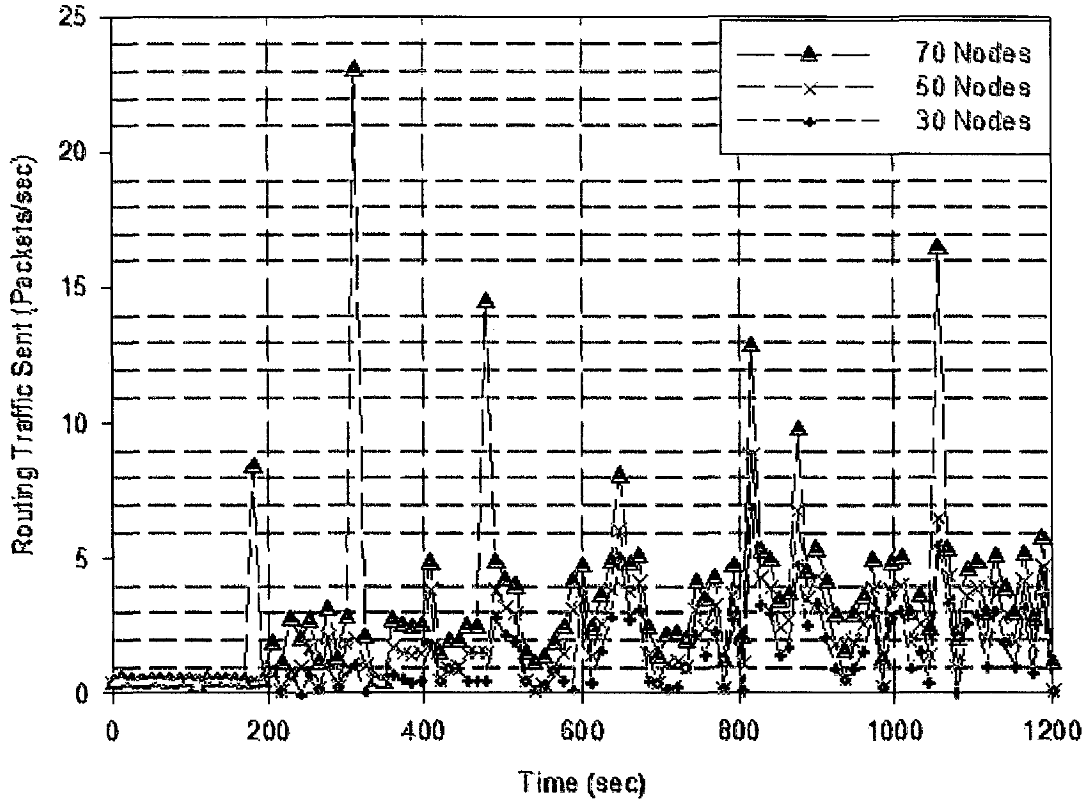


Figure 3.13: Routing traffic sent for DSR protocol under various loads

Figures 3.8-3.13 show the routing traffic received and routing traffic sent in packets/sec, respectively, for various load using the AODV, DSDV and DSR algorithm. Figures 3.8-3.13 show that the network is very sensitive towards load variation. However, in case of 30 and 50 nodes, the difference is minor. As the nodes increases, the performance of the protocols is highly affected. One possible reason may be due to the broadcasting of RREQ message during route discovery. The algorithm uses RREQ packets and broadcasts the RREQ to all the neighbors. As a result, the routing traffic received and routing traffic sent is higher in a network of 70 nodes compared to 50 or 30 nodes. However, at the beginning all networks, regardless of load, take a few moments to set up the network before starting routing traffic. Therefore, we see almost zero performance for all loads in the initial time period. Once the route is established, the performance of the AODV protocol for different load condition shows better results throughout the simulation time except the initial time. Similarly we analyze the performance of different protocols (DSDV & DSR) as shown in figures 3.9-3.13 with varying the load and comparative result has been given in table 3.2.

Table 3.2 Performance Comparison for Different Protocols

	AODV	DSDV	DSR	Figures
Control Traffic Received	Good	Avg.	Avg.	3.3
Control Traffic Sent	Good	Poor	Poor	3.2
Data Traffic Received	Average	Better	Avg.	3.5
Data Traffic Sent	Good	Avg.	Avg.	3.4
Throughput	Better	Avg.	Poor	3.6
Retransmission Attempt	Good	Avg.	Avg.	3.7
Routing traffic sent	Better	Good	Avg.	3.8, 3.10, 3.12
Routing traffic received	Better	Avg.	Avg.	3.9, 3.11, 3.13

Case 3: Impact of delay and throughput analysis for different scenario and compare the results with experimental data for validation of results

In this article we analyses the performance of the network having different load and mobility condition. The impact of throughput and delay has been carried out with different mobility condition and results are compared with the experimental data. Further the work has been extended under different loads (number of nodes in a network) and showed their corresponding performance in terms of average throughput and delay.

The network model shown in figure 3.14 consists of five nodes, which include an application and a profile definition has been created using OPNET. The application and profile definition are used to define the type of traffic sent between the nodes. The network model and AODV protocol are taken for validation and comparison of simulation result with a similar type of experimental model reported by H. Hallani et al. The channel speed of the WLAN is set to 11Mbps, and simulation time is 600 sim-sec. In this work, these are configured to send TCP traffic. The throughput between two nodes is measured by generating TCP packets from the first node and sending them to the second node. The throughput is calculated based on the time it takes these packets to get to the second node. The simulation environment is kept same as shown in table 3.3.

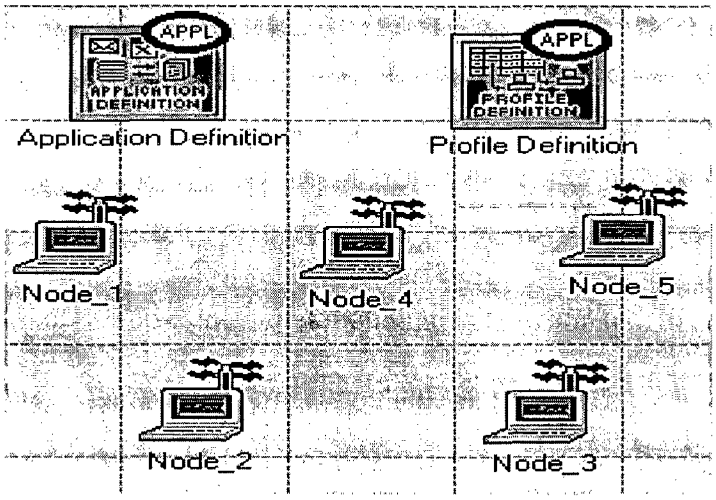


Figure 3.14: Simulation Setup for the Network

In the first scenario, only node 2 and node 4 are involved in the communication. TCP traffic is sent from node 2 to node 4 and the throughput is measured at node 2. In the second scenario, node 2 and node 3 are set up to send TCP traffic to node 4. In the third scenario, node 5, node 3, and node 2 are communicating simultaneously with node 4. In the fourth scenario, node 2 is sending traffic to node 5 to check the effect of having any of the other nodes acting as a relay node between the source and the destination.

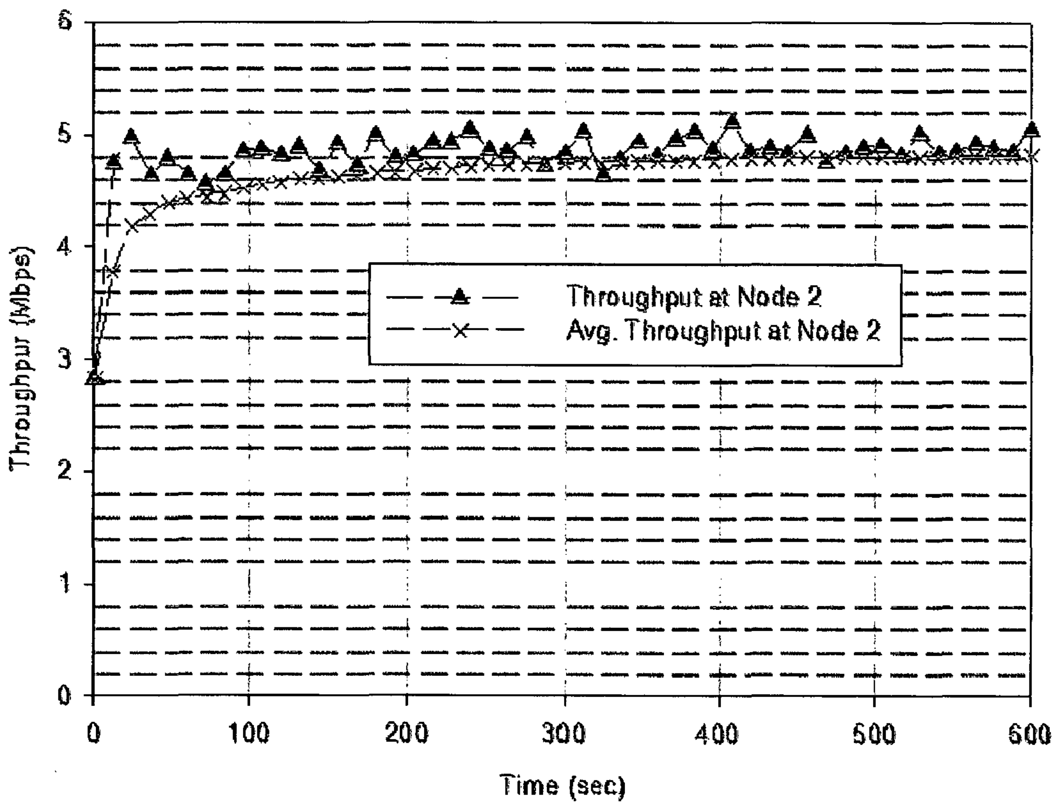


Figure 3.15: Throughput at Node 2 for First Scenario

Table 3.3 Different Scenarios

Scenario	Number of Hops
First	Node 2 and node 4 are communicated
Second	Node 2 and node 3 are involved
Third	Node 2, node 3 and node 5 are involved
Fourth	Node 2 and node 5 are communicated

Throughput Analysis for Different Scenario of Different Protocols

The simulations are carried out for throughput for all the scenarios as reported above. The variation in throughput in all the scenarios is shown in figures 3.15–3.18. All simulations run for 600 sim-seconds. Figures 3.15–3.18 show the throughput of node 2 for first, second, third, and fourth scenario, respectively. It is observed that from the result of first scenario (node 2 and node 4 are involved in the communication), the average throughput at node 2, remains constant at around 4.99Mbps as shown in figure 3.15. TCP traffic is sent from node 2 to node 4 and throughput is measured at node 2.During the second scenario (node 2 and node 3 are set up to send TCP traffic simultaneously to node 4), and measure the average throughput which is remains constant at around 2.76Mbps as shown in figure 3.16. Small fluctuations are observed in the throughput during the simulation. This can be attributed to the nature of TCP, which ensures that data is delivered from sender to receiver correctly, in order, and error-free. Such characteristics can cause delay at node 4, which is trying to respond simultaneously to both node 2 and node 3. When the simulation is carried out for the third scenario (node 5, node 3, and node 2 are communicating simultaneously with node 4) and measure the average throughput which is remains constant at around 1.94Mbps as shown in figure 3.17, the fluctuations in throughput are more noticeable; this is because more nodes are involved in the communication. During the fourth scenario (node 2 is sending traffic to node 5 to check the effect of having any of the other nodes acting as a relay node between the source and the destination), the throughput of node 2 to nearly 1.53Mbps as shown in figure 3.18.

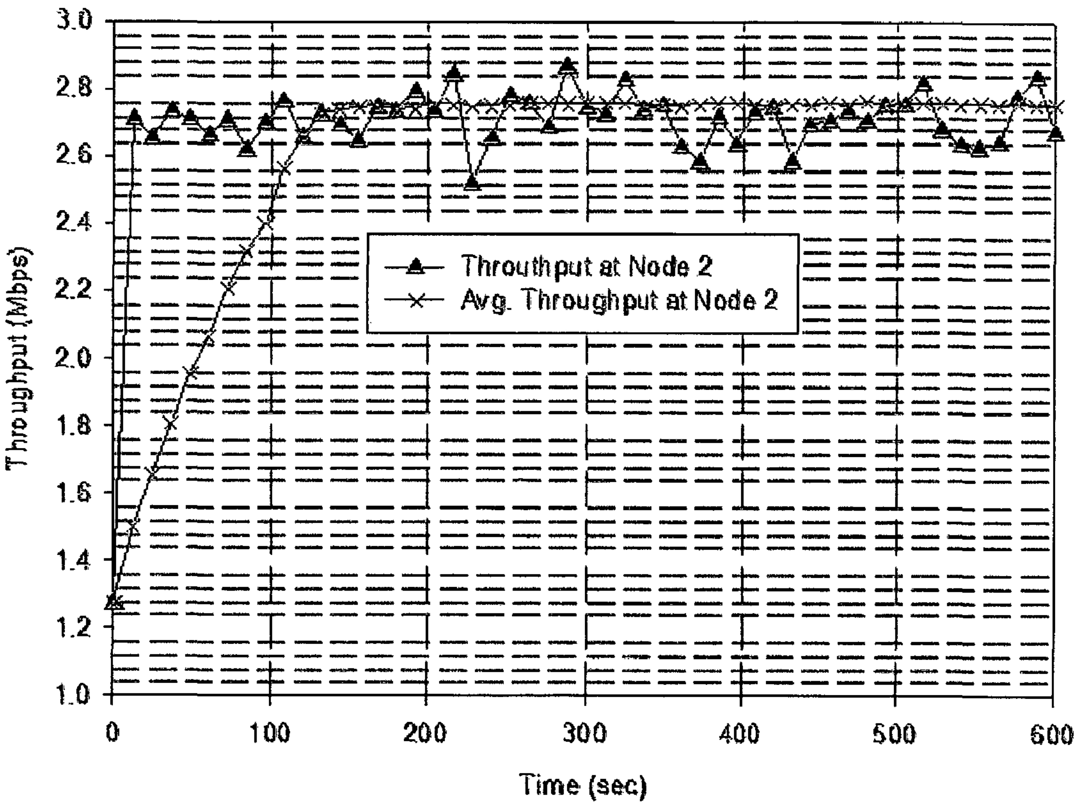


Figure 3.16: Throughput at Node 2 for Second Scenario

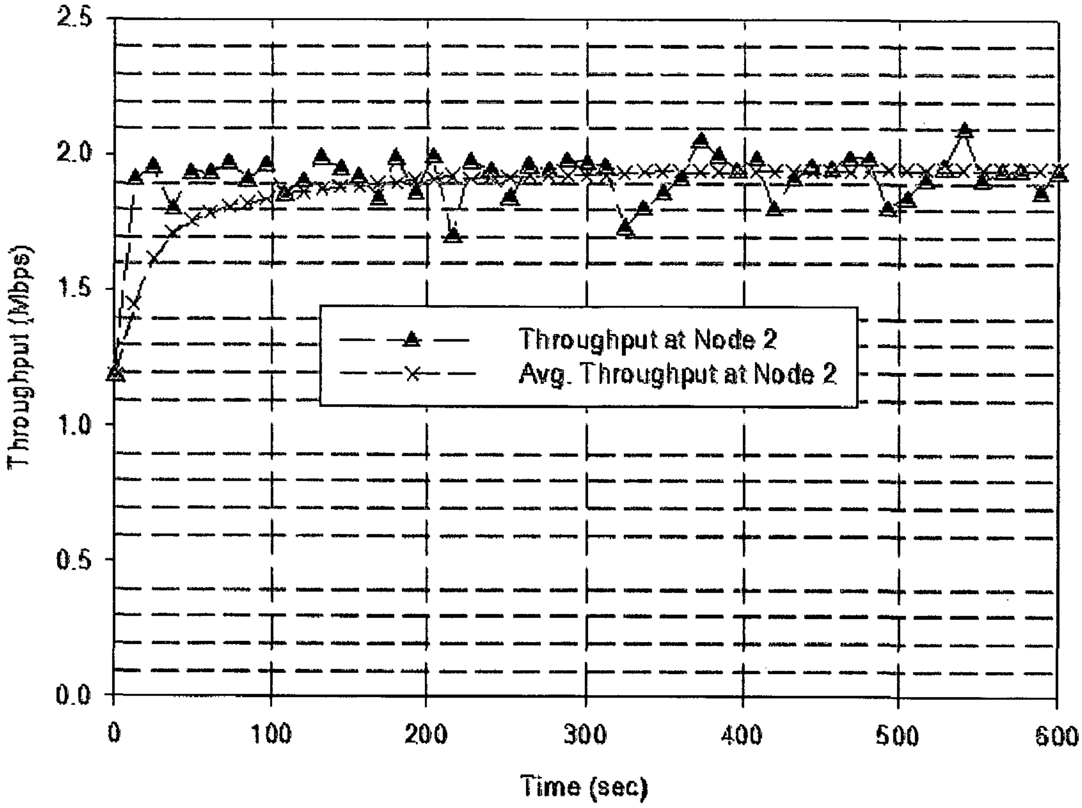


Figure 3.17: Throughput at Node 2 for Third Scenario

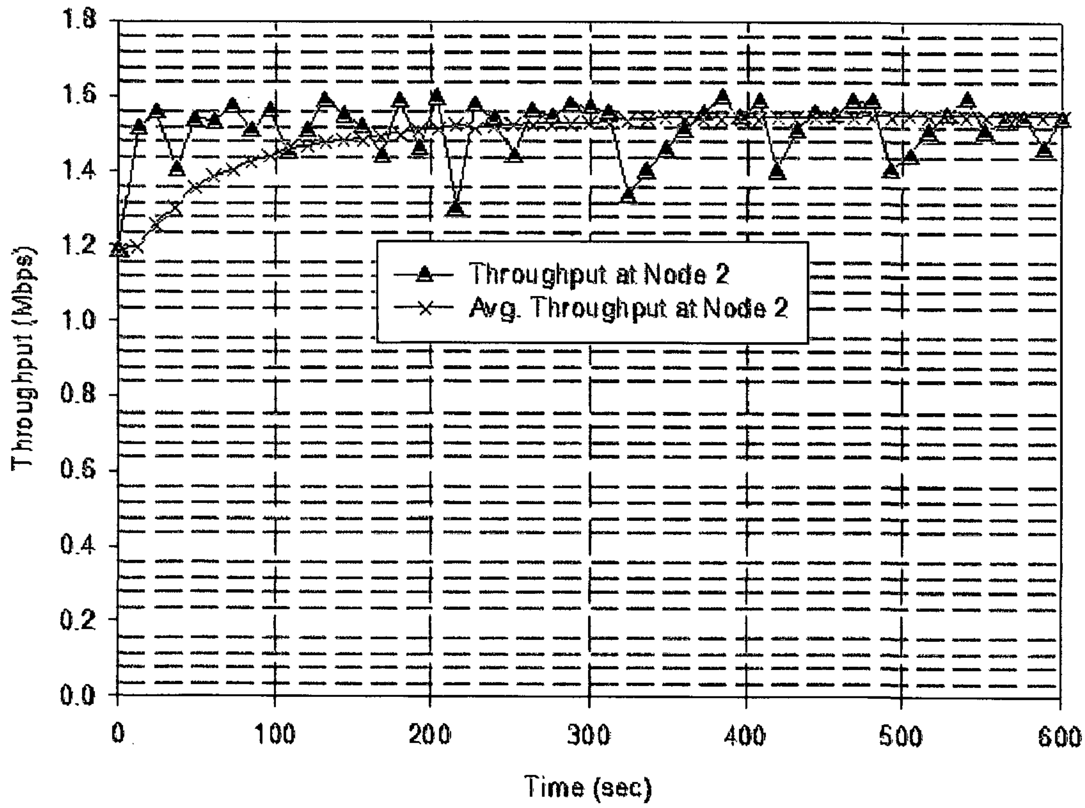


Figure 3.18: Throughputs at Node 2 for Fourth Scenario

As noted before, this is due to the increased latency, as packets have to be forwarded to node 4 first and then delivered to node 1. The drop in throughput between the first, second, and third scenario may be due to the high congestion and the overwhelming of node 4.

Analytic and Simulation Comparison

The throughput and delay for the network (figure 3.14) are calculated between the different node and reported in tables 3.4 and 3.5, respectively. It works by sending an array of length (bytes) for time (seconds). So, to measure the throughput between two nodes, TCP packets are generated from the first node and sent to the second node. The first step in this investigation is to establish some first, which forms a basis for comparison with other conditions and scenarios. This is accomplished by separately measuring the throughput between every pair of nodes in the network. After establishing the first scenario, the changes in throughput and delay under various scenarios are investigated and given in table 3.4 & 3.5 respectively.

Table 3.4 Throughput Values between the Nodes (Mbps)

From/to	Node 1	Node 2	Node 3	Node 4	Node 5
Node 1	----	4.99	3.37	3.71	3.50
Node 2	2.65	----	2.86	2.4	1.53
Node 3	2.11	2.50	----	2.66	2.60
Node 4	2.44	2.64	2.57	----	2.30
Node 5	2.18	2.31	2.33	4.99	----

Table 3.5 Delay Values between the Nodes (Seconds)

From/to	Node 1	Node 2	Node 3	Node 4	Node 5
Node 1	----	0.029	0.018	0.028	0.031
Node 2	1.02	----	1.14	0.96	0.91
Node 3	0.86	1.11	----	1.06	1.14
Node 4	0.89	1.13	0.97	----	0.86
Node 5	0.96	1.50	1.35	0.86	----

To measure the throughput for transmission from node 5 to node 1 is 2.18Mbps, and for node 5 to node 4, it is 4.99Mbps. There are two hops between node 5 and node 4 and only one hop between nodes 5 to node 1. It is observed that from table 3.4 the throughput decreases as number of hops increase. Similarly to measure the delay for above scenario, it is observed that from table 3.5 the delay increases as the number of hops increase. So we increase the number of nodes in the network and compare the throughput and delay of different hops.

To make the simulation scale-up comparable to the prior one, the new network environment is created which is similar to the previous one. The scale-up network model and set the parameter is mention in table 3.1. Figure 3.1 is a snapshot of the network model considered for simulation. The first set of scenarios deals with adding more relay nodes between the source and destination. The simulation results are obtained for the four scenarios shown in table 3.5. Figure 3.20 & 3.21 shows a comparison of the average throughput and delay with different scenario.

Table 3.6 A Network Model for Different Scenarios

Scenario	No. of Hopes	Route
First	Three	Between node 19 to node 1
Second	Five	Between node 19 to node 1
Third	Six	Between node 19 to node 1
Fourth	Seven	Between node 19 to node 1

Figure 3.19 shows the average and total simulation time during running process. Figure 3.20 shows a comparison of the average throughput for four different scenarios enlisted in table 3.6. It can be seen that even though the number of hops in the second route (five hops i.e. node 0, 2, 4, 5 and 10) is less than the number of hops in the third route (six hops i.e. node 0, 3, 4, 6, 10 and 16), the average throughput is smaller. This is due to the fact that the signal quality between node 1 and node 19 through five hops is stronger than the six hops. It is observed from the figure 3.20, that the throughput decreases as the number of hopes increases. The top curve corresponds to the scenario where only node 19 is communicating with node 1 (the average value is about 2.45Mbps). The second curve corresponds to the scenario where five nodes are trying to communicate simultaneously with node 19 (the average value is around 1.55Mbps). The third curve represents the average throughput for the scenario where six nodes are sending traffic simultaneously to node 19 (the value here is around 1.12Mbps). The bottom curve corresponds to the scenario where seven nodes are communicating simultaneously with node 19 (the average value here is around 0.48 Mbps). It can be concluded from the graph in figure 3.20 that more the number of nodes are trying

to communicate simultaneously with the same node the less the throughput will be. Moreover, it is also to be noticed that the throughput is reducing linearly (i.e. it has dropped from 2.45Mbps to 1.55 Mbps which is around 36.7%, and then dropped to 0.48Mbps which is around 30.9%). This scenario deals with increasing the number of nodes trying to communicate simultaneously with one node. The graph in figure 3.21 shows the average delay at node 19 for four different scenarios. The top curve corresponds to the scenario where only node 19 is communicating with node 1 through three different hops (the value here is around 1.8s). The second curve corresponds to the scenario where node 19 are trying to communicate through five different hops with node 1 (the value here is around 2s). The third curve represents the average delay for the scenario where six hopes are sending traffic simultaneously to node 19 (the value here is around 4.1s). The bottom curve corresponds to the scenario where seven hopes are communicating simultaneously with node 19 (the average value here is around 4.2s). It is clear from the graph in figure 3.21 that if the more number of nodes are trying to communicate simultaneously with the same node as the delay increases.

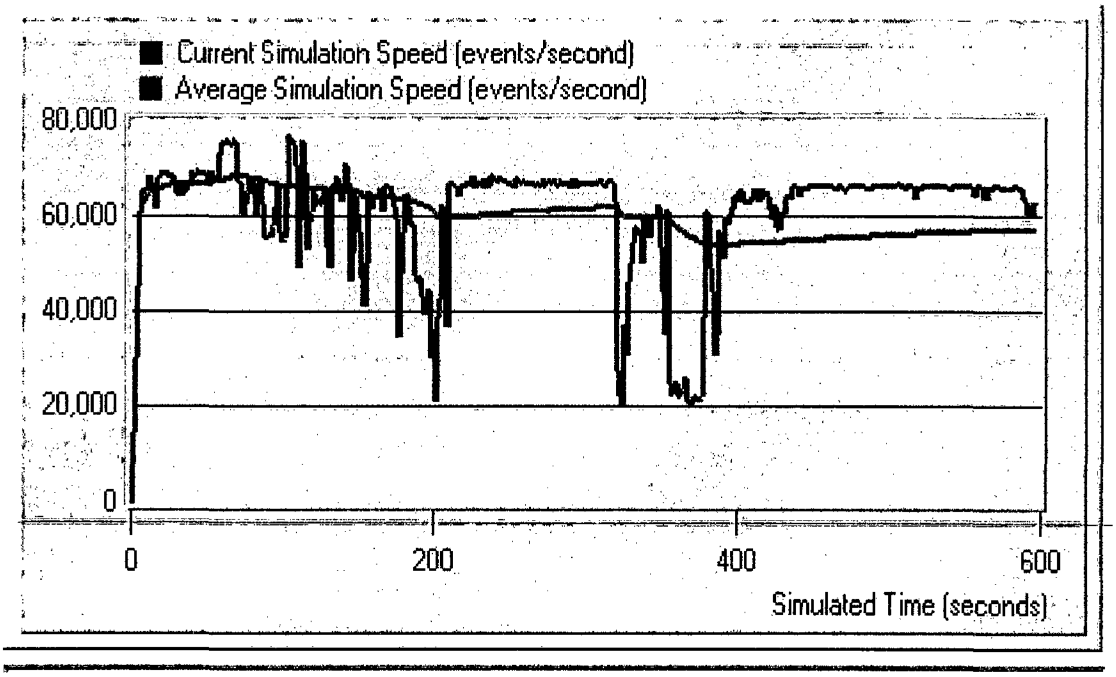


Figure 3.19: Average and Total Simulation Time during Running Process

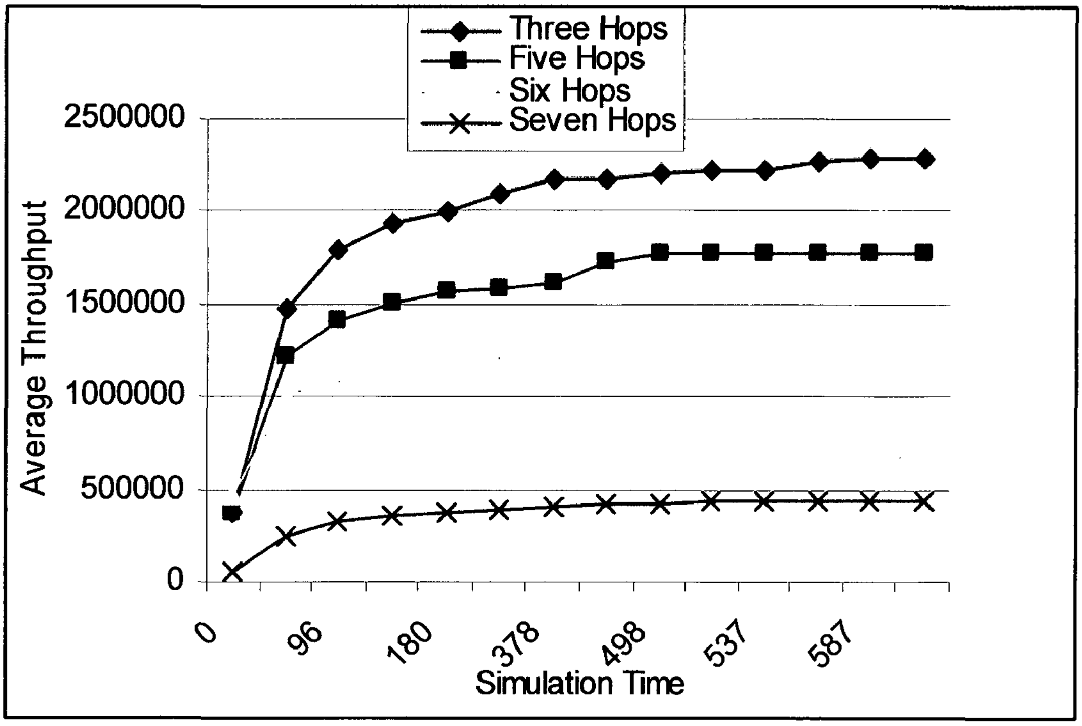


Figure 3.20: Average Throughput Comparison between all the Four Scenarios

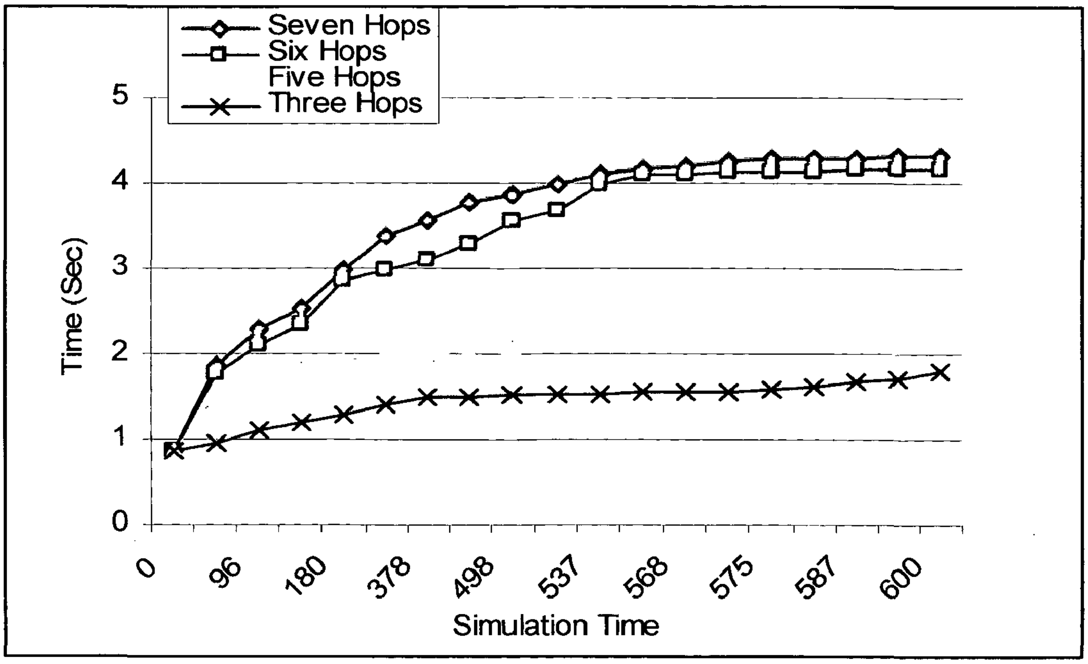


Figure 3.21: Average Delay between all the for Four Scenarios

Case 4: Impact of throughput with mobility for AODV protocol

The work has been extended and applies the mobility to different node of first scenario and sees the effect of throughput. In the first scenario, node 2 & 4 are involved in communication. TCP traffic is sent from node 2 to node 4 and the throughput is measured at node 2, whereas node 4 is mobile with speed of 5m/s. The average throughput value for this scenario is 2.48Mbps as shown in figure 3.22. So, by comparing the two mentioned levels of throughput, it can be noted that the mobility is dramatic effect on the throughput (i.e., reduction from 4.99Mbps to 2.48Mbps). The throughput is decreasing almost 50% due to effect of the mobility.

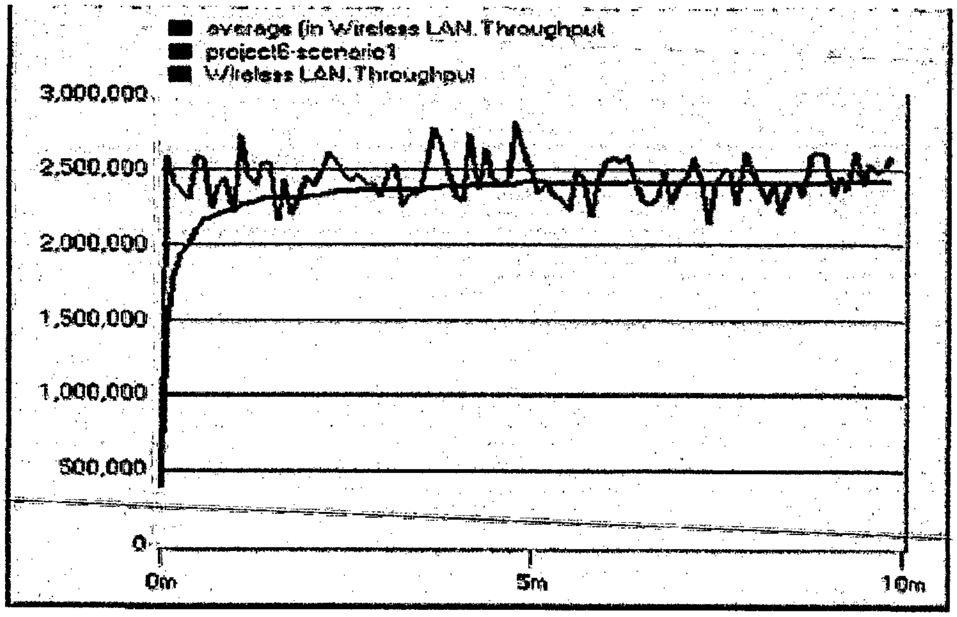


Figure 3.22: Throughput at node 2 whereas node 4 is mobile for first scenario.

Case 5: Impact of throughput for different scenario for DSDV, AODV and DSR protocols.

The performance comparisons of different protocol for different scenario have been given in figure 3.23-3.26. In this figure the results have been reported in terms of actual (Act.) and average (Avg.) throughput. It is clear from table 3.7 that the drop in the throughput occurs in a linear fashion. The throughput drops around 48 percent for the second scenario, while it drops around 66 percent for the third scenario and around 70 percent for the forth scenario. The simulation results reported above are compared with the experimental results reported by Hallani et al. and given in table 3.7.

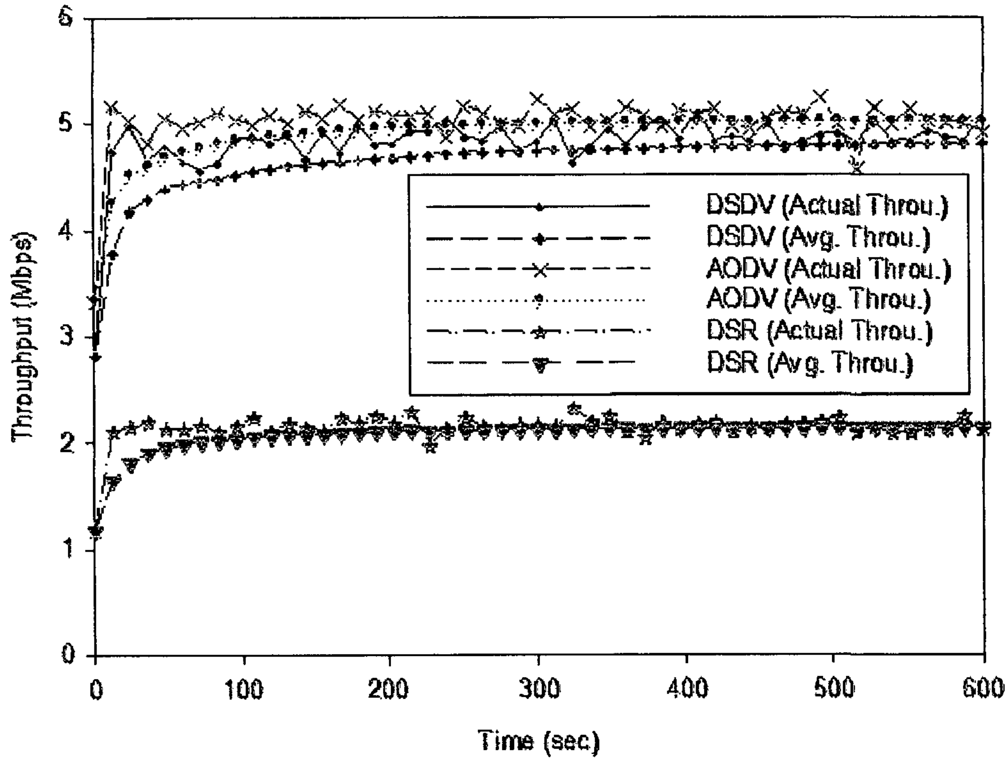


Figure 3.23: Throughput at node 2 for Different Protocol of First Scenario

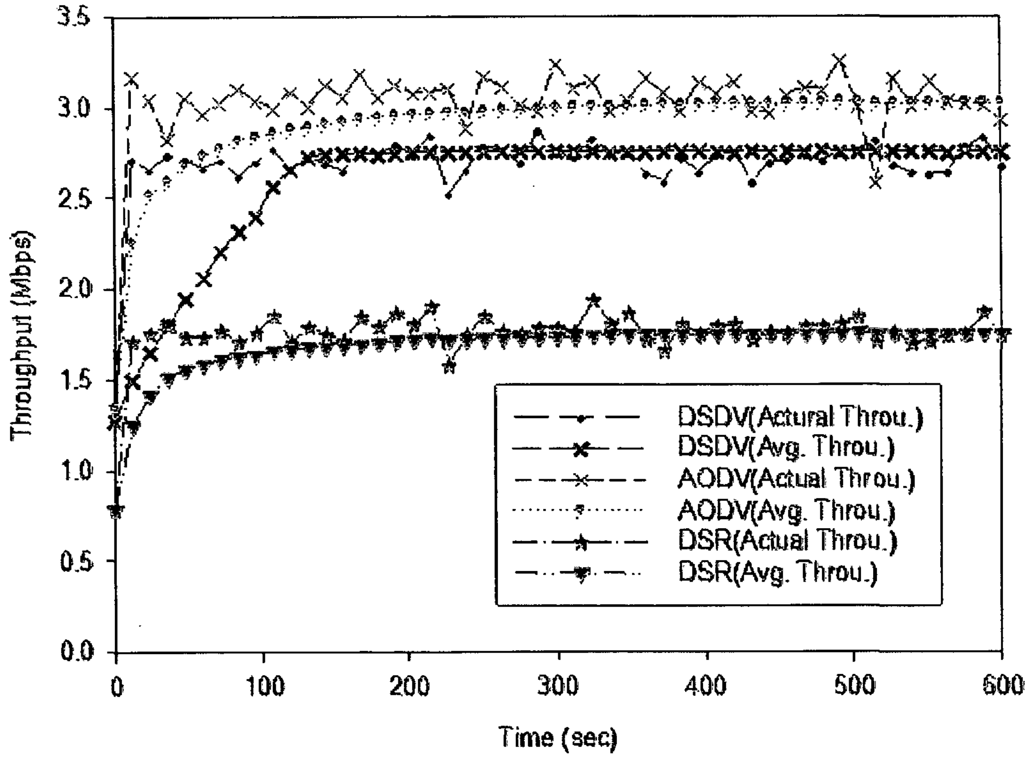


Figure 3.24: Throughput at node 2 for Different Protocols of Second Scenario

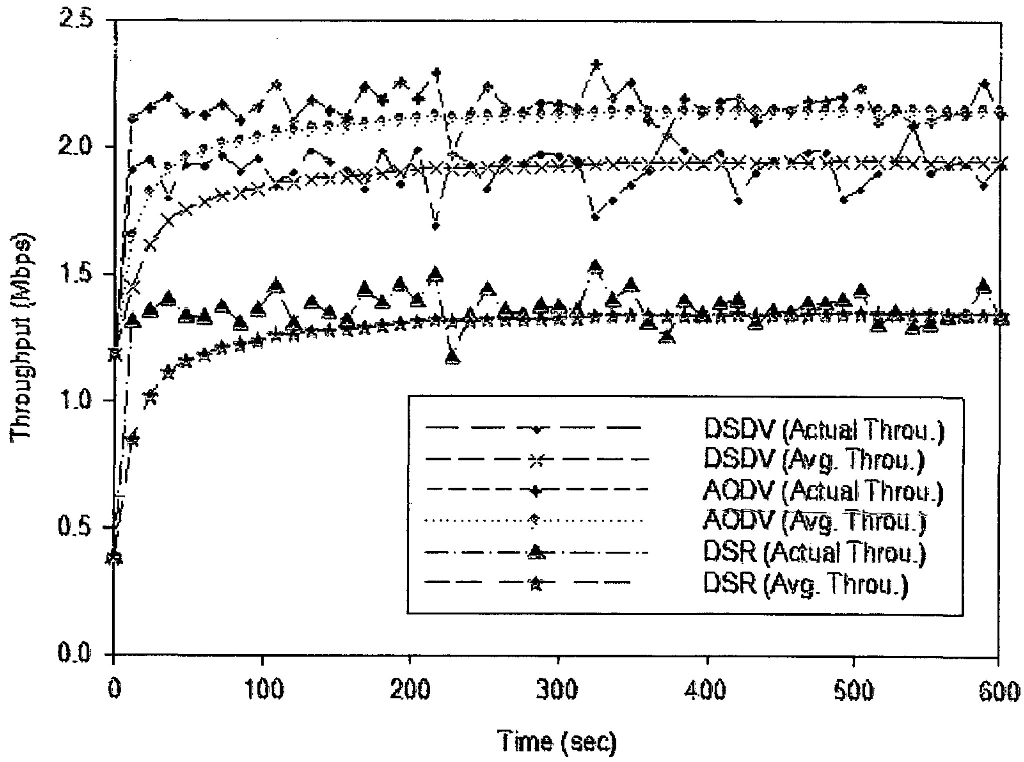


Figure 3.25: Throughput at node 2 for Different Protocols of Third Scenario

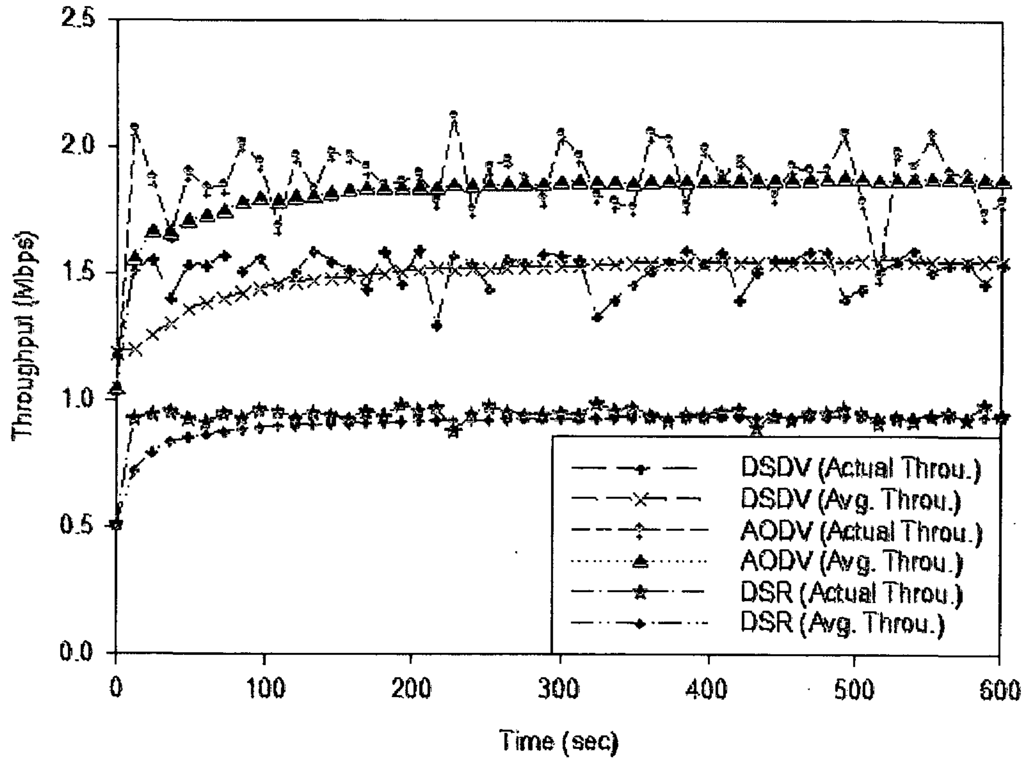


Figure 3.26: Throughput at node 2 for Different Protocols of Fourth Scenario

Table 3.7 Throughput Comparison of Simulation with Experiment Results at Node 2

	Protocols	First Scenario	Second scenario	Third scenario	Fourth Scenario
Experiment		4.53	2.35	1.55	1.28
Simulation	AODV	5.02	3.12	2.15	1.86
	DSDV	4.99	2.76	1.94	1.53
	DSR	2.15	1.75	1.35	0.92

From the table 3.7, it is observed that the AODV protocol shows better performance as compared with DSDV protocol and DSR perform poor performance with respect to DSDV and AODV. It is observed that the average throughput of AODV protocol at node 2 remain constant at 5.02Mbps. Similarly, the average throughput of DSDV and DSR protocol at node 2 remain constant at around 4.99Mbps and 2.15Mbps respectively for first scenario as shown in figure 3.23. It is observed that the average throughput of AODV protocol at node 2 remain constant at 3.12Mbps. Similarly, the average throughput of DSDV and DSR protocol at node 2 remain constant at around 2.76Mbps and 1.75Mbps respectively for second scenario as shown in figure 3.24. It is observed that the average throughput of AODV protocol at node 2 remain constant at 2.15Mbps. Similarly, the average throughput of DSDV and DSR protocol at node 2 remain constant at around 1.94Mbps and 1.35Mbps respectively for third scenario as shown in figure 3.25. It is observed that the average throughput of AODV protocol at node 2 remain constant at 1.86Mbps. Similarly, the average throughput of DSDV and DSR protocol at node 2 remain constant at around 1.53Mbps and 0.92Mbps respectively for forth scenario as shown in figure 3.26.

CHAPTER 4

THE ASSESSMENT OF EFFECT OF CONGESTION ON QOS PARAMETERS FOR ROUTING PROTOCOL (AODV) USING IEEE 802.11 MAC LAYER PARAMETERS & FUZZY APPROACH

4.1 Background & Motivation

Recent studies of deployments of public-area wireless networks have shown that user service demands are highly dynamic in terms of both time of day and location, and that user load is often distributed quite unevenly among wireless nodes [74]. At any one time, a large percentage of the mobile users communicate with a small subset in the wireless LAN. These user concentrations create an unbalanced load in the network, and complicate the capacity planning problem, making it difficult to accommodate heavy, concentrated load in different parts of the network without significant and costly, over-engineering.

Congestion is an unwanted situation in networked systems, where the part of the network is being offered more traffic than its rated capacity. When too many packets are present in the subnet, performance degrades. This situation is called congestion. Hence congestion is defined as the state of network elements, in which network is not able to meet the negotiated performance objective for the established connection. Congestion may be caused by unpredictable statistical nature of traffic and failure of equipments that support the networks. Resource shortage can be the other reasons, but it is often due to inadequate traffic control. Unlike the wired network the analysis of congestion is more difficult in MANET due to the time variant channel capacity and contention among neighbor nodes. The occurrence of a high density of nodes within a single collision domain of an IEEE 802.11 wireless network can result in congestion, thereby causing a significant performance bottleneck. Effects of congestion include drastic drops in network throughput, unacceptable packet delays, session disruptions and other various causes such as uncertainty, randomness and fuzziness. QoS guarantees for real time application or multimedia application require high throughput, low delay and jitter. These QoS guarantees can be achieved by controlling MAC layer parameters. Congestion control mechanism is necessary to makes sure the resources are used optimally and the system has maximum data throughput with the given conditions. In the present analysis the congestion analysis and control is proposed by controlling MAC layer parameter such as contention window and DISF. The scheduler algorithm is used to overcome the above shortcoming in wireless ad hoc networks.

4.2 Related Work

For high-speed communication networks, the explicit rate-based congestion control [75] has been applied where the congestion controls of different users enter the networks dynamics with different delays. Congestion control algorithms for local area network [76], which deals with the problem of quality of service to connections between wireless internets protocol networks with the air interface. This problem is then coped with congestion control and traffic scheduling algorithms: congestion control deals with the problem of computing the traffic relevant to in progress connections which can be admitted into the wireless network without causing the infringing of the QoS, while the scheduling deals with the problem of deciding the priorities for the transmission of the admitted traffic over the air interface. Congestion control algorithm [77] has been applied for wireless network for controlling the congestion among hop-to-hop. In recent years, depending on how challenging the congestion problem is a combination of the algorithms work satisfactorily under congestion circumstances [78]. The existing algorithms for wireless network do not fit in the ad hoc network framework, because of the dynamic behaviour of the topology and increased complexity for network without administration and access point. Recently, fuzzy logic technique [79] [80-81] has also been applied to control the congestion in wireless ad hoc network. C. Gomathy et al. [82] define fuzzy based priority scheduler for different protocol (NTPMR, ODMRP, CAMP). GUI Chao [83] defines different priority controllable architecture based on leaky bucket with priority scheduler for ODMRP protocol. The input parameters such as queue length, data rate and expiry time to find the priority index.

In the proposed research work, the congestion analyses have been carried out in terms of delay, glob load, throughput, packet drop, media access delay. The performance of the network will be enhanced by modification or variation of MAC layer parameter i.e. DIFS and contention window. Further fuzzy based scheme has been proposed to improve the performance of the network in terms of average throughput, packet delivery ratio and end-to-end delay. The input parameters such as buffer occupancy, data rate and expiry time to find the priority index has been taken for analysis. The performance evaluation has been analysed under different load and mobility conditions using OPNET/ns-2 simulator.

4.3 Congestion and its causes

Congestion occurs when the amount of data sent to the network exceeds the available capacity, the routers are no longer able to cope up the demand and they begin losing packets. At very high traffic rate, the performance collapses completely, and almost no packets are delivered. Congestion can be brought about by several factors viz shortage of buffer space, slow links and slow processors.

(a) Shortage of buffer space

If large capacity buffers are used to compensate for shortage of buffer space, many short-term congestion problems will be solved but this will cause undesirably long delays. Suppose the total input rate of a switch is 1Mbps and the capacity of the output link is 0.5Mbps, the buffer will overflow after 16 s with 1Mbyte memory and will also overflow after 1 h with 225Mbyte memory if the situation persists. So, larger buffer size can only postpone the discarding of cells but cannot prevent it.

(b) Slow links

Though the problem of congestion caused due to slow links will be solved if high-speed links become available but this is not always the case, sometimes increases in link bandwidth can aggravate the congestion problem because higher speed links may make the network more unbalanced. Higher speed load can make the congestion condition in the switch worse.

(c) Slow processors

On improving the processor speed, faster processors will transmit more data in unit time. If several nodes begin to transmit to one destination simultaneously at their peak rate, the target will be overwhelmed soon. So, congestion is dynamic problem, any static solutions are not sufficient to solve the problem. All the issues presented above are symptoms not the causes of congestion. Proper congestion management mechanisms are more important than ever.

4.3.1 Congestion issues in wireless networks

Within wireless ad hoc networks, a number of issues further complicate the identification and control of congestion including:

- Interference from other nodes
- Route failures
- Variable quality of radio signals
- Transmitter power.

In the event of packet loss, appropriate action is not easily taken, as identifying the cause of the loss is difficult. There have been various mechanisms proposed to help classify the reason for packet loss, but all add extra complexity, may not be compatible with the existing protocols and none seem to cover all possible causes.

4.3.2 Possible solutions

There are two general solutions to the problem of congestion:

- Congestion avoidance
- Congestion control

Congestion avoidance attempts to predict when congestion is about to occur and reduces the transmission rate at this time. The algorithm should operate in such a manner to keep response time vs. load and throughput vs. load operating to the left of the location of the knee in figure 4.1(a) and (b).

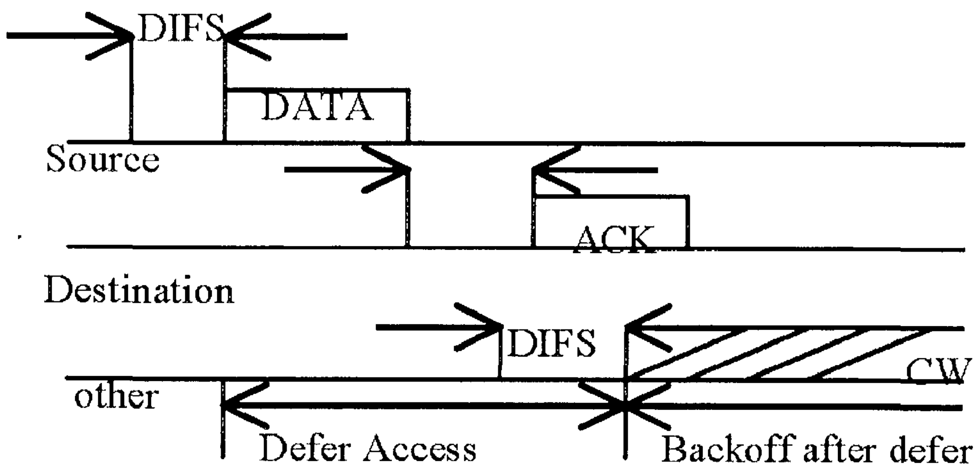


Figure 4.1(a): Basic CSMA/CA scheme

Congestion control attempts to take fuller advantage of the network resources by transferring data at a rate close to the capacity of the network. The capacity of the network can be viewed as the point at which any increase in traffic will increase the delay but not the throughput. Congestion control algorithms, like that of TCP, attempt to increase traffic until the capacity of the network is reached, and then slow the transmission rate. Thus, these algorithms attempt to operate to the left of the cliff in figure 4.1(a) and (b). The variation in delay and throughput with respect to load is shown in figure 4.2.

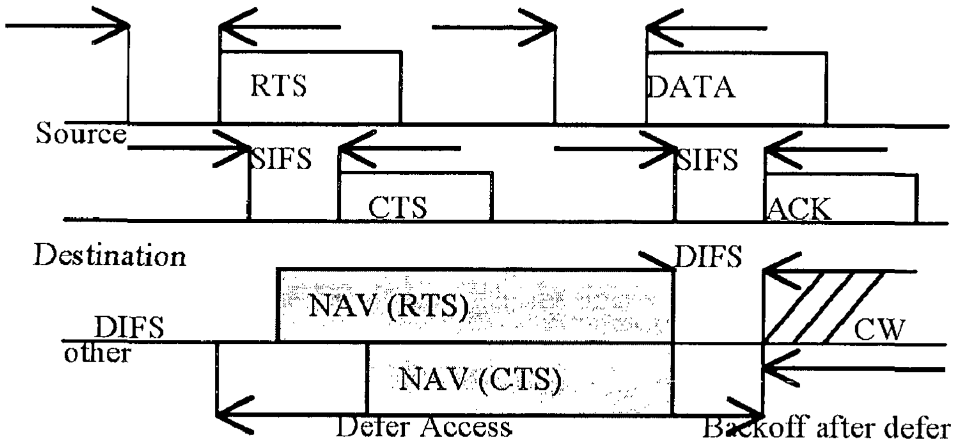


Figure 4.1(b): CSMA/CA and RTS/CTS mode

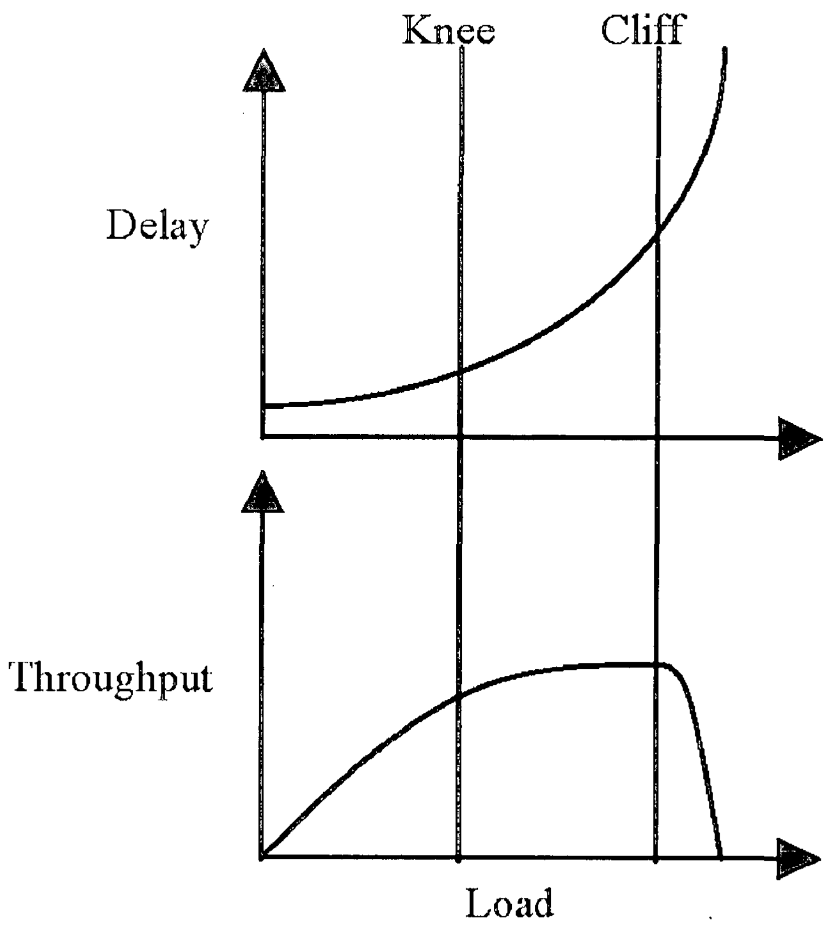


Figure 4.2: Load vs. delay and throughput

4.4 Simulation Environment

The network consists of five node or station and four node starts transmitting to fifth node. All nodes generate 2.16Mbps CBR traffic with packet sizes of 1000 bytes, RTS/CTS exchange is required for most of the packets. The ad-hoc routing protocol is AODV and the channel capacity is 11Mbps. A work space area of 100×100 m have been chosen as shown in figure 4.3 and set their attributes as tabulated in tables 4.1–4.4. All the periphery nodes are having similar attributes. However, central node namely node 1 is deliberately made slower with lesser buffer space and lesser bandwidth when compared with periphery nodes to analyse congestion. The inter arrival time is exp (0.1) for all the nodes unless otherwise specified. All the wireless station nodes and the access points use direct sequenced spread spectrum at the physical layer. All the nodes employ the DCF basic CSMA/CA access mechanism. The nodes transmit with a power level of 0.001 W. Packets received at a node with power less than 7.33E-14 W will make receiver too busy. The maximum throughput in this channel is dependent on the frame size, the RTS/CTS mechanism, and the number of nodes in the network, and the MAC layer parameters such as DIFS and the contention window. For example, when only one CBR source contends for the medium and uses packet of 1000 bytes, the maximum achievable throughput is about 4.8 Mbps. Stations 1, 2, 3 and 4 start their transmissions at 0s, 5s, 10s and 15s to station 5. The throughput obtained by each station at each 1 s interval is evaluated as shown in figure 4.3. To analyses the congestion in IEEE 802.11 networks, a WLAN node model has been created using OPNET and ns2 simulator.

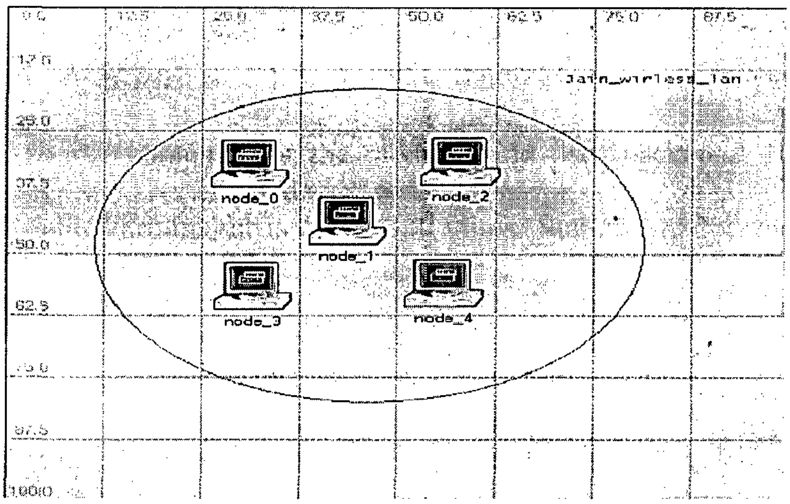


Figure 4.3: Node arrangement

Table 4.1 Traffic generation parameters

	Node 0	Node 1	Node 2	Node 3	Node 4
Start time	Constant (5)	Constant (5)	Constant (5)	Constant (5)	Constant (5)
On	exp (100)	exp (100)	exp (100)	exp (100)	exp (100)
Off	exp (1)	exp (1)	exp (1)	exp (1)	exp (1)

As shown in table 4.1, the traffic generation parameter has been given for above proposed network model (figure 4.3) that include start time, on & off where keeping start time is constant (5), On time is exp (100) & off time is exp (1) for all the above five nodes.

Table 4.2 Packet generation arguments

	Node 0	Node 1	Node 2	Node 3	Node 4
Inter arrival time	exp (0.01)	exp (0.01)	exp (0.01)	exp (0.01)	exp (0.01)
Packet size	exp (1024)	exp (1024)	exp (1024)	exp (1024)	exp (1024)
Off	exp (1)	exp (1)	exp (1)	exp (1)	exp (1)
Seg. size	No Seg.	No Seg.	No Seg.	No Seg.	No Seg.
Stop time	Never	Never	Never	Never	Never
WLAN MAC address	Auto assigned	Auto assigned	Auto assigned	Auto assigned	Auto assigned

As shown in table 4.2, the packet generation parameter has been given for above proposed network model (figure 4.3) that include inter arrival time, packet size, off time, seg. size, stop time & wlan mac address where keeping inter arrival time is exp (0.01), packet size is exp (1), Off time be exp (1), no segment size, stop time is never & wlan mac address has been auto assign for all the above five nodes.

Table 4.3 WLAN parameters

	Node 0	Node 1	Node 2	Node 3	Node 4
RTS threshold	None	None	None	None	None
Fragmentation	None	None	None	None	None
Data rate (Mbps)	11	5.5	11	11	11
Phy. characteristics	DSSS	DSSS	DSSS	DSSS	DSSS
Packet reception power threshold	7.33E	7.33E	7.33E	7.33E	7.33E
Short retry limit	7	7	7	7	7
Long retry limit	4	4	4	4	4
Access Point Functionality	Disabled	Disabled	Disabled	Disabled	Disabled

As shown in table 4.3, the wlan parameters has been chosen for above proposed network model (figure 4.3) that include rts threshold, fragmentation, data rate, phy., characteristics, packet reception power threshold, short retry limit, long retry limit, & access point functionality. Where all the parameters keep constant excepts data rates be 5.5Mbps of node 1 whereas other nodes be 11Mbps.

Table 4.4 Channel parameters setting

	Node 0	Node 1	Node 2	Node 3	Node 4
Band width	1000	500	1000	1000	1000
Freq.	BSS Based	BSS Based	BSS Based	BSS Based	BSS Based
Buffer size	256000	1024000	256000	256000	256000

As shown in table 4.4, the wlan parameters has been chosen for above proposed network model (figure 4.3) that include bandwidth, frequency & buffer size. Where all the parameters keep constant excepts bandwidth & buffer size of node 1 be 500 & 1024000 respectively. The packet transmissions with a power higher than this threshold are considered as valid. Unless the default transmission power is changed, all the WLAN packets should reach their destinations with sufficient power to be valid packets if the propagation distance between the source and destination is less than 300 m as required by the IEEE 802.11 WLAN standard. The distance between any two periphery nodes is kept 25 m. In the simulation model considered here, all the nodes are static and always transmit with a power level of 0.001W. The simulations were carried out for 900 simulation seconds and repeated many times to ascertain validity.

Table 4.5 Default configuration parameter for 802.11 DCF

Parameter	Value
DIFS	50us
CWmin	31
CWmax	1023

No differentiation mechanism is used, i.e., all nodes have the default configuration for differentiation parameters, as show in the table 4.5 All the node have same CWmin and CWmax but different DIFS parameters is given in table 4.6.

Table 4.6 DIFS parameter for DIFS-based scheme

Nodes	DIFS	CWmin:CWmax
1	25us	31:1023
2	35us	31:1023
3	40us	31:1023
4	50us	31:1023

Table 4.7 Contention window sizes

Nodes	CWmin:CWmax	DIFS
1	31-1023	25us
2	41-1024	25us
3	63-2047	25us
4	127-4095	25us

By changing the contention window size and then analyzed the behavior of throughput. Each node station is configured with a contention window interval [CWmin:CWmax] as show in table 4.7. Nodes with smaller intervals have higher priority of accessing the channel compared to node with larger values. So we anticipate stations with smaller interval values to have higher throughput compared to those with larger values.

4.5 Simulation Results & Analysis

Case 1: The congestion analyses have been carried out for different QoS parameter

As explained above that node 1 is deliberately made to cause congestion to see its impact on various performance parameters. The buffer size, bandwidth and data rates have been reduced when compared with other nodes. To analyse its impact on the performance of the network, global parameters and individual node parameters have been observed. The global parameters are chosen as end-to-end delay and load and their variations against simulation time are shown in figures 4.4 and 4.5. Individual node parameters are chosen as throughput, packet drop, media access delay and are plotted in figures 4.6–4.8.

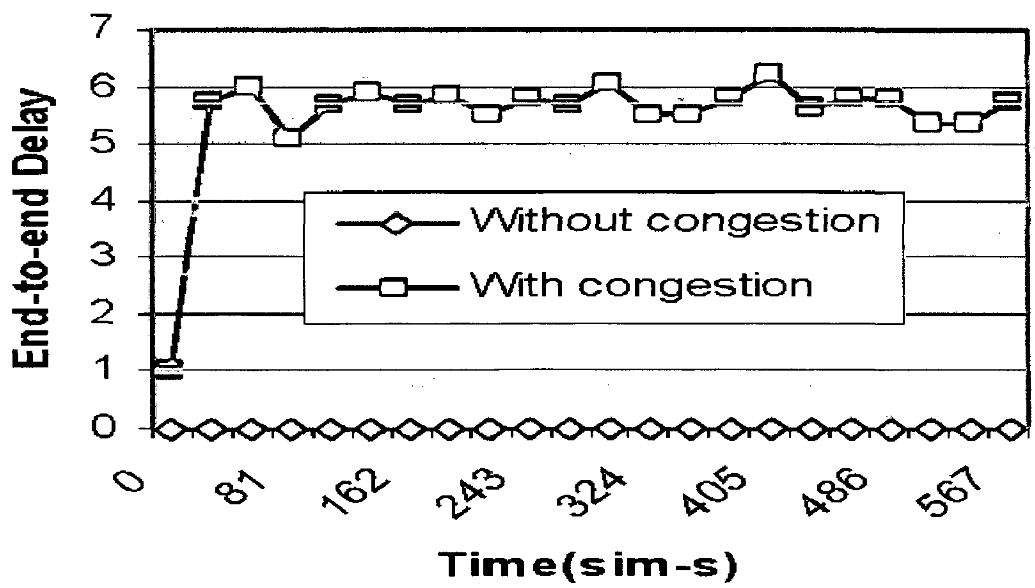


Figure 4.4: Delay with and without congestion situation

From figure 4.4, observing the end-to-end delay of the above model, it is observed that end-to-end delay is very high when compared with the situation when all nodes are having exactly similar attributes (referred as no congestion situation henceforth-blue curve). It is clear that delay is maximum if node 1 is congested whereas without congestion, delay is minimum (zero) when compared with other nodes. The delay of congested node 1 is fluctuates between 5.0 to 6.5 sec. Likewise, the delay values without congestion is almost negligible.

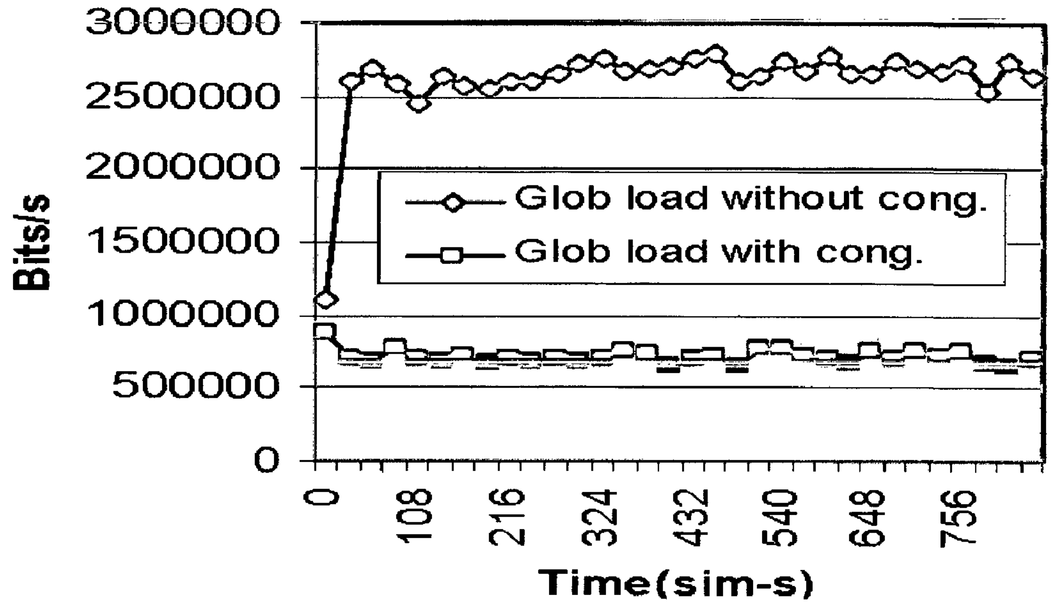


Figure 4.5: Glob load comp

From figure 4.5, observing the load of the of the network, it is observed that when compared with the situation when all nodes are having exactly similar attributes– blue curve, the load falls to 78% during initial transition phase. However, except the above situation the network load reduces to 24–30% of no congestion situation. The impact of congestion situation on various nodes is also studied. The parameters (node) chosen for this study is throughput, packet drops and media access delay.

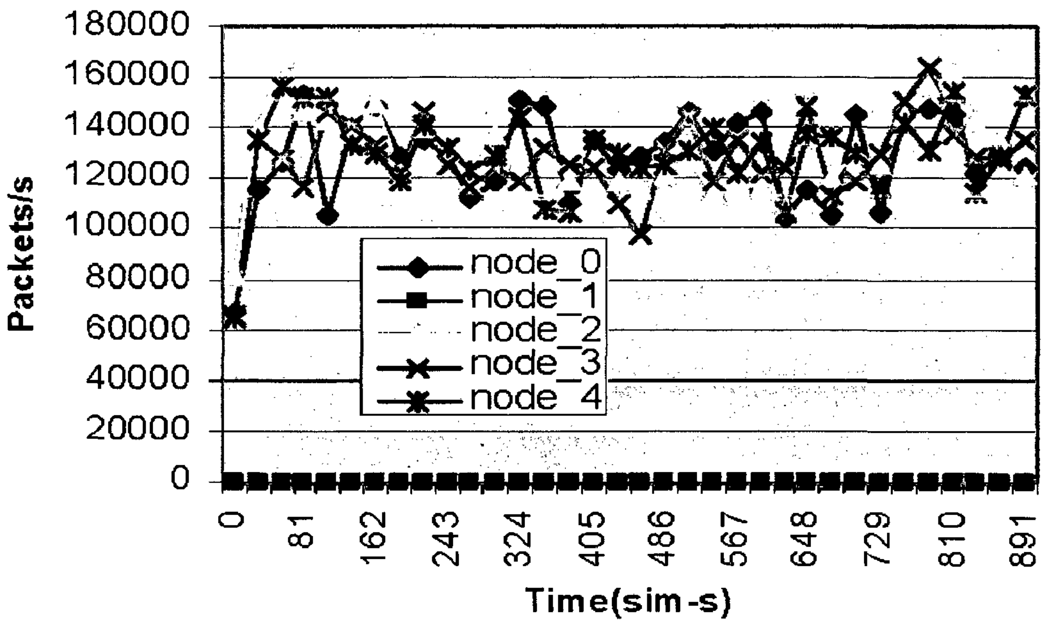


Figure 4.6: Throughput comp of nodes

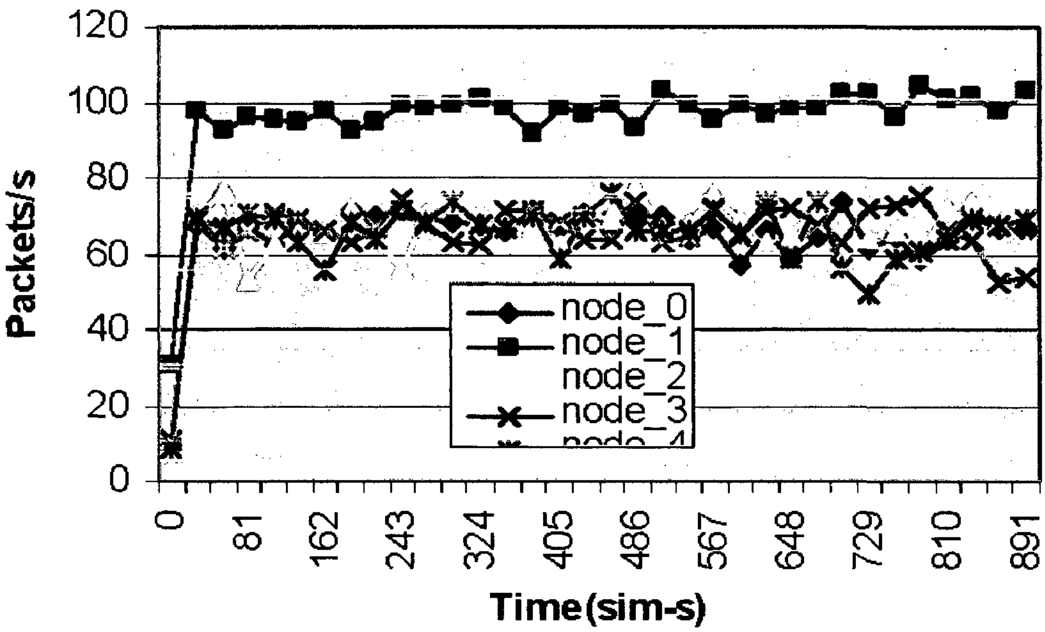


Figure 4.7: Packet drop comp. of nodes

From figure 4.6, it is clear that throughput in congested node (node 1) is minimum (zero) when compared with other nodes. The throughput of node 0 is varying between 153808 and 67638. Likewise, the throughput values corresponding to other nodes, namely node 2, node 3 and node 4, are varying between 167567 and 81522, 164456 and 66383 and 156808 and 64694, respectively.

Packet drop is another important parameter affected by congestion situation. The comparison of packet drops of various nodes against simulation time is shown in figure 4.7. As expected, the packet drop is maximum in node 1 and varies between 105.22 and 31.22. These values are about 120–200% more when compared with other nodes, i.e., periphery nodes. Variation of delay in various nodes against simulation time is shown in figure 4.8. Delay in congested node (node 1) is maximum when compared with other nodes. When compared with node 0, the delay values are 4.26–6.51 times higher except for the initial transition phase. Likewise, the corresponding values for other nodes, i.e., node 2, node 3, node 4 are 4.18–6.17, 4.00–6.46, 4.54–6.92, respectively. Effects of congestion include drastic drops in network throughput, unacceptable packet delays, and session disruptions. Therefore, there arises a compelling need to understand the behaviour of the congested wireless networks. To observe the congestion in IEEE 802.11 networks, we carried out simulations on OPNET simulator taking simple WLAN node model (figure 4.3). We created congestion like situation by deliberately making central node slower with lesser buffer space and lesser bandwidth when compared with periphery nodes and observed its impact on the performance of the network.

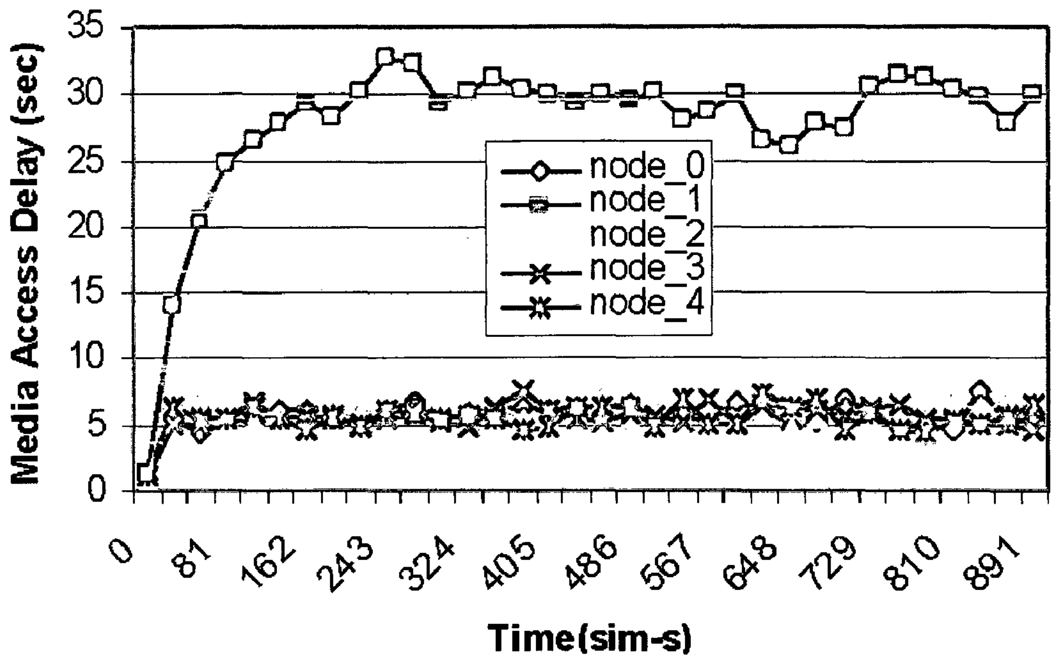


Figure 4.8: Media access delay comp. of nodes

The global parameters were chosen as end-to-end delay and load and their variations against simulation time are shown in figures 4.4 and 4.5. While delay increases with congestion situation, the load reduces in a similar situation. Individual node parameters were chosen as throughput, packet drop, media access delay and are plotted in figures 4.6–4.8. The throughput in congested node is found zero throughout the simulation time. The packet drop in congested node is found to be about 120–200% when compared with other nodes. Media access delay in congested node is found to be between 400% and 692% higher when compared with other nodes.

Case 2: Modification or variation of IEEE 802.11 MAC layer parameter for improvement of network performance

The network consists of five nodes whereas four nodes start transmitting to a fifth node. All stations generate 2.16Mbps CBR traffic with packet sizes of 1000 bytes. The distance between stations is 100meters. The ad-hoc routing protocol is AODV and the channel capacity is 11Mbps. The maximum achievable throughput in this channel is dependent on the frame size used by the sources, the use of the RTS/CTS handshake, and the number of stations contending for the medium, and the differentiation parameters such as DIFS and the contention window. For example, when only one CBR source contends for the medium and uses packet of 1000 bytes, the maximum achievable throughput is about 5.76Mbps. Nodes 1, 2, 3 and 4 start their transmissions at 0s, 50s, 100s and 150s to node 5. The throughput obtained by each station at each 1s interval is evaluated.

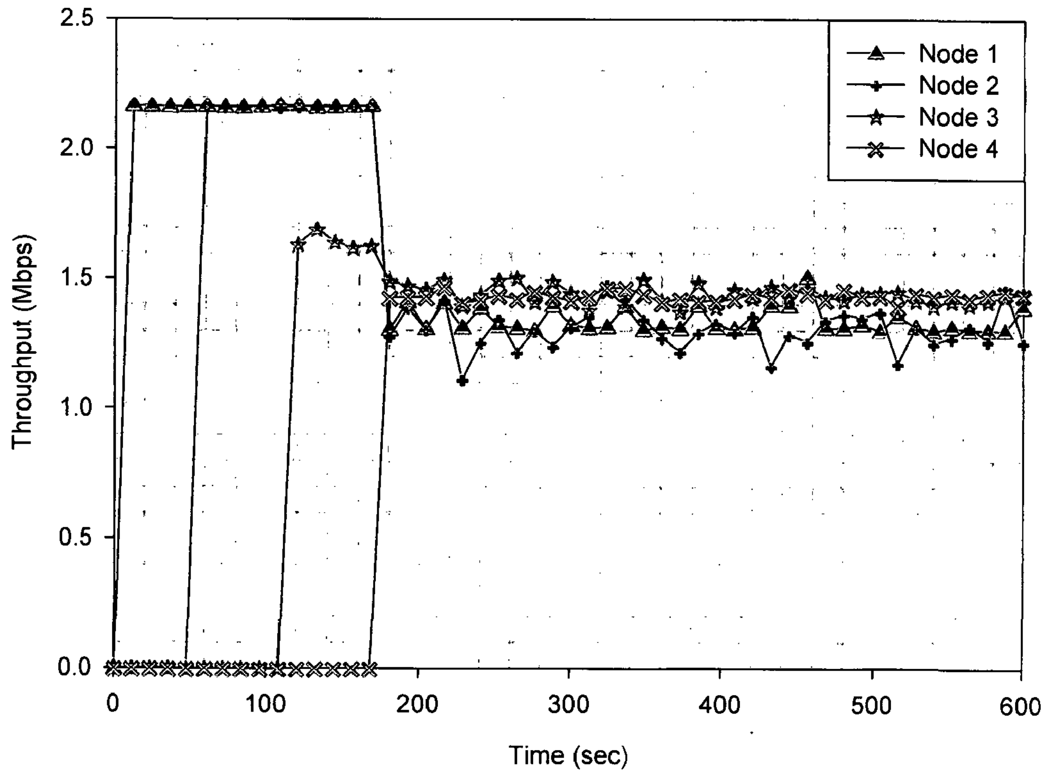


Figure 4.9: Throughput of four nodes with no differentiation

It is observed from the figure 4.9, that there are no differentiation mechanism is used, i.e., all nodes have the default configuration for differentiation parameters, as show in the table 4.5. The throughput of four CBR flows over DCF without any differentiation. It indicates that how DCF is best-effort service in which each station is given equal bandwidth. Figure 4.9 shows the first node starts to transmit at 0 seconds and gets its required bandwidth (2.16Mbps), and then node 2 joins in after 50 seconds, it also gets its required bandwidth. But problems start after 100 & 150 seconds when node 3 & 4 transmits, the bandwidth reduces to about 1.44 Mbps for each station. The introduction of the third & fourth flow causes the total traffic to go up to 5.4Mbps (4 x 2.16 = 8.64Mbps), this is more than the maximum available bandwidth of about 5.76Mbps (this is calculated according to the formula suggested in [84]).

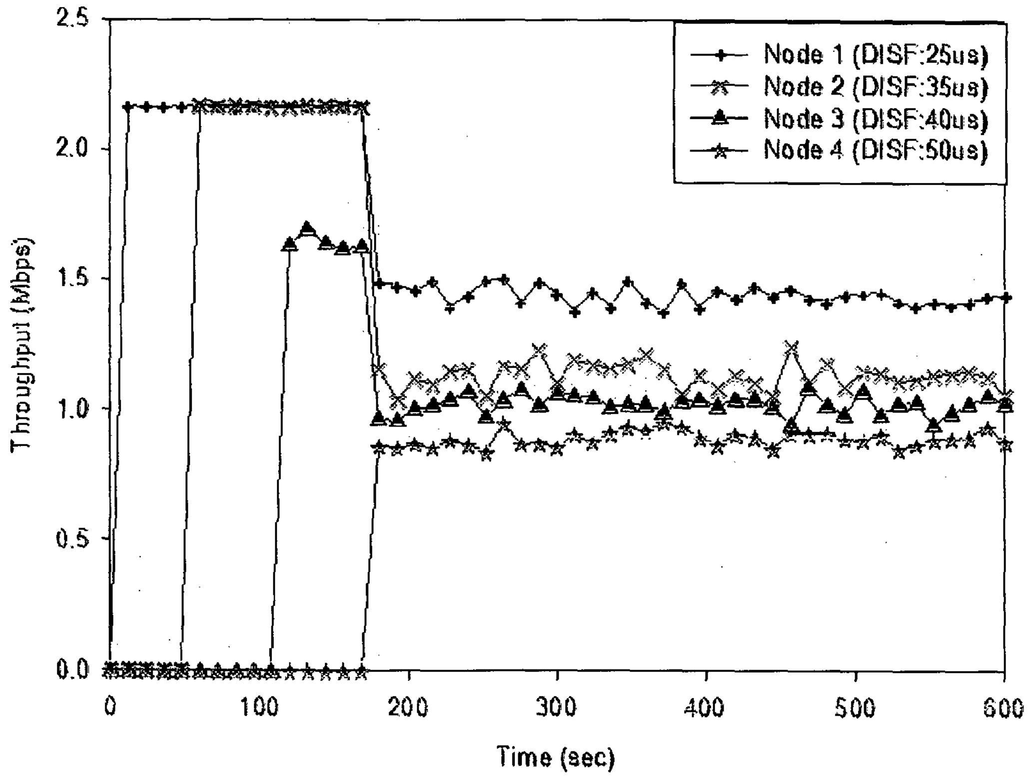


Figure 4.10: Throughput of four nodes with different values of DIFS

Further we have analyzed the performance of the network by modification of DIFS parameter of MAC layer in which nodes are given different DIFS parameters as shown in table 4.6. Figure 4.10 shows the throughput of DIFS-based scheme. Between 0 and 50 seconds, only two stations fairly share the channel because their aggregate rate is inferior to the maximum achievable throughput. When the third and fourth nodes starts transmission, the channel capacity is lower than the total traffic. Node 1 obtains more bandwidth than node 2, 3 and 4, because it has the smallest DIFS. However the throughput decreases with increase in the number of stations. This is mainly attributed to the shared nature of wireless channels. The length of DIFS determines after how many idle slots a station is allowed to count down its (residual) backoff count. If the other parameters are the same, stations with a shorter DIFS will be able to start decreasing their backoff count earlier when the medium is sensed idle. This means that stations with smaller DIFS value will have an advantage in the backoff process. Hence, stations with lower DIFS are expected to get a greater share of the medium capacity (high throughput). For a station with a larger value of DIFS, in each of these sessions it has to wait for a longer DIFS again before it can decrease its backoff count.

To analyze the throughput behavior of the network by changing the contention window. Each station is configured with a contention window interval [CWmin: CWmax] as show in table 4.7. Stations with smaller intervals have higher priority of accessing the channel compared to stations with larger values. So we expect stations with smaller interval values to have higher throughput compared to those with larger values. Figure 4.11 shows clearly that the node 1 with a smaller contention window interval have more bandwidth. Node 2, 3 and 4 have their bandwidth decreased, hence making them share.

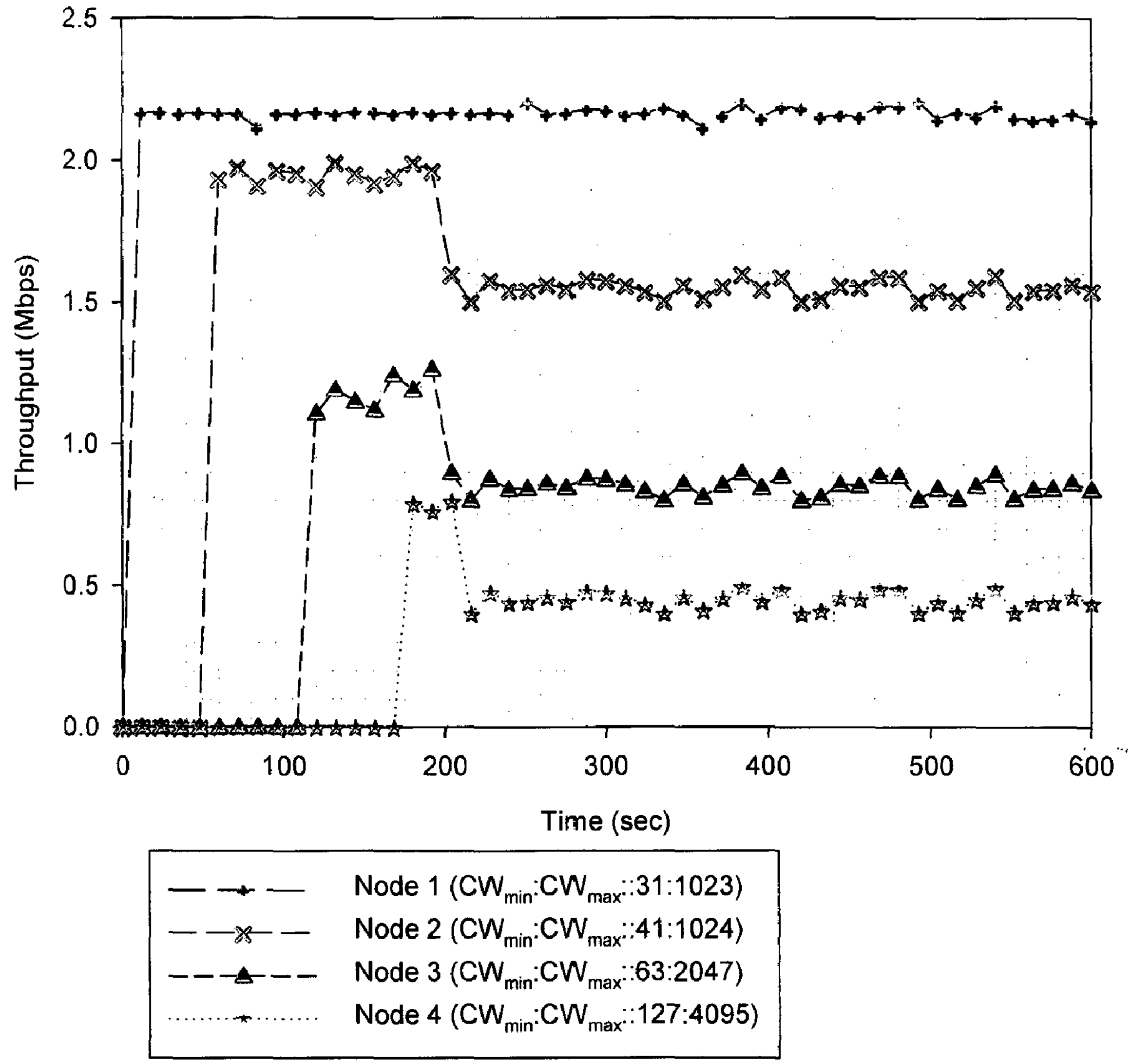


Figure 4.11: Throughput of four nodes with different values of CW

However, node 2 still has more bandwidth compared to 3 & 4 because it has a smaller contention window. The results clearly show that stations with a smaller CWmin value obtain a larger share of the channel capacity than the other stations. It is observed from the figure 4.11 the throughput decreases with increase in the number of stations. If the total number of stations increases, the throughput per node decreases rapidly. The total amount of effective channel capacity drop due to increased number of collisions, and the decreased channel capacity is shared among a larger number of stations. Stations with a smaller CW value have a higher probability to transmit. Therefore, if the other parameters are set equal, stations with a smaller CW value will have a larger share of the medium capacity. This explains the reasons why stations with smaller contention window interval have higher throughput. A smaller CW value means that the number of time slots in the backoff process is also smaller. The result is that less time is spent on the backoff process and therefore a positive impact is expected on the channel efficiency. The second effect will become more dominant in networks with a high number of contending stations. CWmax also contributes to the evolution of the CW in the contending process. Stations with smaller CWmax values are expected to obtain a larger share of the medium capacity. However, as opposed to CWmin, the value of CWmax is only reached after a number of successive collisions with the same packet. This suggests that differentiated CWmax values will only have effect with a relatively high number of contending stations. When a number is "relatively high" depends on the exact values of CWmin and CWmax, together with other parameters. CWmax defines the final CW value of its exponential growing process. Therefore, the value of CWmax is even more critical if collisions take place frequently, such as in a network with a high number of contending stations. A small CWmax value can greatly downgrade the system performance on channel efficiency if the number of contending stations is high. From the above analysis it is observed that if the total number of stations increases the throughput per node decreases rapidly. The total amount of effective channel capacity drop due to increased number of collisions, and the decreased channel capacity is shared among a larger number of stations.

Case 3: Effect on QoS parameter with varying mobility and load condition using fuzzy approach

The mobility of nodes and the error prone nature of the wireless medium pose many challenges like frequent route changes and packet losses. Such problem increases packet delay and decrease throughput. As traffic load in the network increases, the performance degradation gets worse. When traffic load is very high or congested, scheduler algorithm is very effective and efficient on end-to-end performance of wireless ad hoc networks. Research in this area has focused primarily on routing protocols--how to route packets hop by hop as efficiently as possible and medium access control (MAC) how to share the medium efficiently [85]. V. Kanodia et al. [86] have proposed a fuzzy based scheduler the packets is determined based on number of hops the packet has suffered and the buffer size. Also the absence of a base station and forwarding of packets across multiple broadcast regions makes it difficult to satisfy a flow's end-to-end QoS target. To improve the performance and maintain the QoS in MANET the fuzzy based scheduler can be used. There are several scheduling policies have been used for different routing protocols and network scenarios. Different routing protocols use different methods of scheduling. Packet scheduling algorithm has been proposed to improve the performance of congested network. Hence, a scheduling algorithm to schedule the packet based on their priorities to improve the performance of the network. Without scheduling, the packets will be processed in FIFO manner and hence there is frequently dropped the packets. A scheduler should schedule the packets to reach the destination quickly, which are at the verge of expiry. To incorporate the scheduler for the existing routing protocols, various routing protocols are studied [87]. Considering the suitability of the different types of scheduling methods for MANET, several scheduling schemes have been proposed [88]. The drop tail policy is used as queue management algorithm in all scheduling algorithm. It drops packets from the tail of the queue when buffer size is full. When the incoming packet is a data packet, the data packet is dropped. When the incoming packet is a control packet, the last enqueued data packet is dropped. If queued packets are control packets, the incoming control packet is dropped. Except for the no-priority scheduling algorithm, all the other scheduling algorithms give higher priority to control packets than to data packets. In no-priority scheduling, both control and data packets are served in FIFO (first in first out) order as shown in figure [4.12]. In the priority scheduling, control and data packets are maintained in separate queues in FIFO order and high priority is assigned to control packets. In priority scheduling, each node sends its own data packets before forwarding to the other nodes. The other nodes' data packets are serviced in FIFO order. The queue of C1 keeps its own data packets and the queue of C2 and C3 keeps the other nodes' data packets. C1 has strict priority over C2 and C3. We assess whether such greediness adversely affects network performance. Although it is uncommon in wired networks for a node to act as a source and a router concurrently, it is commonplace in mobile ad hoc networks. Currently, only this scheme is used in mobile ad hoc networks [89].

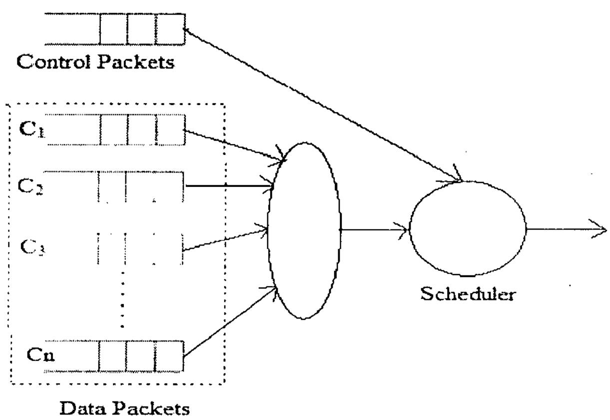


Figure 4.12: Priority scheduler for control and data packets

In this work a fuzzy based priority scheduler for mobile ad-hoc networks, to determine the priority of the packets that serve data packets in FIFO order to improves the QoS parameters in wireless ad-hoc network. Hence, the technique is used to determine which queued packet to process next that improves the overall end-to-end performance. The performance of this scheduler has been analyzed and measured in terms of packet delivery ratio, end-to-end delay and throughput. AODV routing protocol has been used for this analysis using ns2 with wireless extensions as a simulation tool. It is observed that the scheduler provides improvement in the performance of the system, when evaluated under different load and mobility conditions.

4.5.1 PROPOSED FUZZY TECHNIQUE

Fuzzy systems are defined with a strong mathematical basis. What is "fuzzy" in a fuzzy system is the information it deals with. The fuzzy set theory describes incomplete or vague concepts which might be difficult to formulate mathematically. Fuzzy systems are rule based systems. The heart of the fuzzy system is a rule base which consists of a set of "IF-THEN" rules. The rules are statements in which some words are characterized by continuous membership functions. This is why fuzzy logic is sometimes referred to as 'computing by words'. A fuzzy system is basically made of a fuzzifier, a defuzzifier, an inference engine, and a rule base as shown value. The fuzzy inference engine defines how the system should infer through the rules in the rule base to determine the output fuzzy sets.

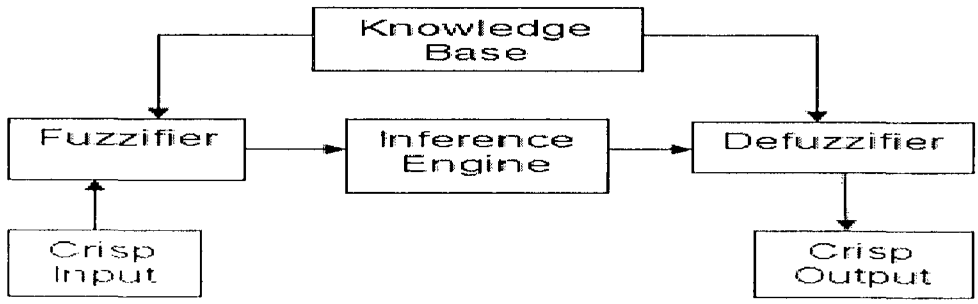


Figure 4.13: Basic Fuzzy Systems

The crisp input value for the different traffic of the mobile nodes based upon the quality of service parameters for the given protocol

Input (1) --------- Expiry Time (ET)

Input (2) --------- Data rate (DR)

Input (3) --------- Buffer Occupancy (BO)

Fuzzy logic implements human experiences and preferences via membership functions and fuzzy rules. The fuzzy scheduler proposed here, calculates the priority index of each packet. The fuzzy scheduler uses three input variables to be fuzzified are, the buffer occupancy, data rate and expiry time are taken as the fuzzy parameters a rule base is formed based upon these parameters to determine the crisp value of the traffic for the given protocols. The inputs are fuzzified, implicated, aggregated and defuzzified to get the crisp value of the output.

Reason for Adopting 'Fuzzy' as a tool:

The controllable elements in the different priority architecture are shown in figure 4.14. The architecture implements two controllers: one controls the queues of the packets using leaky bucket algorithm and scheduler to find the priority index. Without leaky bucket scheme, in data rate of token generation in token pool is kept constant irrespective of arrival rate of the traffic. This results in large packet loss whenever there is a rush at the input of the node, as a node is unaware of the traffic arrival and has been told to generate token at a constant rate. In the different priority controllable architecture as shown in figure 4.14, it has been suggested to set a threshold in data buffer. Whenever the no. of packets in buffer is more than the set threshold value, token generation rate is kept a little more than the otherwise case. Although the results in terms of packet loss probability, delay and throughput have improved significantly by this scheme, margin is still left for improvement.

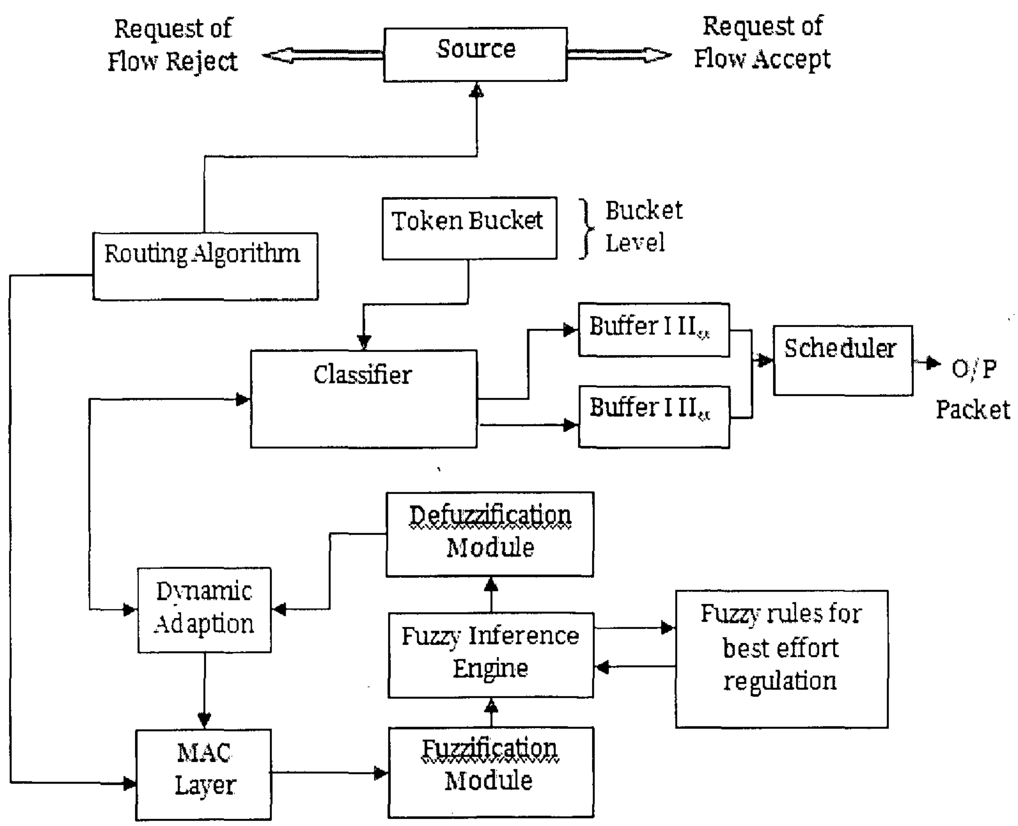


Figure 4.14: Different priority controllable architecture

Here it will be more intuitive if instead of having only two token generation rates based upon the state of buffer, two parameters namely data rate and buffer occupancy are checked repetitively to get an idea of state of traffic at the input and token be generated accordingly. This aim could be easily achieved using fuzzy logic scheme. Fuzzy logic is helpful whenever there is need to handle processes not clearly defined through rigorous models. In ordinary leaky bucket scheme, two states of token generation can be replaced by fuzzy logic. In these scheme states of buffer occupancy, data rate and expiry time at input is replaced by fuzzy sets.

The priority index that has to be associated with each packet is determined using fuzzy logic. The inputs to determine the priority index are the buffer occupancy of the node in which the packet is present, the expiry time of the packet and the data rate. The algorithm is coded in C language and verified using the MATLAB fuzzy logic tool box with FIS editor. Fuzzy logic coding in C language, includes all the basic steps that are involved in designing any fuzzy model. The inputs are received for a particular network model and rules are evaluated using these inputs. Each evoked rule provides an output membership function. These output membership functions are then implicated, aggregated and the crisp priority index is calculated from this aggregated curve using centroid method of defuzzication. The C code for fuzzy scheduler is verified using the MATLAB fuzzy logic tool box. It is given by the graphical representation of the membership functions and helps in precisely evaluating the outputs of a fuzzy system. The same inputs of the network model are applied in this toolbox and the priority index is verified. The simulation for evaluating the proposed fuzzy scheduler is implemented using qualnet library first the task of identification of input variables used in fuzzy logic C code is performed. Then the calculated priority index is used for scheduling the packet. By this way of scheduling, the packets which are about to expire or the packets in highly congested queues are given first priority for sending. As a result of this, the number of packets delivered to the client node, the average end-to-end delay of the packet transmission and the throughput improves. The inputs to the fuzzy system are identified by a complete search of the qualnet environment. The input expiry time is the variable TTL, which is present in the network layer of the simulator. TTL stands for time to live and is set a default value of 64 seconds. For each hop it reduces by 1 second. If the packet suffers excessive delays and undergoes multihop, its TTL falls to zero. As a result of this, the packet is dropped. If this variable is used as an input to the scheduler for finding the priority index, a packet with a very low TTL value is given the highest priority. Hence due to this, the dropping of packets experiencing multihops gets reduced. The next input to the scheduler is the data rate of transmission and it is normalized. The third input to the scheduler is the buffer occupancy of the node in which the packet is present. If the packet is present in a highly crowded node, it suffers excessive delays and gets lost. So, such a packet is given a higher priority and hence it gets saved. The priority index is calculated with the inputs obtained from the network layer. This is then added to the header associated with the packet. Hence whenever the packet reaches a node, its priority index is calculated and it is attached with it. Each node has three queues. Each queue in the node is sorted based on the priority index and the packet with the lowest priority index (is packet with the highest priority), is scheduled next, when the node gets the opportunity to send. By this method of scheduling, the overall performance increases. The performance of the network with the fuzzy code and without the code is studied under various conditions such as variation in network size, mobility of the nodes and the routing protocol used in the simulator.

Membership graph for the three levels of input and output variables

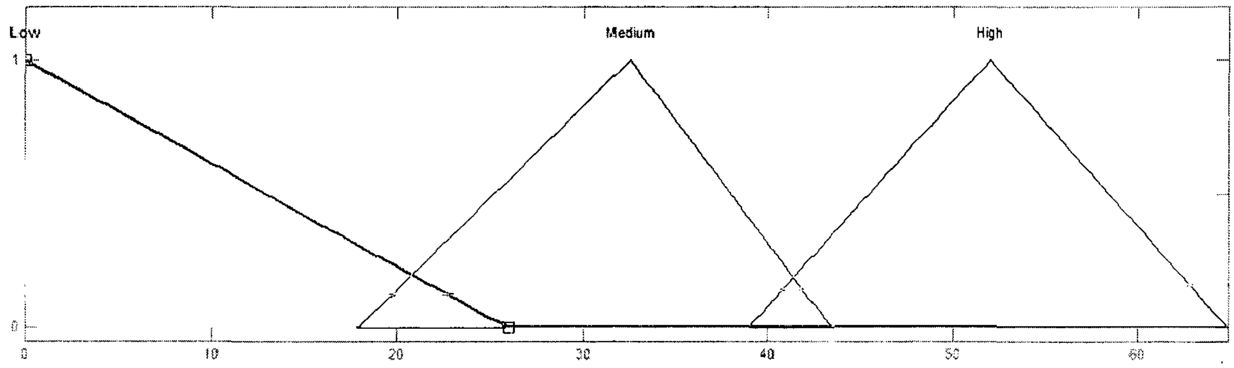


Figure 4.15(a): L, M, and H represent Low, Medium and High membership set respectively, membership values with inputs variables (Expiry Time)

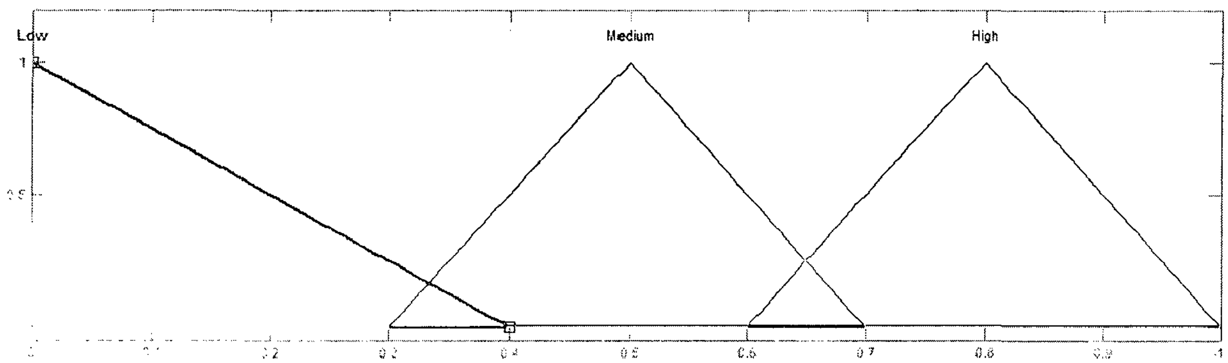


Figure 4.15(b): L, M, and H represent Low, Medium and High membership set respectively, membership values with inputs variables (Data Rate)

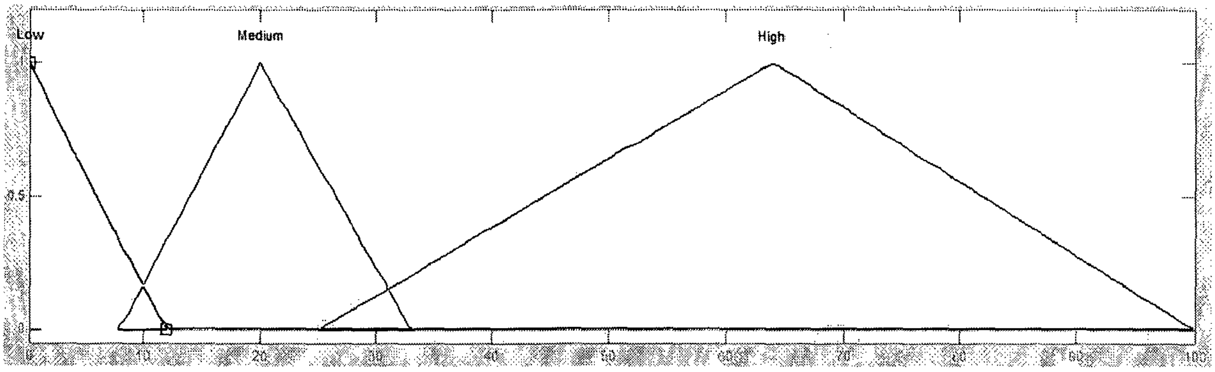


Figure 4.15(c): L, M, and H represent Low, Medium and High membership set respectively, membership values with inputs variables (Buffer Occupancy)

For the three input parameters buffer occupancy, data rate and expiry time with 27 rules for determining the crisp value in table 4.8. The linguistic variables associated with the input variables are Low (L), medium (M) and high (H). For the output variable, priority index, five linguistic variables used are very low (VL), low (L), medium (M), high (H) and very high (VH) as shown in the figures 4.15 (a), (b), (c) & (d). All membership functions are chosen to be triangular. The rule base is split into three tables and the first table gives out the rule base for buffer size low and nine combinations of the other two input variables. The second table gives out the rule base for buffer size medium and the third for buffer size high. The first rule can be interpreted as, "If (buffer occupancy is low) and (data rate is low) and (expiry time is low), then priority index is low".

Since in this rule, data rate and expiry time are low and the priority index is set to be low. Similarly the other rules have been developed. The output priority index, if very low, indicates that packets are associated with low delay, are attached with a very high priority and should be immediately scheduled. Similarly, if the priority index is very high, it indicates that packets are attached with least priority and will be scheduled only after the high priority packets are scheduled. The surface viewer for the fuzzy scheduler in case of constant buffer occupancy, data rate and expiry time is shown in figure 4.16 (a) & (f).

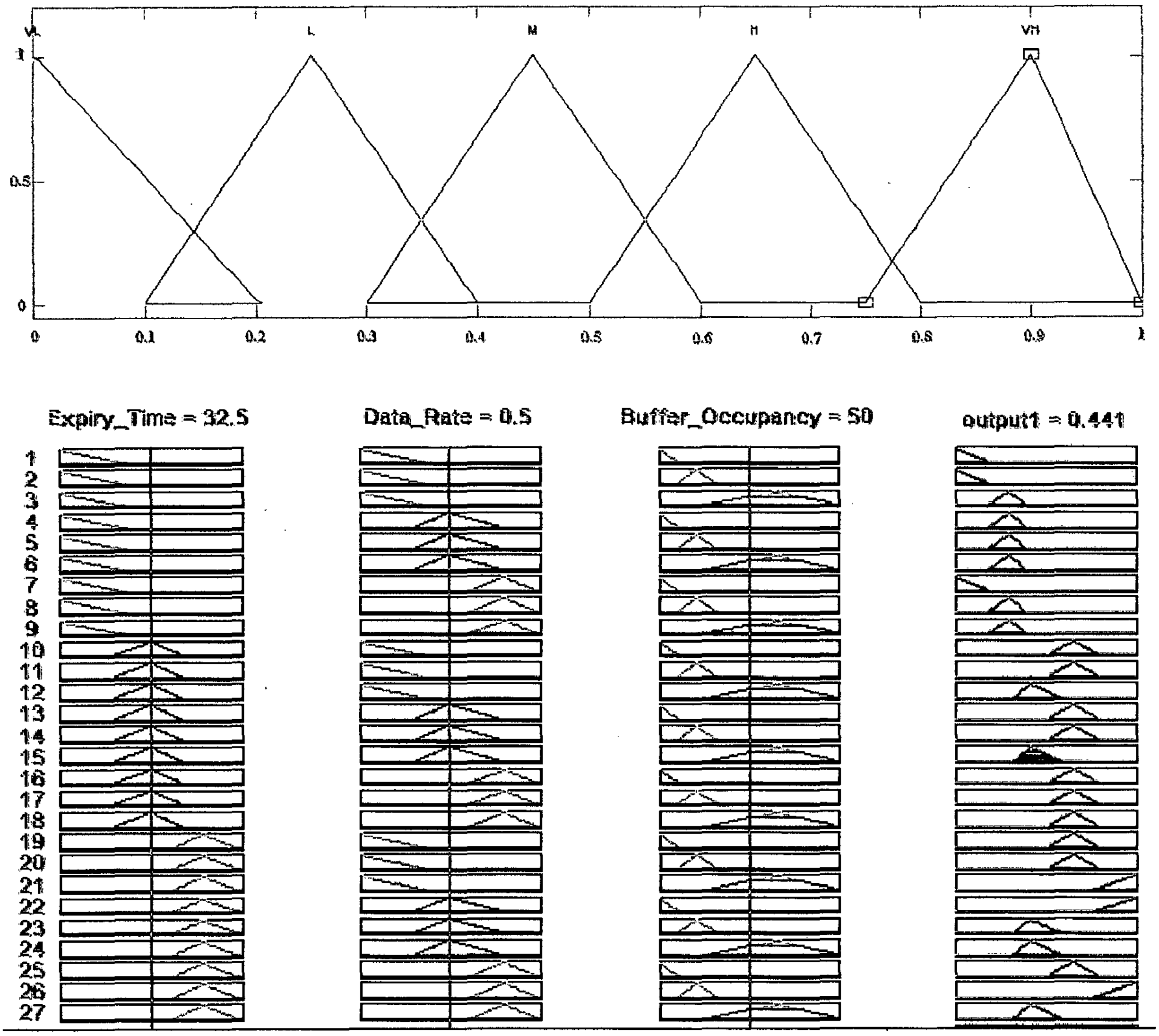


Figure 4.15(d): VL, L, M, H, and VH represent very low, low, medium, high and very high set respectively, membership values with outputs variables

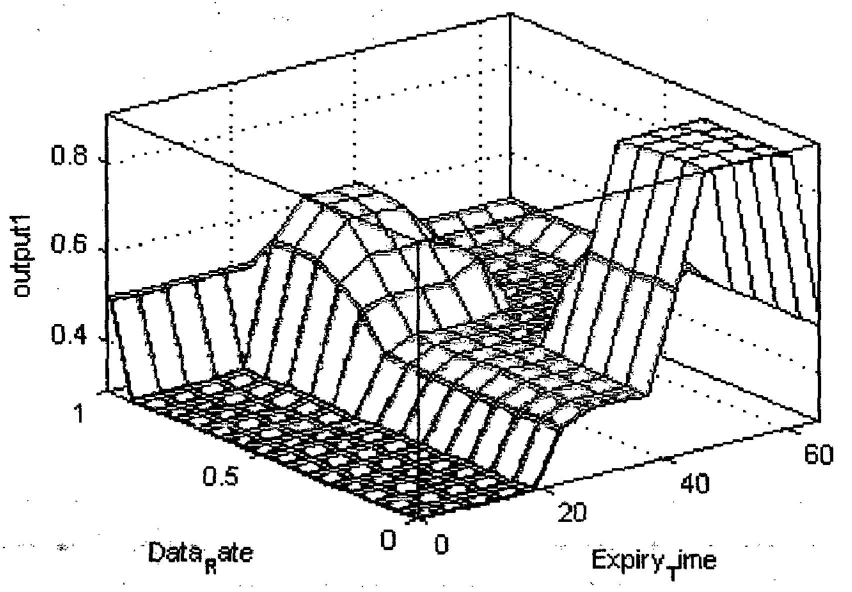


Figure 4.16(a): Surface viewer for the fuzzy scheduler in case of constant data rate and expiry time

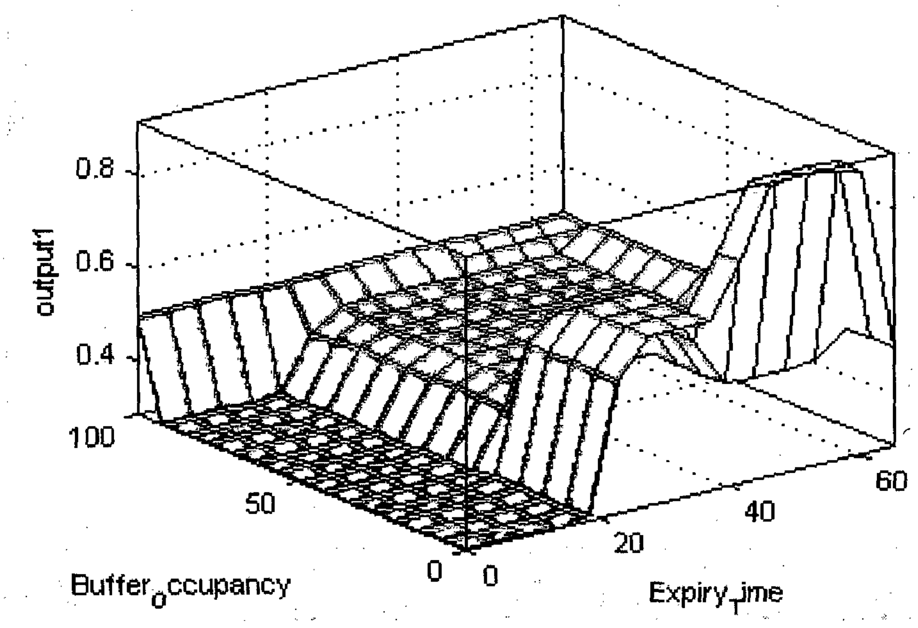


Figure 4.16 (b): Surface viewers for the fuzzy scheduler in case of Buffer occupancy and expiry time

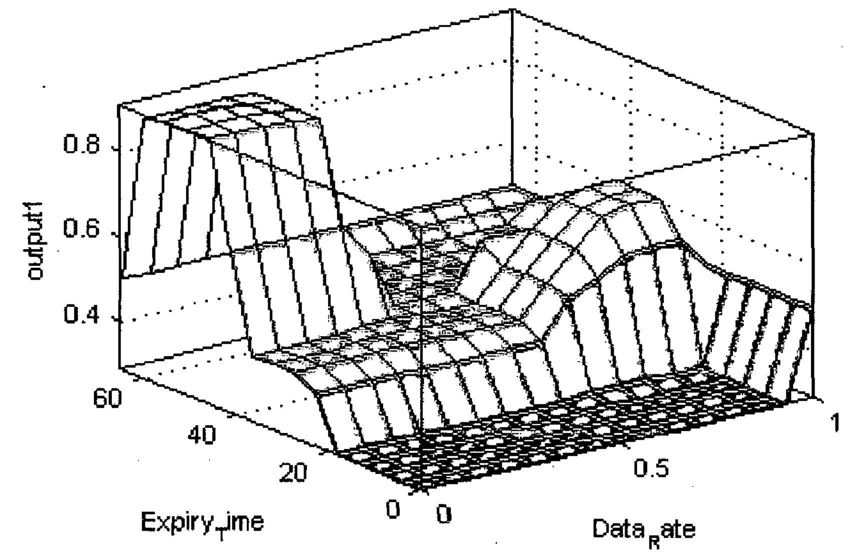


Figure 4.16 (c): Surface viewers for the fuzzy scheduler in case of expiry time and data rate

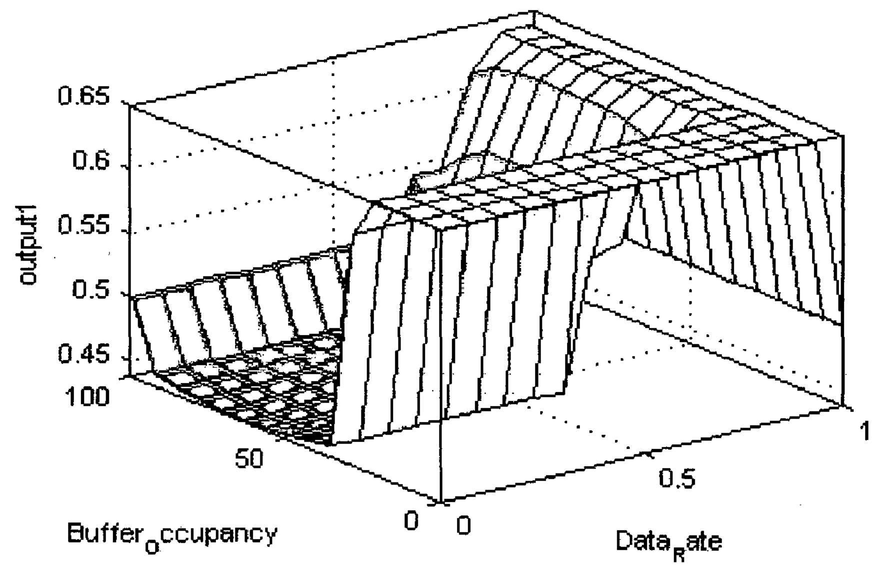


Figure 4.16 (d): Surface viewers for the fuzzy scheduler in case of buffer occupancy and data rate

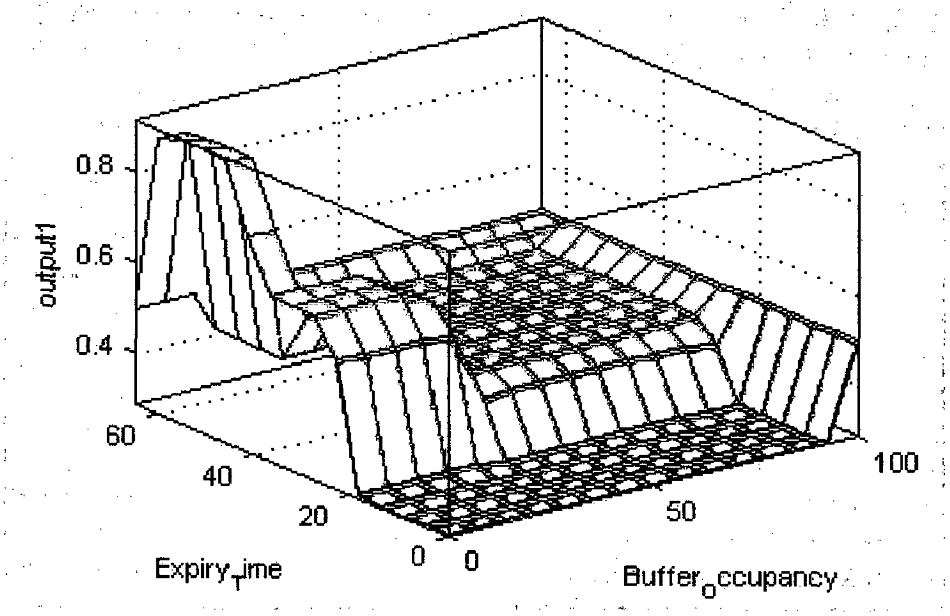


Figure 4.16 (e): Surface viewers for the fuzzy scheduler in case of expiry time and buffer occupancy

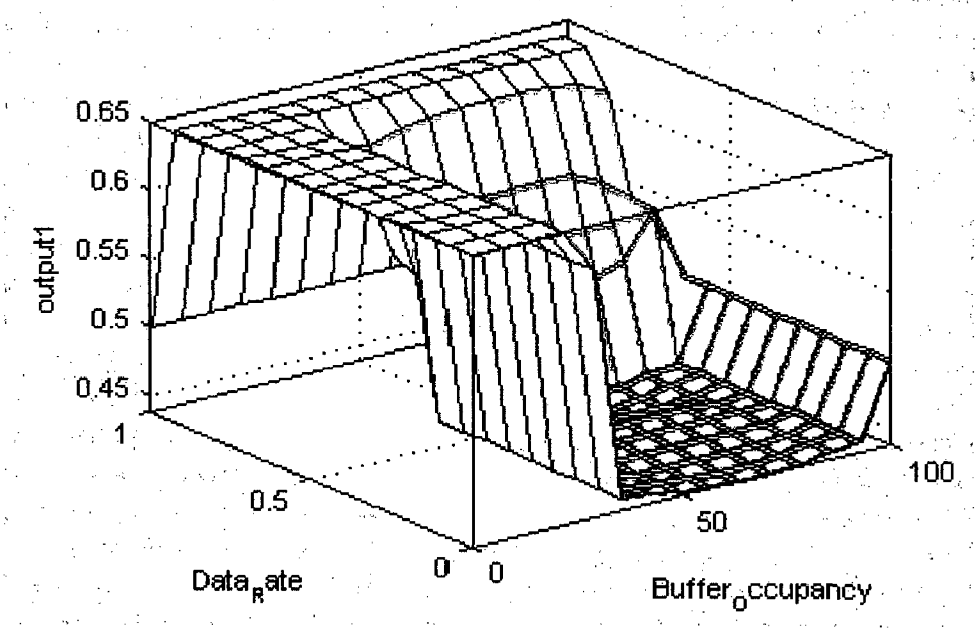


Figure 4.16 (f): Surface viewers for the fuzzy scheduler in case of data rate and buffer occupancy

4.5.2 Simulation Environment and Methodology

The algorithm is evaluated in terms of the metrics such its packet delivery ratio, average end-to-end delay and throughput and the results are presented. Simulation model consists of 5 nodes placed randomly within 100x100 meter area. Each simulation is run for 1200 seconds of simulation time. The wireless channel capacity is 11Mbps. The overall buffer size of the scheduler of each node is 64 packets.

Table 4.8 Fuzzy Rule Base for Data rate (DR), Expiry Time (ET) & Buffer Occupancy (BO)

DR \ BO	L	M	H
Expiry Time (Low)			
L	L	VL	L
M	L	L	L
H	VL	L	L
Expiry Time (Medium)			
L	A	A	VL
M	A	A	VL
H	A	A	A
Expiry Time (High)			
L	H	H	VH
M	VH	M	M
H	H	VH	M

A packet level discrete event ns2 simulator has been used for the analysis. The protocol implementation in ns-2 also maintains a send buffer of 64 packets used during route discovery. Random waypoint model has been chosen for present analysis because it is the most widely used mobility model in previous studies. In this model, a node decides to move to a random location within the grid. When it reaches that location, it pauses for a fixed amount of time, possibly zero seconds, and then it moves to another random location. The maximum allowed speed for a node is 20 meters per second. Constant bit rate (CBR) source have been taken as the data source for each node. Each source node transmits packets at a certain rate, with a packet size of 512 bytes. Source and destination node has randomly been chosen among all nodes. The maximum waiting time in the send buffer during route discovery is 20 seconds. If a packet remains in the send buffer for over 20 seconds, the packet is dropped. The buffer is shared by multiple queues when the scheduler maintains multiple queues. The simulations parameters are mentioned as default values unless otherwise specified are used in table 4.9. Table 4.10 indicates the simulation environment for analysing the performance of the scheduler. The traffic load and the degrees of mobility have been varied for simulations. A movement scenario arranges the movement and the position of the nodes according to the random waypoint model.

4.5.3 Simulation Results & Analysis

The simulation for evaluating the fuzzy scheduler is implemented within the qualnet library. The simulation package qualnet is used to analyze and evaluate the performance of the proposed fuzzy scheduler. The input variables used in fuzzy logic C code are identified. Then the calculated priority index is used for scheduling the data packet. By this way of scheduling, the packets in highly congested queues are given first priority for sending. The priority index that has to be associated with each packet is determined using fuzzy logic. The inputs to determine the priority index are the expiry time of the packet, the buffer occupancy and the data rate. The inputs are received for a network and rules are evaluated using these inputs. Each evoked rule provides an output membership function.

Table 4.9 Simulation Parameter

No. of Nodes	5
Area	100*100 m
Simulation Time	1200 sec
Node Placement	Random
Mobility Model	Random waypoint
Speed	0-20 m/s
Propagation Model	Free space
Channel Bandwidth	11 Mbps
Traffic Type	CBR
Data Payload	1024bytes/packets
Routing Protocol	AODV
MAC Protocol	IEEE 802.11

Table 4.10 Simulation Environment

Processor	2.1 GHz C2D
Hard Disk	320GB
RAM	3GB
Operating System	Windows 2000

These output membership functions are then implicated, aggregated and the crisp priority index is calculated from this aggregated curve using centroid method of defuzzification. As a result of this, the number of packets delivered to the sender, the end-to-end delay of the packet transmission and the throughput improves. The priority index is calculated with the inputs obtained from the network layer. This is then added to the header associated with the packet. Hence whenever the packet reaches a node, its priority index is calculated and it is attached with it. Each node has queues. Each queue in the node is sorted based on the priority index and the packet with the lowest priority index (i.e. packets with the highest priority), is scheduled next, when the node gets the opportunity to send. The performance of the network with the fuzzy code and without the code is analyzed under various conditions such as variation in network load and mobility of the nodes. In this simulation, the mode mobility is set at 0-20 m/s and network traffic load is large. Now the impact of node density on scheduler performance has been evaluated. The packet delivery ratio as a function of number of nodes is shown in figure 4.17.

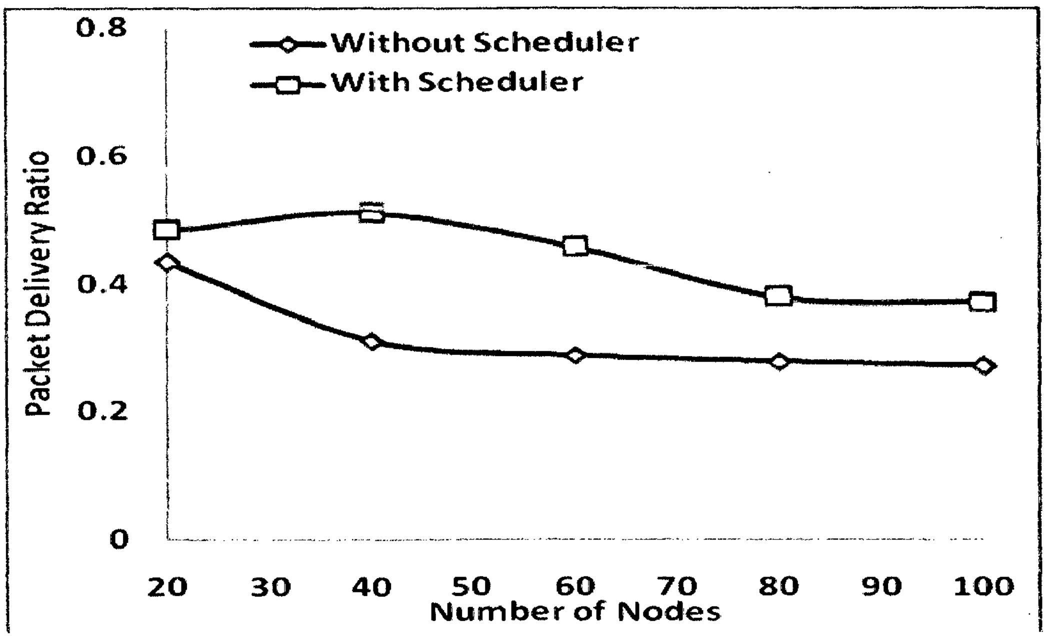


Figure 4.17: Packet delivery ratios as a function of network size

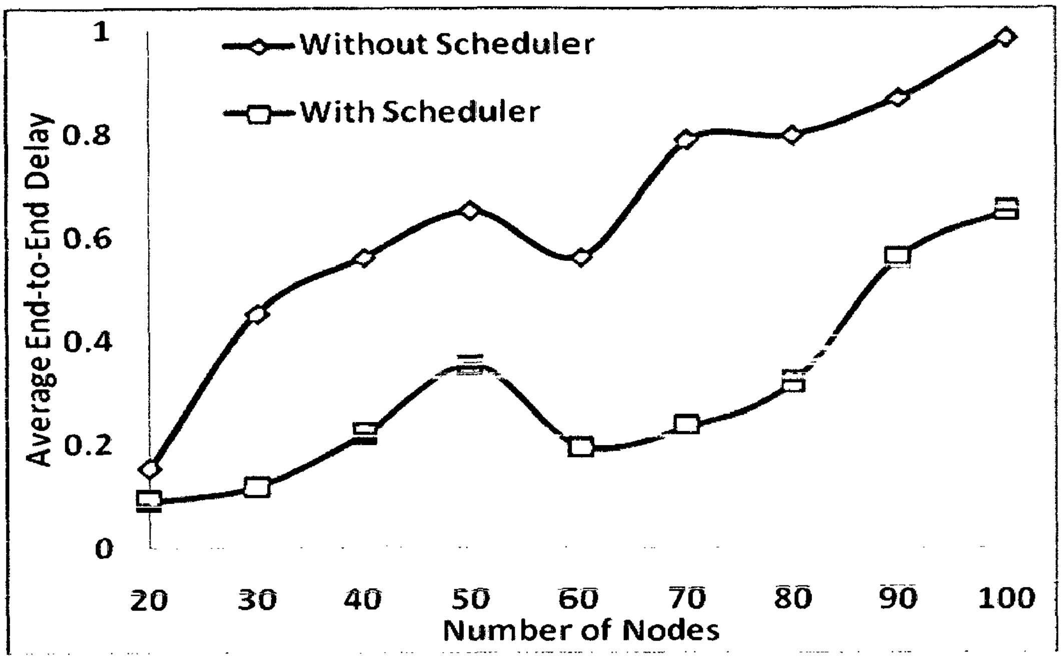


Figure 4.18: Average end-to-end delay Vs network size

The performance of fuzzy scheduler with reference to the packet delivery ratio is much improved as compared with that of one without scheduler. It is also seen that for small loads, the scheduler does not provide much improvement, but the traffic load is increased the improvement is more.

The average end-to-end delay performance as shown in the figure 4.18, it is observed that the end-to-end delay improves by 0.3sec when scheduler has been introduced. A mobility model should attempt to mimic the movement of the mobile nodes in this simulation; each node is moved constantly with a predefined speed. Moving directions of each node are selected randomly. When nodes reach the simulation boundary, they are bounced back and continue to move. The figure 4.19 shows the performance of packet delivery ratio vs mobility, for the simulation with fuzzy scheduler and without scheduler. It is clear that the packet delivery ratio is at the higher side for the network with scheduler. In the fuzzy scheduler, there is a less degradation in performance as the number of nodes increases. This is due to increase in number of hops the packets have to take for reaching the destination. But still, the end-to-end delay in much small compared to that of the network without scheduler. It can be inferred from the figure 4.18 and 4.20 that the fuzzy scheduler provides a better performance in terms of the end-to-end delay and throughput.

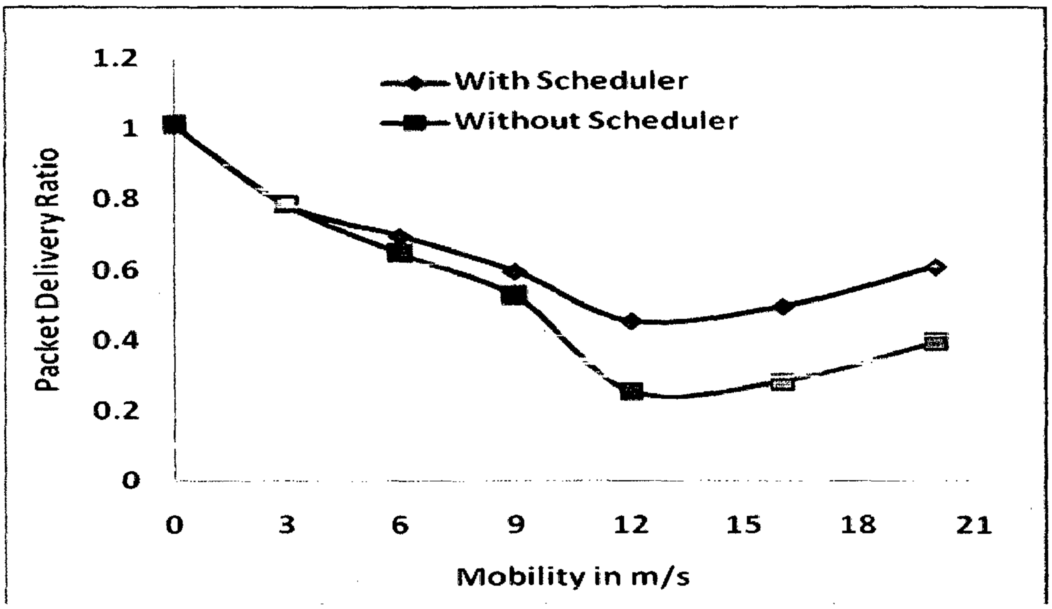


Figure 4.19: Packet delivery ratio Vs mobility

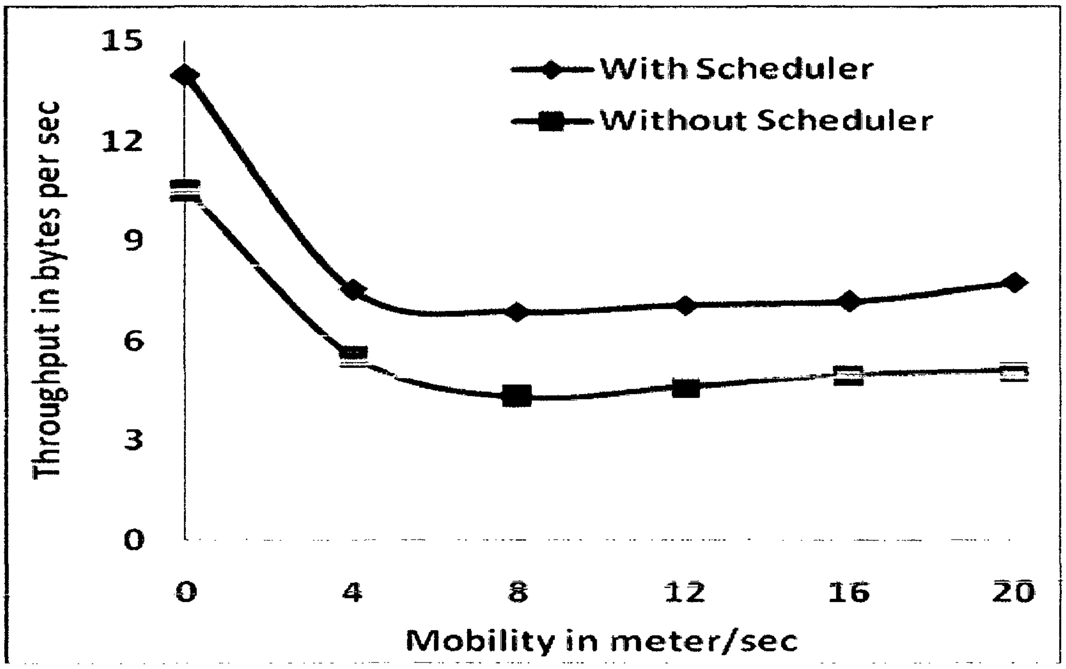


Figure 4.20: Throughput Vs mobility

The performance is evaluated with different seed value and the average value is taken for all the performance metrics. From the simulated results, the packet delivered improves by 2-8% as the mobility increases for a total transmission of packets. From the results it is clear that the fuzzy scheduler works better, and tested under different load and mobility conditions.

CHAPTER 5

Performance Analysis of Bandwidth Control Management of Wireless Ad-hoc Network for AODV Protocol

5.1 Background & Motivation

In recent years, wireless networks are being used for various traffic sources such as integrated services communication is the simultaneous transmission of voice, video and data traffic. Multimedia communications such as video conferencing, video-on-demand, multimedia learning distant learning programs etc. Such applications require stringent QoS requirements in terms of guaranteed bandwidth, sustainable delays and bounded jitters. In view of the remarkable growth in the number of users and the scarcity of bandwidth in wireless networks, an efficient sharing and management of bandwidth among the users becomes a key factor in enhancing the system performance. There is a growing need to support quality of service in mobile ad hoc networks [90], however, this is challenging. Wireless ad-hoc networks represent distributed systems, which interconnect wireless mobile nodes without the need for fixed infrastructure. The popularity of wireless ad-hoc networks in recent years has made bandwidth a demanding parameter. There is a pressing need to develop efficient bandwidth management routing scheme which increases the network performance.

5.2 Related Work

Research on quality of service provisioning in wireless ad-hoc networks may pursue with different goals to satisfy the needs of different users. Le i H. et al. [91] have proposed an adaptive QoS management system in wireless multimedia networks. It is based on admission control and resource-reservation schemes that support non real time quality of service application of wireless network. Calin C. et al. [92] have used algorithm which are admission control and resource-reservation schemes for efficient utility of bandwidth. The algorithm uses R-U functions for allocating and reallocating bandwidth to connections, aiming to maximise the accumulated utility of the system. Anup K.T. et al. [93] & Oliveria C. et al. [94] have developed the scheme based on adaptive bandwidth reservation to provide QoS guarantees for multimedia traffic (e.g., audio phone, video conference, video on demand, file transfer, etc.) carried in high-speed wireless cellular networks. The proposed scheme allocates bandwidth to a connection in the cell where the connection request originates and reserves bandwidth in all neighbouring cells where a connection is established. When a user moves to a new cell, bandwidth is reserved for new cells and bandwidth dynamically adjusted based on the current network conditions. Hong B. K. [95] has proposed a simple distributed adaptive bandwidth reservation scheme and a connection admission test for multimedia mobile cellular networks. The proposed bandwidth reservation scheme depends on the number of handover successes and failures to adaptively control reserved bandwidth for handover, and the admission test is designed to reduce traffic overhead between cells. Ruston H. et al. [96] has developed the new schemes for bandwidth reservation to minimize the call dropping on handoff. These schemes are evaluate using planar graph to model mobile wireless network. Sungwook K.M., [97] has been proposed bandwidth reservation algorithm that adjusts bandwidth reservations adaptively based on existing network conditions. It controls the bandwidth for different priority traffic services based on current network traffic conditions. An algorithm that is able to resolve conflicting performance criteria- bandwidth utilization, call dropping and call blocking probabilities. Siripongwutikorn P. [98] that adjusts bandwidth reservation adaptively based on existing networks conditions. The algorithm given is flexible, responsive to current traffic conditions in wireless networks and tries to strike the appropriate performance balance between contradictory requirements for QoS sensitive multimedia services & provides aggregate loss guarantee to resolve the problem of insufficient bandwidth allocation due to incomplete, inaccurate traffic descriptors supplied by users. The scheme uses the resource-utility functions for allocating and reallocating bandwidth to connections aiming to maximize the accumulated utility of the system. Mona Ei-Kadi [99] has proposed a novel, rate-based, borrowing scheme to allocate the desired bandwidth to every multimedia connection originating in a cell for QoS provisioning in wireless networks carrying multimedia traffic. This scheme ensures that the borrowed bandwidth is promptly returned to the degraded connections. Manthos K. [100] has been proposed a new sampling method for available bandwidth is called ab-probe. It is new model and measurement technique to estimate the path available bandwidth from end-to-end observation of packet dispersion. This work can improve the performance of user sessions, or more generally any network protocol that may need available bandwidth measurement; a very useful quantity, especially for server selection applications, routing, end-to-end transports, adaptive multimedia etc. Lin C. R. et al. [101] has proposed bandwidth routing protocol for quality-of-service (QoS) support in a multihop mobile network. It can be applied to two important scenarios: multimedia ad hoc wireless networks and multihop extension wireless ATM networks. QoS routing protocol contains end-to-end bandwidth calculation and bandwidth allocation. Lin C. R. [102] has developed an admission control scheme which can guarantee bandwidth for real-time applications in multihop mobile networks. This scheme also works in a stand-alone mobile ad hoc network for real-time applications. It contains end-to-end bandwidth calculation and bandwidth allocation. Lin C. R. [103] has proposed the protocol. It is based on admission control scheme that works in a standalone mobile ad hoc network for real-time applications. It also provides bandwidth guarantee feature is important for a mobile network to interconnect wired networks with QoS support. This scheme contains end-to-end bandwidth calculation and bandwidth allocation. Under such a scheme, the source is informed of the bandwidth and QoS available to any destination in the mobile network. This knowledge enables the establishment of QoS connections within the mobile network and the efficient support of real time applications. Gahng-Seop A. et al. [104] has proposed the SWAN model which uses distributed control algorithms to deliver service differentiation in mobile wireless ad hoc networks in a simple, scalable and robust manner. Khoukhi L. et al. [105] have developed a flexible QoS routing protocol for mobile ad hoc network called AQOPC "Ad hoc QoS optimal paths based on metric classes". It provides end-to-end quality of service (QoS) support in terms of various metrics and offers accurate information about the state of bandwidth, end-to-end delay and hop count in the network. It performs accurate admission control and a good use of network resources by calculating multiple paths based on different metrics, and by generating the needed service classes. To regulate traffic, a flexible priority queuing mechanism is integrated. QoS violation detection and adaptive recovery are assured by a mechanism based on the prediction of the arrival time of data packets. The results of simulations show that AQOPC provides QoS support with a high reliability and a low overhead, and it produces lower delay than its best effort counterpart at lower mobility rates. Xue, Q. et al. [106] & Kunz, T. et al. [107] have proposed method for bandwidth estimation and calculation for cross layer design of wireless ad hoc networks, which provides end-to-end quality of service (QoS) support, in terms of bandwidth and end-to-end delay, in mobile ad hoc networks (MANETs).

It is felt that existing models do not consider bandwidth routing algorithm for different type of services i.e. real and non real time application for wireless ad hoc network. Hence the routing algorithm has been proposed in this chapter named as BWCM (bandwidth control management model) that perform allocation and reservation of bandwidth for both real and non real time application of wireless ad hoc network. The developed algorithm establish the path between sources to destination and also create standby route during disconnect the primary path. The QoS parameter has been analysed in terms of end-to-end delay, throughput, rerouting, packet loss, and total number of connection, percentage of different path and probability of bandwidth. The performance in various QoS traffic flows have been examined through ns2 simulator under different mobility condition.

5.3 BWCM Model

The schematic block diagram of bandwidth control management (BWCM) model is shown in figure 5.1 that includes a set of functionalities and mechanisms, which are briefly discussed below:

The model consists of source, admission control, temporary resource reservation, routing protocol and MAC layer. The source has taken the final decision whether the incoming packets or message is rejected or accepted based on the bandwidth as given in table 5.1. In wireless networks, such accountability is made easily by the fact that all stations learn each other's requirements, either directly or through a control station. However, this solution cannot be extended to the ad hoc networks. In an ad hoc network, a host's available bandwidth is not only decided by the channel bandwidth, but also by its neighbour's bandwidth usage and interference caused by other sources, each of which reduces a host's available bandwidth for transmitting data. A major challenge in multimedia networks is the ability to account for resources so that bandwidth reservations are placed on them. To support algorithm for real & non-real time applications, we have to know not only the minimal delay path to the destination, but also the available bandwidth for it.

Admission control that provides a path, from source to destination, without interfering with nearby ongoing traffic. It is classified into measurement-based and calculation-based methods. In measurement-based schemes are based on throughput and delay. Whereas, calculation-based method build certain performance criteria for evaluating the status of the network. It is based on local computation of the available bandwidth by each node of the network based on information that is sent by its neighbours through routing protocol (AODV). Upon arrival of bandwidth allocation requests from new calls, the admission control first checks for bandwidth availability. If bandwidth is available, bandwidth is allocated to new calls are considered for allocation. The model is to determine whether the available resources in a network that meet the requirements of a new flow while maintaining bandwidth levels for existing flows and co-ordination among the packets. Accordingly, the decision is performed on the acceptance or rejection of a flow. This function is conducted together by the source node and other intermediate nodes mechanisms.

Admission control that calculates the bandwidth and is responsible for receiving the connection request and allocates the bandwidth. When incoming message or packets are routed through the network, the bandwidth estimation is required before performing admission control. In wireless ad hoc networks the channel of each node is shared with all its neighbours. Wireless communication channels are shared by all nodes within transmission range; therefore, all nodes within a transmission area assert for the limited channel bandwidth. Because of the shared medium, a node can successfully use the channel only when all its neighbours do not transmit and receive packets at the same time. Cansever, Derya H. et al. [108] derive formulae to estimate the available bandwidth in an ad-hoc network using shared links.

$$MUB_i = \sum l_{ij}, \forall j \in \text{Neighbourhood of i}$$

MUB_i is the maximum unused bandwidth, and l_{ij} is the total traffic between nodes i and j. But, since the traffic between neighbours of a node also interfere; these traffics must also be taken into consideration to calculate the maximum available bandwidth (MAB_i).

$$MAB_i = MUB_i - \sum_j \sum_k l_{jk,} \forall j \in \text{ Neighbourhood of i, } \forall_k \text{ Neighbourhood of j}$$

AODV routing protocol has been used for maintaining the local connectivity of all the nodes that uses HELLO message. All nodes broadcast their *MUB* and their local bandwidth requests. The source node sends the route request message to the entire neighbouring node for checking the available bandwidth to be sure that the flow passes through the all nodes. Destination nodes send route reply to reserve the resources. Available bandwidth is computed if the nodes know not only *lij*, but the *MABi* computed by their neighbours. Then, the available bandwidth ABi to allocate new reservations at node i is given by

$$AB_i = \min\left\{MAB_{i,} MAB_j\right\}, \forall j \text{ Neighbourhood of i}$$

Temporary resource reservation process that released the connection link or bandwidth after complete the communication. The resource reservation arranges for the allocation of suitable end-system and network resources to satisfy the user QoS specification. The resource reservation interacts with the algorithm to establish a path through the network in the first instance then, based on admission control at each node, end-to-end resources are allocated.

The model is to determine whether the available resources in a network meet the requirements of a new flow while maintaining bandwidth levels for existing flows. Accordingly, the decision is performed on the acceptance or rejection of a flow. This function is conducted together by the source node and other intermediate nodes mechanisms. The computation of the right status duration needs to take into account the number of hops between the source and the particular node and also the delays between the intermediate nodes. The detail analysis of the bandwidth calculation has been given in Appendix 1.

Wireless networks generally have limited resources in terms of both device capabilities and network bandwidth availability. Based on the feedback information about the network from the MAC layer, the source node has a final decision to accept or reject the user QoS requirements. This feedback measure is the packet delay measured by the MAC layer, which is calculated by the difference between the time of receiving an acknowledge packet and the time of sending a packet to the MAC layer. The overall average MAC delay is simply calculated using formula as suggested by Gahng-Seop Ahn et al. [104],

$$d = \frac{P_{on1}n_1 + P_{on2}n_2}{S}$$

Assume there are two types of traffic (real and non-real type traffic) of mobile devices in the shared channel medium. Class 1 and Class 2 represent real-time UDP traffic and best effort TCP traffic, respectively. Each of the n1 Class 1 mobile devices has an active UDP session, and each of the n2 Class 2 mobile devices has an active TCP session. An idle mobile device as a mobile device whose MAC layer is idle and interface queue empty. If a mobile device is not idle then it is busy. Where P_{on1} & P_{on2} is the collision probability for a class *i* mobile device at each time slot. Where S represent the total throughput of the system (in packets/sec). The detail analysis of the delay is given in Appendix 2.

This allows the model to measure the local available bandwidth at each node in the network. The measured available bandwidth is then used by the model to decide if the flow can be admitted for a particular service. The estimation of the end-to-end available bandwidth is performed by sending a request from source node toward the destination.

Table 5.1 QoS classes and application

QoS class	Bandwidth Requirement	Application Type
1	256 Kbps	Non-real-time flow with normal service
2	512 Kbps	Non-real-time flow with preference service
3	2 Mbps	Real-time flow with normal service
4	4 Mbps	Real-time flow with preference service

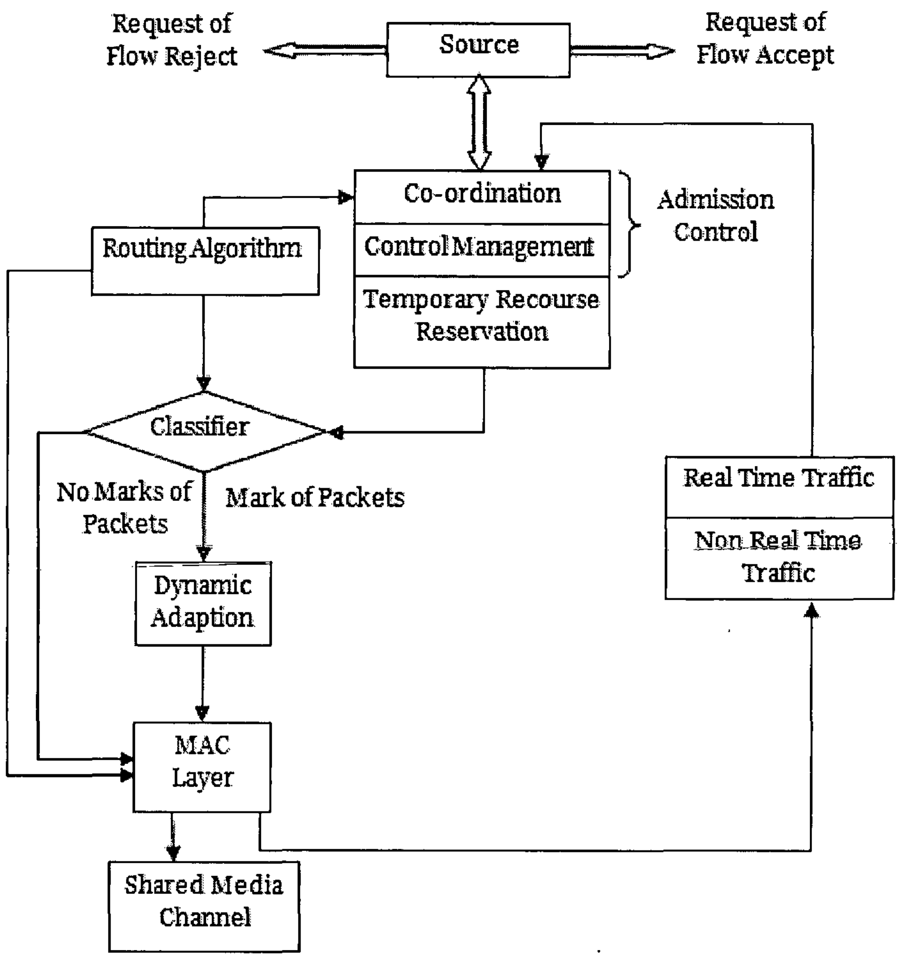


Figure 5.1: A BWCM model of mobile ad hoc network

The flowchart contains three main modules: (i) path or route create, (ii) admission control and resource reservation and (iii) path or route repair. Figure 5.2 shows a flowchart which summarizes the three modules.

The source node starts to create the path from source to destination by using a proposed algorithm. The node ID and the location information reaches to neighbouring nodes through the beacon broadcasting to the one-hop neighbours that are located within the transmission range of this node. A list is generated based on the distance between neighbour and destination.

The source node sends a route request message. If the packet loss ratio (PLR) is more than the required threshold value, it sends a route failure message back to the source node. After receiving the route failure message, the source node starts the route discovery procedure again to create new path.

After the destination receives the route request message, it assigns the required bandwidth to every node in the route. The destination sends an admission request message to the next node. The message contains the source route and the bandwidth required for every node in the route.

If node admits the flow, it broadcasts a “Reservation Request” message to all its neighbours, asking for their bandwidth availability. The message contains information of the bandwidth required for transmitting from the next node. If node cannot admit the flow, it sends an “Admission Refused” message to the next node.

After receiving an “Admission Refused” message, it starts a route repair procedure. In the case that node sent a “Reservation Request” message, the neighbouring nodes check their local available bandwidth. If a node finds out there are sufficient resources available, it reserves this bandwidth temporarily for the flow, and sends the “Reservation Accepted” message; otherwise, the node sends a “Reservation Refused” message.

If the reservation is accepted from all the neighbours, it forwards the “Admission Request” message to the other node in the source route; otherwise, if node received a reservation refusal, it sends an “Admission Refused” message to node which in turn starts a route repair procedure. The procedure is repeated until the source node is reached.

When the destination receives the “Route Request” message, it records the source route and then assigns the bandwidth required for every node in the route, using only the total number of hops.

The destination sends an “Admission Request” message containing the source route and the bandwidth required for every node in the route. Upon receiving the “Admission Request” message, node sends a “Reservation Request” message to the controller, indicating the required bandwidth.

If node receives a “Reservation Accepted” message, it forwards the “Admission Request” message to the source route; otherwise, if node receives a “Reservation Refused” message from the controller, it sends an “Admission Refused” message to the other node in this route. If node receives an “Admission Refused” message, it will start a route repair procedure.

A BWCM model should be accepted only if there is enough available bandwidth and omitting signal-to-interference ratio, packet loss rate, etc. This is because bandwidth guarantee is one of the most critical requirements for real-time applications. Bandwidth in time slotted network systems is measured in terms of the amount of free slots. The goal of the routing algorithm is to find a shortest path such that the available bandwidth on the path is more than the minimal requirement.

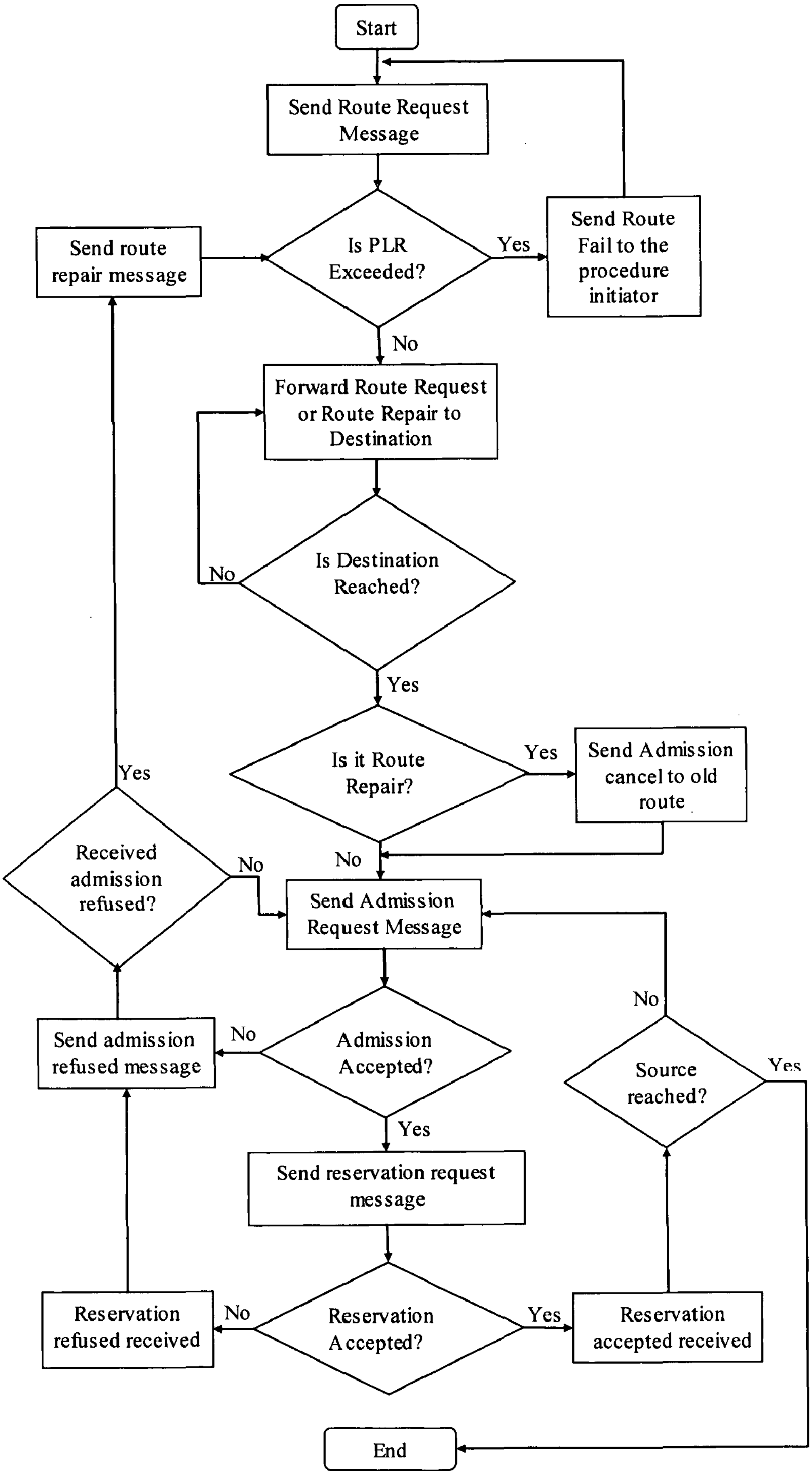


Figure 5.2: The flowchart for BWCM model

5.3.1 AODV Protocol

Ad hoc On-demand Distance Vector Routing (AODV) is an algorithm for the operation of ad hoc networks. AODV provides loop free routes even while repairing broken links. Because the protocol does not require periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements. The AODV algorithm is a confluence of both DSR and destination sequenced distance vector (DSDV) protocols. It shares on-demand characteristics of DSR, and adds the hop-by-hop routing, sequence numbers and periodic beacons from DSDV. It has the ability to quickly adapt to dynamic link conditions with low processing and memory overhead. AODV offers low network utilization and uses destination sequence number to ensure loop freedom. It is a reactive protocol implying that it requests a route when needed and it does not maintain routes for those nodes that do not actively participate in a communication. An important feature of AODV is that it uses a destination sequence number, which corresponds to a destination node that was requested by a routing sender node. The destination itself provides the number along with the route it has to take to reach from the request sender node up to the destination. If there are multiple routes from a request sender to a destination, the sender takes the route with a higher sequence number. This ensures that the ad hoc network protocol remains loop-free.

Basic Operations of AODV

1. Path Discovery
2. Route Table Management
3. Link Breakage
4. Path Maintenance

5. Local Connectivity Management

6. Local repair

The algorithm uses different messages to discover and maintain links. Whenever a node wants to try and find a route to another node, it broadcast a route request to all its neighbours. The route request propagates through the network until it reaches the destination or a node with a fresh enough route to the destination. Then the route is made available by unicasting a route reply back to the source. The algorithm uses HELLO messages that are broadcasted periodically to the immediate neighbours. These HELLO messages are local advertisement for continued presence of the node and neighbour using routes through the broadcasting node will continue to mark the routes as valid. HELLO messages can be used to maintain the local connectivity of a node. AODV uses HELLO message to send bandwidth information to neighbours, so that they can make necessary reservations based on the available bandwidth.

5.3.2 Algorithm & BW Calculation

The transmission time scale is organized in frames, each containing a fixed number of time slots. The entire network is synchronized on a frame and slot basis. The frame synchronization mechanism is implemented with techniques similar to those employed in the wired networks [109] and for wireless network in [103]. Each frame is divided into two parts, first the control and second the data phase as shown in figure 5.3.

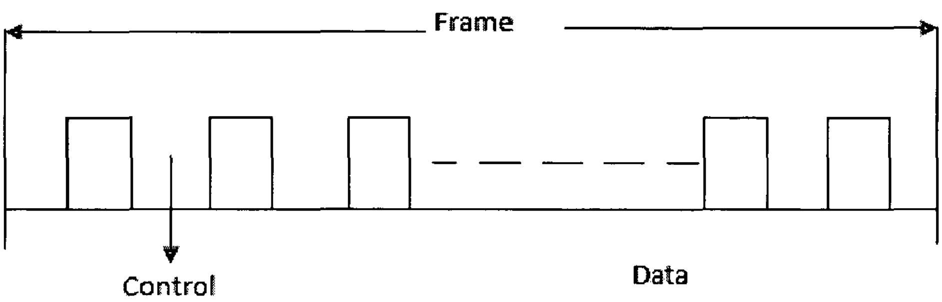


Figure 5.3: Frame Structure

The size of each frame in the control phase is much smaller than the one in the data phase. For example in each time frame, the data slot in the data phase is 5ms, and the control slot in control phase is 0.1ms. Assume there are 16 data slots in data phase. So the frame length is 20*0.1+16*5=82ms. Since the number of data slots is less than the number of nodes, nodes need to compete for these data slots. Each node takes turns to broadcast its information to all of its neighbours in a predefined slot, such that the network control functions are performed distributively. It is assumed that the information can be heard by all of its adjacent nodes. In a noisy environment, where the information may not always be heard perfectly at the adjacent nodes, an acknowledgment scheme is performed in which each node has to ACK for the last information in its control slot. By exploiting this approach, there is one frame delay for the data transmission after issuing the data slot reservation. Ideally, at the end of the control phase, each node has learned the channel reservation status of the data phase. This information will help one to schedule free slots, verify the failure of reserved slots and drop expired real-time packets. The detail of end-to-end bandwidth calculation has been given in Appendix 3. The developed algorithm maintains the routing table (two alternative routes in the algorithm, i.e., SR_1 and SR_2); SR_1 has larger bandwidth than

SR_2. The "PR" and "SR" in the algorithm mean the primary route & standby route respectively. It is notable that the primary route is shortest, but is not necessary to have the largest bandwidth. When a host generates a new call, it uses the algorithm to construct the path. In the algorithm, the route that satisfies the QoS requirement in order to precedence PR, SR_1, and SR_2 is chosen. The chosen route will be the primary route. That is, the next entry in the routing table may be changed depending on the requirement. After choosing the primary route, the source node will send out a call setup message to next. Upon receiving the message, the next node will run the protocol in the algorithm to reserve bandwidth for the new call. Because of high mobility, a topology change destroys the primary route; node will try to rebuild a new path immediately, using either SR_1 or SR_2. Thus, a new route from the breakpoint will be established by sending call setup message node-by-node to the destination. The source–destination pair of a call is randomly chosen, and their distance must be greater than one. Once a call request is accepted on a link, a data slot is reserved automatically for all the subsequent packets in the connection. The window is released when either the session is finished or the packet is received. There are three types of services (S) for the offered traffic. S_1, S_2 and S_4 need one, two, and four data slots in each frame, respectively. The total simulation time is 10^6 ms. A new call is generated every cycle (82 ms). The inter arrival time of packets within a S_1 session is an exponential distribution with 100 ms on average. Similarly, the mean values of the inter arrival time for S_2 and S_4 are 50 and 25ms, respectively. The maximal queuing delay of a data packet within a node is set to four frame lengths (4x82=328 ms). If a packet stays in a node more than that time, it will be dropped.

The featured of the algorithm:

1. This feature is important in both variable bit-rate (VBR) multimedia applications and mobile wireless networks. For VBR applications, upper layer will request different bandwidth support if the whole network status changes such as born and death of other traffics. Even in constant bit-rate (CBR) applications, any mobile node's movement will cause different requirement of service.

2. The algorithm state observer detects performance saturation, estimates network states, and provides feedback path to the model and upper layer protocols. The maximum possible changing rate of system state including bandwidth, tolerable packet loss rate, packet size, packet delay, and delay variance.

3. In this algorithm to reduce the computation complexity.

However, the algorithm suffers the following problems:

1. Uncertainties and dynamics in network states: The measurement of network states is very difficult since there are too many affecting factors, which many of them are unknown and are dynamically changing with time. This situation is more obvious in wireless mobile networks. Therefore, formalization of the network behaviour is very difficult and we need an effectively observer to estimate network states.
2. In some applications especially variable bit rate (VBR) streaming in mobile wireless networks are usually dynamic. Cross-layer corporations are required.

These features of the proposed model is important since in wireless networks mobile nodes with limited resources usually move among transmission range area, request immediate heavy traffic flows, and then cause traffic profiles to be changed.

5.4 Simulation Environment and Methodology

In order to better understand the properties of the BWCM model, the simulation considers a multiple scenarios of real and non real time and TCP best-effort traffic. The video and voice flows representing real-time traffic and data flow representing the non-real time traffic. The performance evaluation of the proposed model has been analysed with the ns2 simulator. Simulation modelled a network of 20 mobile nodes placed randomly within 100x100 meters and shares a 5.5Mbps radio channel with its neighbouring nodes. Each simulation is run for 1200seconds of simulation time. A free space propagation model is used in our simulation. Video traffic is modeled as 200Kbps constant rate traffic with a packet size of 512bytes. Voice traffic is modeled as 32Kbps constant rate traffic with a packet size of 80bytes and data traffic is modeled as 16Kbps constant rate traffic with a packet size of 1024bytes Multiple simulations run with different seed values are conducted for each scenario and collected data is averaged over those simulated results. Data sessions with randomly selected sources and destinations have been simulated. The traffic load is varied, by changing the number of data and the effect is evaluated with AODV routing protocols. The AODV protocol is chosen as the routing protocol referred to in figure 5.1.

5.5 Simulation Results & Analysis

From figure 5.4 shows that percentage call of rerouted path due to disconnect the path by varying the mobility. If any of the connected paths is disconnect, the virtual connection between sources to destination needs to be rerouted. The curve indicates that S_1, S_2 and S_4 are uniform for all traffic flows. During the call setup, each source-destination has been randomly chosen to determine its services (S) type. It is observe that the rerouting the percentage of calls is increasing while increasing the variation of mobility. That is, frequently disconnect the path or route while increasing the mobility. When mobility is 20m/s of S_1 about 54% of the connection needs to be rerouted. Similarly when mobility is 20 m/s of S_2 & S_4, about 48% & 44% of the connections need to be rerouted. The figure indicates that the result is independent of QoS of traffic flows because what we measure is the fraction of connections that have already received a route and need to be rerouted during their active periods. The results as shown in figure 5.5 indicate that the average throughput decreases as mobility increases. Frequent broken the established path occur while increase the mobility in wireless ad hoc that requires different routing path for new connection between source to destination that gives the results more end-to-end transmission delay and increases the packets loss. From the simulation results it is observed that the high QoS connection has high throughput on average because of the high input rate. By using slot reservation method makes the input packet flow have lower queuing delay to avoid the packet loss. Figure 5.6 indicate the average delay because path length is not same for all packets due to rerouting. The hop delay is computed from the end-to-end delay divided by the path length. Only selective packet has been considered because it has came from different path due to rerouting. The concept of selective packet this can reduce the end-to-end delay. But slot reservation limits the queuing delay. If we want to limit the delay the input rate should be less than processing rate. From the simulation results it is indicate that the S_1 connection has a stable hop delay of about 92ms, which is near to the frame length (82 ms). Similarly S_2 and S_4 have stable hop delay of about 69 and 55ms respectively. For lower delay, the more slots are allocated per frame, means packets has a higher probability to be transmitted sooner. From figure 5.7 the simulation results shows that the amount of connection of different services. The current system bandwidth is 16 data slots in each time frame. There are about 34 connections of S_1 traffic simultaneously in the system at a mobility of 20 m/s (16 connections for S_2 and 6 connections for S_4). Similarly there are about 32 connections of S_1 for the mobility of 10 m/sec (20 connections for S_2 and 12 connections for S_4). Based on the results indicate that the amount of connection decreases with increasing the mobility. Figure 5.8 indicate that the amount of packet loss for varying mobility. The maximal queuing delay of a packet within a node is limited to four frame lengths (328 ms). If a packet stays in a node more than 328 ms, it will be dropped. Packets are served in first-in/first-out (FIFO) order.

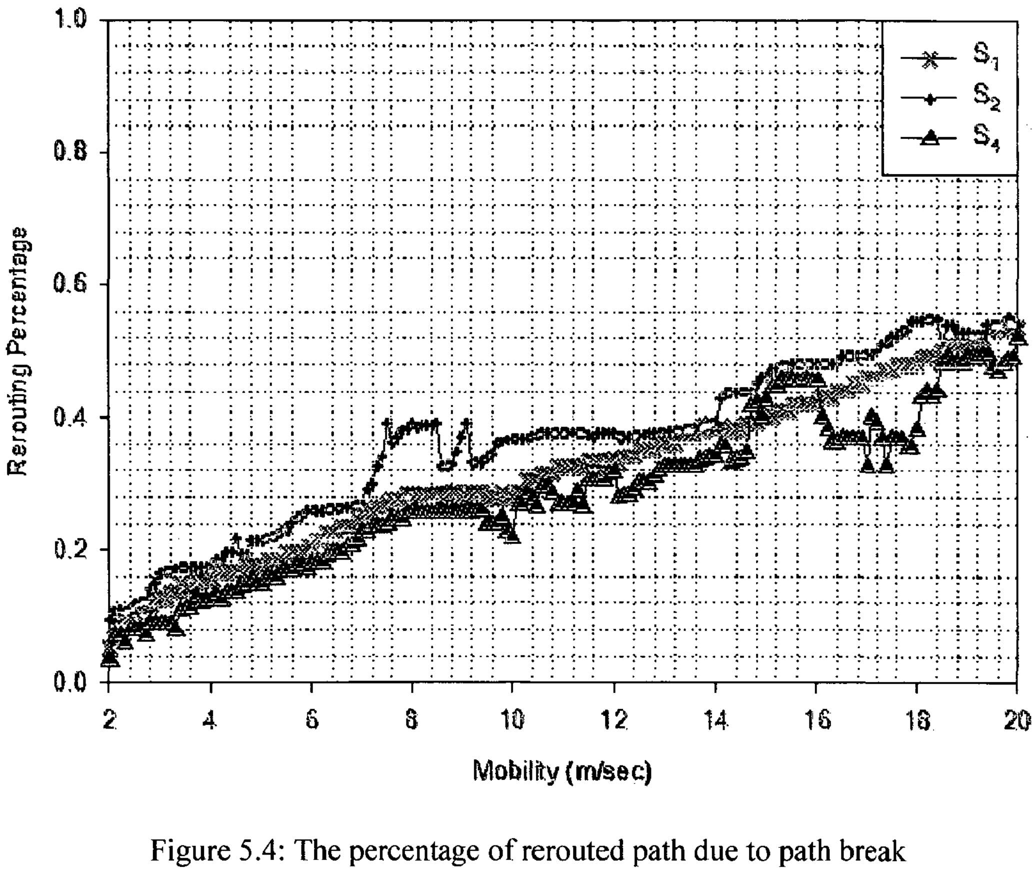


Figure 5.4: The percentage of rerouted path due to path break

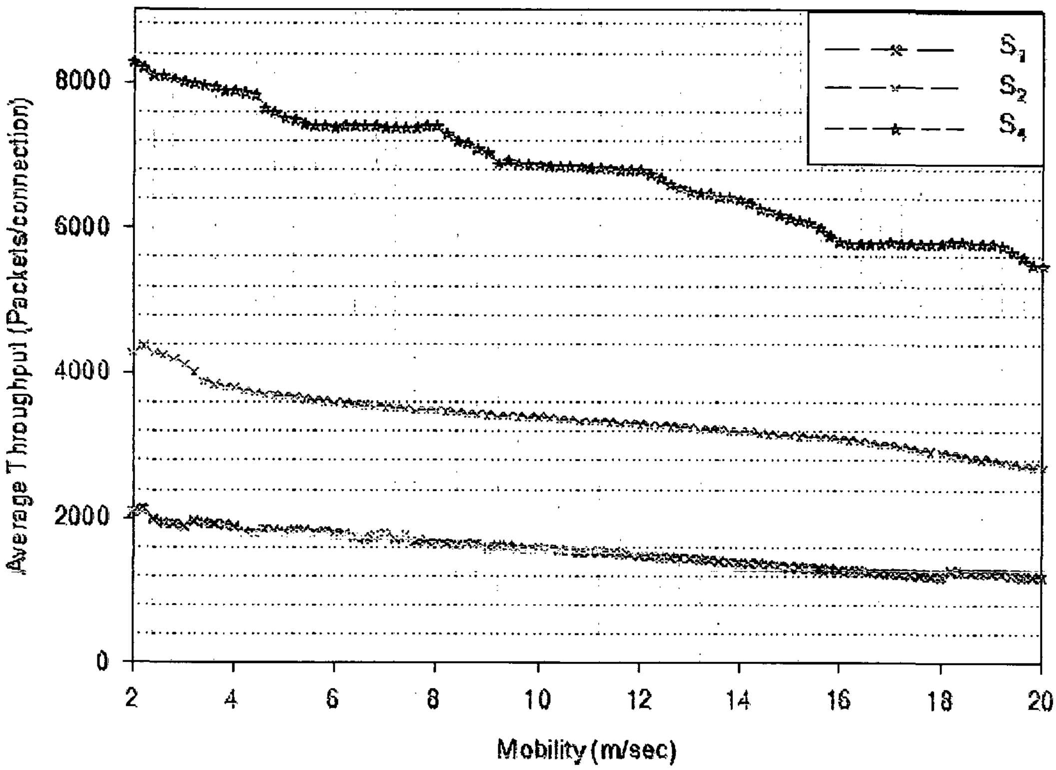


Figure 5.5: Average throughput of different QoS's

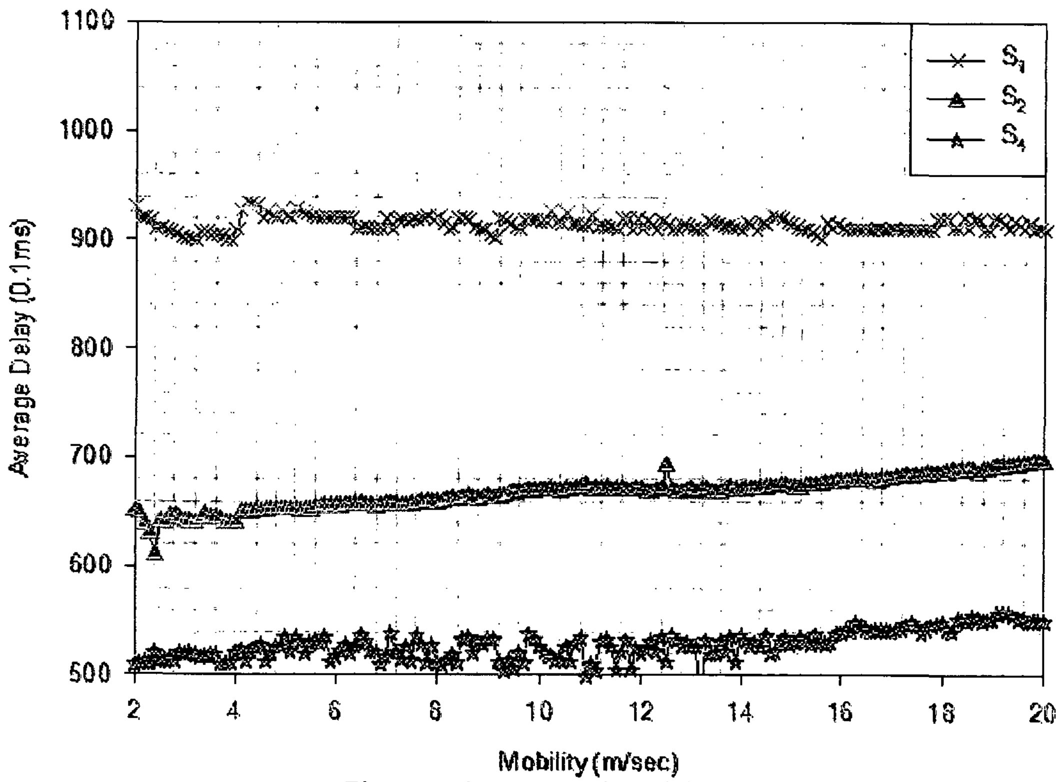


Figure 5.6: Average hop delay

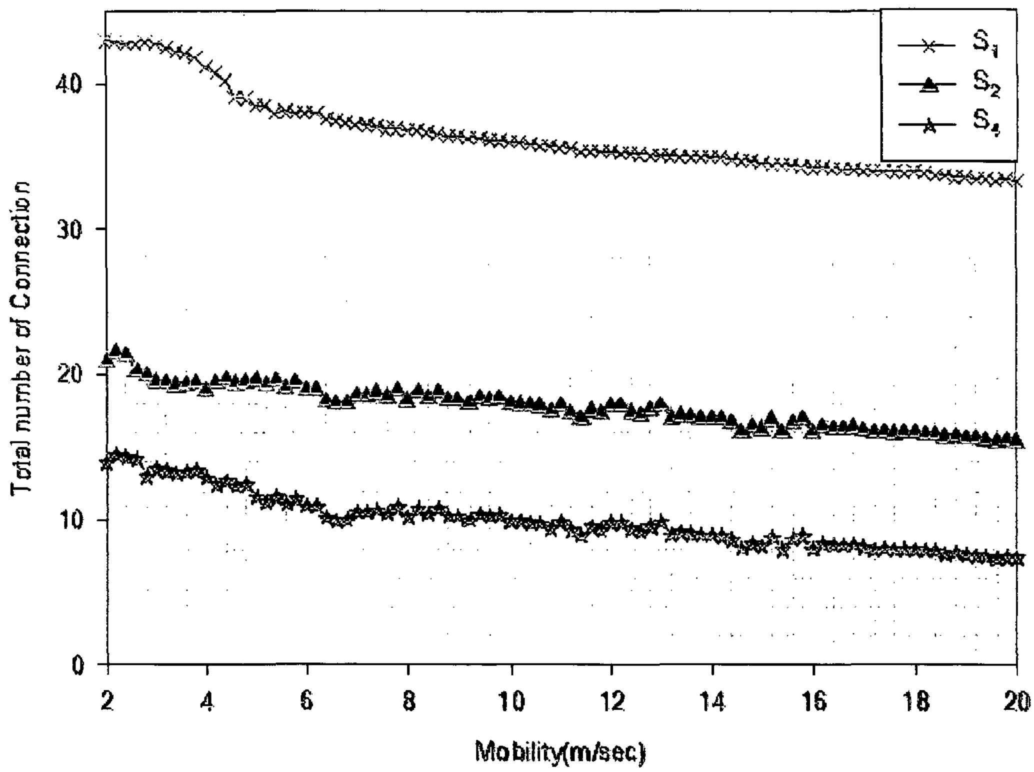


Figure 5.7: The total number of connections

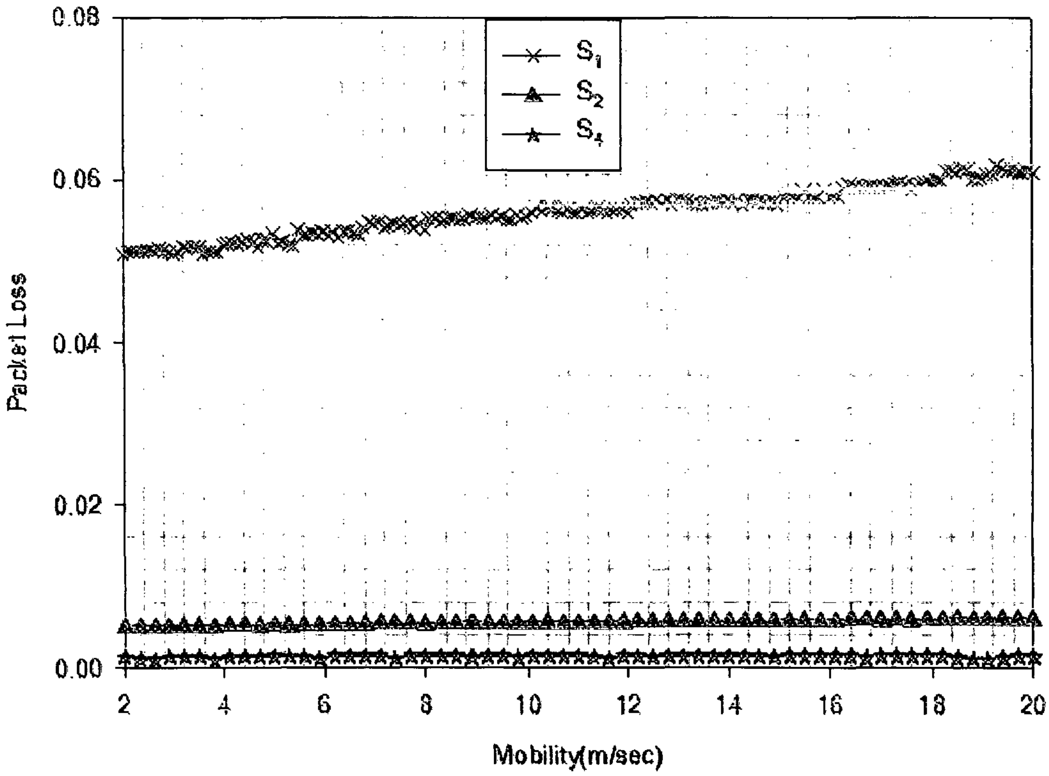


Figure 5.8: Packet loss per host

From the results it is indicate that at a mobility of 20 m/sec, the packet loss is about 6.1% (for S_1) or less (0.8% for S_2 and 0.3% for S_4,). It is observed from the results that the packet loss rate increases with increasing the mobility. But overall affect of the packet loss rate is low as increasing the mobility because its time is small. Therefore, the time has a lower probability to be over 328ms. A new call is generated at every two cycles (i.e., around 164ms). The reserved slots will be released, if no data packet is sent over the reserved slots for ten cycles (i.e., 10x82=820ms). To set up a new call, each node has been considered to run the algorithm in Appendix 4. Figure 5.9 shows that at a mobility of 20 m/s, 96% of calls that use primary route at the source node can set up the connection successfully, and 4% will fail because of outdated bandwidth information.

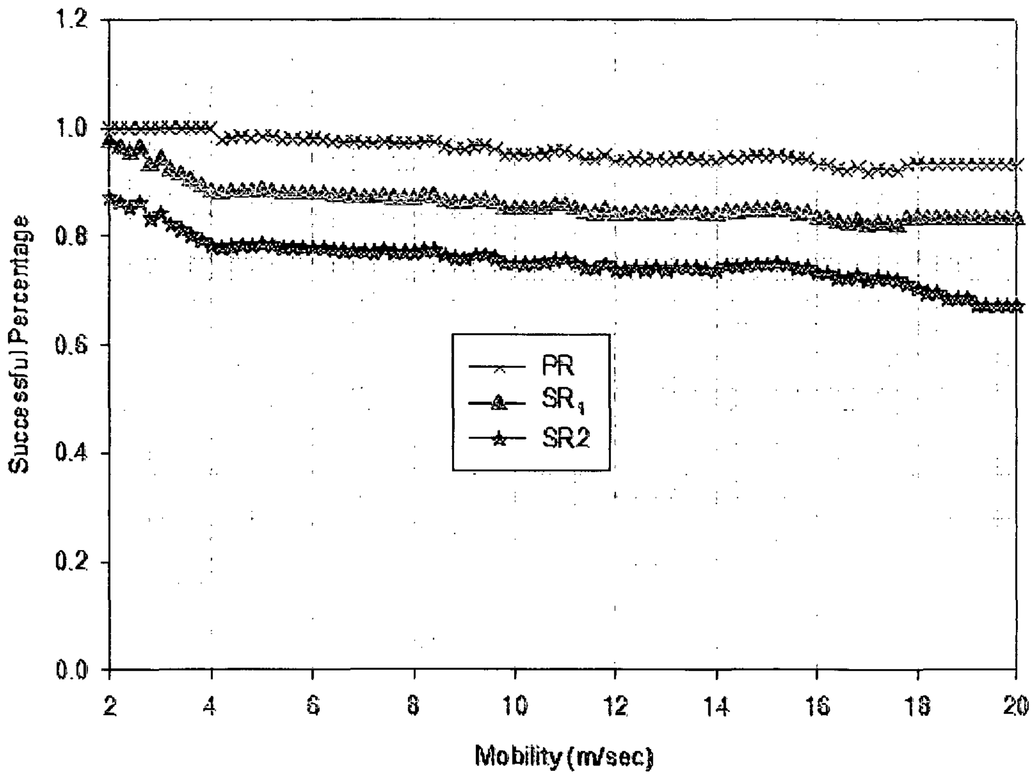


Figure 5.9: The successful percentage of different connections for the QoS requirement

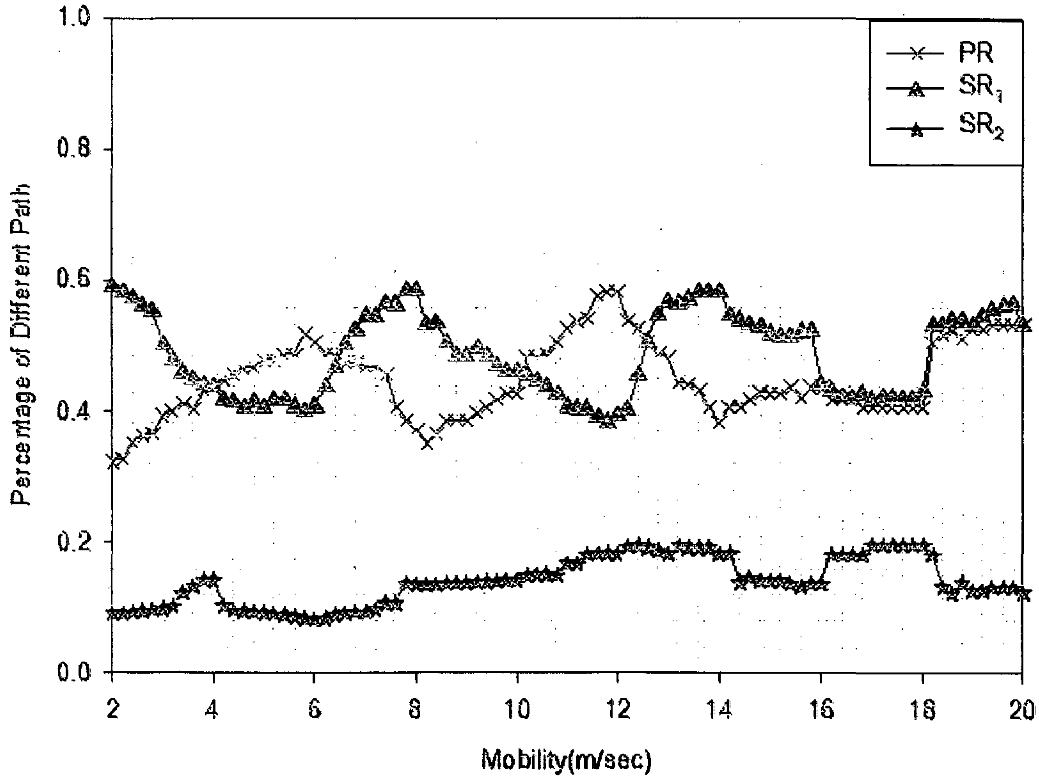


Figure 5.10: Route selection at the source for a given connection

Due to mobility, the path bandwidth information is changed dynamically. If a node does not receive the newest bandwidth information, then the connection setup may fail at some intermediate node because of lack of bandwidth. It indicates the effect of the "possible" outdated bandwidth information on the primary route (PR) and the standby routes (SR_1 and SR_2). From the simulation results, it is observed that no matter which route is selected at the source, we still have high probability (for example, 96% for PR, 82% for SR_1, and 67% for SR_2 at a mobility of 20m/sec) to construct a connection successfully. That is, the effect of mobility on the route selection that establishes a connection is not too strong. For a given connection of a call, it may be constructed by a different route at the source.

According to algorithm for making a connection (Appendix 5), in figure 5.10 near 35–55% of connection's are setup through the primary route under different mobility. Similarly, 41–59% of connection's are through SR_1 under different mobility. From the simulation result, it is found that the standby route is useful. The primary route is the shortest route calculated by the AODV algorithm. However, if all source–destination pairs only consider the shortest path, there will be some hot spots that lack enough bandwidth. Once a call request is passing through those nodes, it will be spurned. Thus, this is the reason why there are only 35–55% of connection's that can pass through the primary route. There is only about 12% of connection's using SR_2. This means that if primary route and SR_1 do not have enough bandwidth, there is a small probability for SR_2 to have enough bandwidth.

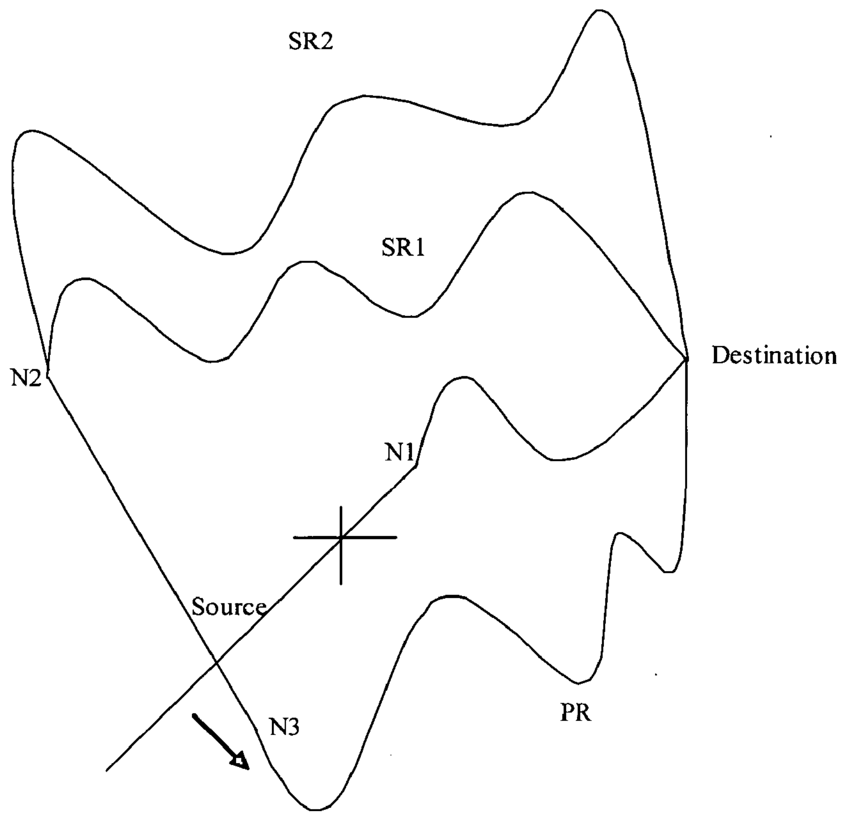


Figure 5.11: Standby path is made if primary path fails.

When a link of a connection is broken, the new connection can be made from the breakpoint as shown in figure 5.11, if there exists enough bandwidth in a standby route. If there are no bandwidth in standby path to block traffic flow from source to destination. In the worst case condition, a new connection will be rebuilt from the source node and released all slots by old connection. All reserved slots by the old connection will be freed hop-by-hop.

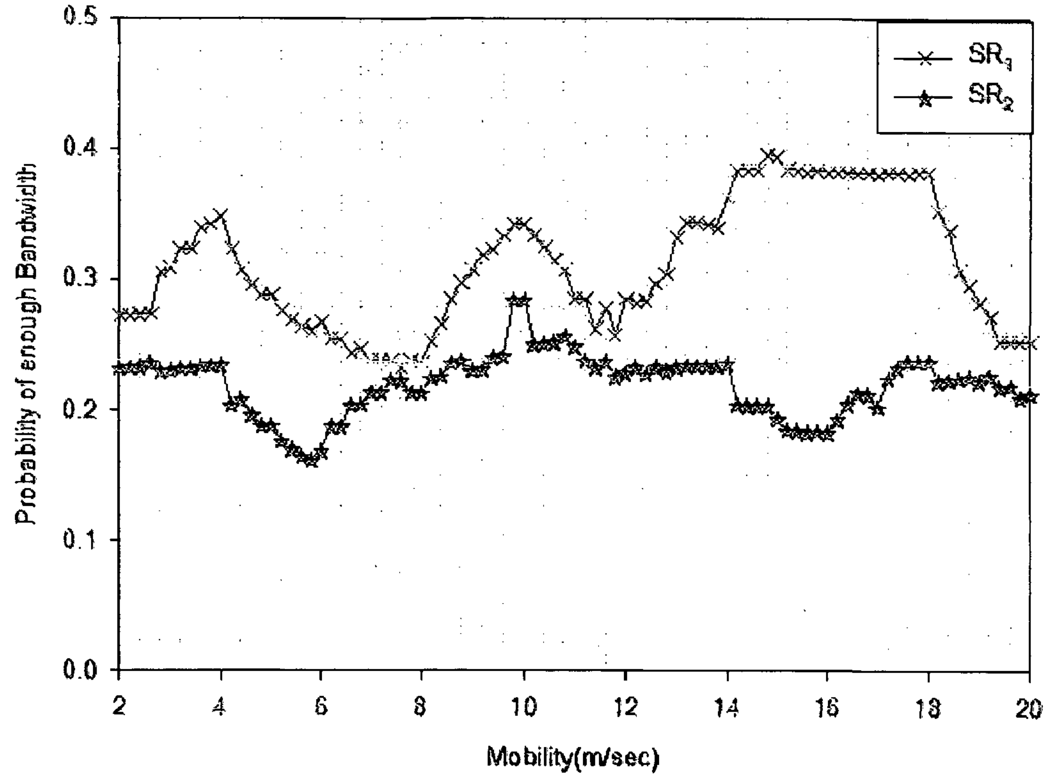


Figure 5.12: Probability of the breakpoint having different path

Figure 5.12 shows the probability of detecting a feasible alternate route at the breakpoint according to the current bandwidth information before the new call setup begins. At a mobility of 20m/sec, there is a probability of 0.33 for SR_1 (0.23 for SR_2), which has enough bandwidth to the destination at the breakpoint. A feasible alternate route depends on the set of neighbours. However, the node speed is not necessary to result in a greater chance of having good neighbours who have larger bandwidth. Therefore, the mobility does not affect the probability.

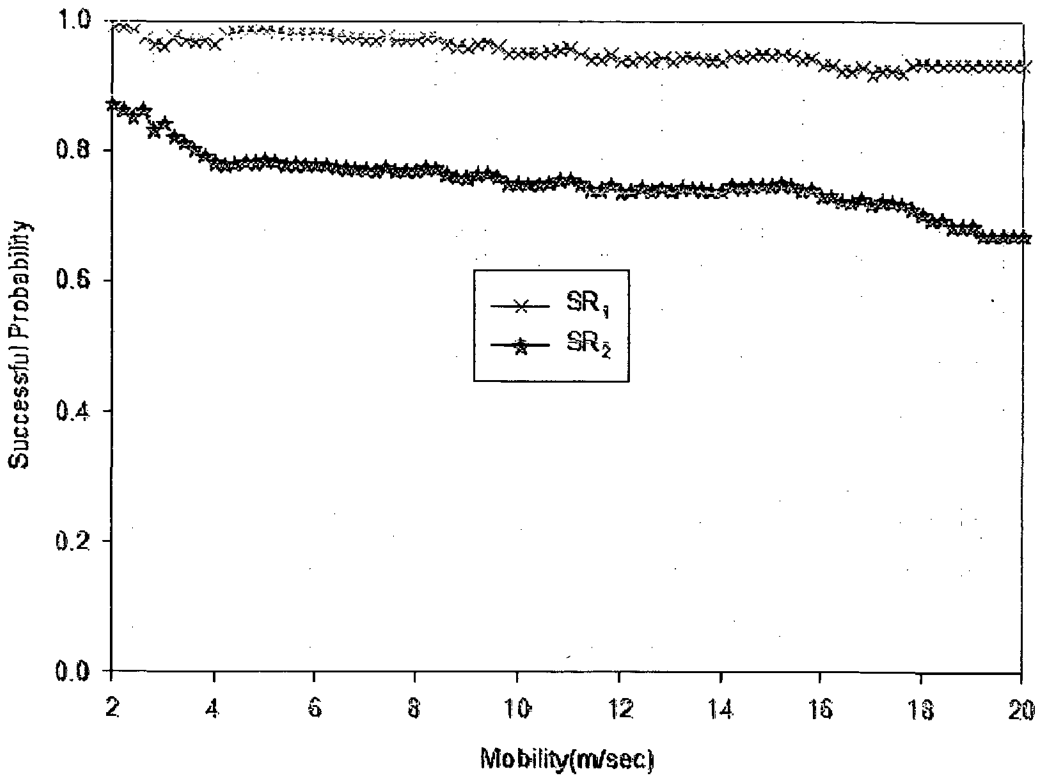


Figure 5.13: The successful probability of a call setup at the breakpoint

Figure 5.13 shows the probability of a successful call setup given a purportedly feasible path (i.e., either SR_1 or SR_2) at the breakpoint to the destination. The SR_1 path has a probability of more than 0.9 to set up a new call setup in low mobility. The results shows that at the high mobility, the probability is still more than 0.8. It is observed from the results that in high mobility, there is a little chance of a successful call setup. When the system is saturated, the node speed does not cause an intermediate node between the disconnect point to the destination to see another neighbour who has enough bandwidth. When combines the results in figures 5.14 and 5.15 it is observed that there is little probability of having another route at the breakpoint. However, the backtracking increases the probability. If it is consider the set of nodes from the source to the disconnect point along the path, the probability of having a route at any one of these nodes will be much higher than the case of just considering the disconnect point. Bandwidth calculation algorithm has been given in Appendix 4. This information lets us envision whether a connection is established on a given route before the call setup commences. If we only use the AODV algorithm and the reservation algorithm (Appendix 5), then a new call may be blocked in some intermediate node that is saturated. No source can construct a virtual connection via the saturated node until one of the connections over the node ends its transmission, and the bandwidth becomes available. Mobile nodes exchange bandwidth information periodically. The data is propagated hop-by-hop and cannot reach all nodes immediately. It is compare the call blocking rate of two systems that are running the same routing algorithm (i.e., AODV) and the reservation algorithm. But only one of both has the bandwidth information in the routing table. The call blocking rates are for input traffic during 10ms of the simulated time. In this simulation, we run 100 simulations (each of length 10ms) with different initial topologies to compute the averages. The call generating rate is one call every two frames (i.e.2*82=164ms). Thus, there are $(1/164)\text{x}10^6$=6098 calls generated during 10ms. Observe that about 11% calls will be blocked if there is no bandwidth information. However, only from two to three calls of the 6098 calls will be blocked if the source node has the bandwidth information. This information lets the source node determine if a new call should be blocked. In addition, this information is seldom underestimated by our algorithm. That is, the reliability of the information is high. Thus, this knowledge enables more efficient call admission control.

CHAPTER 6

CONCLUSIONS AND SCOPE FOR FUTURE WORK

Based on the literature review it is observed that current high speed network research is dominated by the wired and wireless networks. The field of wireless communications and networks has witnessed amazing growth in recent decade. It has become one of the fastest growing telecommunications segment. Wireless communications systems have found widespread use and have become an essential tool for numerous people in their daily life. The next generation of wireless networks will use the infrastructure less network (MANET) carry diverse media such as data, voice, and video. Therefore, it is necessary to provide quality delivery with regard to some parameters such as throughput, delay, and bandwidth etc., some for sensitive applications using voice and video media for example.

This chapter concludes the thesis by summarizing important results of the present work. The scope for future work in the area is also included.

6.1 The assessment of effect on QoS parameters of static & dynamic networks for different protocols

The performance of network using different routing protocols has been analyzed. To accomplish this, simulation is carried out using a number of ad hoc routing protocols, which includes dynamic source routing (DSR), destination sequenced distance vector (DSDV) and ad hoc on-demand distance vector (AODV) using OPNET/ns-2 simulator. In chapter 3 most used commonly protocols for ad hoc networks with 20 nodes and data rate is 11Mbps are analyzed for different scenario of different protocols (AODV, DSDV, and

DSR) and compare the results with experimental data for validation of results. From the analysis it is concluded that the QoS performance is affected by types of different protocols.

The comparison of commonly used protocols using various performance metrics is summarizes in table 3.2.

- AODV shows good performance for the control traffic received, control traffic sent, data traffic sent, throughput and retransmission attempts.
- However, DSDV shows better performance for data traffic received.
- DSDV and DSR show an average level of performance for the control traffic received and data traffic sent retransmission attempt respectively.

Further the work has been extended to analyses the performance of the network having different load and mobility conditions.

- AODV shows better performance by varying the no. of nodes for the routing traffic sent and received. Whereas DSDV and DSR show good and average performance for routing traffic sent and received respectively (figures 3.8-3.13).
- Throughput decreases as number of hops increase, similarly the delay increases as the number of hops increase (figure 3.20 and 3.21 respectively).
- In the case of AODV, effect of the mobility of nodes the throughput is decreasing (i.e., reduction from 4.99Mbps to 2.48Mbps) almost 50% (figure 3.22).

Analysis of Throughput for different scenarios:- The comparison of throughput is analyzed with experimental data for different scenario of different protocols.

- For validation of results, simulated results compare with experimental results (table 3.7), based on the analysis it is observed that the simulated results are closely resembled to the experimental results.

Scope for future work:

- We only analysis a network of moderate size due to limitations of the simulator. Increasing loads up to a few hundreds of nodes could provide strength in terms of real-life applications.
- This study included only one mobility model throughout the simulation. Different mobility models may give different results for ad hoc routing protocols. So the performance of QoS parameters based upon different mobility models can be analyzed.
- A simulation model that includes performance relative to security issues could provide future researchers, as well as ad hoc network protocol users, a well-deserved criterion for choosing a reliable and safe protocol.
- Since the simulation is confined to three protocols, DSR, AODV, and DSDV. Additional ad hoc network protocols could be added for comprehensive performance evaluation.

6.2 The assessment of effect of congestion on QoS parameters for routing protocol (AODV) using IEEE 802.11MAC layer parameters and fuzzy approach

In the present work, issue of congestion in IEEE 802.11 networks has been studied and analyzed. An OPNET simulation is used to estimate the effect of congestion situation on the performance of the network. Simulations are carried out on 5 nodes (node 1 is congested) with varying data rates (5.5 and 11Mbps). Simulations are carried out for 600, and 900 simulations-seconds. The analysis concludes that:

- For every node number of dropped data packets (parameter) in congested node are found to be zero throughout the simulation duration.
- The delay is maximum if node 1 is congested otherwise it is minimum. The delay of congested node 1 is fluctuates between 5.0 to 6.5 sec. Likewise, the delay values without congestion is almost negligible (figure 4.4).
- Load of the of the network falls to 78% during initial transition phase. Apart from this in no congestion situation the network load reduces to 24-30% (figure 4.5).
- Throughput in congested node (node 1) is minimum (zero) when compared with other nodes. The throughput of node 0 is varying between 153808 and 67638. Likewise, the throughput values corresponding to other nodes, namely node 2, node 3 and node 4, are varying between 167567 and 81522, 164456 and 66383 and 156808 and 64694, respectively (figure 4.6).
- Packet drop in congested node found to be about 120-200% as compared to other nodes (figure 4.7).
- Media Access Delay in congested node is observed between, 400-692% higher as compared to other nodes (figure 4.8).

The work is further extended to analyse the differentiation levels offered by modifying MAC parameters, such as DIFS and contention window. Then the throughput is analysed using these mechanism for different scenarios such as no differentiation as shown in tables 4.5-4.7. Simulations are carried out for 600 simulations-seconds. All stations generate 2.16Mbps CBR traffic with packet sizes of 1000 bytes. The distance between stations is 100meters. The analysis concludes that:

- The bandwidth reduces to about 33.33%, when increasing the number of nodes in the network. Initially nodes are using equal bandwidth (figure 4.9).
- The throughput of DIFS-based scheme. Between 0 and 50 seconds, only two stations fairly share the channel because their aggregate rate is inferior to the maximum achievable throughput (figure 4.10).
- Node 1 obtains more bandwidth than node 2, 3 and 4, because it has the smallest DIFS. However the throughput decreases with increase in the number of stations. This is mainly attributed to the shared nature of wireless channels (figure 4.10).
- Stations with smaller intervals have higher priority of accessing the channel compared to stations with larger values. So we expect stations with smaller interval values to have higher throughput compared to those with larger values.
- The stations with a smaller CWmin value obtain a larger share of the channel capacity than the other stations. Throughput decreases with increase in the number of stations. If the total number of stations increases, the throughput per node decreases rapidly. The total amount of effective channel capacity drop due to increased number of collisions, and the decreased channel capacity is shared among a larger number of stations (figure 4.11).

- CWmax also contributes to the evolution of the CW in the contending process. Stations with smaller CWmax values are expected to obtain a larger share of the medium capacity. However, as opposed to CWmin, the value of CWmax is only reached after a number of successive collisions with the same packet.

Further fuzzy based scheme has been proposed to improve the performance of the network in terms of average throughput, packet delivery ratio and end-to-end delay. The input parameters such as buffer occupancy, data rate and expiry time to find the priority index has been taken for analysis.

- The performance of fuzzy scheduler with reference to the packet delivery ratio is much improved as compared with that of one without scheduler. It is also seen that for small loads, the scheduler does not provide much improvement, but the traffic load is increased the improvement is more.
- End-to-end delay improves by 0.3 sec when scheduler has been used (figure 4.18).
- Fuzzy scheduler provides a better performance in terms of the end to end delay and throughput (figure 4.18 and 4.20).
- Packet delivered improves by 2-8% as the mobility increases (figure 4.19).

Scope for future work:

- The performance of all the above networks can be simulated simultaneously for 4-G network environment.
- Fuzzy approach can be applied to get minimization of congestion in the networks.

- In future, modification of MAC parameters can also be applied for different scenario such as varying the load and mobility.
- Comprehensive performance evaluation and different data sources can be studies for recently reported protocol. New protocol can developed for application like military tacktical radio, etc.

6.3 Performance Analysis of Bandwidth Control Management of Wireless Ad hoc Network for AODV Protocol

In view of the remarkable growth in the number of users and the scarcity of bandwidth in wireless networks so an efficient sharing and management of bandwidth among the users becomes a key factor in enhancing the system performance.

A network consists of 20 mobile nodes placed randomly within 100x100 meters and shares a 5.5Mbps radio channel with its neighboring nodes. Simulations are carried out for 1200 simulations-seconds. The different QoS parameters have been analyzed for wireless ad hoc networks using ns2 simulator under different mobility conditions. The analysis concludes that:

- The routing algorithm has been developed that perform allocation and reservation of bandwidth for real and non-real types of services.
- The developed algorithm establish the path between sources to destination and also create standby route during disconnect the primary path.
- When mobility is 20m/s of S_1 (Service using slot 1) about 54% of the connection needs to be rerouted. Similarly when mobility is 20 m/s of S_2 (Service using slot 2)

& S_4 (Service using slot 4), about 48% & 44% of the connections need to be rerouted (figure 5.4).

- The average throughput decreases as mobility increases (figure 5.5).
- Frequent broken the established path occur while increase the mobility in wireless ad hoc that requires different routing path for new connection between source to destination that gives the results more end-to-end transmission delay and increases the packets loss.
- According to algorithm for making a connection in figure 5.10 near 35–55% of connections are setup through the primary route under different mobility. Similarly, 41–59% of connection's are through standby route under different mobility.

Scope for future work:

The work presented in this thesis can be extended in the following directions

- Since the simulation is confined to one protocol (AODV). Additional ad hoc network protocols could be added for comprehensive performance evaluation.
- QoS performance can be analyzed using Neuro-fuzzy and Genetic Algorithm (GA) approach.
- Security aspects can be investigated for getting assured QoS.
- New algorithm can be designed and developed for integrated wired and wireless networks.

REFERENCES

1. Corson M., S. Batsell, and J. Macker. Architectural considerations for mobile mesh networking. http://tonnant.itd.nrl.navy.mil/mmnet/ mmnetRFC.txt, May 1996. Request for Comments Draft.
2. IETF-Working-Group, "MANET: Mobile Ad hoc NETworks," www.ietf.org/html.charters/manet-charter.html.
3. Kuosmanen, P., 2002. Classification of ad hoc routing protocols, Finnish Defence Forces, Naval Academy, Finland. Available from <http://keskus.hut.fi/opetus/ s38030/k02/Papers/12-Petteri.pdf>.
4. Perkins, C.E., and P. Bhagwat, 1994. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers, Computer Communications Review pp. 234–244.
5. Jacquet, P., P. Muhlethaler, and A. Qayyum, 1998. Optimized Link State Routing Protocol, Internet Draft, draft-ietf-manetolsr- 00.txt.
6. Johnson, D.B., Maltz, D. A., Dynamic source routing in adhoc wireless networks, in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, pp. 153–181, 1996.
7. Perkins C., B.-R. E., and D. S., "Ad hoc On-demand Distance Vector routing," Request For Comments (Proposed Standard) 3561, Internet Engineering Task Force http://www.ietf.org/rfc/rfc3561.txt?number=3561, July 2003.
8. M. Scott Corson, S. papademetriou, Philop Papadopolous, Vincent D. Park and Amir Qayyum, "An Internet MANET Encapsulation Protocol (IMEP) Specification", Internet draft-ietf-manet-imepspec01.txt, August 1998. Work in progress.

9. Philippe Jacquet, Paul Muhlethaler and Amir Qayyum, "Optimized Link State Routing Protocol", Internet draft, draft-ietf-manet-olsr-00.txt, November 1998. Work in progress

10. Mingliang Jiang, Jinyang Li and Yong Chiang Tay, "Cluster Based Routing Protocol (CBRP) Functional specification". Internet draft, draft-ietf-manet-cbrp-spec-00.txt, August 1998. Work in progress

11. Vincent D. Park and M. Scott Corson, "Temporally-Ordered Routing Algorithm (TORA) Version 1: Functional specification", Internet draft, draft-ietf-manet-tora-spec-01.txt, August 1998. Work in progress.

12. Raghupathy Sivakumar, Prasun Sinha and Vaduvur Bharghavan, "Core Extraction Distributed Ad hoc Routing (CEDAR) Specification", Internet draft, draft-ietf-manet-cedar-spec-00.txt, October 1998. Work in progress.

13. Ni, S.Y, Tseng, Y.C, Chen, Y. S and Sheu, J.P., "The Broadcast Storm Problem i Mobile Ad Hoc Network", ACM-1999, MOBICOM' 99 PP.151-162.

14. Tanenbaum, A.S., "Computer Networks", IIIrd Edition, Published by Prentice Hall of India Pvt. Limited, New - Delhi, pp. 61-64, 1997.

15. Agrawal, D.P and Zeng, Q.A., "Introduction to Wireless and mobile systems", 2nd Edition Published by Thomson, 498 pages, ISBN 0534-49303-3M, April 2005.

16. Williams B and Camp T., "Comparison of Broadcasting Techniques for Mobile Ad hoc Networks", Proc. 3rd ann. Workshop Mobile and Ad Hoc networking and computing, MOBIHOC pp-194-205. June 2002.

17. Lou, W and Wu, J., "On Reducing Broadcast Redundancy in Ad Hoc Wireless Networks", IEEE Transactions on mobile computingVol.1, No.2 Apr-Jun 2002, PP.111-122.

18. Corson, S. and Macker, J., "Mobile Ad Hoc Networking: Routing Protocol performance Issues and Evaluation considerations", RFC 2501 Jan 1999.

19. http://www.opnet.com/, December 2002.

20. Network Simulator 2 (NS-2) Homepage. <URL:http://www.isi.edu/nsnam/ns/ >Accessed September 2005.

21. Kevin Fall and Kannan Varadhan. The NS Manual. Technical report, The VINT Project, January 2002

22. XGraph homepage <URL:http://www.isi.edu/nsnam/xgraph/ >, Accessed November 2005

23. Kelley Colin, Thomas Williams, and others, "Gnuplot Home page", <URL: http://www.gnuplot.info/faq/>, Accessed Nov 2005.

24. IEEE 802.11 WG, Reference number ISO/IEC 8802-11:1999(E) IEEE Std 802.11, 1999 edition. International Standard [for] Information Technology - Telecommunications and information exchange between systems-Local and metropolitan area network Specific requirements - Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999B.

25. http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm (2005).

26. C. Bisdikian, An overview of the Bluetooth wireless technology, IEEE Communication Magazine, December 2001.

27. Web site of the Bluetooth Special Interest Group: http:// www.bluetooth.com/.

28. Web site: http:// www.zurich.ibm.com/cs/wireless/bluetooth.html

29. M. Ergen, S. Coleri, P. Varaiya. QoS Aware Adaptive Resource Allocation Techniques for Fair Scheduling in OFDMA Based Broadband Wireless Access

Systems. IEEE Transaction on Broadcasting, vol.49, December 2003.

30. Understanding Wi-Fi and WiMAX as Metro-Access Solutions. Intel White Paper. Online: http://www.intel.com

31. Axiotis, D.I., Al-Gizawi, T., Peppas, K., Protonotarios, E.N., Lazarakis, F.I, Papadias, C., and Philippopoulos, P.I., "Services in Interworking 3G and WLAN Environments", IEEE Wireless Comm., vol. 11, no. 5, pp. 14-20, Oct. 2004.

32. IEEE 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, Oct. 1, 2004.

33. IEEE P802.16/Cor1/D2, Corrigendum to IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, Apr. 2005.

34. L. Bisdounis. HiPERLAN/2 vs IEEE 802.11a: Physical Layer. Intracom. Online: http://easy.intranet.gr/paper 10.pdf.

35. Nair, R., Crawley, E., Rajagopalan, B., and Sandick, H., "A framework for QoS based routing in the internet," Aug. 1998, RFC 2386.

36. Macker, J.P., Corson, S., "Mobile ad hoc networks (MANET): routing technology for dynamic, wireless networking", in Basagni, S., Conti, M., Giordano, S., Stojmenovic, I., (Eds.), "Ad Hoc Networking", IEEE Press Wiley, New York, 2003.

37. Li, B., "QoS-aware adaptive services in mobile ad-hoc networks", in: Proceedings of the Ninth IEEE International Workshop on Quality of Service (IWQoS 2001), Lecture Notes in Computer Science, vol. 2092, Springer, Berlin, 2001, pp. 251–268.

38. Hannan, X., Chaing, C.K., Winston, S.K.G., "Quality of service models for ad hoc wireless networks", in: M. Ilyas (Ed.), Handbook of Ad Hoc Networks, CRC Press,

New York, 2003 (Chapter 28).

39. Braden, R., Clark, D., and Shenker, S., "Integrated Services in the Internet Architecture- an Overview", IETF RFC1663, June 1994.

40. Blake, S., "An Architecture for Differentiated Services", IETF RFC2475, December 1998.

41. Xiao, H., Seah, W.K.G., Lo, A., Chua, K.C., "A flexible quality of service model for mobile ad-hoc networks", IEEE VTC2000-spring, Tokyo, Japan, May 2000.

42. Nikaein, N., Bonnet, C., Moret, Y., and Rai, I.A., "2lqos- two layered quality of service model for reactive routing protocols for mobile ad hoc networks", in *Proceeding of SCI - 6th World Multiconference on Systemics, Cybernetics and Informatics*, 2002.

43. Nikaein, N., Bonnet, C., "Layered quality of service model for routing in mobile ad hoc networks," in *Proceeding of WMAN*, 2003.

44. Xiao, X., and Ni, L.M., "Internet QoS: a Big Picture," IEEE Network Magazine, March 1999.

45. Aurrecoechea, C., Campbell, A.T., and Hauw, L., "A survey of qos architectures", *Multimedia Systems*, 1998.

46. Lee, S.B., and Campbell, A.T., "INSIGNIA: In-band Signaling Support for QOS in Mobile Ad Hoc Networks", Proc of 5th International Workshop on Mobile Multimedia Communications (MoMuC, 98), Berlin, Germany, October 1998.

47. Guerin, R., Blake, S., and Herzog, S., "Aggregating RSVP-based QoS Requests", Internet draft, draft-guerin-aggreg-RSVP-00.txt, Nov. 1997.

48. Ahn, G.S., Campbell, A.T., Lee, S.B., and Zhang, X., "INSIGNIA," Internet Draft, draft-ietf-manet-insignia-01.txt, Oct. 1999.

49. Lu, S., Bharghavan, V., and Srikant, R., "Fair Scheduling in Wireless Packet Networks", Proceedings of ACM SIGCOMM, San Francisco, California, 1997.

50. Keshav, S., "An Engineering Approach to Computer Networking: ATM Networks, the Internet, and the Telephone Network", Addison-Wesley professional computing series, 1997.

51. Wang, Z., and Crowcroft, J., "QoS routing for supporting resource reservation", JSAC, Sept. 1996.

52. Chen, S., and Nahrstedt, K., "An Overview of Quality-of-Service Routing for the Next Generation High-Speed Networks: Problems and Solutions", IEEE Network, Special Issue on Transmission and Distribution of Digital Video, Nov.-Dec. 1998.

53. Sinha, P., Sivakumar, R., and Bharghavan, V., "CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm", IEEE Infocom'99, New York, NY. March 1999.

54. Chen, S., and Nahrstedt, K., "Distributed Quality-of-Service Routing in Ad-Hoc Networks", IEEE Journal on Special Areas in Communications, Vol. 17, No. 8, August 1999.

55. Lin, R., and Liu, J.S., "QoS Routing in Ad Hoc Wireless Networks," IEEE Journal on Selected Areas in Communications, August 1999.

56. Bharghavan, V., "Performance of multiple access protocols in wireless packet networks", International Performance and Dependability Symposium, Durham, North Carolina, Sept. 1998.

57. Jain, A.K., Sharma, S.C., Jha, R., and Lal M., "MAC Protocols In Mobile Ad Hoc Networks", published *in* IETECH Journal of Communication Techniques, Vol. 1, No 1, 006 – 012, 2007.

58. Muir and Garcia-Luna-Aceves, J.J., "An Efficient Packet-sensing MAC Protocol for Wireless Networks", ACM Jounal on Mobile Networks and Applications, Vol. 3, No. 2, pg. 221-234, August 1998.

59. Sobrinho, J.L., and Krishnakumar, A. S., "Quality-of-Service in Ad Hoc Carrier Sense Multiple Access Wireless Networks", IEEE Journal on Special Areas in Communications, Vol. 17, No. 8, August 1999.

60. Lin, C.R., and Gerla, M., "MACA/PR: An Asynchronous Multimedia Multihop Wireless Network", Proceedings of IEEE INFOCOM'97, 1997.

61. Kumar Manoj & S.C. Sharma "Trade-off of Various QoS Parameter in Wireless Adhoc Network for Different Protocols" International Journal of Information of Computer Application in Engg. Tech. and Sciences Vol. 1(1), pp. 83-92, 2008.

62. Kumar Manoj & S.C. Sharma "Impact on Throughput and Delay Analysis in Wireless Ad-Hoc Network IEEE 802.11b" IEC Journal of Annual Review of Communication, International Engineering Consortium, USA. Volume 61, pp. 317-325, December 2008.

63. Kumar Manoj, S.C. Sharma & A.K. Jain "Effect of QoS Parameter in Wireless Ad-Hoc Network (IEEE 802.11b)" International Journal of Hybrid Computational Intelligence, Vol. 1, No.2, pp. 197-203, July-December 2008.

64. Kumar Manoj, S.C. Sharma & A.K. Jain, "Analysis and Effect of Delay & Throughput in Mobile Ad-hoc Network (IEEE 802.11b) for AODV Protocol" Journal of Cooperation among University, Research and Industrial Enterprises (CURIES), Vol. 1. No. 2, pp. 16-22, July 2008.

65. Kumar Manoj, S.C. Sharma & A. K. Jain "An Analysis of throughput management in

wireless ad hoc network" National Journal of IT & Management, Vol. 2 no. 1 pp. 54-60, Oct. 2008.

66. Kumar Manoj, Parmanand, S.C. Sharma & S.P. Singh "Performance of QoS Parameter in Wireless Ad hoc Network (IEEE 802.11b)" Proceedings of the World Congress on Engineering and Computer Science 2009, Vol. I, pp. 280-284, WCECS 2009, October 20-22, 2009, San Francisco, USA.

67. Corson, S. and Macker, J., "Mobile Ad Hoc Networking: Routing Protocol performance Issues and Evaluation considerations", RFC 2501 Jan 1999.

68. Jain, A.K., Sharma, S.C., Jha, R., and Dixit, A., "A Research Review on MANET Protocols", International Journal of Computer Science and Knowledge engineering (IJCSKE), Vol. 1, No: 1, pp. 39-46, 2007.

69. S. Ahmed and M. S. Alam "Performance Evaluation of Important Ad Hoc Network Protocols" EURASIP Journal on Wireless Communications and Networking, Volume 2006, Issue 2, pp. 42 – 42, 2006.

70. E. Celebi, "Performance evaluation of wireless multi-hop adhoc network routing protocols," http://cis.poly.edu/~ecelebi/esim.pdf.

71. P. Chenna Reddy, Dr. P. Chandrasekhar Reddy, "PERFORMANCE ANALYSIS OF ADHOC NETWORK ROUTING PROTOCOLS" Academic Open Internet Journal (ISSN 1311-4360), Volume 17, 2006.

72. Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Jorjeta Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols" International Conference on Mobile Computing and Networking Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking

Dallas, Texas, United States Pages: 85-97, 1998.

73. H. Hallani, S. A. Shahrestani, and F. H. Stootman "Wireless Ad-Hoc Networking: Analysis and Validation of Simulation Results" TENCON 2005-2005 IEEE Region 10 Conference; pp. 1162-1167, Melbourne, Australia, 2005.

74. T. Plesse, C. Adjih, P. Minet, A. Laouiti, A. Plakoo, M. Badel, P. Mu¨ hlethaler, P. Jacquet, J. Lecomte, OLSR performance measurement in a military mobile ad hoc network, Elsevier Ad Hoc Networks 3 (5) 575–588, 2005.

75. E. Altman, T. Basar, and T. Srikant. "Congestion control as a stochastic control problem with action delays". *Automatica*, vol. 35 (No.12), 1999. pp. 1937-1950.

76. F. D. Priscoli and A. Isidori. "A control engineering approach to integrated congestion control and scheduling in local area networks". *Control Engineering Practice*, vol.13 , pp. 541-558, 2005.

77. Y. Yi and S. Shakkottai. "Hop-by-hop congestion control over a wireless multihop network". In *IEEE INFOCOM'04*, pp.1214-1224, July 2004.

78. V. Jacobson. "Congestion Control and Avoidance". Computer Communications Review, vol.18 (4):314-329, Aug. 1988.

79. Rea, S., and Pesch, D.: Multi-metric routing decisions for ad hoc networks using fuzzy logic. In Proceedings of 1st International Symposium on Wireless Communication Systems, Mauritius, pp. 403-407, 20- 22 September, 2004.

80. L. Khoukhi, S. Cherkaoui, "FuzzyCCG: A Fuzzy Logic QoS Approach for Congestion Control in Wireless Ad Hoc Networks", Q2SWinet '05, , Montreal, Quebec, October

13, 2005.

81. X. Zhang, S. Cheng, M. Feng, W. Ding, "Fuzzy Logic QoS Dynamic Source Routing for Mobile Ad Hoc Networks", The Fourth International Conference on Computer and Information Technology (CIT'04), pp. 652-657, 2004.

82. C. Gomathy, S. Shanmugavel: "Supporting QoS in MANET by a Fuzzy Priority Scheduler and Performance Analysis with Multicast Routing Protocols" EURASIP Journal on Wireless Communications and Networking 2005:3, 426–436, 2005.

83. GUI Chao "Method of Enhancing QoS with Fuzzy Controller Based Priority of the Packets in Ad Hoc" in Journal of Communication and Computer, USA, , Volume 3, No.11, 40-44, Nov. 2006.

84. Jangeun Jun, Pushkin Peddabachagari, Mihail Sichitiu "Theoretical Maximum Throughput of IEEE 802.11 and its Applications" Proceedings of the Second IEEE International Symposium on Network Computing and Applications, page: 249, 2003.

85. T. Nantagopal, T. Kim, X. Gao, and V. Bharghavan. Achieving MAC layer fairness in wireless packet networks. In Proceedings of ACM MOBICOM, Boston, MA, August 2000.

86. V. Kanodia, C. Li, A. Sabhanval, &.Sildeghi and E.Knightly, "Distributed Priority Scheduling and medium access in Ad-hoc networks," ACM Wireless networks Vo1.8, November 1, 2002.

87. Royer E. M. and Chai Keong Toh." A Review of current muting protocols for Ad-hoc Networks", IEEE Personol Commut,. vol. 6, no. 2, pp. 46-55, April 1999.

88. C. Li and E. Knightly, 'Coordinated network Scheduling: A Framework for End to End services" Proc. of IEEE ICNP'OO, Osaka. Japan, Nov. 2000.

89. Ren, F.Y.; Ren, Y.; Shan, X.M. Design of a fuzzy controller for active queue management. Computer Communications, Vol. 25, no. 9, pp. 874-883, 2002.

90 S-B. Lee, G-S Ahn, X. Zhang, and A.T. Campbell, "INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks", *Journal of Parallel and Distributed Computing* (Academic Press), Special issue on Wireless and Mobile Computing and Communications, Vol. 60 No. 4 pp. 374-406, April 2000.

91 Le i Huang, Sunil Kumar, C.Jay Kuo,"Adaptive Resource Allocation for multimedia QoS Management in wireless Networks", IEEE Transaction on Vehicular Tech., vol. 53, no.2, March 2004.

92 Calin Curesu and Simin Nadjm-Tehrani,"Time-Aware Utility-Based Resource Allocation in Wireless Networks", In: IEEE Trans. on Parallel and Distributed system, vol. 16, no.7, July 2005.

93 Anup K.Talukdar, B. R. Badrinath and Arup Acharya, "On Accommodating Mobile Hosts in an Integrated Services Packet Networks", IEEE IFOCOM 97, pp. 1046-1053.

94 C. Oliveria, J. BKim and T. Suda, "Adapative Bandwidth Reservation Scheme for high speed Multimedia Wireless Networks", IEEE JSAC, vol. 16, no.6, pp. 858-874, 1998.

95 Hong Bong Kim,"An Adaptive Bandwidth Reservation scheme for Multimedia Mobile Cellular Networks", In: Proc of IEEE International Conference on

Communication, Seoul, Korea, 2005.

96 Ruston Hutclens, Samar Singh, "Bandwidth Reservation Strategies for Mobility Support of Wireless Connections with QoS Guarantees", *In: Proc. Australian Computer Science Conference (ACSC)*, Melbourne, Australia, vol. 4, pp 119-128, Jan. 2002.

97 Sungwook K.M., Pramod K. Varshney,"An Adaptive Bandwidth Reservation Algorithm for QoS Sensitive Multimedia Cellular Networks", In: IEEE Vehicular technology conference, Vancouver, Canada, September 2002.

98 Peerapon Siripongwutikorn, Sujatha Banerjee, David Tipper, "Adaptive Bandwidth control for Efficient Aggregate QoS Provisioning", In: Proc. IEEE Globecom, Taipei, Taiwan, 2002.

99 Mona Ei-Kadi, Stephan Olariu,"A Rate-Based Borrowing Scheme for QoS Provisioning in Multimedia Wireless Networks", IEEE Transaction on Parallel and Distributed Systems, vol. 13, no. 2, February 2002.

100 Manthos Kazantzidis, Dario Maggiorini and Mario Gerla, "Network Independent Available Bandwidth Sampling and measurement", In: Proc. 2nd International workshop on QoS-IP, LNCS 2601, pp.117-130, Milano, Italy, 2003

101 C. R. Lin and J.-S. Liu, “QoS routing in ad hoc wireless networks,” IEEE J. Select. Areas Commun., vol. 17, pp. 1426–1438, Aug. 1999.

102 C. R. Lin “Admission Control in Time-Slotted Multihop Mobile Networks” IEEE Journal on Selected Areas in Communications, Vol. 19, No. 10, Oct. 2001

103 C. R. Lin "On-demand QoS routing in multihop mobile networks" INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE ,USA, Volume 3, pp. 1735-1744, 2001

104 Gahng-Seop Ahn, Campbell, A.T., Veres, A. & Li-Hsiang Sun "SWAN: service differentiation in stateless wireless ad hoc networks" Proceedings. IEEE INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. vol. 2, pp. 457- 466, 2002.

105 L. Khoukhi, S. Cherkaoui, "Flexible QoS Routing Protocol for Mobile Ad Hoc Networks", In Proc. of the 11th IEEE International Conference on Telecommunication (ICT2004), Brazil, Aug. 2004.

106 Xue, Q. and Ganz, A., "Ad hoc QoS On-demand Routing (AQOR) in Mobile Ad hoc Networks," in Journal of Parallel and Distributed Computing (JPDC), February 2003.

107 Kunz, T., Ge Y., and Lamont, L., "Quality of Service Routing in Ad-hoc Networks Using OLSR," in Proceeding of the 36th Hawaii International Conference on System Science, 2003.

108 Cansever, Derya H., Arnold M. Michelson, and Allen H. Levesque. Quality of service support in mobile ad-hoc IP networks. In MILCOM 1999 - IEEE Military Communications Conference, number 1, pages 30.34, Oct 1999.

109 Y. Ofek, "Generating a fault tolerant global clock using high-speed control signals for the MetaNet architecture," *IEEE Trans. Commun.*, Vol. 42, no. 5, pp. 2179–2188, 1994.

APPENDIX 1

Analysis of Delay

For that purpose, an UDP control packet is exploited by using an additional field "BW" that contains initially the value of the requested bandwidth "BW_{req}". At each intermediate node, a comparison is performed between the value of BW and the available bandwidth "BW_{avai}" of the current node. The value of the field BW is updated if it is bigger than the value BW_{avai} of the current node. When the destination receives the UDP control packet, BW represents the minimum bandwidth available along the path, and it is copied from UDP to a newly generated short replay message. The latter packet is transmitted back to the source node and at the same time the temporary resource reservation process is performed. Additional fields are used during temporary resource reservation mechanism, which are stored in each intermediary node in order to specify the "temporary reservation status" of the node, the "status duration" and the "flow identifier". The first field is set to value of the reserved bandwidth and the status duration is set to a certain value "T". T indicates the period of time within which the temporary reservation is performed. Note that even when the temporary reservation is performed by a flow, other flows can also exploit the available resources of the node. The reserved bandwidth is released just after the expiration of T duration. The evaluation of the right status duration to be set at a particular node is explained in the following. The computation of the right status duration needs to take into account the number of hops between the source and the particular node, and also the delays between the intermediate nodes. Let consider Δt the temporary reservation interval of a flow in a given intermediate node. During Δt, other flows originating from other source nodes can also use the available resources. Let λ, be the target delivery rate which defines the desired percentage of packets to be sent within the QoS constraint, where $\lambda = 1$ corresponds to best QoS guaranty and $\lambda = 0$ corresponds to the best-effort transmission. Then, (1) verifies the probability that Δt is lower than a given time value δ and the flow request to be accepted.

$$P[\Delta t \leq \delta] \geq \lambda - - - (1)$$

A good evaluation of (1) requires the destination to be acquainted with the statistical descriptions of delay of each node along the path. However, in many cases, the statistical distribution of such parameter can be approximated by a Gaussian distribution. Under this hypothesis, and assuming independency among nodes statistics, the temporary reservation time among the nodes turns out to be a Gaussian variable. If we consider x_{Tr} and σ^2_{Tr} the statistical average and variance of the random variable T_r, respectively (T_r is the temporary reservation time in a given node), then the temporary reservation interval statistics can be expressed as in (2)

$$P[\Delta t \leq \delta] = 1 - Q\left(\frac{\delta - m_{T_x}}{\sigma_{T_x}}\right) --- (2)$$

Q represents the complementary distribution function of a Gaussian variable with mean 0 and variance 1. Let υ be the actual time satisfaction provided by the intermediate node as given by (2). Hence, the flow request would be satisfied even if the average temporary reservation time was increased to the value m_{Tx} given by (3)

$$m_{T_x} = \upsilon - \sigma_{T_r} Q^{-1}[1-\lambda] --- (3)$$

The satisfaction of the requested target delivery rate for a given flow is met if the temporary reservation time is greater than m_{Tx} (m_{Tx}, is the time bound of the temporary reservation interval). After the expiration of m_{Tx}, the temporary reservation status of a node is set to zero. Thus, the released resources could be used by other flows, this permits a good utilization of available resources in the network. Assume there are two classes of mobile devices in the shared channel environment. Class 1 and Class 2 represent real-time UDP traffic and best effort TCP traffic, respectively. Each of the *Class* 1 mobile devices has an active UDP session, and each of the Class 2 mobile devices has an active TCP session. We define an idle mobile device as a mobile device whose MAC layer is idle and interface queue empty. If a mobile device is not idle then it is busy. Denote the portion of time that a class i mobile device is busy as $P_{on,i.}$ From [108] a busy class *i* mobile device's transmission probability in each time slot is represented as,

$$\tau_1 = \frac{2.(1-2p_i)}{(1-2p_i)(W+1)+p_iW\left(1-(2p_i)^m\right)} --- (1)$$

Where p_i is the collision probability for a class i mobile device at each time slot. W is the initial back-off window, and $W2^m$ is the maximum back-off window in the IEEE 802.11 protocol. By following the procedure in [109], the collision probability can be represented as,

$$p_1 = 1-(1-p_{on,1}\tau_1)^{n_1-1}(1-p_{on,2}\tau_2)^{n_2}$$

$$p_2 = 1-(1-p_{on,2}\tau_1)^{n_1}(1-p_{on,2}\tau_2)^{n_2-1} \quad ---(2)$$

The probability that one or more packets are sent to the channel at each slot is then,

$$p_{tr} = 1-(1-p_{on,1}\tau_1)^{n_1}(1-p_{on,2}\tau_2)^{n_2} \quad ---(3)$$

and the probability of a successful transmission each slot is,

$$P_s = n_1 p_{on,1}\tau_1(1-p_{on,1}\tau_1)^{n_1-1}(1-p_{on,2}\tau_2)^{n_2} + \frac{n_2 p_{on,2}\tau_1(1-p_{on,1}\tau_1)^{n_1}(1-p_{on,2}\tau_2)^{n_2-1}}{P_{tr}} \quad ---(4)$$

The total throughput of the system (in packets/sec) can be represented as,

$$S = \frac{P_s P_{tr}}{(1-P_{tr})\sigma + P_{tr}(P_s T_s + (1-P_s)T_c)} \quad ---(5)$$

Where σ is the length of a time slot, which is 20µs in all our simulations. T_s and T_c are the times needed to send un-collided and collided packets, respectively, on the channel. T_s and T_c are calculated from the packet length distribution, taking into account the overhead of the MAC and physical layers. The length of collided packets is approximated as the maximum length of two collided packets. The overall average MAC delay can be simply calculated using little's formula as,

$$d = \frac{P_{on,1}n_1 + P_{on,2}n_2}{S} \quad ---(6)$$

In this simulation, video sessions are modeled as CBR sources and the FTP sessions have an infinitely long file sizes that lasts for the whole simulation period. It is observed that uncontrolled system as the original system, and the system with the proposed feedback control as the proposed system. Because it is difficult to use a simple model to characterize the flow control of TCP/IP, coupled with a queuing system on top of the MAC layer, and the MAC layer and traffic shaper (for the proposed model), we evaluate the quantity $P_{on,1}$ and $P_{on,2}$ during the simulation as an approximation of this complex system. With $P_{on,1}$,$P_{on,2}$, n_1,n_2 known, we solve (1), (2) for p_1,p_2,τ_1, τ_2 then from (3), (4), (5), (6), the overall average delay is computed.

APPENDIX 2

BANDWIDTH RESERVATION

A major challenge in multimedia networks is the ability to account for resources so that bandwidth reservations can be placed on them. In cellular networks, such accountability is made easily by the fact that all stations learn of each other's requirements, either directly or through a control station. However, this solution cannot be extended to the multihop environment. To support QoS for real-time applications, we need to know not only the minimal delay path to the destination, but also the available bandwidth on it. The model is to determine whether the available resources in a network can meet the requirements of a new flow while maintaining bandwidth levels for existing flows, co-ordination among the packets. Accordingly, the decision is performed on the acceptance or rejection of a flow. This function is conducted together by the source node and other intermediate nodes mechanisms. For that purpose, an UDP control packet is exploited by using an additional field "BW" that contains initially the value of the requested bandwidth. At each intermediate node, a comparison is performed between the value of BW and the available bandwidth of the current node. The value of the field BW is updated if it is bigger than the value available bandwidth of the current node. When the destination receives the UDP control packet, BW represents the minimum bandwidth available along the path, and it is copied from UDP to a newly generated short replay message. The latter packet is transmitted back to the source node and at the same time the temporary resource reservation process is performed. Additional fields are used during temporary resource reservation mechanism, which are stored in each intermediary node in order to specify the temporary reservation status of the node, the status duration and the flow identifier. The first field is set to value of the reserved bandwidth and the status duration is set to a certain value "T". T indicates the period of time within which the temporary reservation is performed. Note that even when the temporary reservation is performed by a flow, other flows can also exploit the available resources of the node. The reserved bandwidth is released just after the expiration of T duration. The evaluation of the right status duration to be set at a particular node is explained in the following. The computation of the right status duration needs to take into account the number of hops between the source and the particular node, and also the delays between the intermediate nodes. Let consider Δt the temporary reservation interval of a flow in a given intermediate node. During Δt, other flows originating from other source nodes can also use the available resources. Let λ, be the target delivery rate which defines the desired percentage of packets to be sent within the QoS constraint, where $\lambda = 1$ corresponds to best QoS guaranty and $\lambda = 0$ corresponds to the best-effort transmission. Then, (1) verifies the probability that Δt is lower than a given time value δ and the flow request to be accepted.

$$P[\Delta t \le \delta] \ge \lambda --- (1)$$

A good evaluation of (1) requires the destination to be acquainted with the statistical descriptions of delay of each node along the path. However, in many cases, the statistical distribution of such parameter can be approximated by a Gaussian distribution. Under this hypothesis, and assuming independency among nodes statistics, the temporary reservation time among the nodes turns out to be a Gaussian variable. If we consider x_{Tr} and σ^2_{Tr} the statistical average and variance of the random variable T_r, respectively (T_r is the temporary reservation time in a given node), then the temporary reservation interval statistics can be expressed as in (2)

$$P[\Delta t \le \delta] = 1 - Q\left(\frac{\delta - m_{T_x}}{\sigma_{T_x}}\right) --- (2)$$

Q represents the complementary distribution function of a Gaussian variable with mean 0 and variance 1. Let υ be the actual time satisfaction provided by the intermediate node as given by (2). Hence, the flow request would be satisfied even if the average temporary reservation time was increased to the value m_{Tr} given by (3)

$$m_{T_x} = \upsilon - \sigma_{T_r} Q^{-1}[1-\lambda] --- (3)$$

The satisfaction of the requested target delivery rate for a given flow is met if the temporary reservation time is greater than m_{Tr} (m_{Tr}, is the time bound of the temporary reservation interval). After the expiration of $m_{Tr,}$ the temporary reservation status of a node is set to zero. Thus, the released resources could be used by other flows, this permits a good utilization of available resources in the network. In the model, suppose there are n nodes each of which at most has m traffic categories. Every node **i** has basic rate Bi and the total network capacity is B. The distributed controller has two sets of. One input set is the goal delay matrix [Dgi] where each Dgi is a row vector of m goal delays dij's for traffic categories j's of node i. Each goal delay dij is related with the packet size lij and the desired bandwidth bij. Thus we have

$$B = \sum_{i=1}^{n} B_i = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}$$

$$d_{ij} = \frac{l_{ij}}{b_{ij}}, j > 1 \qquad \text{---- (4)}$$

$$d_{gi1} = \frac{l_{i1}}{B_i - \sum_{j=2}^{m} b_{ij}}$$

The traffic category (j = 1) with lowest priority uses the remaining bandwidth for transmission. The other input set is the tolerable delay variation (Ei) where each Ei is a row vector of m desired tolerable delay variations $\varepsilon\, ij$ for traffic categories j's of node i. In the network, the elements in Dgi and those in Ei are dependent. Real and non-real time applications such as digital audio and video have much more stringent QoS requirements than traditional applications. For a network to deliver QoS guarantees, it must reserve and control resources. A major challenge in multihop, multimedia networks is the ability to account for resources so that bandwidth reservations can be placed on them. In wireless networks, such accountability is made easily by the fact that all stations learn of each other's requirements, either directly or through a control station. However, this solution cannot be extended to the multihop wireless environment. To support QoS for real and non-time applications, we need to know not only the minimal delay path to the destination, but also the available bandwidth on it. A BWCM mode should be accepted only if there is enough available bandwidth and omitting signal-to-interference ratio, packet loss rate, etc. This is because bandwidth guarantee is one of the most critical requirements for real-time applications. "BW" in time slotted network systems is measured in terms of the amount of free slots. The goal of the QoS routing algorithm is to find a shortest path such that the available bandwidth on the path is above the minimal requirement. To compute the "BW" constrained shortest path, we not only have to know the available bandwidth on each link along the path, but we also have to determine the scheduling of free slots.

APPENDIX 3

Algorithm & Bandwidth Calculation

The transmission time scale is organized in frames, each containing a fixed number of time slots. The entire network is synchronized on a frame and slot basis. The frame synchronization mechanism be implemented with techniques similar to those employed in the wired networks [107] and for wireless network in [101]. Each frame is divided into two parts, first the control and second the data phase as shown in figure 1.

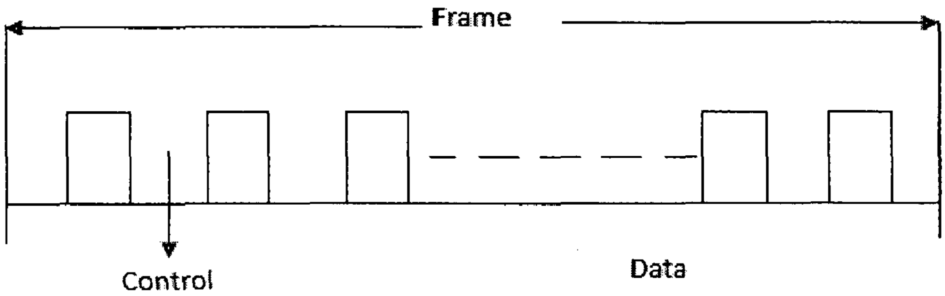


Figure 1 Frame Structure

The size of each frame in the control phase is much smaller than the one in the data phase. The model is used to perform all the control functions, such as temporary resource reservation, co-ordination, control management, routing protocols AODV, etc. Each node takes turns to broadcast its information to all of its neighbors in a predefined slot, such that the network control functions are performed distributive. We assume the information can be heard by all of its adjacent nodes. In a noisy environment, where the information may not always be heard perfectly at the adjacent nodes, an acknowledgment scheme is performed in which each node has to ACK for the last information in its control slot. By exploiting this approach, there may be one frame delay for the data transmission after issuing the data slot reservation. Ideally, at the end of the control phase, each node has learned the channel reservation status of the data phase. This information will help one to schedule free slots, verify the failure of reserved slots, and drop expired real-time packets.

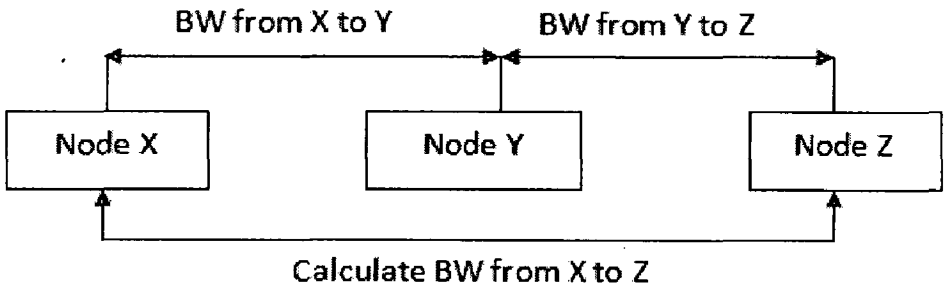


Figure 2 Calculation of end-to-end BW

Because only adjacent node hears the reservation information, the free slots recorded at each node are different. It defines the set of the common free slots between two adjacent nodes to be the link bandwidth. As shown in figure 2, in which X intends to compute the bandwidth to Z. Assume that the next hop is Y. If Y can compute the available bandwidth to Z, then X can use this information and the link bandwidth to Y to compute the bandwidth to Z. It is define the end-to-end bandwidth between two nodes. If two nodes are adjacent, the path bandwidth is the link bandwidth. Consider the example in figure 2, and assume that one hop distance is between Z and Y.

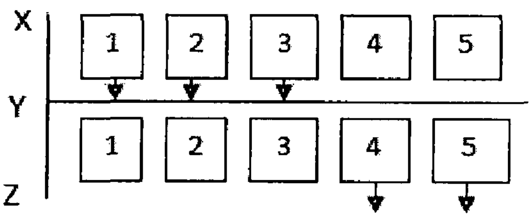
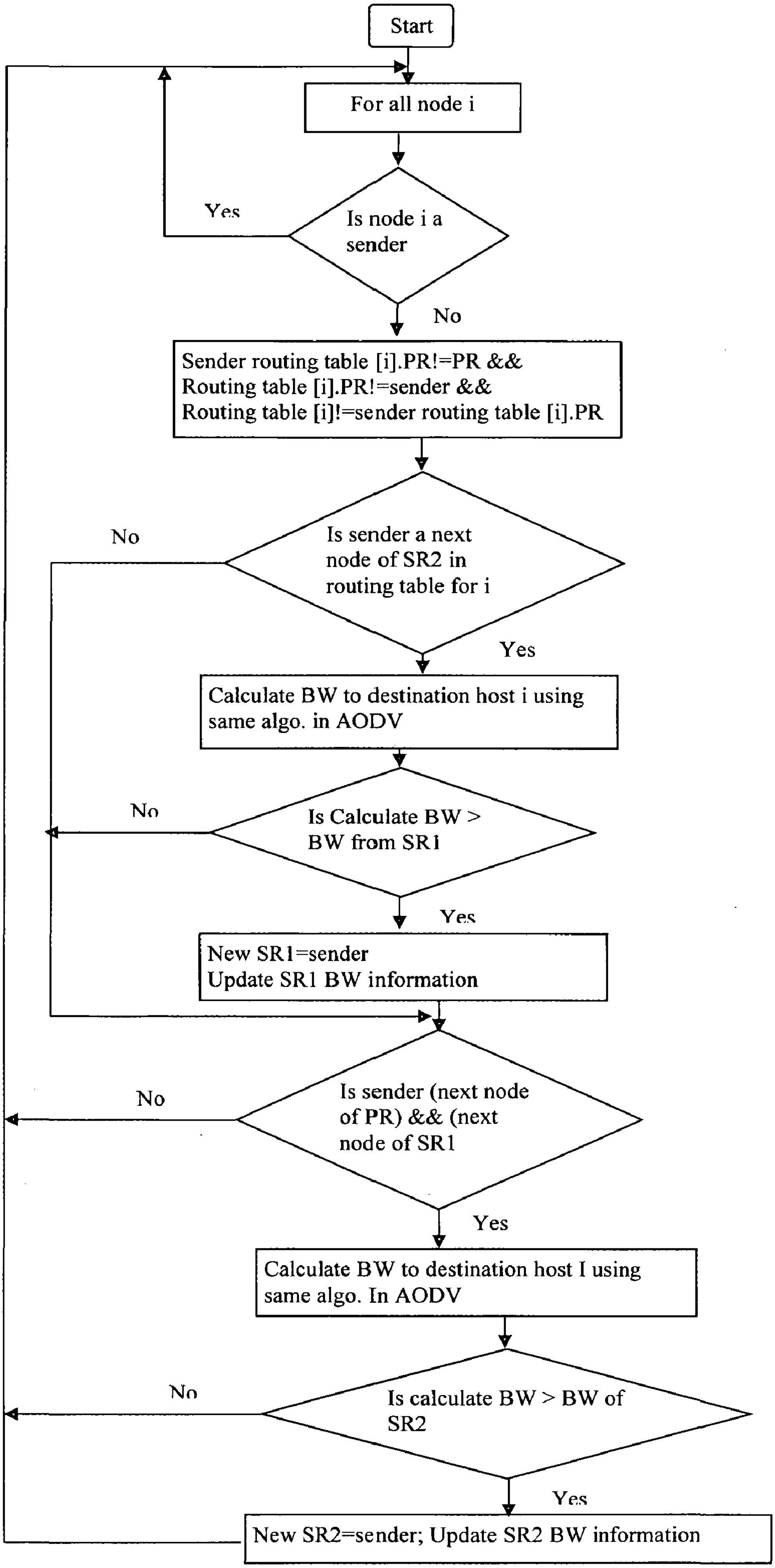
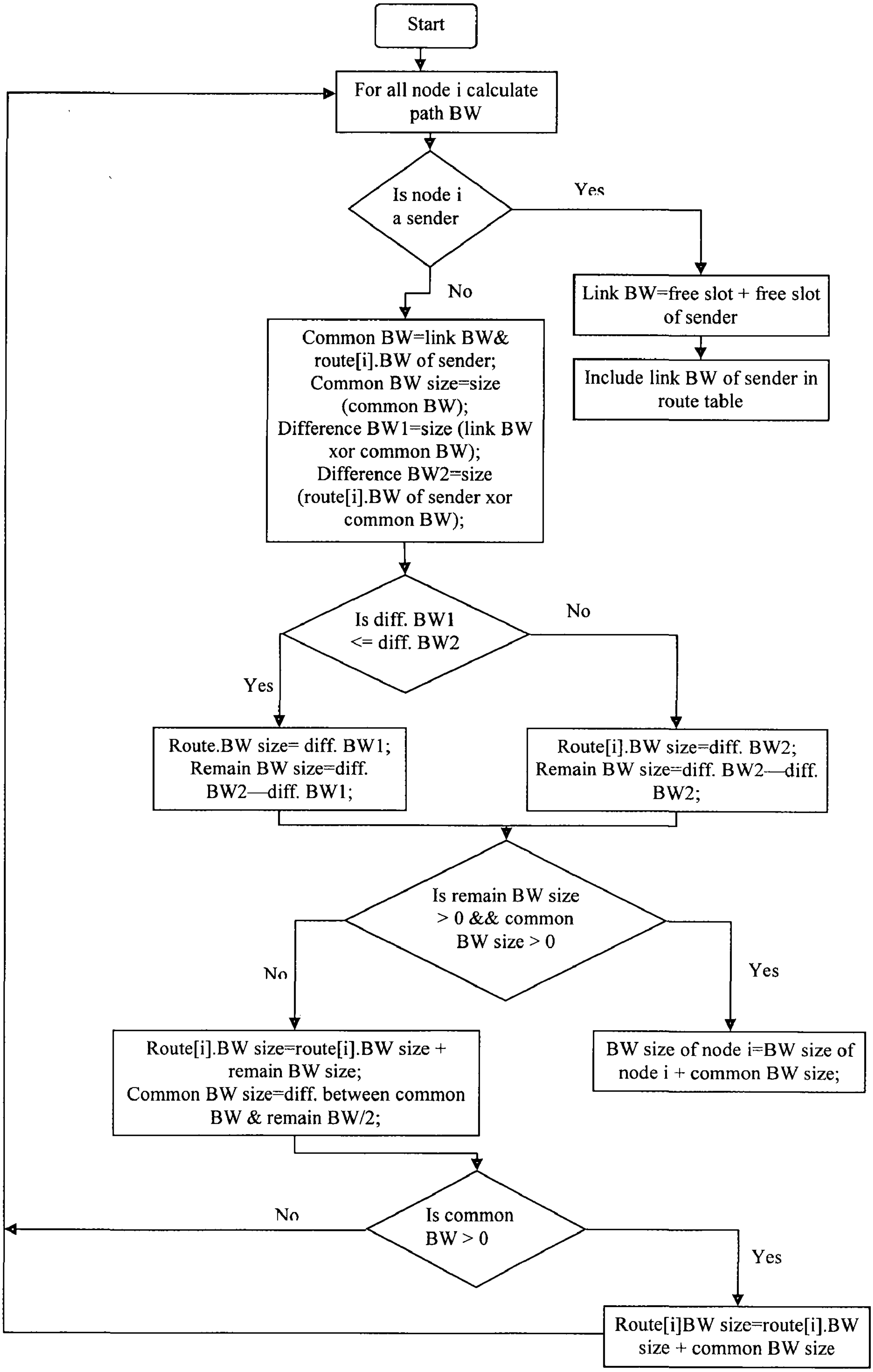


Figure 3 Containing Case

Assume the link bandwidth of both (Z, Y) and (Y, X) are the different as in figure 3. If X uses slots 1, 2, 3 to send the packet to Y, then Y can use 4, 5 slot to forward packet to Z. This is because Y cannot be in transmitting and listening Z, denoted as p_BW (X, Z), can be {1, 2, 3}, and its size is three. In this case, five free slots can only contribute two slots for path bandwidth. If there are only three free slots on both links, then the size of path bandwidth is [3/2] = 1. Similarly, four free slots can contribute two slots for path bandwidth is [4/2]=2. Assume l_BW(Z,Y) = 2,3 and l_BW(Y,X) = (1, 2, 3, 4, 5). If X uses slot 2, then Y cannot use slot 2 anymore. So in this case, X should first use slots in l_BW (Y, X) - l_BW (Z, Y) to maximize system utilization. Therefore, if X uses slots 1, 4, 5 then B can use slots 2, 3. So path_BW (X, Z) = (1, 4, 5), and its size is three.

Similarly, we can use the same way to process the case of $l\_BW(Z, Y) \subset l\_BW(Y, X)$. In this case, Y must use slots in "$l\_BW(Z, Y) - l\_BW(Y, X)$" first. If $l\_BW(A, B) \cap l\_BW(B, C)$, no conflict will occur. If C can choose either slots 3 or 4, and B chooses slot 2. So path_BW (C, A) = (4), and its size is one. If $l\_BW(Z,Y) \cap l\_BW(Y,X) = \phi$, no conflict will occur. The algorithm maintains the routing table (two alternative routes in the algorithm, i.e., SR1 (SR1(standby route 1) and SR2 (standby route 2)); SR1 has larger bandwidth than SR2. The "PR" in the algorithm means the primary route. It is notable that the primary route is shortest, but is not necessary to have the largest bandwidth. When a host generates a new call, it uses the algorithm to construct the path. In the algorithm, the route that satisfies the QoS requirement in order to precedence PR, SR1 and SR2. The chosen route will be the primary route. That is, the next entry in the routing table may be changed depending on the requirement. After choosing the primary route, the source node will send out a call setup message to next. When receiving the message, the next node will run the protocol in the algorithm to reserve bandwidth for the new call. Because of high mobility a topology change destroys the primary route; node will try to rebuild a new path immediately, using either SR1 or SR2. Thus, a new route from the breakpoint will be established by sending call setup message node-by-node to the destination.


Start
For all node i
Is node i a sender
Yes
No
Sender routing table [i].PR!=PR &&
Routing table [i].PR!=sender &&
Routing table [i]!=sender routing table [i].PR
Is sender a next node of SR2 in routing table for i
No
Yes
Calculate BW to destination host i using same algo. in AODV
Is Calculate BW > BW from SR1
No
Yes
New SR1=sender
Update SR1 BW information
Is sender (next node of PR) && (next node of SR1
No
Yes
Calculate BW to destination host I using same algo. In AODV
Is calculate BW > BW of SR2
No
Yes
New SR2=sender; Update SR2 BW information


Start
For all node i calculate path BW
Is node i a sender
Yes
No
Link BW=free slot + free slot of sender
Include link BW of sender in route table
Common BW=link BW& route[i].BW of sender; Common BW size=size (common BW); Difference BW1=size (link BW xor common BW); Difference BW2=size (route[i].BW of sender xor common BW);
Is diff. BW1 <= diff. BW2
No
Yes
Route.BW size= diff. BW1; Remain BW size=diff. BW2—diff. BW1;
Route[i].BW size=diff. BW2; Remain BW size=diff. BW2—diff. BW2;
Is remain BW size > 0 && common BW size > 0
No
Yes
Route[i].BW size=route[i].BW size + remain BW size; Common BW size=diff. between common BW & remain BW/2;
BW size of node i=BW size of node i + common BW size;
No
Is common BW > 0
Yes
Route[i]BW size=route[i].BW size + common BW size

different protocol of different scenario and for validation the results are compared with experimental data of AODV protocol.

3.3 Simulation Environment

Simulation environment consists of 20 wireless nodes forming an ad hoc network, moving about over a 100 m x 100 m flat space. Each run of the simulator accepts as input a scenario file that describes the exact motion of each node and the exact sequence of packets originated by each node, together with the exact time at which each change in motion or packet origination is to occur. The simulation parameters are given in table 3.1. Figure 3.1 is a snapshot of the network model considers for simulation. For evaluating the effect of variation on different protocols- routing traffic received and sent, data traffic received & sent, control traffic received & sent, throughput, retransmission attempts and delay. Protocol evaluations are based on the simulation using OPNET/ns2 simulator.

Table 3.1 Simulation Environment

Area (m)	100 x 100
Physical Characteristics	DSSS
Packet Reception Power Threshold	5.33 E-14
Mobility Model	random waypoint
Node Placement	random uniform
Buffer Size	128000
Fragmentation Threshold	512
Data Rate (Mbps)	11
No. of Nodes	20

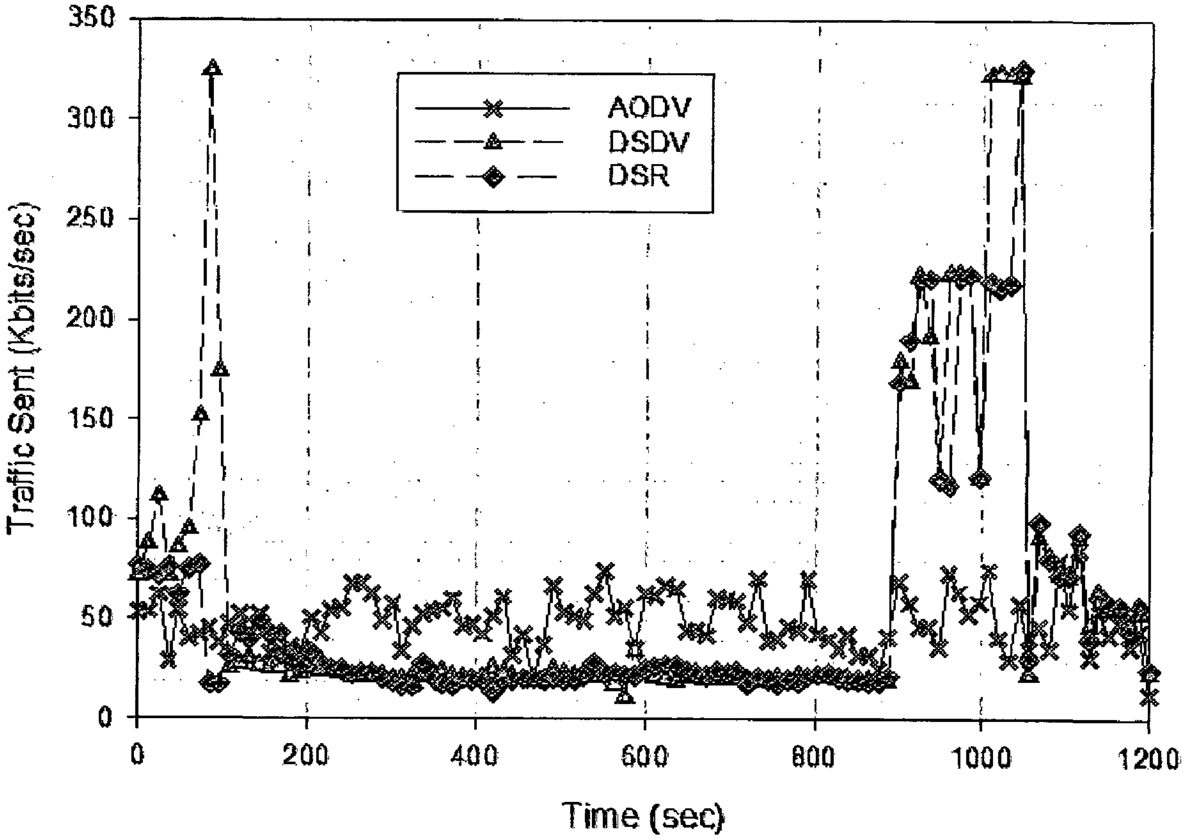


Figure 3.2: Control traffic sent for different protocols

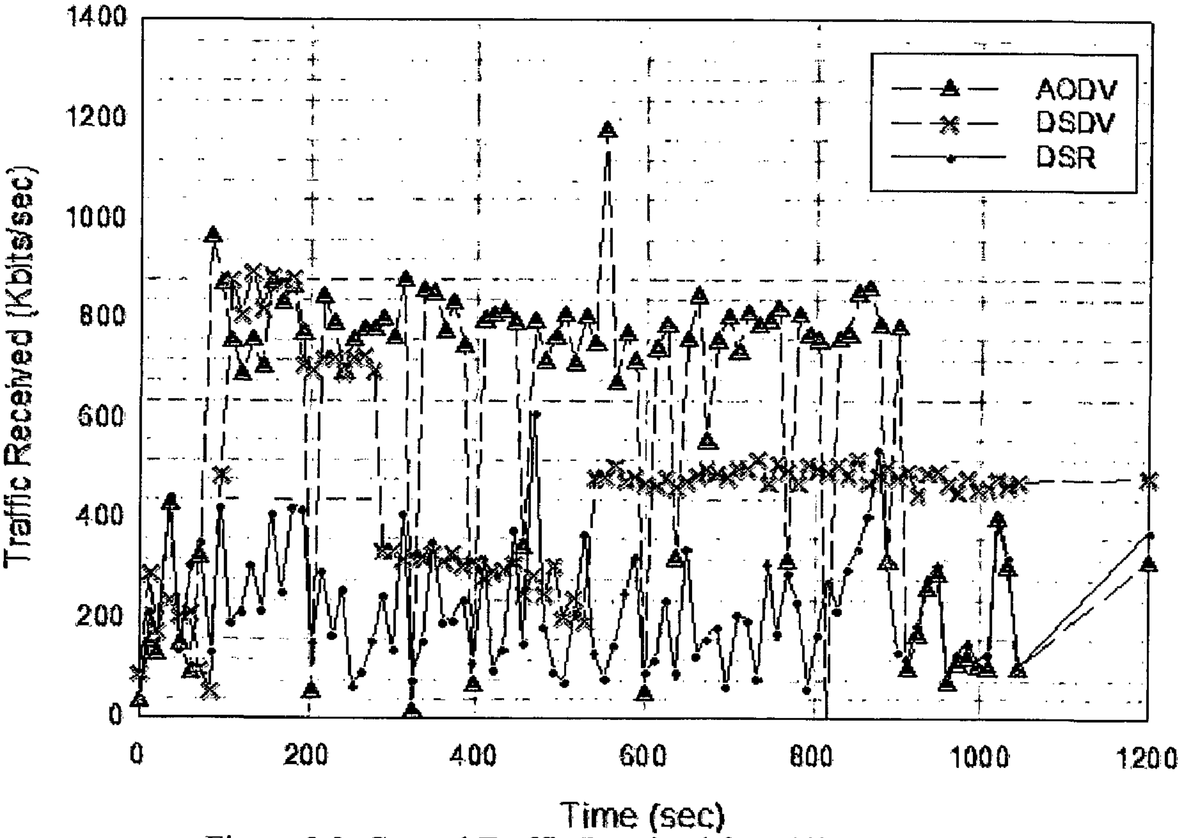


Figure 3.3: Control Traffic Received for Different Protocols