

BL ✓
/

FOR REFERENCE ONLY

14 JAN 2008

ProQuest Number: 10290220

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10290220

Published by ProQuest LLC (2017). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Nottingham Trent University
School of Computing and Informatics

Wireless Intelligent Distributed Systems Based on Mobile Ad hoc Networks

Amirahmad Rafati

Supervisors: **Dr. Evtim Peytchev**
Prof. Andrzej Bargiela

A thesis submitted in partial fulfilment of the requirements
of Nottingham Trent University for the degree of Master
of Philosophy

September 2006

427837

40 0786138 8



MPHIL/06

RAF

ACKNOWLEDMENTS

I would like to express my profound gratitude to Doctor Evtim Peytchev, my supervisor, for his exemplary guidance, mentorship and for his constant support and patience. He always gave me the opportunity to explore and experiment new research ideas and shapes my research thinking process. It was the invaluable experience I will always remember.

Thank you very much for your concern and friendship during my research at NTU.

I would like to thank Professor Andrzej Bargiela for his useful comments and advice on my papers.

I would like to thank my examiners Professor David Al-Dabass and Professor Christophe Claramunt for their invaluable comments regards my work and dissertation.

Special thank to Professor John Henshall for his valuable assistance in research methodology course and friendly supports during my study. You are my great friend.

I would like to thank the computer department team and Boots library staff and especially Mr. Ian Rogers who provided me all requested research papers, microfilms dissertation and conferences in shortest time.

I earnestly thank my cousin, Mr. Teflise, without his support and encouragement I could not stay in Nottingham.

Finally, I would like to express my profound love to my parents and my sister for their endless love, and constant support.

ABSTRACT

One of the most exciting objectives for research in the next generation of Intelligent Transport Systems (ITS) and Wireless Metropolitan Area Networks (WMAN) is building the wireless information exchange model for car-to-car or car-to-infrastructure communication. The proposed in this research framework, called VehINet, is in line with both approaches' services, provides all necessary functionality and has a great potential for Local Based Services (LBS).

The overall aim of this dissertation is presenting a new architecture for ad-hoc wireless communication network to exchange of information between vehicles in urban environment. In such a network, the nodes communicate with each other directly or through each other (the so called multi-hop mode).

This Vehicular Interaction Network (VehINet) fulfils two information delivery objectives: to avoid driving hazards and to deliver diverse web-based services (IP-based) to drivers and passengers.

Simulation tests have proved the feasibility and effectiveness of communicational infrastructure to service applications based on this model. The usefulness of introduced solutions for improving the performance has also been measured here. Furthermore, distributed MAC protocol as the base layer to cater routing and QoS has been investigated and the performance of probable algorithms has been tested for core services. In addition, the routing issue has been thoroughly studied and candidate protocols have been tested for two types of communicational system in this research.

The simulation environment was also useful to evaluate a number of QoS issues linked to the Mobile Ad hoc Networks (MANET) and to measure the effect of each factor on service quality. The simulator environment also proved the tolerance of VehINet against external factors on service quality.

I believe that the presented model and the results of this research can be used as a baseline for vehicular communication study and provide the guideline for better implementation of mobile networks in future.

TABLE OF CONTENTS

1. Introduction

1.1 Research Motivations	1
1.2 Research Objectives	5
1.3 Dissertation Outline	6

2. Research Background

2.1 Location-Based Services	7
2.2 Previous Projects and Current Systems	9
2.2.1 Inter-Vehicle Communication Projects	11
2.2.2 Vehicle-Roadside Communication Projects	14
2.3 Conclusion	15

3. Proposed Architecture

3.1 System Definition	16
3.2 VehINet Structure	17
3.3 VehINet and New Services	20
3.4 VehINet Communication System and Available Technologies	21
3.4.1 Wireless Standards in Layer One and Two	25
3.4.2 Network Layer and Routing	28
3.4.2.1 Positioning Systems	30
3.4.2.2 AP Layout and Proposed Relaying	32
3.4.3 Transport Layer	35
3.4.4 Application Layer and Service Modes	37
3.5 System Feasibility	38
3.5.1 SDC Simulation Test	41
3.5.1.1 Role of Radio	43
3.5.1.2 Role of Node Speed	47
3.5.1.3 Role of Packet Size	49
3.5.1.4 Role of Directional Antenna	50
3.5.2 LDC2 Simulation Test	52
3.5.3 LDCAP Simulation Test	55

4. VehINet and MAC Layer	
4.1 MAC Layer in Ad Hoc Networks	59
4.2 MAC Simulation Test	63
4.3 Conclusion	67
5. VehINet and Routing Protocols	
5.1 Routing in MANET and challenges	69
5.1.1 Topology-Based RP	70
5.1.1.1 Proactive RP (Table-driven)	71
5.1.1.2 Reactive RP (On-demand)	71
5.1.1.3 Hybrid RP	75
5.1.2 Position-Based RP	76
5.2 SDC Routing	78
5.3 LDC Routing	79
5.3.1 RP Simulation Test	80
5.4 Conclusion	84
6. VehINet and QoS Challenges	
6.1 QoS Implementation Approaches and Wireless Networks	85
6.2 QoS in MANET and VehINet	87
6.2.1 QoS and SDC Services	89
6.2.2 QoS and LDC Services	90
6.3 Affecting Factors on QoS	93
6.3.1 Precipitation Impact on SDC and LDC Services	95
6.3.2 QoS of Mix-Mode LDCAP Services	96
6.4 Conclusion	98
7. Conclusions and Further Works	
7.1 Research Contribution and Major Achievements	100
7.2 Further Works	101
References	104
Appendix	
A. Specification of Simulation Tools used in research	
B. Contents of the included CD	
C. Some of the application used in QualNet models	
D. QualNet Model used in motorway scenario	

ACRONYMS AND ABBRIVIATIONS

ACK – Acknowledgment

AODV – Ad hoc on-demand distance vector

ADAS - Advanced Driver Assistance Systems

AP – Access Point, the terminal of local servers to serve MNs

API – Application Programming Interface

CBR – Constant Bit Rate

CDMA – Code-Division Multiple Access

CoS - Class of Service

CS – Central Server such as main server at traffic control organization

CSMA / CA- Carrier Sense Multiple Access with Collision Avoidance

CTS - Clear-To-Send

CTS – Centralized Traffic Systems

DGPS – Differential Global Positioning System

DiffServ - Differentiated Services

DSDV – Destination Sequenced Distance Vector

DSR – Dynamic Source Routing

EP - Emergency Packets

Geocast – Broadcast in a limited geographic area

GIS - Geographic Information Systems

GPS – Global Positioning System

ISP - Internet Service Provider

ITS – Intelligent Transport System

IVC – Inter-Vehicle Communication

ISM – Industrial, Scientific and Medical frequency band

IWS – Incident Warning System

LAN – Local Area Network

LBS – Location-Based Services

LDC – Long-Distance Communication

LDC1 – Long-Distance Communication for Geocast short messaging

LDC2 – Long-Distance Communication for unicast long messaging

LDCAP – Long-Distance Communication with Access Point

LOS – Line-of-Sight

LS – Local Server
 LU – Light User (a device with low processing power, battery and routing ability)
 MAC - Media Access Control Layer
 MAN – Metropolitan Area Network
 MANET - Mobile Ad hoc Network
 MCBR – Multicast Constant Bit Rate
 MN – M-node – Mobile Node
 MSC – Mobile Switching Centre
 NetD – VehINet
 NetF – Ad hoc Network between Mobile nodes and static stations
 NS2 – Network Simulator Version 2
 ODMRP – On-Demand Multicast Routing Protocol
 OSI - Open Systems Interconnection
 OSPF – Open Shortest Path Forward
 PDA – Personal Digital Assistant
 POI – points-of-interest
 PU – Power User (a device with high processing power, battery and routing ability)
 QoS - Quality of Service
 Ra – Receiving antenna
 RP – Routing Protocol
 RS – Relay Station
 RSVP - Resource Reservation Protocol
 RT – Routing Table
 RTCP - real time control protocol
 RTP - real time transport protocol
 RTS - Request-To-Send
 SDC – Short-Distance Communication
 SDC RT - Short-Distance Communication Routing Table
 SN – S-node- Static Node (play the similar role of base station in cellular)
 SOTIS – Self-Organizing Traffic Information System (a research under Fleetnet project)
 SP – Shortest Path
 SPS - Satellite Positioning System
 SPSR - Satellite Positioning System Receiver
 Ta – Transmitting antenna
 TCP – Transmission Control Protocol

TDMA – Time-Division Multiple Access
TD-SCDMA – Time-Division Synchronous Code Division Multiple Access
TKIP - Temporal Key Integrity Protocol
ToS - Type of Service
TTI – Traffic and Travel Information Systems
UDP – User Datagram Protocol
UMTS - Universal Mobile Telecommunications system
UTRA TDD – Universal Terrestrial Radio Access with Time-Division Duplex
VehINet - Vehicular Interaction Network
VoIP - Voice over IP
VRN – Vehicle-Roadside Network
VVN - Vehicle-Vehicle Network
WAAS - Wide Area Augmentation System
WAP - Wireless Application Protocol
WMAN – Wireless Metropolitan Area Network
WTCP – Wireless TCP
ZRP – Zone Routing Protocol

Chapter 1

Introduction

Since the advent of the wireless devices for computers, great number of networks has migrated to wireless platforms and more and more services have been presented based on them.

A MANET is a decentralized network of nodes which share a wireless channel to send and receive packets to each other asynchronously in one hop or through multiple hops.

Following seeking methods to improve the performance of current traffic control systems, a new MANET architecture based on vehicles namely VehINet is proposed. New services are defined for this network and also the advantages compared to the traditional methods have been enumerated and evaluated. In addition a number of other LBS services can be launched on this infrastructure.

The constrained parameters which affect the quality of related services for this network have been also investigated. Some modifications presented aim to overcome system limitations but more study is required to measure the effects of these factors to better control the bursty nature of Ad hoc networks in different traffic scenarios (turning, cross section, roundabout).

1.1 Research Motivation

Vehicle industry is growing fast and with attention to limited capacity of roads, traffic congestion and accidents impose heavy cost on economy. The EU figures in 2001 show 1,300,000 accidents per year with the cost of €160 billion equal to 2% of EU GNP [1, 2]. This study also proves that the capacity of roads has not increased with the same rate as vehicle numbers and also the main cause of the delay in roads are incidents.

ITS and Traffic and Travel Information systems (TTI) have developed some answers to these needs to decrease the costs [3]. Based on the function similarity, the ITS and TTI terms have been used interchangeably throughout the dissertation.

Figure 1.1 shows a new generation of ITS systems and the blue and yellow part present the area which wireless technology can help to improve system function.

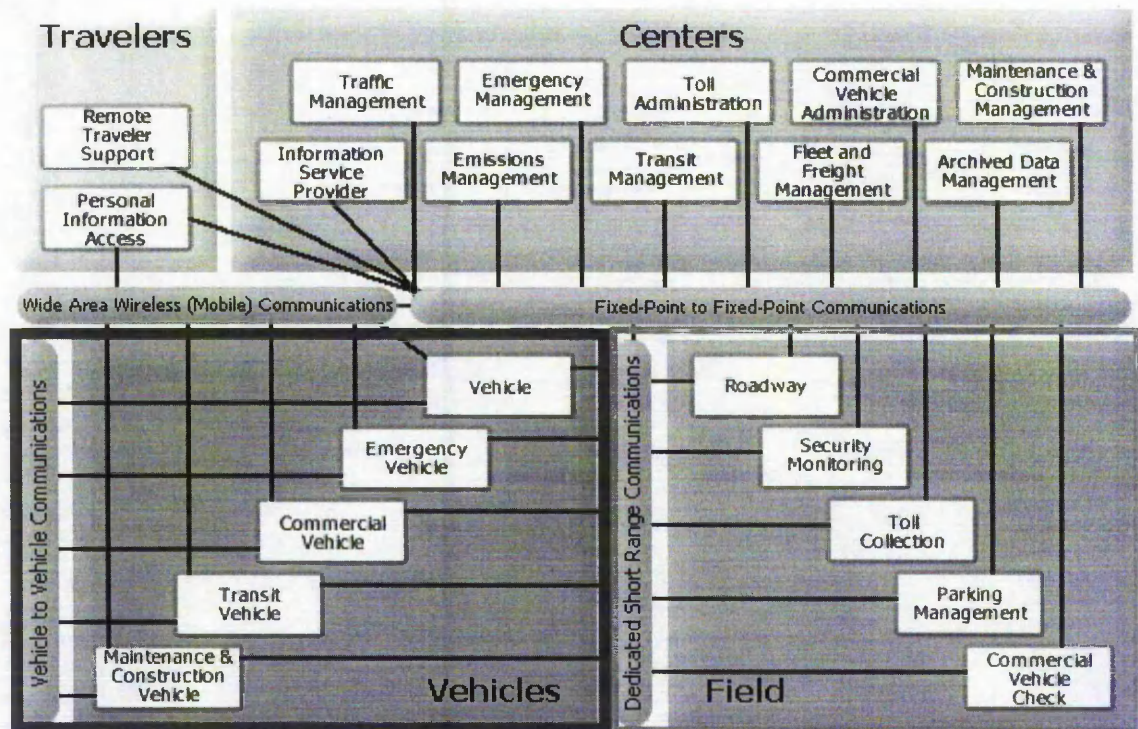


Figure 1.1 Physical entities in US National ITS Architecture version 5 [3]- Red and green mark shows the scope of project for Core and Add-on services

The early form of TTI before computer era was broadcasting information by radio, which is still in use. The second generation of these systems came into reality by invention of computers and their accessories such as cameras. Managing traffic lights and informing passengers through SMS or Internet as a product of this generation have assisted traffic and people greatly but they also have some drawbacks. The driver as a first and major link of the traffic and data generation receives the data with a great latency. For example the 2nd generation of ITS systems unable to inform the driver about road obstacles (Figure 1.2)

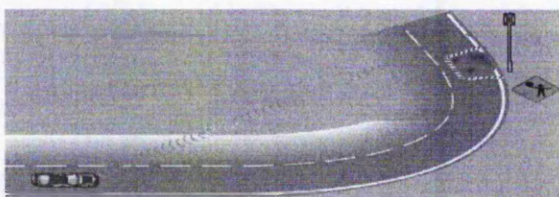


Figure 1.2 warning about construction site in advance by TTI

These two generations, which includes the majority of TTI systems in market, work in centralized manner or Centralized Traffic System (CTS) which heavily rely on network

infrastructure. Although this style brings proper managerial function but the nature of these systems from drivers' point of view is offline.

Wireless technology has enabled third generation of TTI to cover the drawback of CTS systems in two directions. By using wireless devices for legacy systems, and by using wireless enabled vehicle which fulfil proper level of connectivity with users (more updated data). The first one has primarily developed for Telematics and information applications such as updated bus schedule [4, 5]. The later, which is generally part of Advanced Driver Assistance Systems (ADAS) and can work independently from CTS has attracted significant research attention [6-9]. This is also the focus of the current research proposed model which tries to fill the gaps of using centralized systems only, because:

- Centralize control systems are slow response systems, which is not proper for real time decision making. In practice the majority of traffic data are generated close to the vehicles, it is time consuming for ITS to percept an accident by monitoring traffic-light; the vehicle near the accident can propagate alerts faster. This has great similarity with the nature of services in service industry sector. E.g. in hotel and restaurant, the services are not storable (they are perishable) and if it not consumed in time, they are useless.
- Centralize TTI propagate data in a vast area (radio or Internet base) which is suitable for pre-trip use and not effective for en-route drivers.

From managerial point of view, traffic control like other control systems has centralized characteristic but the following nature of traffic information, justifies the necessity of distributed management:

- Traffic information mainly generated by vehicles (sources of data)
- Traffic information are most useful in vehicles (best consumer of data)
- Majority of traffic data has short lifetime and should be consumed quickly
- Traffic information mainly useful for vehicles in a local area or geographical neighbour

These features shift the controllability feature to lower levels of ITS management tree. The strategic decisions such as city planning and distribution of traffic lights remain in

the control of higher nodes but logistics such as selecting the best route should be decided by lower levels. This indicates the value of VehINet and LBS in ITS.

The proposed system does not replace the CTS system but delegate part of their tasks to lower levels of the architecture – such as vehicle computer systems. The synergy of hybrid system by collaboration of CTS and VehINet increase the performance of ITS and bring following benefits:

- Prevents traffic accident and traffic jam
- Provide Location Base Services (LBS) which is able to data filtering (barring irrelevant data)
- Performs dynamic traffic control and incident management
- Performs better strategic planning
- Vehicle tracking

The research on the cause of rear-end accidents in US highways shows 88% of accident are preventable by a warning system (figure 1.3) and the most effective place to implement this system is inside the vehicles.

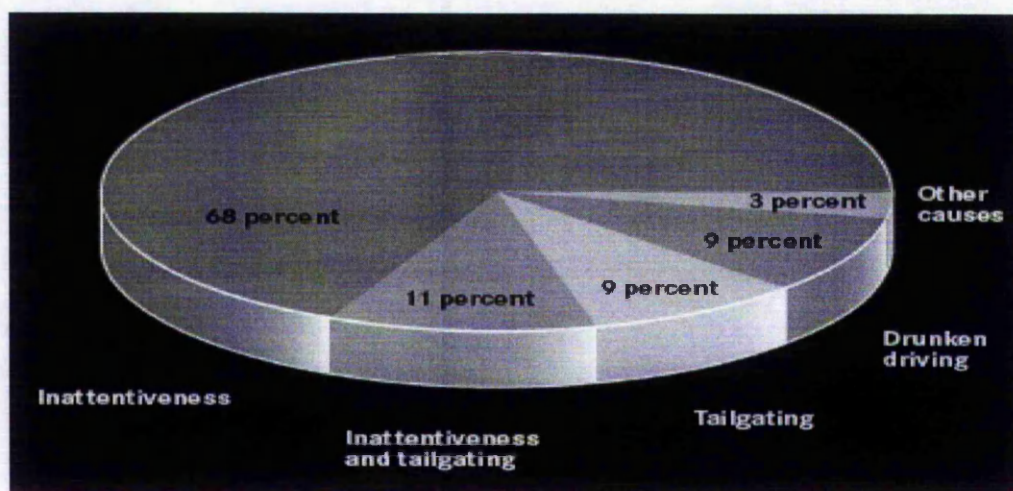


Figure 1.3 Causes of rear-end collisions on U.S. highways [16]

By combining the ADAS tools to wireless enabled nodes in VehINet, following benefits are identifiable:

- Less accident, casualties and traffic jams
- Queue-less toll collection by auto billing cars

- Vehicle theft reduction by auto-tracing cars
- Fair insurance cost by the help of driving history and vehicle mileage
- Auto charging driver for parking use in city
- Automatic ticketing and billing driver for speeding and other traffic offences (no need policing by radar or camera)

Following applications can be develop based on the proposed scheme and current systems:

- New cruise control (bypassing radar limitations such as blocking by cars and environmental conditions such as rain)
- Dynamic Shortest Path (SP) finding
- Intelligent journey planning
- Remote vehicle diagnose system based on car performance
- Telephony on WiFi as a killing application
- LBS such as, tourist information system and advertisement by shops, restaurants, parking, garage and so.

1.2 Research Objectives

The aims of this project is design a communicational system based on high speed MANET in vehicles to work as part of a new distributed ITS which enables ITS to:

- Prevent accident and assist safe navigation (Real-time service)
- Inform drivers of hazards in advance (Real-time service)
- Cooperate with local ITS centre regards traffic information
- Communicate with road base networks

Other computing and networking objectives include:

- Design a high speed wireless system as part of the new ITS system to assist drivers for self navigation and hazard prevention (core services) which also gives traffic-related information and internet services through communication with stationary networks (add-on services)

- Feasibility study of system achievability and measuring the factors influencing the system - prove the robustness of VehINet to overcome intermittent nature of the network and maintain service quality in acceptable level
- Find solutions for efficient and reliable service with less contention and interference

1.3 Dissertation Outline

In chapter 2, after encountering the MANET applications, some of the latest systems in ITS and WMAN are evaluated, and analyzed from different aspects and the shortcomings of each one investigated.

After defining the VehINet system and components in chapter 3, a top-down structure of system introduced and a detailed view of the communicational system in network layers analyzed. An extensive evaluation of the system feasibility is presented and simulation tests for different services are documented.

In chapter 4, the distributed MAC algorithms are investigated and various approaches to control flooding by location-aware MAC are scrutinized. Simulation tests made a comparison between various MAC protocols.

In chapter 5 after presenting an introduction of routing algorithms, the features of candidate routing protocol for VehINet to cover system service requirements has analyzed. Simulation test for on-demand routing are last part of this chapter and they validate the latest research findings.

In chapter 6, the QoS issue in VehINet is discussed and the methods implementing QoS are scrutinized. The factors affecting service quality are identified and finally the simulation result shows the effect of weather and mix-modes services on VehINet.

Chapter 7 summarizes the project achievements and research contribution to high-velocity MANET to be implemented in vehicles to apply in urban and off city roads.

Chapter 2

Research Background

This chapter starts with closer look at the LBS systems and further reviews and evaluates the research about the models and solutions presented in ADAS, ITS and WMAN.

2.1 Location-Based Services

Mobile phone companies and Internet service providers similar to other centralized information systems, provide some services which address general public subscribers. Location Based Services (LBS) based on ad hoc networks heralds new applications which are not possible by centralized system. LBS supply customized information based on the mobile user's current location and due to this is the killer application of the mobile commerce. For example, a visiting nurse can quickly locate patient information when she is close to that patient's house. The advantages of LBS include:

1. Better targeting the destination markets
2. Increase the effectiveness of volatile services (with short lifetime) like food and tourist industry
3. Reducing redundant travels, reduce the traffic and air pollution
4. Reduce the price of services by better advertising and filtrate target customers
5. Reduce the price of goods by direct buying and selling from/to local agents

The first three are highly valuable from ITS point of view. The cost of information in this method is mainly cheaper due to removing inefficient central agent. The drawback of this system can be increasing of the radio wave pollution and inability to serve some centralized applications.

By collaboration between LBS and centralized system more services are possible e.g. Internet services for passengers to utilize the time in traffic jam. In general LBS Services can be classified as:

- **Emergency services** -it is a location based emergency service application that pinpoint your location and pass it to the appropriate authorities. In US, all

wireless carriers provide a certain degree of accuracy in pinpointing the location of mobile users dialling 911.

- ❑ **Tracking** - Fleet applications typically entail tracking vehicles to the interest of the company to know whereabouts are the vehicles/agents. Tracking also can enable mobile commerce services. A mobile user could be tracked and provided with the information that he predefined of his desires, such as notification of a sale on food at the near restaurant.
- ❑ **Location based information** - The GPS determines the user location and LBS application provides a list of sites within certain proximity of user. For instance searching for a tourist site by using Wireless Application Protocol (WAP) on mobile phones.
- ❑ **Location based billing**- Through location based billing by arrangements with the wireless serving carrier the user could have all-together-billing for communications in different places.

LBS applications highly depend on the following technologies:

- ❑ **Positioning** - such as the Satellite Positioning System and network based positioning (triangulation of the signal from cell sites serving a mobile phone). Table 2.2 shows the required position accuracy for LBS applications. ITS applications and VehINet need high precision positioning.
- ❑ **Geographic Information Systems (GIS)** - It allows administering base map data such as manmade structures (streets, buildings) and terrain (mountains, rivers) by detecting these data from coordinates and vice versa. It helps look up yellow pages and landmarks; calculate optimal routes and render custom maps. GIS is also used to manage point-of-interest (POI) data such as location of gas stations, restaurants, nightclubs, etc. Some GIS keep information about the radio frequency characteristics of the mobile network to determine the serving cell site of the user.

Application	Accuracy	Application	Accuracy
News	Low	Gaming	Medium
Directions	High	M-Commerce	Medium to High
Traffic Information	Low	Emergency	High
Point of Interest	Medium to High	Sensitive Goods Transportation	High
Yellow Pages	Medium to Low	Child Tracking	Medium to High
Car Navigation	Medium to High	Pet Tracking	Medium to High
Personal Navigation	High	Electronic Toll Collection	Medium to High
Directory Assistance	Medium to High	Public Management System	Medium to High
Fleet Management	Low	Remote Workforce Management	Low
Car Tracking	Medium to High	Local Advertisement	Medium to High
Asset Tracking	High	Location-Sensitive Billing	Medium to Low

Table 2.1 LBS applications and required level of accuracy [10]

The heart of LBS systems is the location engine, and the software consists of Geocoding (street address to coordination), Reverse Geocoding modules (map matching by using geometric, probabilistic and fuzzy techniques) and routing. Figure 2.1 shows the components of a location engine (Kivera) used in AT&T friend finding WAP-based application. Routing is responsible to find optimal route through a variety of best routes including shortest route, fastest route and non-charging freeway route.

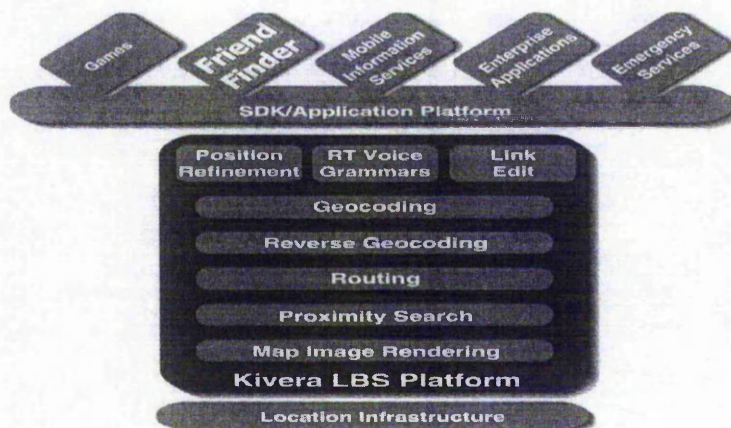


Figure 2.1 Kivera location engine components [11]

2.2 Previous Projects and Current Systems

The closest system rivalry VehINet services are CTS wireless sensor network [12-14] and wireless infrastructural network like WMAN. Irrespective of expensive deployment of wireless sensors, the system delay is unacceptable due to complexity of process in local servers. The second method faces the following shortcomings:

- Extensive implementation of MAN network with loads of AP is costly.
- MAN is specific to metropolitan area and implementing APs in off-city roads impossible.
- Lack of response to real-time services.

Some of the ADAS techniques like radar-based system [15, 16] and vision systems [17-19] are other competitors of wireless in VehINet. The Radar systems for accident free driving have following drawbacks:

- No method for detection pedestrian
- Blocking by other cars
- Affected by environment condition such as rain and snow
- Lack of coverage except using lots of transceivers e.g. 8 or 10 around the car
- Lack of information about other object components such as distance, speed
- Passive (slow) perceptions of change in object coordination
- Huge blind spots due to work in line of sight

Vision systems are able to classify objects and can detect non-metallic obstacles such as pedestrian but have the following drawbacks:

- Severely affected by environment condition such as night, fog, rain and snow
- Near object detection
- Slow processing and low precision
- Lack of information about object components such as distance, speed
- Passive (slow) perceptions of change in object coordination
- Huge blind spots due to work in line of sight

It is nice to mention that the wireless-based solution has indisputable advantage to other methods like vision and radar-base systems include:

- Providing more complete information about Traffic
- Ability to run lots of other services based on it

But wireless systems should be used in collaboration with other ADAS methods to cover its drawbacks such as:

- Passive nature, ineffective when other vehicles not equipped with such a system
- Subject to natural causes like rain and snow
- Inadequate security due to using air medium
- Subject to interference (unreliability factor)

2.2.1 Inter-Vehicle Communication Projects

CarTalk2000 [20] – It was a three-year (2001-2004) European research project (5th framework) focusing on new driver assistance systems based on Inter-Vehicle Communication (IVC). This project solely focuses on car-to-car communication for hazard avoidance and has no provisioning for infrastructural link and LBS application.

The system test based on three cars equipped with DGPS positioning and Ethernet interface card (802.11b) has shown satisfactory result [20]. Here the communications happens based on flooding and practically no routing is necessary. The two types of socket, UDP and Raw, have used for internal (Ethernet) and external communication respectively (figure 2.3). The routing algorithm has designed on UDP socket (IP +Port number) to interface between application and router (figure 2.4).

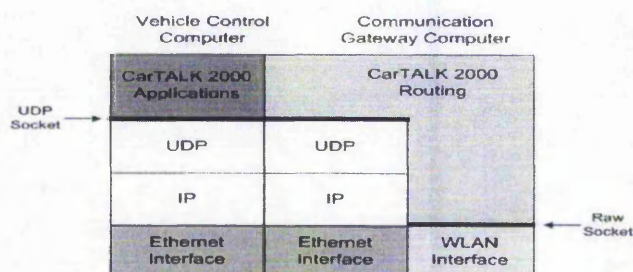


Figure 2.3 UDP Socket and raw socket in CarTalk2000 [20]

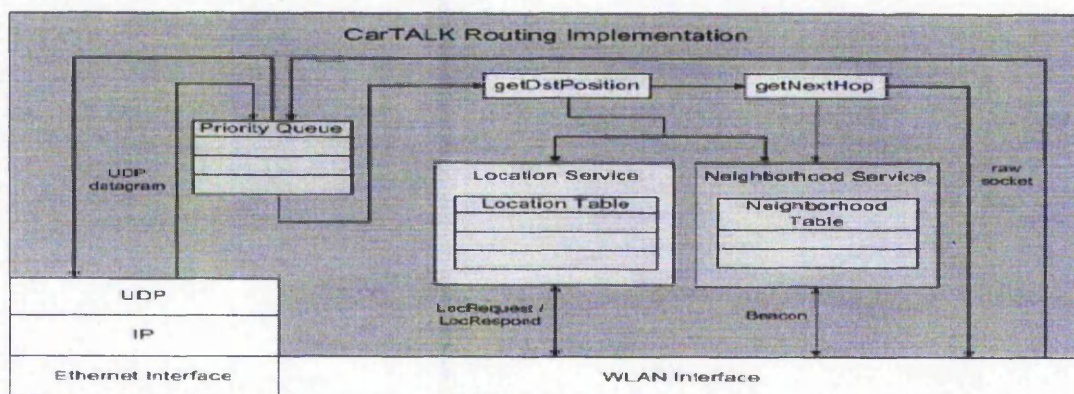



Figure 2.4 Routing mechanisms in CarTalk2000 [20]

UTRA TDD and TD-SCDMA, standards with both characteristics of CDMA and TDMA, has been suggested communication carrier in CarTALK2000. This standard has low data rate and works in UMTS license band (Table 2.2). Also using IP address is redundant for short messaging in flooding method.



UMTS

Standard	TD-SCDMA	UTRA-TDD	UTRA-FDD	CDMA2000	UWCC136	DECT
Freq. band	unpaired	unpaired	paired	paired	paired	unpaired
IMT-2000	IMT-TD IMT-2000 CDMA TD (time division) TDD-LCH	IMT-TD IMT-2000 CDMA TD (time division) TDD-MCR	IMT-DS IMT-2000 CDMA DS (direct spread) W-CDMA	IMT-MC IMT-2000 CDMA MC (multi carrier)	IMT-SC IMT-2000 TDMA SC (single carrier)	IMT-FT IMT-2000 FDMA/TDMA
Core network compatibility	GSM MAP	GSM MAP	GSM MAP	ANSI-41	ANSI-41	ISDN
Primary standardisation bodies	3GPP 3GPP	3GPP	3GPP	3GPP2	TIA (US)	ETSI

TDD

Table 2.2 ITU-2000 standardized systems and the place of UTRA-TDD and TD-SCDMA [21]

Table 2.3 shows that the three types of services on CarTalk2000 use different data rate, message size and transmission range. The differentiation method based on messaging interval is not secure and in situations like high density of messages can face more delay for propagation. The different message size increases the MAC delay to accept messages which consequently reduces the performance of system from real-time point of view.

	IWF	CBLC	CODA
One-Hop transmission Range [m]	1000	500	500
Multihop	+	+	-
Broadcast	+	+	+
Unicast	-	-	+
Priority	+	-	+
Repetition rate [Hz]	1-10-25-50	1-10-20-50	20-50
Maximum delay [ms]	40-100	100	100
Bite-rate required [bps]	t.b.d.	t.b.d.	t.b.d.
Incident Triggered	+	-	-
Message Size	Short	Medium	Medium

Table 2.3 the attribute of three types of services on CarTalk2000 [21]

To have 0.55m tolerance in 200km/h, 10ms messaging interval is suggested that consumes lots of bandwidth. Project suggests beaconing Piggybacking and sending beacon information with data (static beaconing used in test system). Dynamic beaconing option, due to strong influence of environmental factors (weather and obstacles) has declined. Based on flooding, beaconing has practically no use for car-to-car communication. Dynamic change of messaging interval can be better substitute for dynamic beaconing.

Redmill and Fitz [22] - Their research tested at Ohio University is the first project which suggested dual range dual frequency for Incident Warning System (IWS). They

used high bandwidth 5.8GHz DSRC for short distance communication (400m) and low bandwidth 220 MHz for long distance communication (8-10km) with central base stations (refer table 2.4).

Specification		LDC BS to Vehicle	LDC Vehicle to BS	SDC Vehicle to Vehicle
Physical Layer	Frequency	220.5626 MHz	221.5625 MHz	5.8 GHz
	Xmit Power	4 W (38 dBm)	0.5 W (27 dBm)	10 mW (10 dBm)
	Antenna	Omni	Omni	Omni Horiz 5 dBi
	Range	8-10 km	8-10 km	400 m
MAC Layer	MAC	Broadcast Reservation	Slotted Aloha Reservation	Non-persistent CSMA
	Xmit Rate	6.4 Kbps	4.8 Kbps	512 Kbps
	Xmit Interval	1 second	1 second	100 msec
JPEG	Size			16-24 Kbyte
	Packet Size			900 bytes, 20 msec

Table 2.4 Communication System Specification in Redmill and Fitz research [22]

To limit the contention in long distance they differentiated frequencies for uplink and downlink. Diversity of scenarios and applications tested in their study is prominent for instance they tested image transmission (jpeg) between MNs in stationary state.

Although their result is in acceptable range but using omni-directional antenna by increasing node numbers exponentially increases the contention and decrease system usefulness. Also the low-bandwidth frequency used for long distance communication limits the service types and is only suitable for small messaging applications. In the same time, it can highly increase the wave interference and the load of central node.

SOTIS [23, 24] - Self-Organizing Traffic Information System, a research based on three years (2001-2003) FleetNet project [25] which studied IVC for TTI. The simulation in NS2 [26] with TDMA standards, 1Mbit/s data rate in 2.4GHz frequency and 1000m range proves the accuracy and delay of this system (refer to table 2.5). The result also proves that even if 2% of cars were equipped with wireless the TTI can work in acceptable level instead of CTS.

Road length	140 km and 110 km
Number of lanes	2 per direction
Deceleration prob.	0.4
Constitution of traffic	15% slow vehicles, 85% regular vehicles
Desired velocity	108 km/h (slow), 142 km/h (regular)
Avg. headway (exp. distr.)	2 s, 3 s, 4 s
Number of vehicles	≈ 7500, ≈ 10000, ≈ 15000
Mean Velocity	95.6 km/h, 101.3 km/h, 106.4 km/h

Table 2.5 Parameters used in SOTIS simulation test [23]

Although research concludes that low number of communications, two per second, is proper for TTI current tasks, but it is not efficient for emergency information and MN safe navigations. Also by using 500ms interval, the problem of contention has been ignored here.

2.2.2 Vehicle-Roadside Communication Projects

By introducing UMTS and WLAN, applying wireless to serve vehicular applications has been the subjects of many projects [27-29]. WLAN for use in metropolitan area has been more in focus to form a global ubiquitous network [30-33].

Cisco Model - Cisco presented router 3200 [34] for a WMAN based on 802.11b/g in 2002. This router, which was planted in vehicles, is the heart of Cisco model for WMAN (Figure 2.3). This model has implemented in Baltimore police department in 2004 and has been also planned to apply for monitoring London Soho area by wireless Closed-Circuit Television (CCTV) systems [35].

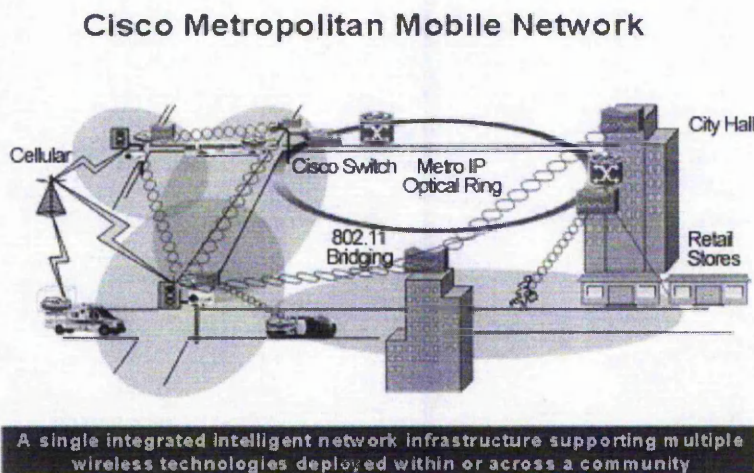


Figure 2.3 Schematic view of Cisco Metropolitan Mobile network [34]

In this model, each mobile device maintains its wireless connection with the centre during move, hence tracing nodes is the default service here. The modular design of router makes the system extendable for example it is possible to have two wireless cards to be able to communication with static devices too.

To meets high standards in the Department of Homeland and Department of Defence the security of system guaranty by adding PC/104 card (equipped with 168-bit Triple Data Encryption by Western DataComm IPE-2M encryptor). This solution transmits encrypted packets through an IPSec tunnel to bypass the security weaknesses of the Wired Equivalent Privacy (WEP) standard defined for 802.11b networks.

Irrespective of the high price of routers, the model does not stress on communication between dynamic nodes and mainly customized to communicate between mobile nodes and base stations.

2.3 Conclusion

This study shows that even in best conditions using a single method for ADAS is vulnerable. For instance if all vehicles are equipped with wireless system it can not prevent or detect the human or animals in the road hence applying hybrid method like radar detection systems is advisable.

The background study about IVC projects and systems revealed that there has been no unique research to encompass the requirements of a system for accident prevention and traffic control system.

CarTalk2000, the most extensive research for accident prevention system, mainly focuses on the design of system to work by cellular technology. This study generally formulates the characteristics of such a system and terminates with a successful test on 802.11 systems. Based on the short bandwidth of UMTS technology giving information services like Web-based system has not been possible in this system. In the same time, it did not include methods for communications control.

The study also showed that the only research resulted in a real market product is Cisco study on wireless routers which partly covers the TTI systems need. This system is designed for light applications like police and other emergencies and has not been tested in the calibre of a navigation system in crowded scenarios for great number of vehicles.

This study revealed that the research in this area is still in early stages and needs great attention. The importance of current project stems in the gap of research in this field caused by the relative novelty of the wireless systems in above applications.

Chapter 3

Proposed Architecture

This chapter presents the new communicational architecture and defines specifications and requirements of the project to be able to serve all new applications. The network technologies in each layer have been reviewed with a holistic view to system functionality from different angles.

The proposed infrastructure does not hope to replace old services but improves them and makes a foundation for new applications. The challenges facing this model and presented solutions for better implementation are described later.

3.1 System Definition

VehINet is an autonomous, loosely connected mesh network of high mobility vehicle (M-nodes). This Vehicle-Vehicle Network (VVN) system has three objectives:

- Incident warning system (autonomous, real time)
- Traffic information service with or without ITS transaction
- Service to external users

The first two tasks have vital role in VehINet and make it part of Modern ITS system [3]. The later task consists of ITS and commercial service. Here the VehINet also acts as a bridge to connect external users (or networks). The commercial services implicitly assist the traffic systems to minimize travel time by informing the users of local services.

From VehINet point of view the users of VehINet consists of internal-users like drivers and passengers; and external-users through Type2 or Type3 network

Based on VehINet interactions with others wireless enabled systems (figure 3.1), there are two types of Vehicle-Roadside Networks (VRN):

- Type2- for Power-User (PU) communication with VehINet in mobile and stationery mode

- Type3- for Light-User (LU) communication with VehINet only in stationery mode

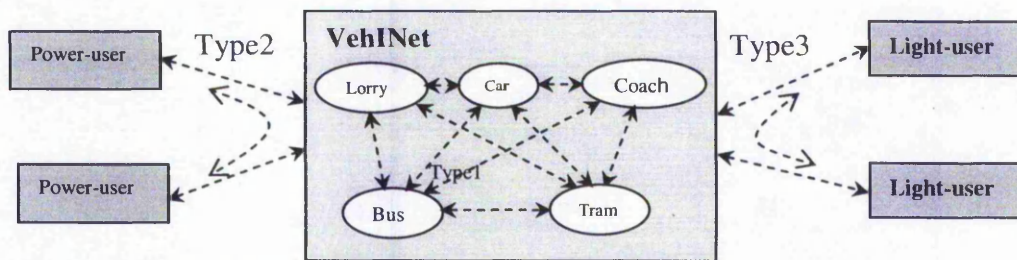


Figure 3.1 VehINet Communication with other networks

PU, users with more process power and routing ability, can be part of wired network such as Enterprises, ITS or stand-alone wireless devices like hotels and shops. LU includes pedestrians with handheld wireless devices. Both PU and LU are able to, request a service and serve a request or advertise a service. The VehINet acts as an intelligent bridge to establish communication between LUs, PUs or LU-PU. Each M-node (MN) is responsible to communicate with others MNs about traffic issue or other services through static nodes (S-nodes). In this research the VehINet services also referred as core (Real-time ITS) services and add-on (ITS and commercial) services.

By inheriting MANET characteristics such as independent data generation by each node and stochastically source-destination definition, the target system should:

- Be able to do multi-hop transmission
- Adapt to topology change
- Adapt to node speed
- Dynamically allocate resources like data rate, transmission range and routing

3.2 VehINet Structure

The main focus of VehINet is making reliable communication between computer-equipped vehicles in order to alert each other of the probable hazards and to avoid collision. VehINet can be part of a modern ITS system (Figure 3.2). Here, each MN is member of two MANET networks:

- NetF, Wireless network between S-nodes (SNs) and Mobile Nodes (MNs)
- NetD (VehINet), Wireless network between MNs (wireless enabled vehicles)

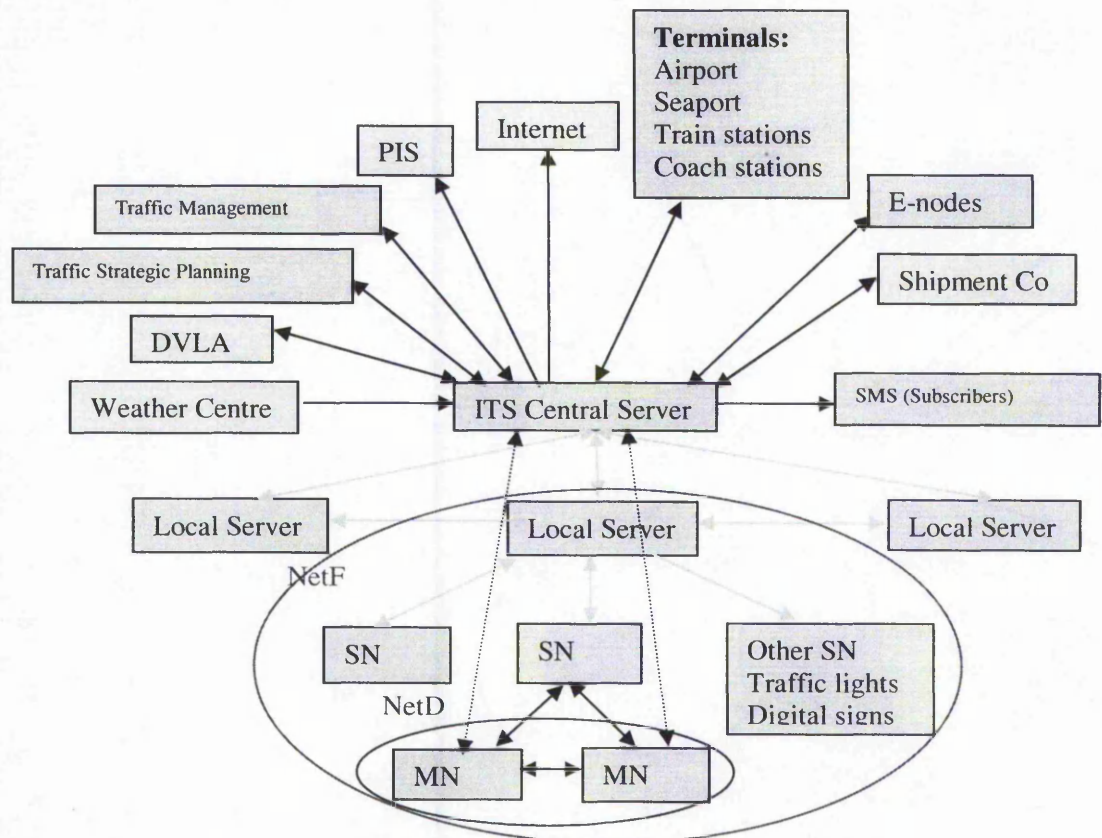


Figure 3.2 VehINet place in ITS Hierarchy of elements

Figure 3.2 shows the main elements of modern ITS system which consists of: MNs, Local Servers (LS), SNs and Central Server (CS). In other words, there are three subsystems, which interact with each other. Although in comparison with LS, the CS function is more strategic, they have great similarity in function. LSs are essential for better information management and improving system response time. Strategic planning is more or less concentrated in CS tasks. The main flow of data from MN to CS, by and large is raw data but vice versa consist of commands and strategic solutions. The SN can be repeater, router or Access Points (AP). S-node also includes one-way terminals such as traffic light, bridges and barriers. In comparison with cellular networks, LSs play the role of Mobile Switching Centre (MSC) and SNs play the role of Base Station (BS).

MNs broadcasts (Geocast) small warning packet about imminent hazards (break down, obstacles) and position change (overtake, lane change, breaking, accelerate). Forwarding critical messages is among other tasks of MNs, which should be restricted by packets timestamp and aging byte.

The major role of NetF is to disseminate important traffic messages (such a traffic jam and road under construction) to MNs and secondly, to provide add-on services to them (finding shortest path, parking hunting, weather forecast, promotion advertises for gas stations, restaurants and shops). These services have diverse characteristics and needs to be disseminated in unicast, multicast and broadcast manner. Due to this, servers are responsible for MNs handover between SNs. The MNs act intelligently in following ways:

- Observing priority of incidents
- Selective message sending
- Learning hazard situations based on driving style

VehINet general requirements include:

- Reliable wireless systems in each mobile node for real-time automated communication with other vehicles in meaningful range.
- Satellite Positioning System Receiver (SPSR) like GPS receivers for self-positioning; when there is no access to GPS satellites like canyon effects in cities the system count on vehicles coordination system, a hotlink system to calculate next position based on steering and speed. The ITS infrastructure can also assist Vehicles by network positioning (triangulation of the signal from Access point) but the system often can ignore this option due to weakening effect on system robustness.
- An updatable digital map of road network includes Geographic Information Systems (GIS) database with data includes:
 - Man-made structures
 - Terrain (mountains, rivers)
 - Point-Of-Interest (POI) and Yellow page information such as location of gas stations, restaurants, nightclubs, etc
 - A downloadable table of SN coordination
- A Navigation system, to map current node coordination with GIS and map
- An optional table of bus routes and their timetable would assist the vehicles to estimate the traffic load ahead. Without this table, the bus server (after a threshold) broadcast messages and warn other vehicles of heavy traffic in front of them. Vehicles such as Lorries and coaches can be helpful in roads out of cities.

As figure 3.3 shows, the MN computing module should process the data from first two modules with the data deduced by the two WiFi systems and internal sensors. Updatable databases of SN coordination and bus schedule (route and time) play an important role for VRN and traffic forecast respectively.

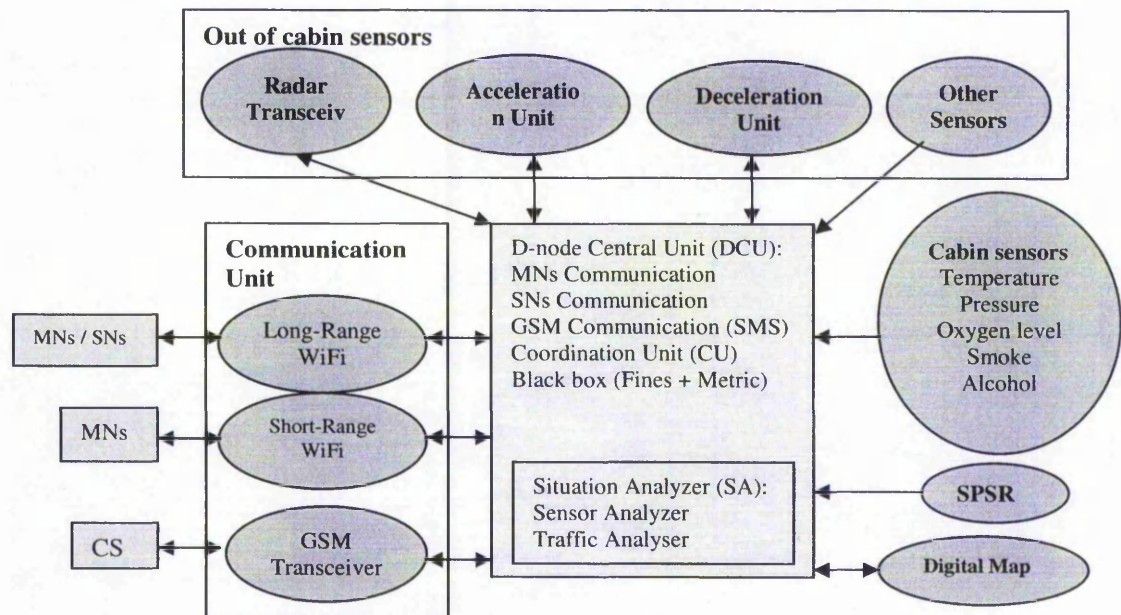


Figure 3.3 Schematic views of an ADAS-equipped MN internal components and flow of data

It is worth to mention that some vehicles like buses and trams can act as a powerful server and data repository and carry valuable traffic data, because of:

- Using pre-defined route
- Following a schedule
- Regularly stop in defined locations

3.3 VehINet and New Services

Various applications have proposed for IVC systems [36] and VRN [37]. The VehINet in transaction with road-base networks provide following services in three categories:

1. Services based on VVN includes:

- Assist drivers to avoid and prevent collisions
- Routing information such as road blocking or accidents ahead
- Intelligent shortest path finding

- Friend finding through chatting by passengers
- E-advertisement

2. Services through bridging with VRN includes:

- Auto emergency services instead of phone calls
- Routing information
- Mature shortest path service
- Car park finding
- Tracking vehicles or fleet by related corporate or police
- High-speed tolling
- E-advertisement

3. Services to LU in stationery state by VehINet or through VehINet includes:

- New type of emergency services instead of cellular phone calls
- Routing information
- Location based information e.g. for tourism purposes when they passing by sites
- Tracking mobile devices
- Streaming service like Telephony
- E-advertisement

LU services are not concern of this research and the project only focuses on the first two services. By removing common applications in each group, the services can be summarised as:

- A. Incident warning
- B. Traffic Route warning
- C. E-advertisement and emailing
- D. Vehicle tracking
- E. Telephony

The proposed model is also applicable in military applications like MIMICS project [38] to platoon intelligent unmanned vehicles and Cisco 3200 mobile router for military communications.

3.4 VehINet Communication System and Available Technologies

Our system consists of two separate networks - an Ad Hoc and a volatile, loosely connected wireless network. These mobile networks inherit the bursty unpredictable characteristics of mobile networks, which affect the standard OSI protocol stack, such as:

- Coverage and Handover
- Low bandwidths
- Compromised QoS
- Compromised Security Encryption techniques
- Low power devices
- Nomadicity and coordination detection

Each MN has two communication units.

- Short Distance Communication Unit (SDC) for MNs-MNs data exchange
- Long Distance Communication Unit (LDC) for MN-MN and MN-SN data exchange

Using two communicational systems help to:

- Improve the reliability of SDC system and protect its real time specification
- Increase the system robustness and cover more distance in roads and highway
- Diversify services (in LDC area)
- Efficient cooperative routing

From LDC point of view, MNs act as a:

- Thin clients for driver and
- Client for passenger requests like Internet access through LS or direct communication with MN
- Server for LS and MNs requests
- Bridge (router) to server handheld requests through LS

Hence technically, target system has following type of communications:

1. SDC (MN-MN), for broadcast-based core services (safe navigation and accident warning)
2. LDC1, LDC (MN-MN) for broadcast-based core services instead of SDC tasks in longer distances
3. LDC2, LDC (MN-MN) for unicast-based add-on services
4. LDCAP, LDC (MN-SN or MN-MN-SN) for unicast and multicast-based add-on services through AP

The first three IVC are the sole services of VehINet for internal use (based on Vehicle-Vehicle). The core service in SDC and LDC1 requires following specifications:

- System must respond to messages in specific time needed to prevent accident by break or change in direction.
- System must work independently without information from road-base networks
- System must work automatically without driver control
- Due to lack of reliability of air medium, to satisfy the required timing, system must completely test for all conditions before launching.

The proposed requirements for each category would be:

SDC requirements:

- Short transmission range (50-100m)
- Low latency messaging interval 20ms
- Short packet size (<100 byte)
- Periodic 1-hop directional geocasting
- Tackling 100km/h relative velocity

LDC1 requirements:

- Long transmission range to 200m
- Messaging interval ≤ 50 ms
- Short packet size (<100 byte)
- Periodic 1-hop directional geocasting

LDC2 requirements:

- Adaptive radio range = 300m

- Directional unicasting (=Point-to-Point communication (P2PC))
- Delay performance of 50ms for voice application (time to reception \leq 100ms)
- Adaptive data rate
- Multi-hopping should be possible

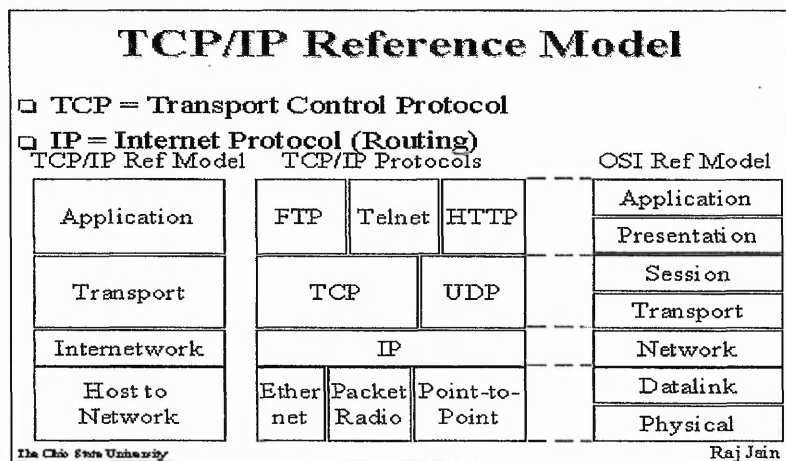
LDCAP requirements:

- Radio range = 300m
- Channel management and bandwidth partitioning
- Directional unicasting / multicasting
- Omni-directional geocasting (for alarm messages)
- Enough bandwidth for to serve MNs, here delay performance of 50ms for voice communication
- Adaptive data rate
- Multi-hopping (2-hop) should be possible

The most important factor in system effectiveness is time to receive packets. For example with 70 mp/h node-speed (112.63 km/h = 31.28 m/s), one second delay in decision-making costs 31m; therefore the system must react in milliseconds. Cartalk2000 suggest 10ms messaging for 200km/h. Research suggests 25-50ms messaging interval for covering majority of accidents. It is worth mentioning, that the time to reception is another factor which affects the aging of the messages. A value more than twice of the intended interval can endanger the system precision.

The suggested packet size of 50-byte is big enough to house node necessary information such as: transmitter id, timestamp, type of message, coordination, road and lane id, speed, brake status, indicator status, acceleration status, steering status and angle, vehicle id (type and class). A 100-byte packet size can include two nodes situation, node itself plus another node. Adaptive radio increases the load of LS and is not preferable for LDCAP.

All available communication technologies to fulfil communicational requirements use TCP/IP layers (figure 3.4). For real time application such as VehINet some level of integration between layers is mandatory and application can exist in all layers above physical layer. This integration also improves the speed of the system.



4

Figure 3.4 TCP/IP in compare with OSI model [39]

3.4.1 Wireless Standards in Layer One and Two

To secure the core service real-time objectives, the research suggests using two radio systems in physical layer (in MNs). This separates the traffic of two networks, reduces the radio interference and packet contention.

Air media in comparison with wired medium has some drawbacks which can limit the bandwidth such as:

- Time-varying channel (time-shifted signal) - signal power varies due to multi-path propagation.
- Half duplex data transfer

The first can be controlled by adaptive transmission power and the second can be solved by directional antenna. The advantages of directional antenna include:

- Better bandwidth managing by preventing flooding in all direction
- Full duplex communication is possible by applying two cards (first two layers)
- Solve the hidden and exposed node issues due to directing the traffic flow

Note that directional antenna will reduce the field of view and increase cost of system development.

The radio communications in Ad hoc mode has evolved through IEEE standards and WiFi technology (802.11abg). WiFi systems are first candidate to give services in

WMAN models [40, 41]. The research is aiming to use WiFi standards for VehINet, 802.11a for SDC and 802.11g for LDC. Using license free frequency band (ISM) is the advantage of both methods, which reduces the cost of network implementation. The research does not suggest using 802.11 as an over the counter solution because lots of modifications are needed such as MAC modification to have a location aware system.

The negative point of first one is short coverage and the second standard is being limited to three channels. Also using 2.4GHz frequency which is already used by Bluetooth devices makes 802.11bg unreliable for LDC. The probable solution is using two lower channels of 802.11 for LDC in other unit.

Using WiFi standards for VehINet is not a straightaway solution. Based on the fact that these wireless standards has primarily build for office and fix point use, it is not possible to directly apply them for high mobility MANET without any modification. For example, IEEE 802.11a has enough channels (12) to handle packet communication but 10ms beaconing broadcast needed for 0.5m position accuracy tolerance in 200km/h [42], easily saturates the channels, incurring missing packets and throughput loss.

In SDC system, the flow of meaningful packets is in counter-direction of MNs move (coloured arrows in figure 3.4). Using two directional antennas for each node separates the flow of data for sent and received packets. This makes it possible to broadcast to selected recipients and has the following advantages:

- Availability of all bandwidth for transmission or receive
- Elimination of the produced noise by nodes in same direction as major factor to reduce contention
- Reduction of noise generated by nodes in opposite direction

The maximum 6cm wavelength of radio in 802.11a makes it possible to define two directional antennas in each node, Receiving antenna (Ra), at the head of node and Transmitting antenna (Ta), at the back of MN. Although this approach makes the design more complicated, it isolates the incoming and outgoing traffic of data. Directional antenna also decreases the radio interference and unwanted packets in two-way roads but it does not remove them completely (Red arrows in figure 3.5).

The effect of directional-antenna is very important in open areas like roundabout where the number of links grows exponentially and in the dual carriage ways.

In two-way road the noise level would be more for nodes in speed lanes. By limiting the view angle of antenna the performance increase but it makes some blind areas on left and right side of the nodes.

Range of antenna also can increase the interference and makes redundant packets in the flow. The transmitted data is useless (noise) for nodes far from origin node. The effective transmission range is node distance which rules by node speed (high speed by default means nodes are far from each other).

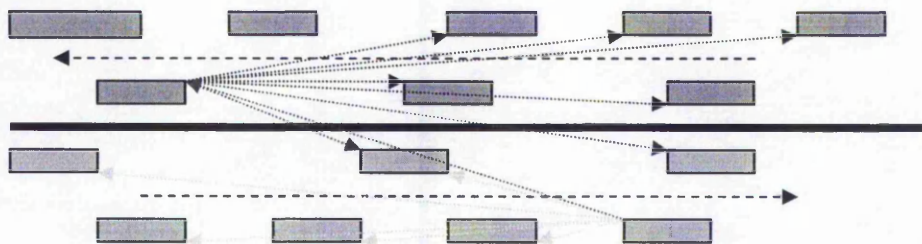


Figure 3.5 Role of direction antenna in decreasing the redundant packets in two-way road (dashed lines show the driving direction and red arrows present the unwanted noise on vehicles on opposite lane)

There are also two nascent technologies for high mobility broadband wireless access in licensed band, 802.16e (2 – 11Ghz in 120-150km/h range) and IEEE 802.20 (0.5-3.5Ghz in 250km/h range). The second one seems more suitable for above applications but both are in preliminary development stage. IEEE 802.16 in high frequency (line-of-sight) is suitable for NetF backbone (yellow lines in figure 3.2).

The UMTS (3G cellular) is a parallel technology to provide LDC services but:

- UMTS has lower data rate. It theoretically works in 128Kbps, 384Kbps and 2.05 Mbps respectively in fast moving state, slow moving state (walking) and stationary state [42]. In compare, VehINet expects to work in 2-11Mbps (moving state) and 54Mbps (stationary).
- UMTS use expensive cellular infrastructure in licensed bandwidth but VehINet use free ISM spectrum.

3.4.2 Network Layer and Routing

The function of this layer is closely related to two lower layers and specifically MAC layer. Network layer has following functions: address translation, select routing strategy based on ToS, neighbour discovery based on map and GPS and location service (send data in right direction).

IP address is a logical unique address and consists of two parts, network address and local address (host or machine address). In TCP/IP, the IP uses instead of MAC ID (48 bit Ethernet address) to better manage address and billing customers. In a local network, Address Resolution Protocol (ARP) is use to map local IP addresses to Physical address or MAC address).

Due to inability of IP in mobile scenarios, Mobile IP (MIP) has emerged as a solution to handle Layer 3 mobility of a roaming node without service disruption. It supports transparency above IP layer and executable on cellular and WLAN. MIP assigns to MN by LS during communication and should be kept until end of communication. It is essential that each MN has a home address too.

By referring to figure 3.6, the server has several levels to authenticate the mobile user and protect the MIP signalling messages:

- Mobile node with home agent
- Mobile node with foreign agent
- Mobile node with AAA infrastructure

Visiting a public WLAN spot...

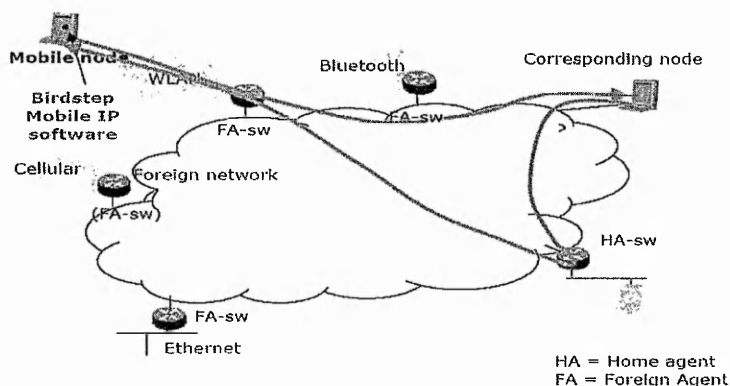


Figure 3.6 Connect home agent through foreign agent [43]

Assigning MIP is a time consuming task and having a home address is redundant for the people who use this system. In practice, although Mobile IP brings flexibility of service (no need to manually reconfigure for connection to a new network) and security through authentication but has following disadvantages too:

- Connection delay to connect mobile device to Internet through its registered ISP
- Each ISP needs an agreement with other networks to give this service and due to this not all network support Mobile IP.
- In some proprietary networks like Military and NASA using two IP is not favourable due to security issues.

MIP only supports the mobility where a mobile node is one hop away from the router. The challenge is to accommodate MANET subnets in such a way that a MANET node, which may be multiple hops away from a router, could be accessed from anywhere. The migration of mobile nodes into and out of MANETs is catered while maintaining connectivity.

For core services based on VVN using IP is unnecessary. LDC services can use IP to get Internet services due to popularity of TCP/IP standard. In general, this standard is not suitable for mobile devices due to its overhead. Research suggests using MAC address instead of IP to reduce the complexity of system. MAC address can translate to virtual IP address in LS to keep the system compatible with Internet services. NanoIP [44] is another solution to replace TCP/IP layers. Figure 3.7 shows the NanoIP stack and the gateway required for VRN protocol translation.

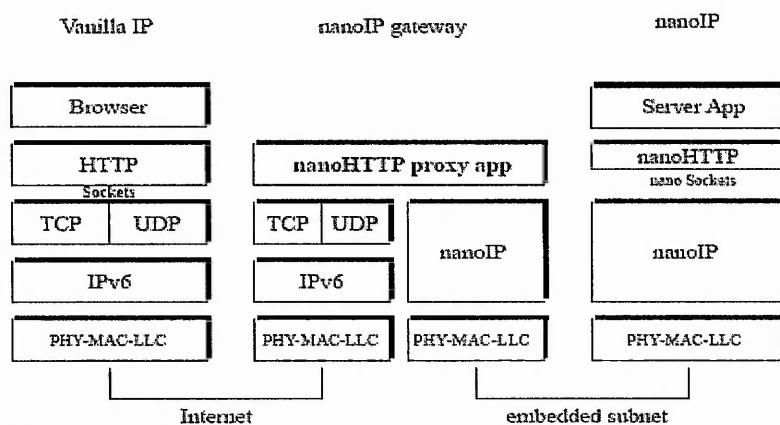


Figure 3.7 The stack of NanoIP gateway [44]

3.4.2.1 Positioning Systems

MN use position information to reference coordination and analyze the situation to find the probability and seriousness of hazard for core services. It also helps to detect and filter the correct data packets (packet from node ahead). Then positioning is a must to interpret SDC messaging and each data packets in SDC and LDC1 should carry a field for coordination. Positioning in LDC2 and LDCAP has major role in routing service. The importance of precise coordination and map quality in communications is measured in [45].

The basic methods for positioning based on two fix points are triangulation and trilateration. Based on the infrastructure systems the positioning system in open area includes:

- Network base – generally by measuring the signal strengths of AP like Nibble system [46].
- Satellite base – by triangulation with 3 or 4 satellite

Network base methods implemented by cellular systems such as GSM and Mobile Positioning System [47] have low precision (Table 3.1) and not useful in VehINet.

Name	Category	Tracking/ Positioning	Mechanism	Medium	Precision
GPS	Satellite	Positioning	TOA	Radio	25 m
DGPS	Satellite	Positioning	TOA	Radio	3 m
WAAS	Satellite	Positioning	TOA	Radio	3 m
Active Badge	Indoor	Tracking	COO	Infrared	Cell
WIPS	Indoor	Positioning	COO	Infrared	Cell
SpotON	Indoor	Tracking	Signal Strength	Radio	3 m
Active Bat	Indoor	Tracking	TOA	Ultrasound/Radio	0.1 m
Cricket	Indoor	Positioning	TOA	Ultrasound/Radio	0.3 m
RFID	Indoor	Tracking	COO	Radio	Cell
Visual Tags	Indoor	Both	Video	Optical	Depends on camera resolution
GSM	Network	Both	COO, AOA, TOA	Radio	Cell, distance in 555 m steps
MPS	Network	Both	COO, AOA, TOA	Radio	150 m
Nibble	Network	Positioning	Signal Strength	Radio	3 m

Table 3.1 comparison the positioning systems precision [11] (COO: Cell of Origin, TOA: Time of Arrival, AOA: Angle of Arrival)

The best off-the-shelf tool for node location is satellite positioning system (SPS) used in vehicles navigation system [48-50]. One-way communication mechanism of GPS with CDMA brings two types of services:

- Precise Positioning Service (P-code) in 1227.6MHz and precision with 22m horizontal and 27.7m vertical precision
- Standard Positioning Service (C/A code) in 1575.42MHz with 100m horizontal and 156m vertical precision

The Differential GPS (DGPS) and Wide Area Augmentation System (WAAS) are two current systems for correction the GPS precision by the help of base station (figure 3.8 and 3.9). The precision of DGPS is getting to 1-3m.

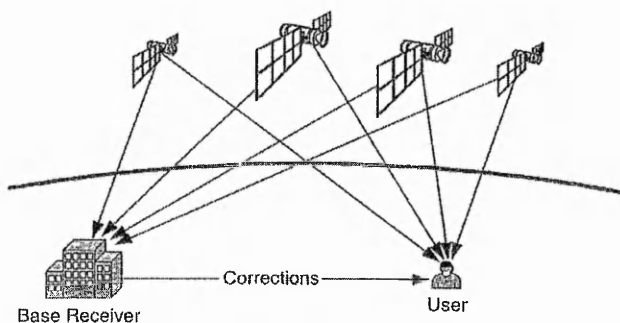


Figure 3.8 DGPS mechanism to improve GPS precision [51]

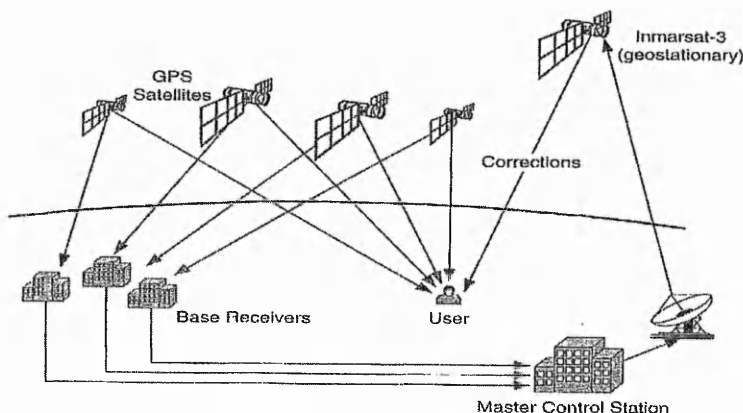


Figure 3.9 WAAS mechanism to improve GPS precision [51]

By referring to table 3.1, the best precision in DGPS and WAAS is 3m but GPS also influence by following factors:

- Clock rate: with all precision makes 1.5m error
- Fluctuation of the orbits: caused by gravitational forces of sun and moon (2.5m)
- Disturbance of the atmosphere: weather pressure (0.5m)
- Disturbance of the ionosphere: signal spreading by particles (5m)
- Multipath error: by reflected signals (0.6m)

Irrespective of SPS lack of precision, it cannot respond to the following events which also cause raising false alarm by situation analyzer:

- In overpass and underpass situation
- In mountainous road (how MN interpret a packet from nodes above of it?)
- In tunnel and in high-rise buildings area (canyon effect)

Then auxiliary methods should be combined to correct navigation (figure 3.10). The correction module is responsible to calculate and correct coordination to cover the gap of SPS precision and unavailability in above cases. The following fusion method functions by referencing previous position and monitoring speed and change of direction. Monitoring the age of received nodes is another auxiliary method [75].

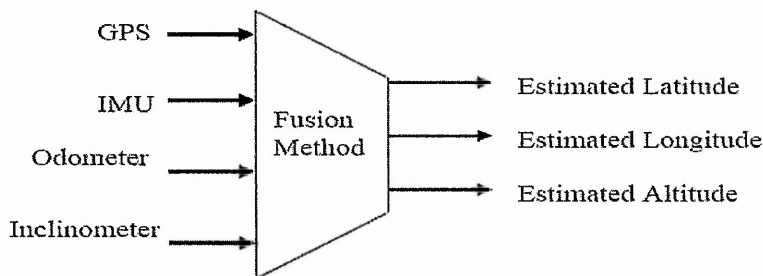


Figure 3.10 Coordination adjustments by odometer, inclinometer and Inertial Measurement Unit (IMU) [52]

3.4.2.2 AP Layout and Proposed Relaying

There are two approaches for SN implementation:

- Make SNs as intelligent as possible or in other words use only AP. This method accelerates the service speed but has drawbacks such as:
 - Expensive to implement, due to the huge number of LS caused by limited range of wireless communication
 - Heavy cost of maintenance and lack of flexibility for upgrade
- SNs consists of multiple relays (repeaters) connected to AP

The later is the approached selected in our model. SN is an intelligent hub (transceiver), as a point of interconnection between the WLAN and fixed wired network.

AP Distribution follows the similar pattern of cell phone antenna (density based on population and nature of terrain) but here the factors defining the size and shape of cell are more such as:

- Traffic model (one way, two way, roundabout, cross roads)
- City layout and street structure (old style or Manhattan)
- Number of LS

Based on the number of roads around intersection and using directional antenna, usually three to six antennas (normally four) is required in each relay point. The switch connects satellite APs to main AP (through LOS beam) which itself is connected to local server through wire. Implementing Relay Station (RS) is a solution to reduce infrastructure deployment cost (figure 3.11 and 3.12).

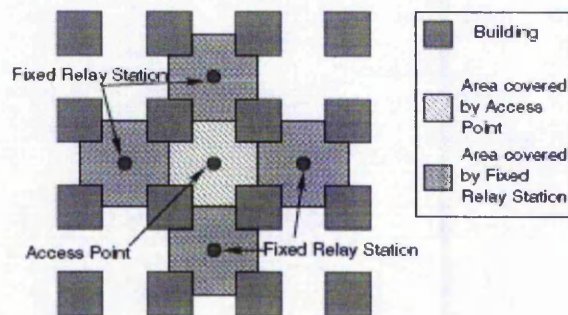


Figure 3.11 Schematic view of 2-hop cell in Manhattan scenario [53]

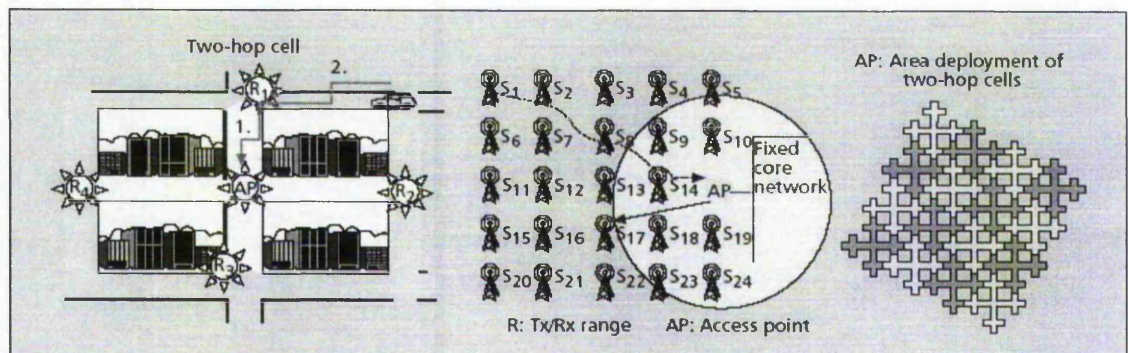


Figure 3.12 Left: a Manhattan city scenario with one AP and four RSs covering the shadowed areas around the corners shown in grey. Middle: a schematic view of the scenario. Right: wide-area coverage using the basic element (left) and two groups of frequencies [54]

The fix RS should be decode-and-forward node (repeater or bridge) to filter the noise. In this case, if we suppose four relays have connected in Line-of-sight (LOS) to AP and each relay consists of 4 antennas (AP has 4 directional antennas too) then each AP should serve 20 flows of data. By assuming that 20 vehicles request service on each

flow then AP ideally should manage 320 requests. If AP responds to WMAN requests by laptop and handheld users, then the requests are more diverse and require a very powerful AP. This is only an ideal scheme and in fact not every MN uses the system in the frequency of cellular systems. If half of the MN request traffic information, the system should have a provision of a one server for 10 AP.

Deploy multiple relaying (cooperative relaying) or using more than two hops (RS+AP) is also possible (figure 3.13) but it can increase the response delay in peak time and endanger the ITS core objectives. MAN services with streaming applications and Mobile IP roaming maybe needs a very smart and powerful AP such as a computer station.

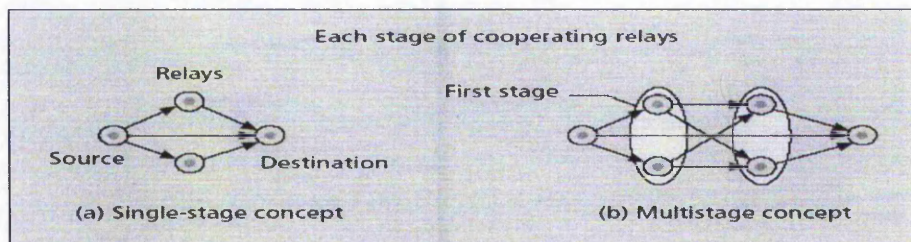


Figure 3.13 The concept of cooperative relaying [55]

Mesh networking approach ensures an even distribution of bandwidth over large areas but in WiFi it requires lots of AP. This area has researched more in WMAN area and among different layouts, Structured Mesh provides a cost effective method in comparison with cellular meshed deployments. Different experiences such as test in US Air Force Lab support cost advantages of 3-radio Structured Mesh at least 64 times over cellular [56].

In cellular network subscribers have nearly no role in handoff and only base stations dealing with handover but in our case every node has a table of base stations, which helps to reduce servers roaming cost.

Soft handoff technology (zero connections interrupt) used by CDMA systems is not ready made feature for contention base WiFi. In CDMA, all repeaters use the same frequency channel for each mobile phone set, no matter where the set is located. Each set has an identity based on a code and because no change in frequency (as in FDM) or timing (as in TDM) occurs as a mobile set passes from one base station to another, there are practically no dead zones.

In theory by allocation of 1Mbps bandwidth for each MN an AP with 54Mbps transfer rate can serve up to 54 users in 400m safe range. It is preferable to have 4 AP with 4 corner directional antennas to cover cars around a typical crossroad (each AP directly connected to LS). If we include 100m overlap then the distance of two AP in different pylon should not exceed 800m.

Handover mechanism is specified in MAC layer of 802.11 and the procedure consists of three phases:

- Detection (discovery of the need for handover)
- Search (acquisition of the information needs to do handover)
- Execution (consist of authentication, re-association and handover)

	D-Link 520	Spectrum24	ZoomAir	Orinoco
Detection	1630 ms	1292 ms	902 ms	1016 ms
Search	288 ms	98 ms	263 ms	87 ms
Execution	2 ms	3 ms	2 ms	1 ms
Total	1920 ms	1393 ms	1167 ms	1104 ms

Table 3.2 Handover time for different IEEE 802.11b cards [57]

Handover time can be reduced by applying following methods:

- Overlapping detection and search phase
- Optimize beaconing (60ms suggested in [57])
- Using another channel for search phase during transmission to eliminate this phase completely
- Active scanning
- Pre-authentication

The first two modifications are possible in VehINet but the rest can waste the bandwidth. Regarding node speeds, handover happens very frequently and it is a sensitive issue for LDC. It needs proper attention and buffering in servers to avoid loss of packets.

3.4.3 Transport Layer

SDC generally counts on small packets and needs no service guarantee. It selectively broadcasts small packets of data in specific direction with UDP protocols. CarTalk2000

[21] estimates the probability of UDP packet loss in this method is negligible (10^{-8}). In SDC, due to the short lifetime of packets and also for better analysis of the situation, packet hopping is limited. Forwarding packets can be managed by hopping byte and nodes intelligent filtration. The exception is Emergency Packets (EP) with longer life time and less filtration. The EP should propagate in both directions and for LS destinations (LDCAP). Due to increase of the system precision each node dedicates part of its bandwidth to route other nodes messages (two messages in one packet).

In comparison with SDC, LDC needs routing and has more sophisticated transport protocol. MNs keep and update a list of the MNs ahead, which is extracted from the received packets. This Routing Table (RT) helps to multi hop for LDC through MNs. Data packets implicitly bring information for MN about traffic flow based on MNs attributes like coordination and speed included in packets. The digital map helps to better interpret the above data. Filtration should happen to update the RT based on MNs in the same direction of move.

In normal conditions, when SDC system is enabled, LDC uses routing data obtained through:

- SDC RT, which keeps nodes ahead coordination and speed
- Updatable list of SN coordination
- Dynamic and static beaconing (depends of mobility) to recognize MNs for multi-hopping especially in area with poor AP access

In this case, only backward route discovery by LDC (through directional antenna) completes the neighbourhood table. In general cases, the data packets disseminate in opposite direction of the move except for:

- EPs, due to their importance for cars in opposite direction.
- Military and reconnaissance mission applications (through LDC).

Limited LDC multi-hopping is essential because intensive trust on AP would saturate the system capacity. Meanwhile multi hopping increase the node numbers on AP can cause system unreliability which gets worse due to blocking effect of buildings

When vehicle approaching an incident with blocked vision due to road curvature, buildings around or road nature (like hill), the communication is possible through MNs moving in opposite direction (by forwarding EP) or nearest SN.

Due to diversity of services based on LDC, it needs a hybrid transport protocol to treat the services differently.

TCP is the widely used transport protocol for Internet. Using TCP for wireless environment without modifications is impossible. For example TCP normally treat dropped packets as an indication of network congestion, and therefore throttle transmissions until lost packet is detected (by managing sequence numbers). This is the wrong strategy when packets are corrupted by transmission over a noisy wireless channel, because for such packets immediate retransmission is much better than delayed retransmission.

Due to limited packet hopping (2-hop) to utilize the air media, sequencing in TCP is less sophisticated in VehiNet. Then a simplified TCP is needed for MN-MN or MN-SN communications such as TCP Lite, Reno and Tahoe algorithms.

3.4.4 Application Layer and Service Modes

The Application layer in our system combines the function of all three layers above Network layer. The services are different based on the mobility of users. VehiNet users categories based on their mobility as:

1. High-mobility users -Vehicle drivers and passengers
2. Low-mobility users- Pedestrians using hand-held device such as mobile phone and PDA
3. No-mobility users – Travellers using Internet, ITS controller, fleet and freight admin

The following services can develop based on the proposed architecture:

- Core services - short messaging with real-time nature through SDC and LDC1
 1. Emergency accident information
 2. MN status declaration for better navigation (accident prevention and avoidance)

- Add-on services includes WMAN services (or Internet) and ITS through LDC2 and LDCAP
 1. Dynamically SP finding and bypass traffic jam
 2. Smoothing traffic issues (not enough speed to pass the crossroad)
 3. Parking hunting
 4. Promotion advertise for hotels, restaurants, shops, Gas station
 5. Light Internet-based services

Core services have automatic characteristic and work without drivers or passenger's intervention or request. Some of Add-on services have the same nature (refer to Figure1).

The classification of VehINet services based on the bandwidth is:

- Very light applications (small messaging)
- Light applications (email and HTTP)
- Middle weight applications (Voice, sound streaming)

The mechanism of the first one through SDC and LDC1 is intelligent pushing data (passive data receiving) [59] but for the rest through LDC2 and LDCAP, pulling data is also the nature of application.

Applications require high bandwidth like file downloading is not supported in dynamic mode. In other word, system prevents such downloading until getting to stationary position but Internet access for passengers is part of the requirements.

The research discusses the limitation of each service type and brings suggestions to overcome shortcomings.

3.5 System Feasibility

Previous study on technological advances proved the feasibility of this research and some project achievements in this field support part of our findings. Here the research has applied to the simulator environments of QualNet [60] and (OPNET) [61] to test the capacity of system infrastructure for launching the aforementioned services.

QualNet is a commercial version of GloMoSim (Global Mobile Information Systems Simulation Library), a simulation environment for wireless network developed on C language originally in University of California, UCLA. One of the main features of QualNet is configuring and editing network properties out of simulation GUI environment. It also provides flexibility to run tests in batch mode.

In comparison with QualNet, OPNET has better tools to make Graph and charts out of resulted data. OPNET designer is a specific tool to design and make the customize protocols. The research aimed to implement a MAC protocol to work with directional antenna in OPNET.

Note that simulation environment dictates some restrictions to the model. For instance, QualNet simulation environment forces the following restrictions:

- Unsupervised use of directional antenna or smart antenna. In smart antenna, directional transmission mechanism is controlled by simulator e.g. the nodes can dynamically change the antenna focus in one of eight fix map-related directions but our scenarios need two antenna (one for receive and one for transmit) with nodes-related direction (north and south of MNs).
- Restrictions for manipulating beacon message, needed for SDC communication
- Difficult to simulate broadcasting (node by node application assigning needed)
- Dynamic change of transmission range is not possible
- Testing two radios for each node in one scenario is impossible

Then modelling system faces following challenging issues:

- Testing with omni-directional antenna is not precise and faces lots of redundant data
- Filtering transmitted and received packets are difficult
- Testing the relevant received data is difficult and needs manual process
- Configuring directional antenna is difficult specially for crossroad scenario

Fore better metering the performance, the following factors discarded in the simulation tests:

- The effect of manmade structures in the city that make

- Obstruction for SDC
- Multi-path noise for LDC
- The limited range of transmission
- Multi-hopping

Here, the SDC and LDCAP systems are tested separately but the research believes that a hybrid test can improve the results especially for LDCAP (by using SDC RT). Feeding the satellite position information to nodes to emulate the real model and experiencing position based routing for LDC1 and LDCAP are among the next steps in this research.

Due to the differences in behaviour of system when vehicles have low-speed (stop-go) and high-speed [62] and based on the side-effect of nodes in opposite lanes the following scenarios candidates for simulation:

- Crossroad scenario (figure 3.14) as a platform for SDC and LDC test in low-speed (5-13 m/s = 30mile/h) with 1second pause
- Motorway scenario (figure 3.15) as a platform for SDC test with directional antenna in high-speed (10-32 m/s = 70mile/h)
- One-way road scenario as a platform for SDC test without noise on Ta in high-speed

In some scenarios, stationary models have been used as a baseline to benchmark the performance of system in move. Nodes have predefined IP address and communicate without SPSR, SDC RT and multicasting used instead of broadcasting.

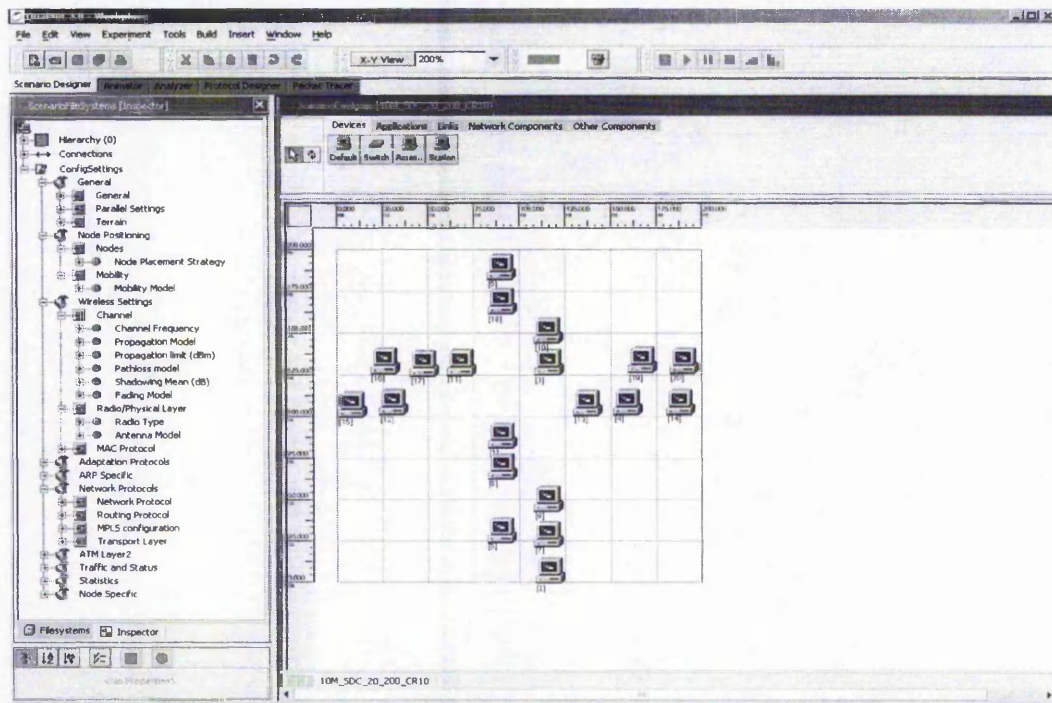


Figure 3.14 Crossroad scenarios in QualNet to test SDC/LDC between 20 nodes in low speed ($5\text{--}13\text{m/s} = 11\text{--}30\text{ Mile/h}$) with random 1 Sec pause in $200 \times 200\text{m}$ area

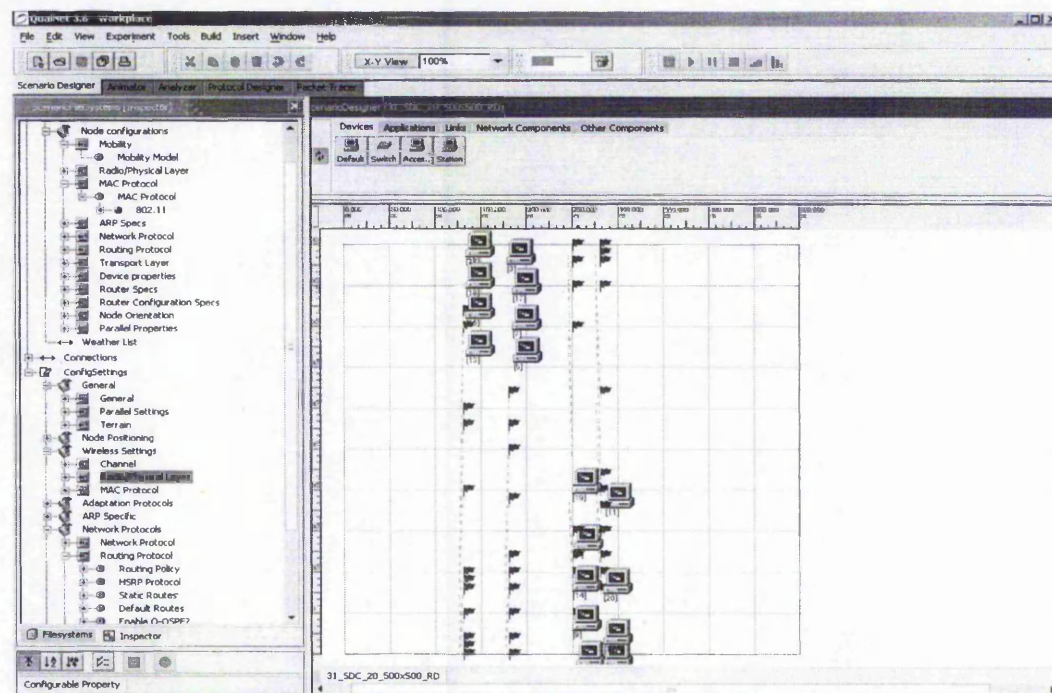


Figure 3.15 Two-way road (motorway) scenarios in QualNet to test SDC between 20 nodes with directional antenna in high speed ($10\text{--}32\text{m/s} = 22\text{--}71\text{Mile/h}$) in 500m road

3.5.1 SDC Simulation Test

Functionally, SDC and LDC1 deliver the same service through different communicational system. The selected channel frequency for the first one is 5GHz and

2.4GHz for the LDC1. Fix data transmission range (370m) and fix data transmission rate, 6Mbps and 2 Mbps, have selected for SDC and LDC respectively.

In comparison with SDC, LDC1 transmits in longer intervals which yields lower throughput but the range of communication and vehicle distance can partly justify this time-gap for real-time services. The research expects higher performance in synergy of two communication systems especially for LCD services but projects assume that each sub-system should work autonomously.

Here a calculation to find the capacity of the media has explained. To have 20ms intervals of packet transmission which means 50 times per second, the ideal throughput needed for data transfer and receive would be 10Kbps ($100 \times 50 \times 2$). By observing the ideal throughput of 802.11a means 54Mbps, then the system would have capacity for 5400 ($54 / 10$) communications in the same time without including interference. The time for receiving from the same antenna has not been included too. How many nodes can share this capacity in the same time? Based on broadcasting nature of system the number of communications increases quickly by increasing the number of nodes (n factorial), this means 7 nodes ($7! = 5040$) nearly saturate bandwidth capacity. To improve the system performance and better use of bandwidth two mechanisms are suggested:

- Limit the radio range based on car density
- Directional transmission of data

To have a realistic number of nodes in each scenario if assuming 4 lane road (2 in each direction) and each node with 2 square meter then 50m would be filled with 100 nodes ($4 \text{ lane} \times 25 = 100$) in stationary (SDC does not work in stationary). Observing space between cars, thus 50 nodes in move is a meaningful number. In LDC1 the nodes have more distance from each other and this number is justified by using longer range of transmission. 20 nodes used in simulation models to test the system before saturation point. It also makes the model configuration easier e.g. defining the waypoint for 20 nodes would be more difficult.

Note that in practice the data produced by 5 to 7 nodes ahead of MN is enough to effectively prevent accidents. Based on the field of view in directional antenna, twice of this would be the maximum communication on each node.

The first method of improving performance which is cheaper is solely possible by monitoring the node speed. However, this solution is not enough. But as mentioned before, based on the nature of communication in SDC and LDC1, in most cases only the flow in opposite direction of the move is meaningful. In few cases like emergency, the messages are sent in both directions. This makes it possible to use the second method. Directional antennas make it possible to:

- Separate the flows of incoming and outgoing packets
- Transmit and receive in the same time by having 2 units (wireless cards)

Regarding the first approach, in dynamically adjusted antenna gain, the number of flows for 4 cars in single lane is 4 (equal the number of nodes). This makes efficient distribution of data packets with less contention. Even with this solution, on two-ways roads, the other lane traffic affects the performance of the opposite lane traffic (noise on Ta). In simulations assumed that each node can hear all unwanted messages (noise) from other nodes.

The validation process is generally based on other simulations results and theoretical figures. Evaluation of simulation result with others work was difficult due to lack of publication in this field partly because of the importance of new applications for industry.

3.5.1.1 Role of Radio

The most important performance criteria are the percentage of received packet and average end-to-end delay between sending and receiving packets.

Scenario: SDC and LDC1 on 200x200m crossroad with 20 nodes

Simulation time: 30s

Radio: 802.11ab with omni-direction antenna, propagation delay 1us

RP: On-Demand Multicast Routing Protocol (ODMRP)

Node Speed: static / low-speed

Application: Multicast Constant Bit Rate (MCBR), packet size 100 byte, interval 10, 25, 50 and 60ms

To emulate the broadcasting and flooding behaviour, MCBR application has used. Each node sends 100 byte packets 500 times to other 19 nodes (with 10-60 ms interval). The routing protocol, ODMRP is a mesh-based multicast scheme and uses a forwarding group concept to scope flooding. It applies on-demand procedures to dynamically build routes and use soft state to maintain multicast group membership.

Multicasting experience depicts (figure 3.16 and 3.17 exp. 1 and 2) the degradation of system performance in low interval (<15ms). Improvement is negligible between 20ms and 50ms (figure 3.17 exp. 2 and 3). The LDC1 gets to stability in 50ms interval and higher interval (here 60ms) does not improve performance drastically (figure 3.16 and 3.17 exp. 11 and 12). The optimum interval for LDC1 should be around 50ms and 20ms for SDC.

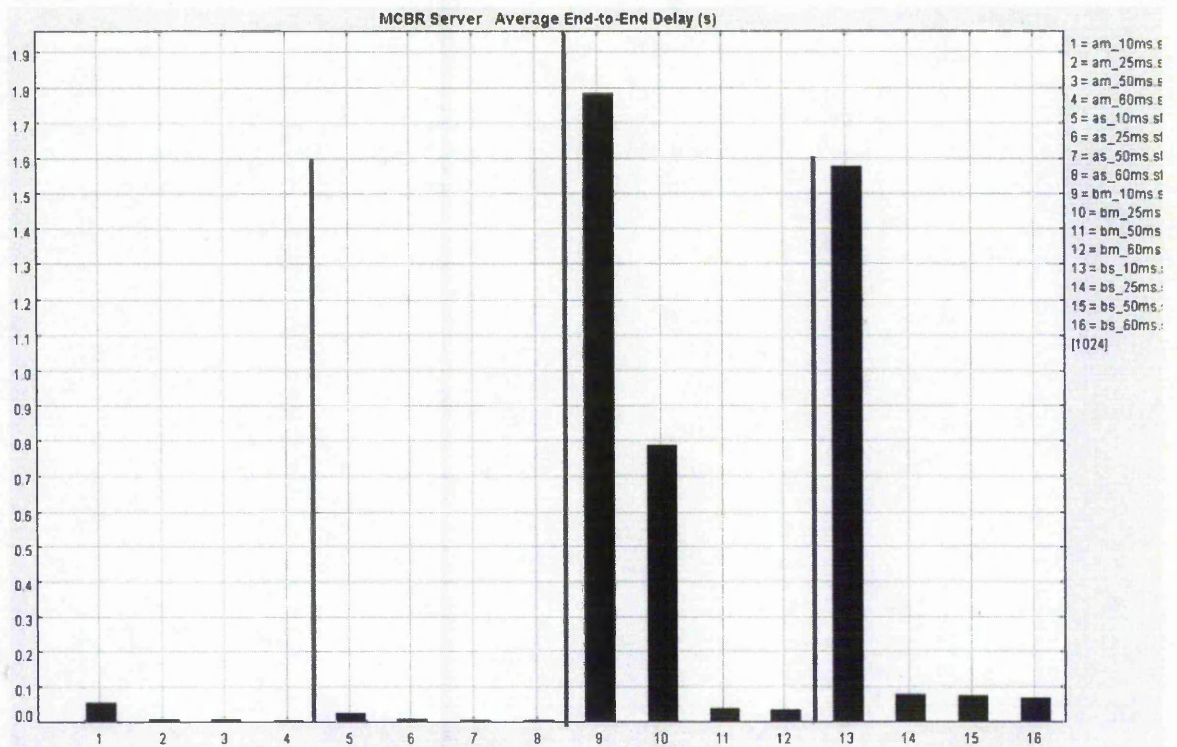


Figure 3.16 Average delay in mobile (exp. 1-4, 9-12) and stationary scenarios (exp. 5-8, 13-16) for SDC (exp. 1-8) and LDC1 (exp. 9-16)

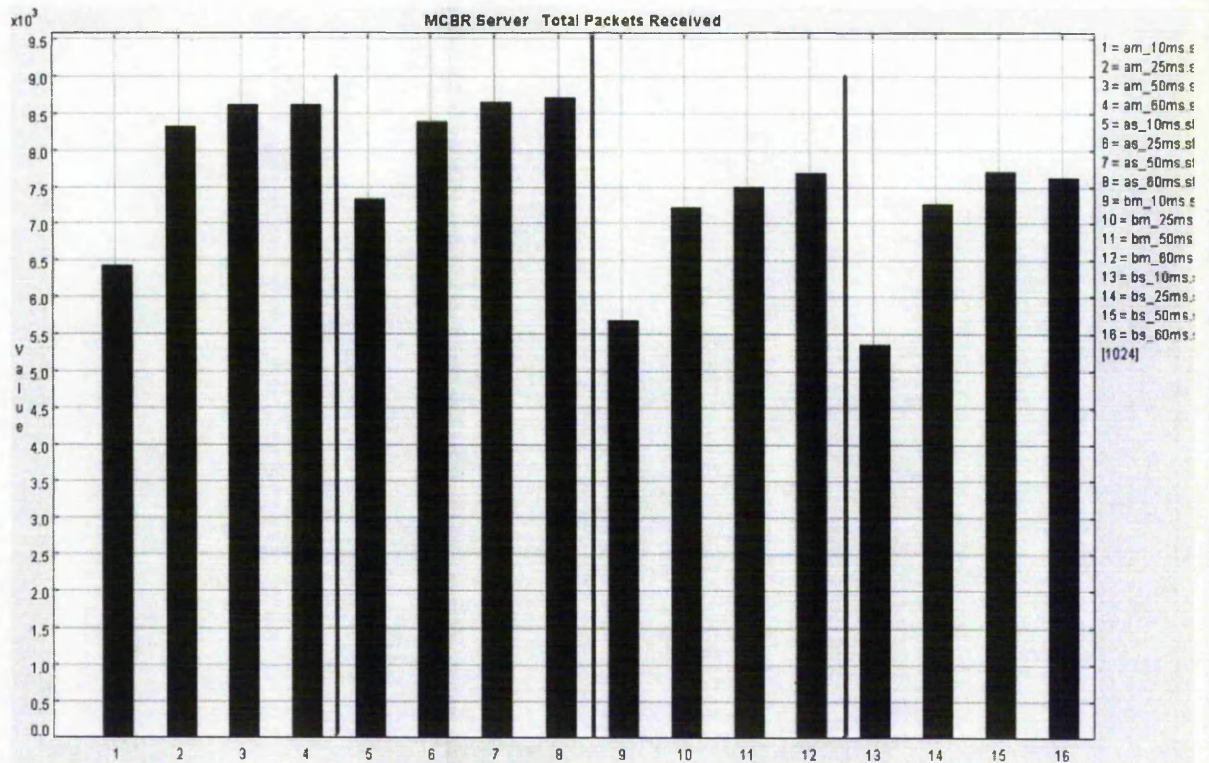


Figure 3.17 Number of packet received in mobile (exp. 1-4, 9-12) and stationary scenarios (exp. 5-8, 13-16) for SDC (exp. 1-8) and LDC1 (exp. 9-16)

This simulation shows:

- Optimum intervals for SDC is 25ms (exp. 2, 6) and 50ms for LDC (exp. 11,15).
- The performance by having reasonable interval are 84% and 77% for SDC and LDC respectively
- System high sensitivity to intervals specially for LDC

Above scenario repeated for low speed nodes with different data transfer rates, means 6Mbps and 54 Mbps for SDC and 2Mbps and 11Mbps for LDC. The 25 and 50ms interval used for SDC and LDC respectively.

The resulted figure 3.18 shows the direct role of data transmission frequency on delay performance. In both SDC (compare exp. 1 with exp. 2) and LDC (compare exp. 3 with exp. 4) systems higher transmission rate improve the delay and number of received packets. Although the delay improves, there is an optimum point (rate) which also depends on the node numbers. Number of dropped packets increase when data rates increase (figure 3.19). This proves the value of dynamic transmission range control in decreasing the noise and performance boost.

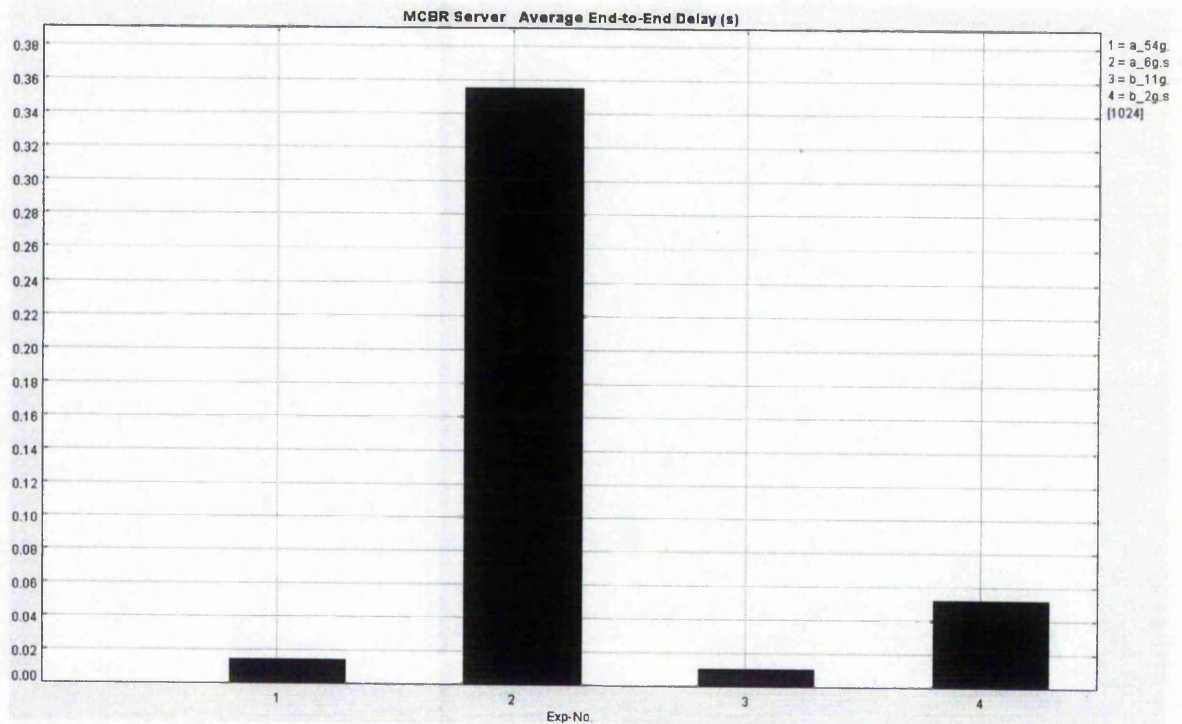


Figure 3.18 Impact of data transmission rate on delay performance in SDC for 54Mbps and 6Mbps (exp. 1 and 2) and in LDC1 for 11Mbps and 2Mbps (exp. 3 and 4)

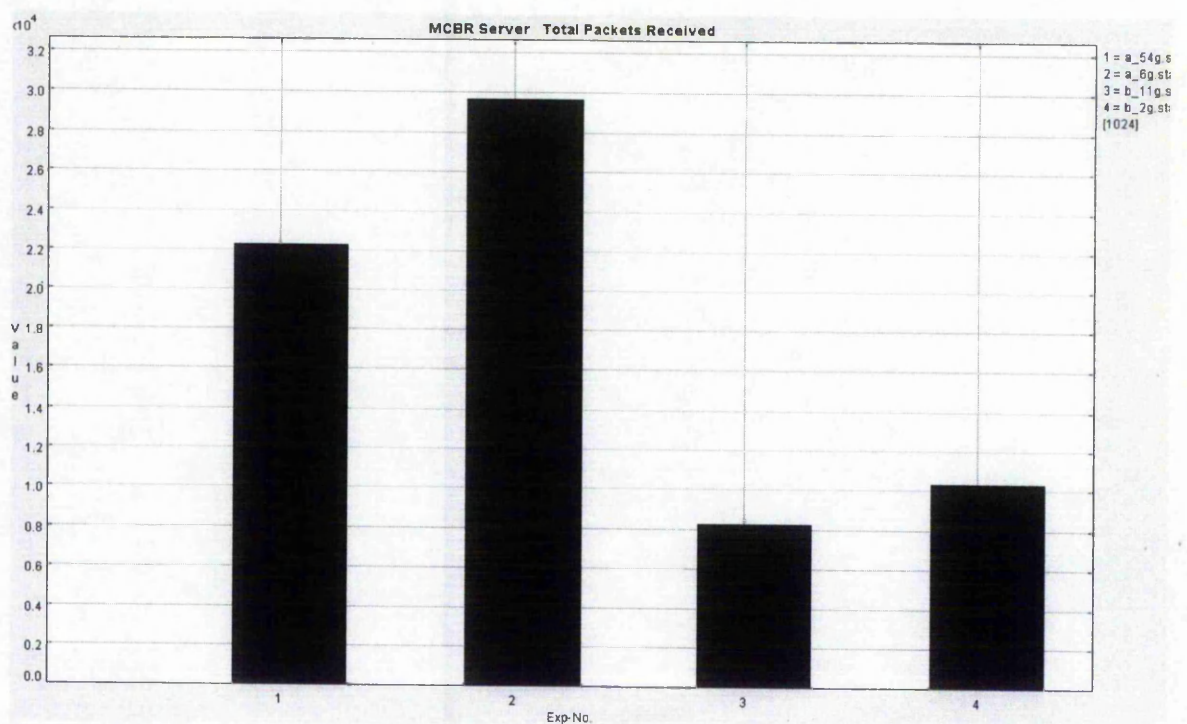


Figure 3.19 Impact of data transmission rate on packet dropping in SDC for 54Mbps and 6Mbps (exp. 1 and 2) and in LDC1 for 11Mbps and 2Mbps (exp. 3 and 4)

This simulation result proves:

- Higher data rate reduces the delay from 0.36s to 0.015s in SDC (exp. 1) but the number of received packets is also reduced
- High sensitivity of SDC system to transmission speed

- Decreases in the number of received packet (exp.1, 2) show a trade-off between this component with delay, probably due to the contention. Change in transmission range cause the same effect.
- Test with directional antenna can yield a clearer view of system capacity due to filtering the useful packets. It would be easier to find the optimum transfer rate in this case

3.5.1.2 Role of Node Speed

The simulation result in previous section (figure 3.17) shows the negative impact of speed (stop-go) on performance (compare exp. 2 and 6 for SDC and exp. 11 and 15 for LDC1). Although the mobility decreases performance but the difference is negligible.

To better check the role of performance in speed, the above scenario repeated with high speed nodes without stop. Maximum speed, 32mps, is above real world experience in crossroad, it has been selected to challenge the system endurance in open areas.

The experience with high speeds depicted in figure 3.20 and 3.21 shows the speed does not affect the system performance much (compare exp 5 with 6 for SDC and exp 9 with 10 for LDC1). The unexpected result in experience 1- 4 returns to system overflow state. Figure 3.20 shows that even 25ms is not the optimum for SDC system (exp. 3 and 4). Result also proves the validity of calculations about system performance by using omni-directional antenna and broadcast in vast area. The result concludes that node speed has minor influence on performance.

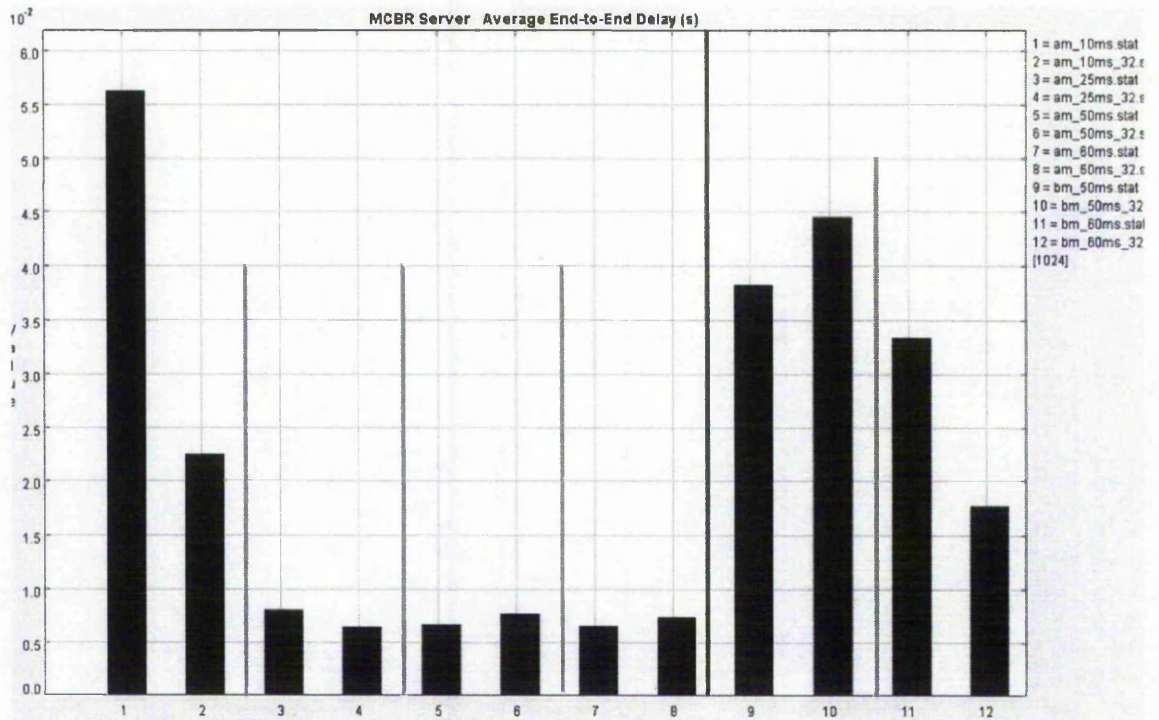


Figure 3.20 Average delay in stationary and mobile scenarios in SDC (exp. 1-8) and LDC1 (exp. 9-12)

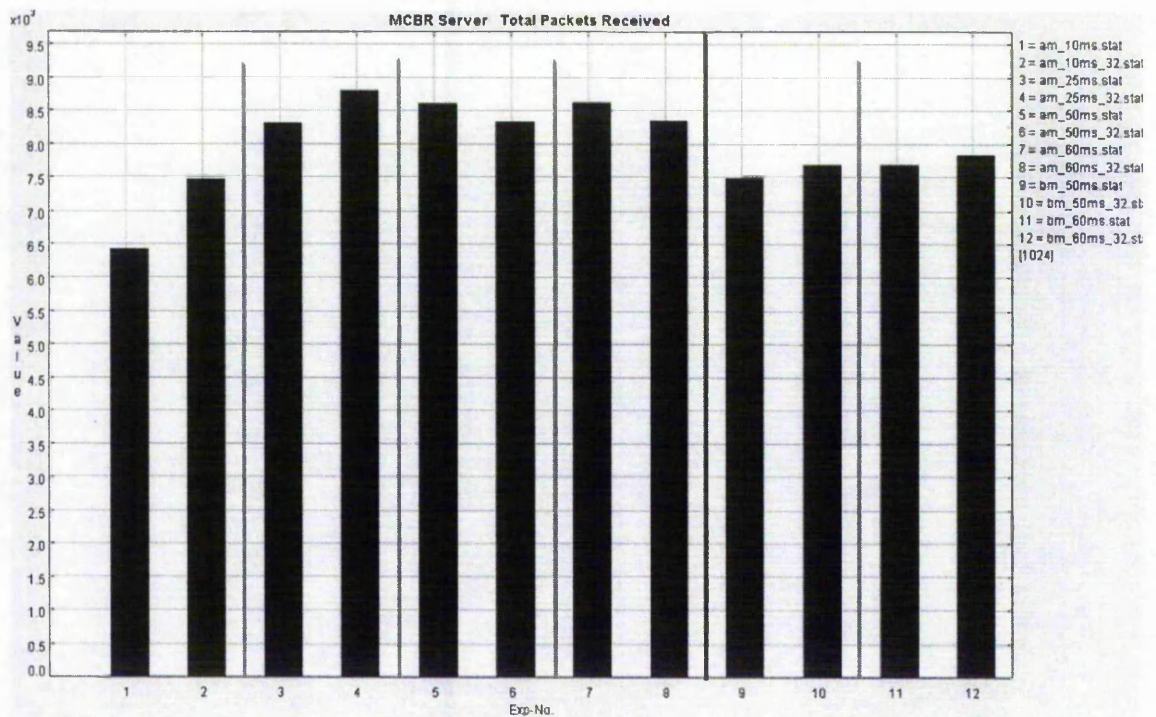


Figure 3.21 Packet received in stationary and mobile scenarios in SDC (exp. 1-8) and LDC1 (exp. 9-12)

The result shows:

- The speed of node has direct effect on delay, here from 0.006s to 0.008s in SDC (exp. 5,6 and exp. 7,8) and the number of received packets reduces 86% to 84%

- Minor impact of node speed on system performance
- Decreases in the number of received packet on exp.1-4 can be partly related to instability of system

3.5.1.3 Role of Packet Size

Following scenario consider the role of packet size in performance:

Scenario: SDC on 200x200m crossroad with 20 high speed nodes

Simulation time: 30s

Radio: 802.11a with omni-direction antenna, propagation delay 1us

Application: MCBR 500 times multicast, packet size 50, 100, 200 Byte, interval 10, 20, 25 and 30ms

Figure 3.22 shows that the packet size has a direct effect on delay and sharply reduces the number of received packets (Figure 3.23). The performance deficiency is worsening for higher intervals (exp. 3, 6, 9 and 12) in a way that even longer interval cannot compensate. The 50 bytes and 100 bytes packet size with 25ms interval yields the best performance (exp. 7 and 8)

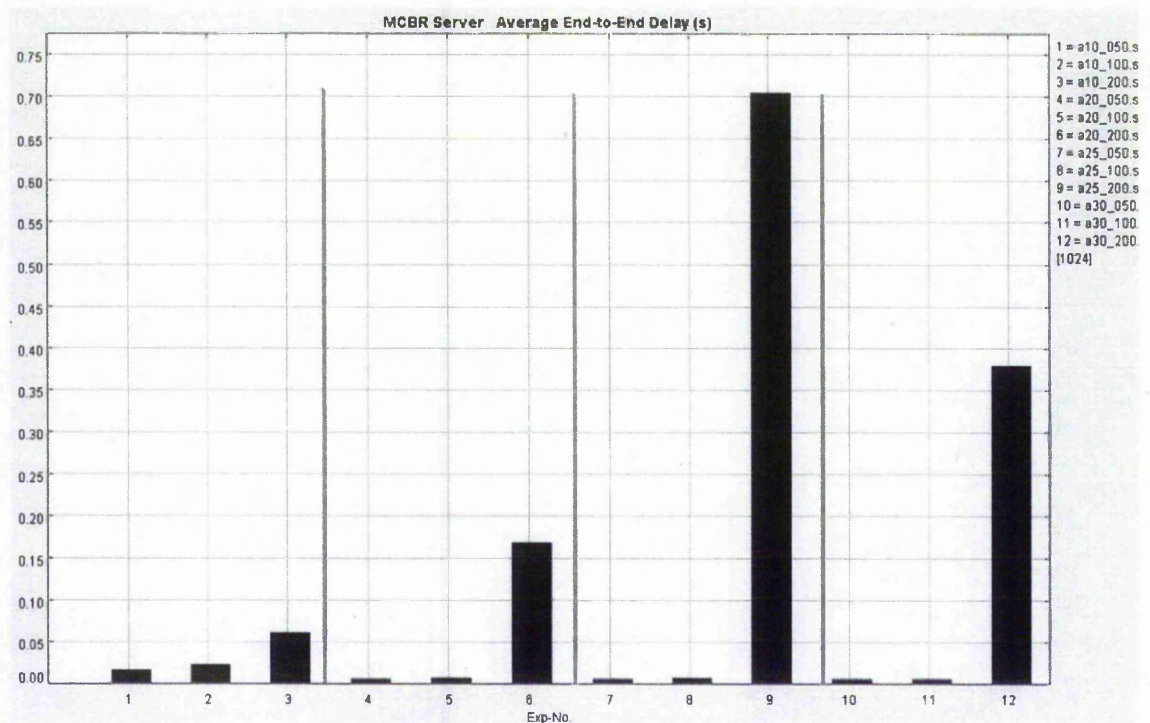


Figure 3.22 Effect of packet size (50, 100 and 200 byte) on SDC delay performance

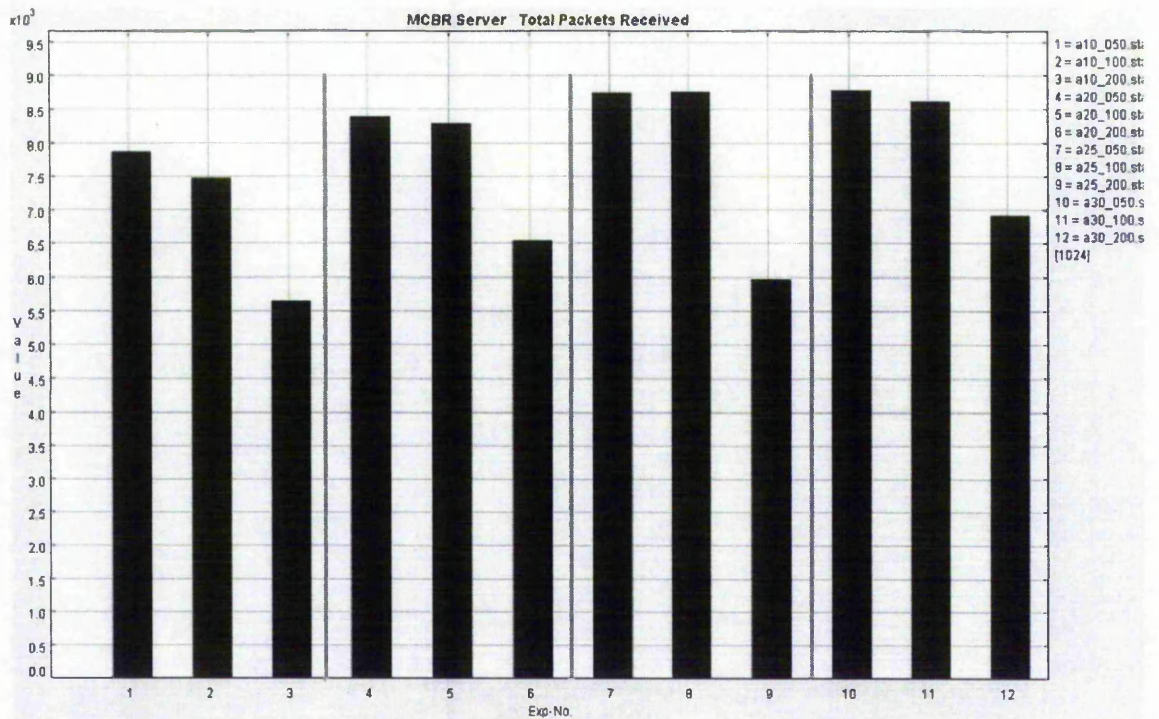


Figure 3.23 Effect of packet size (50, 100 and 200 byte) on SDC received packets

The result shows:

- The packet size has major impact on delay and received packets (exp.3,6,9)
- The optimum packet size is between 50-100 byte. Decrease in the number of received packets is acceptable

3.5.1.4 Role of Directional Antenna

Due to time-consuming nature of directional-antenna configuration for crossroad scenarios, it has only been used for one-way and two-way road scenarios.

Here the effect of directional antenna (north-south) in performance has been measured. In two-way scenario, 10 nodes move in north-south direction and 10 nodes vice versa. The selected angle of view is 60 degree.

Scenarios: SDC and LDC1 on 500m route for 20 nodes in 4-lane two-way (exp. 1- 4), 3-lane one-way (exp. 5- 8) and 10 nodes in 2-lane one-way (exp. 9-12)

Simulation time 60s

Antenna: Directional (exp. 1, 3, 5, 7, 9, 11) and omni-directional (exp. 2, 4, 6, 8, 10, 12)

Node speed: 140-180km/h

Application: MCBR (2000 times), packet size: 50Byte with 25ms and 70ms interval for SDC and LDC respectively

Figure 3.24 and 3.25 proves that in all scenarios directional antenna improve the delay performance. Comparing exp1 and 2 with exp5 and 6 reveal nearly 40% packet losses in

two-way road. This packet drop is partly justifiable by receiving wrong messages from other directions. Narrowing view angle of antenna can improve the performance but it also decreases the sensitivity of system to nodes getting close from sideways (blind area) like overtake scenario. The result was quite satisfactory and presents the value of directional communication.

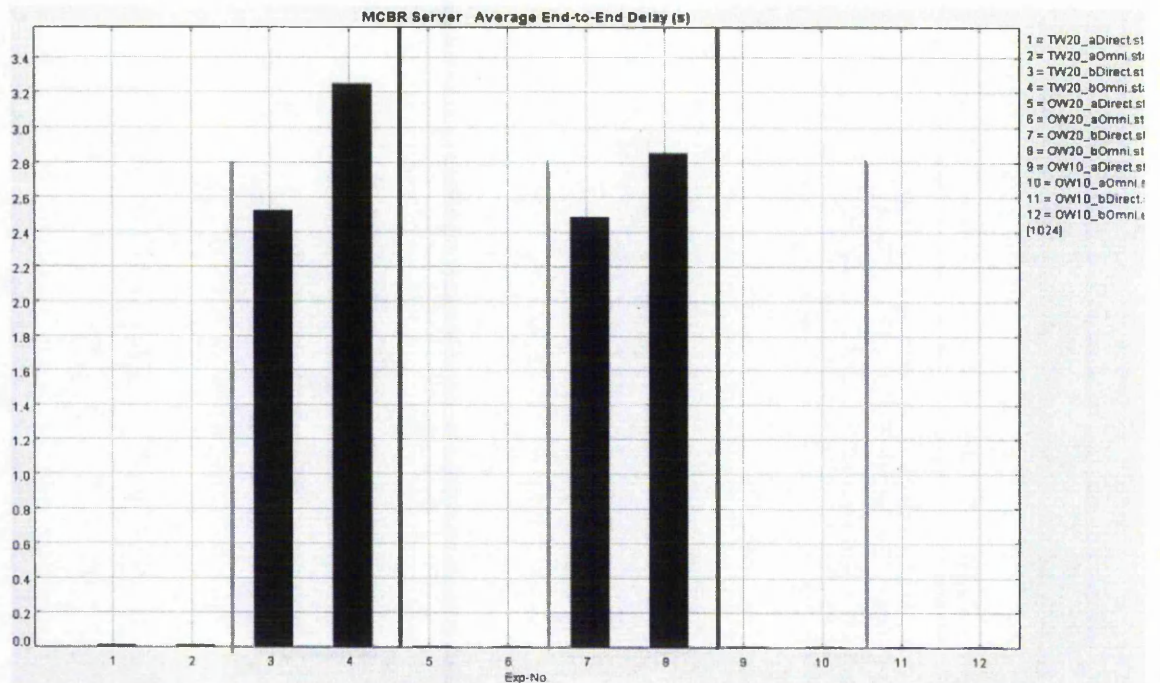


Figure 3.24 Average delay in two-way (exp. 1-4) and one-way (exp. 5-8 with 20 nodes and exp. 9-12 with 10 nodes) scenario in SDC (exp. 1, 2, 5, 6, 9 and 10) and in LDC1 (exp. 3, 4, 7, 8, 11 and 12)

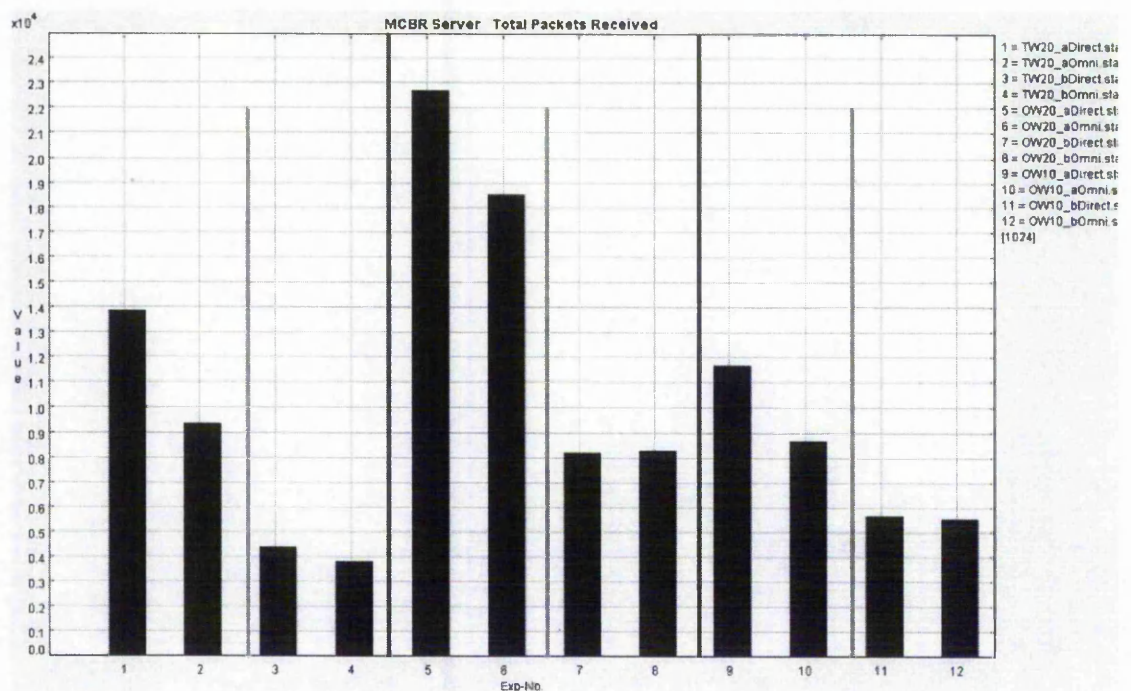


Figure 3.25 Packet received in two-way (exp. 1-4) and one-way (exp. 5-8 with 20 nodes and exp. 9-12 with 10 nodes) scenario in SDC (exp. 1, 2, 5, 6, 9 and 10) and in LDC1 (exp. 3, 4, 7, 8, 11 and 12)

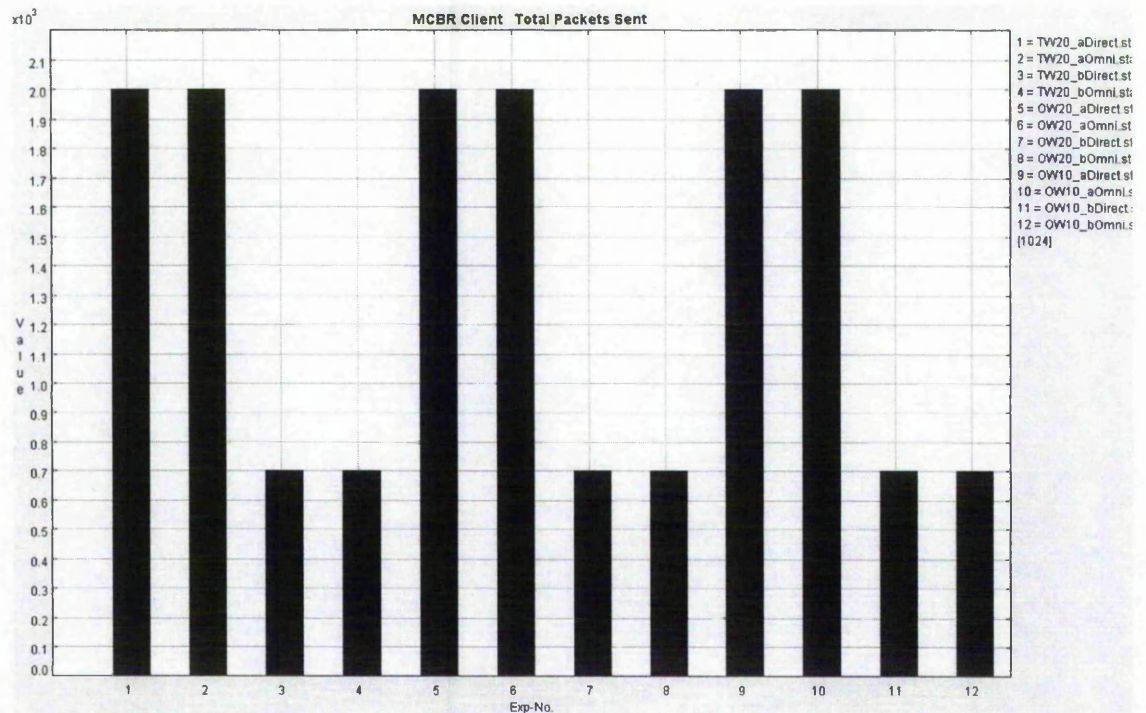


Figure 3.26 Total packet sent in two-way (exp. 1-4) and one-way scenario (exp. 5-8 with 20 node and exp. 9-12 with 10 node) in SDC (exp. 1, 2, 5, 6, 9 and 10) and in LDC1 (exp. 3, 4, 7, 8, 11 and 12)

The result shows:

- Directional antenna has a great impact on both delay and received packet performance (comparing exp.1 and 2, 70% in compare with 48% of received packets)
- Delay is not acceptable for LDC in one-way and two-way (exp. 3,4 and 7,8). The reason partly relates to the number of nodes (refer to improved delay on exp. 11 and 12)

3.6.2 LDC2 Simulation Test

Here the test is run to check the feasibility of voice services between MNs. The reason for selecting VoIP is due to its complicated streaming characteristics; low bandwidth, real time and full duplex.

Scenario: 200x200m crossroad with 20 nodes / Simulation time: 80s

Radio: 802.11b with omni-directional antenna

Node speed: stationary / low-speed / high-speed

Application: VOIP with 50ms packetization interval and 50s call duration

Delay affects VOIP system in two ways:

- Delay in an absolute sense can interfere with the rhythm of inquiry and reply in human conversation.
- Delay variations, also known as jitter, can create unexpected pauses that may impair the intelligibility of the speech itself and cause the quality of voice to be jerky.

Then performance criteria for voice applications are the jitter and delay. RTP is the general transfer protocol responsible for streaming voice in IP networks. It accumulates voice samples for up to 100ms to reduce the amount of overhead transmitted with the voice stream. Packetization interval above 50ms is lowering quality and recognisable by human ear.

Referring to figure 3.27, mobility increases the jitter and it hits the performance more in stop-go scenario (exp. 2) due to probably change in direction after each stop. Although round trip delay is more for high-speed (figure 3.28 exp. 3) the average one way delay shows reasonable value below 22ms in all cases (figure 3.29).

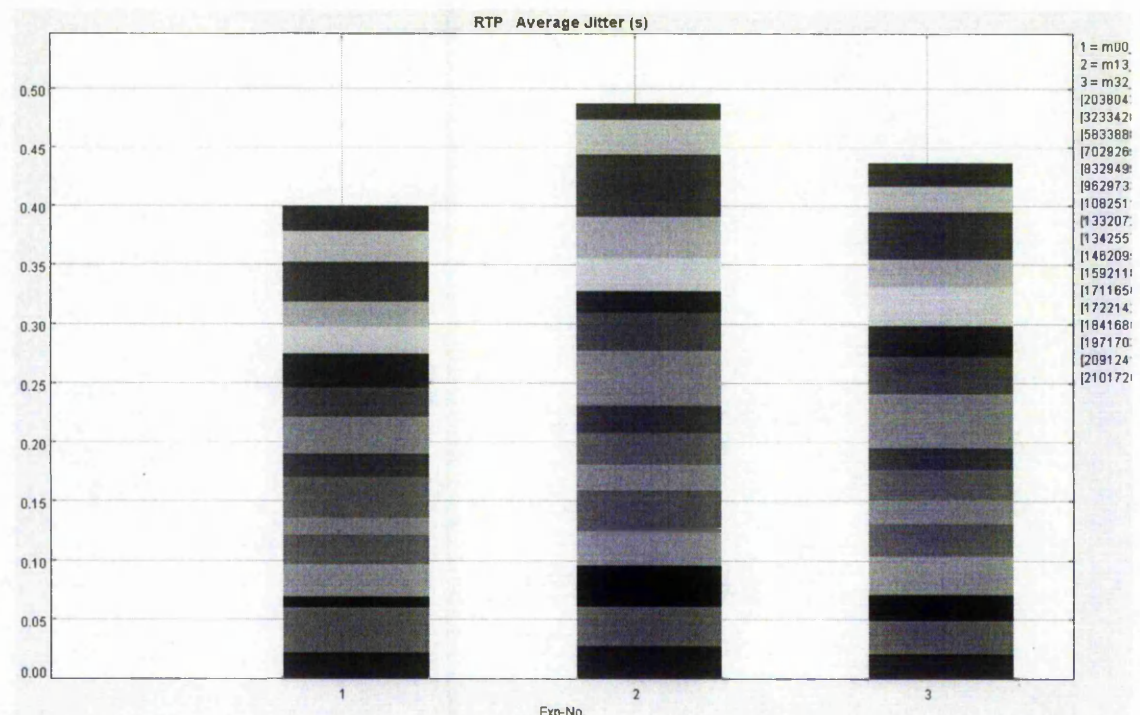


Figure 3.27 Average voice jitter for stationary (exp. 1) low-speed (exp. 2) and high-speed (exp. 3) scenarios

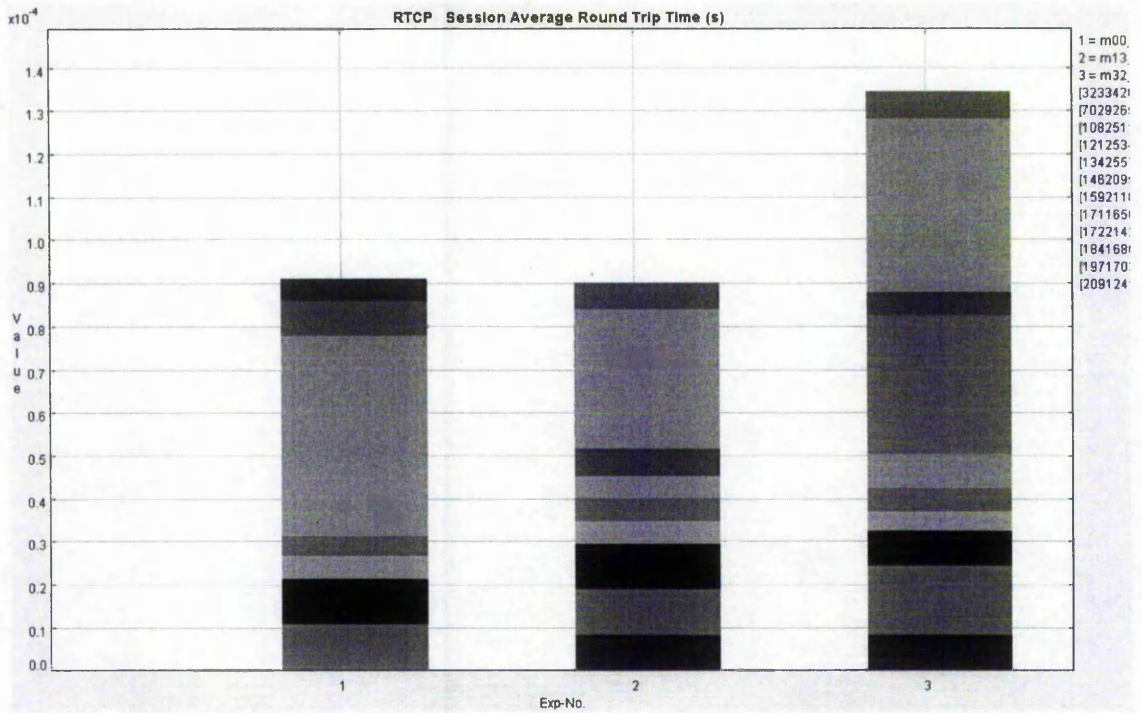


Figure 3.28 Average RTCP delay for stationary (exp. 1) low-speed (exp. 2) and high-speed (exp. 3) scenarios

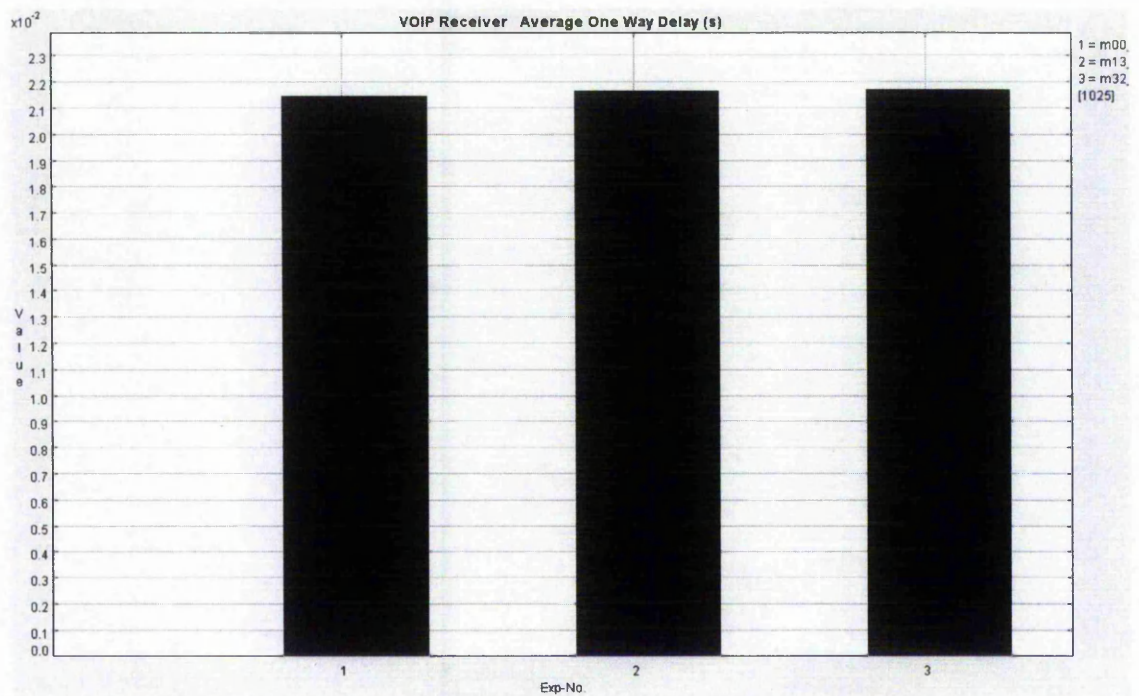


Figure 3.29 Average packet delay for stationary (exp. 1) low-speed (exp. 2) and high-speed (exp. 3) scenarios

To summarize the result of simulation on mobility effect on LDC2:

- Average jitter is in acceptable level (exp.1 against 2 & 3)
- Stop-go scenario has more impacts on jitter (exp. 2) but RTT experience worst condition on high speed situation (13ms).

- One way delay is in acceptable level (0.02s) for all scenario

This proves that LDC2 can cater for voice communications between nodes but the model should repeat and challenge more nodes. Better validation procedure should apply for more precise metering.

3.6.3 LDCAP Simulation Test

Voice communication imposes a great overhead on APs but it is a proper experience to test system ability for roaming and handling topology changes. Roaming impose additional delay on LS. Here the focus is the server ability to handle calls. In VoIP applications, due to network congestion, some frames may be dropped. While non real-time push services (such as e-mail) may recover from such a loss using frame re-transmission, the additional delay caused by re-transmission will in most cases make the conversation unintelligible or will cause talker overlap (one participant cuts off the other's speech because of long delay). The scenario 3.6.2 has been repeated for VOIP application through AP nodes for 11Mbps transfer rates. These tests focus on single hop propagation of packets and the effects of handoff did not count due to use one AP without relay.

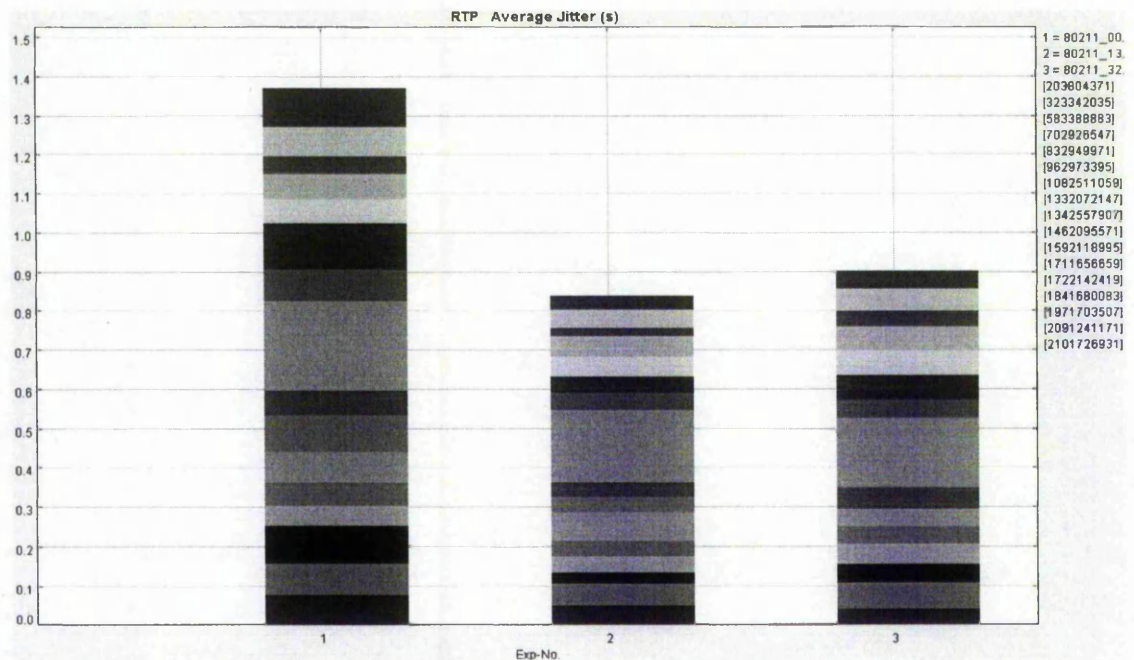


Figure 3.30 RTP jitter in stationary (exp 1), stop-go (exp 2) and high-speed (exp 3) scenarios

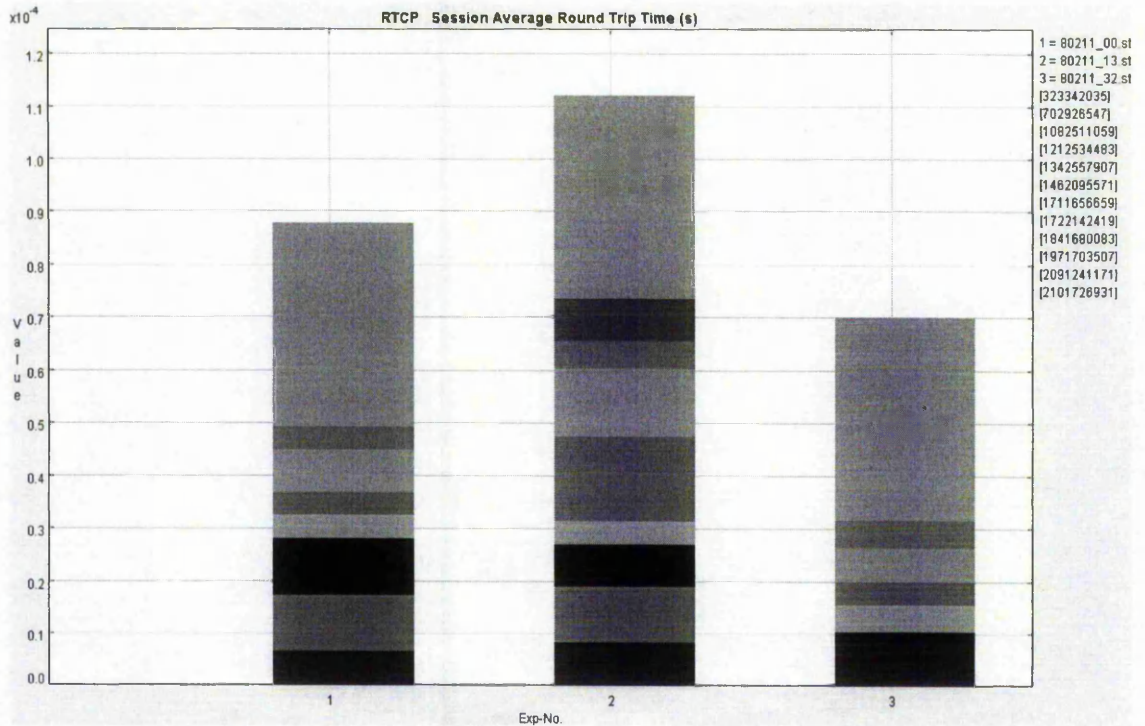


Figure 3.31 RTCP round trip time for packets in stationary (exp 1), stop-go (exp 2) and high-speed (exp 3) scenarios

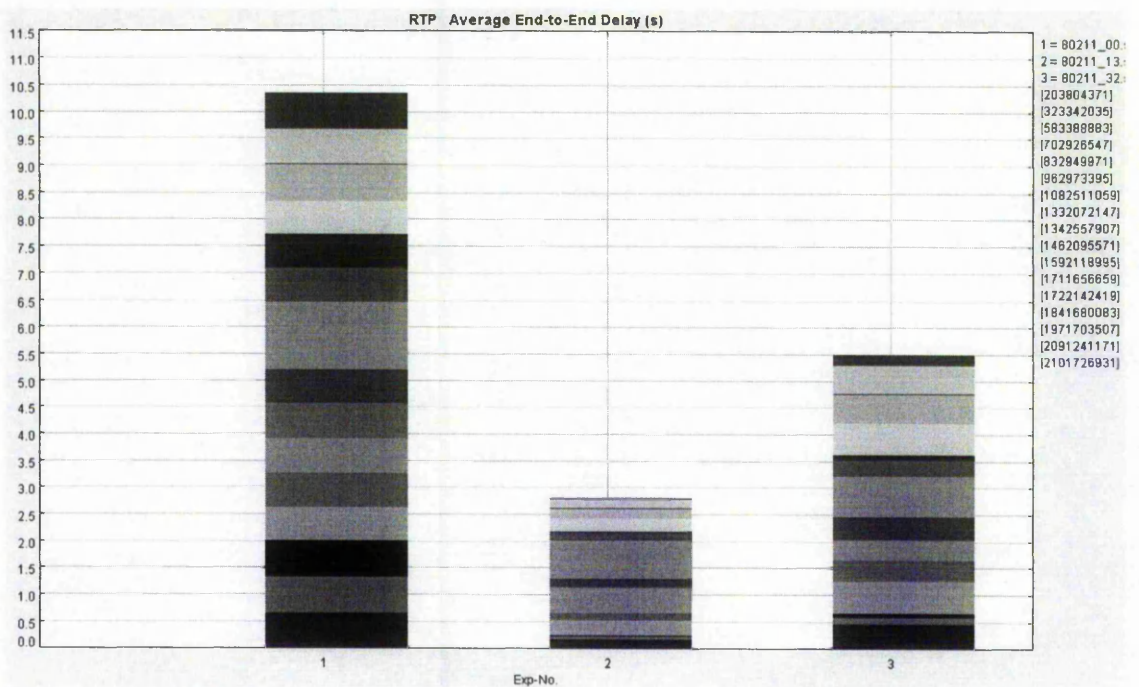


Figure 3.32 RTP delay in stationary (exp 1), stop-go (exp 2) and high-speed (exp 3) scenarios

Nearly all results (figure 3.30, 3.31 and 3.32) shows that mobility has improved performance. The result did not include dropped packets. In other words the result proves that using one channel is not suitable to manage simultaneous voice communication.

In comparison with LDC2 the jitter has increased sharply which returns to the limited capacity of access point (the grey area in chart). The betterment of jitter performance in stop-go and high speed is not realistic. It is mainly due to disconnecting communication. This suggests better validation criteria to measure service performance.

Chapter 4

VehINet and MAC Layer

In OSI, Data link layer consists of two sub-layers, Media Access Control (MAC) and Radio Link Control (RLC). The first is responsible for channel access, scheduling, recovery packet collisions, handling hidden and exposed nodes. The RLC or upper layer deals with channel allocation, neighbour discovery (based on radio & range), power control and GPS location.

The role of MAC layer is quite vital for VehINet services.

- Primary packets evaluation happens in this level (using and forwarding packets or discarding)
- Observing the real time feature of system mainly depends on the performance of this layer

The MAC should be smart enough to judge about seriousness of packets based on the direction of move, coordination of sender node. Message type, breaking flag, breaking level and hopping counter are among the other factors should be considered. No means of guarantying is required because of packet transmission is in one direction.

Proposed MAC specification for SDC includes:

- Simple, no need to beaconing and routing
- Less information pass to upper layers
- One flow of data for receiving and one for sending
- Communicate by directional Geocast
- Specially awareness MAC to verify the packet information and making routing table
- Fully random access MAC

The MAC layer for add-on services would be more complete to observe the routing issue. 2-way handshake procedure is required in this mode. The probability of hidden node problem which generally solves by 4-way handshake should be defined and discussed for these services. The proposed MAC specification for LDC includes:

- Work in dual mode, as SDC or as LDC2 and LDCAP
- Complicated due to routing for LDC2 and LDCAP
- Communicate by directional Geocast and unicast
- Specially awareness MAC is a must to decide about nearest AP by priori knowledge available in digital map
- Coordination between source and destination is not necessary for all services but Ack signals are needed to detect contention (LDC2 and LDCAP)

The spatially awareness MAC is needed for both unicast and Geocast data transmission, to fulfil the requirements of VehINet. This Mac which able to work with dual directional antenna system brings major benefits as:

- Separation of data flow (incoming/outgoing)
- Utilizing two directional antenna
- Using coordination system in this level

In this chapter first a general view of MAC Layer for Ad hoc and research background has represented and later the simulation tests have compared few MACs for VehINet services.

4.1 MAC Layer in Ad Hoc Networks

Figure 4.1 represents a classification of wireless MACs. The MANET has no entity to manage access algorithms and frequency band therefore polling methods used in centralise MAC protocols like Point Coordination Function of 802.11 is useless. Furthermore VehINet uses distributed MAC and the only available method to use channel is random access.

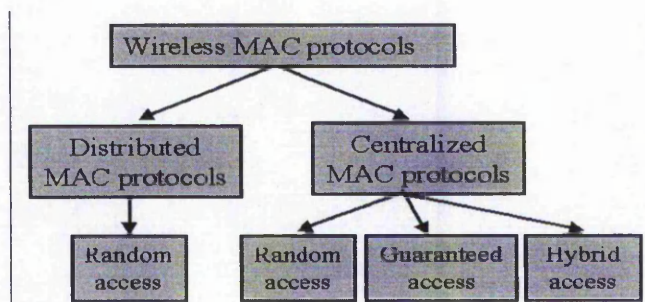


Figure 4.1 Wireless MAC protocols classification [17]

Distributed MACs is divided in two categories: those working without any kind of coordination between the stations like Aloha; and those that coordinate between stations like CSMA, 802.11 DCF, Multiple Access Collision Avoidance with Piggyback Reservation (MACA/PR) and Slotted-Aloha. The later methods are not fully random.

In Aloha, the simplest and fully random MAC protocol, packets are transmitted as soon as generated and collision packets are re-transmitted after a random time delay.

Carrier sensing and collision avoidance mechanism are the first mechanism for coordination between stations. Carrier sensing refers to listening to the physical medium to detect any ongoing transmissions, where hidden and expose nodes could be involved. Collision avoidance technique is a mechanism into the protocol that minimises the probability of a collision.

The operation of the CSMA consists of listening to the channel and abstaining from every transmission when the Carrier Sensing indicates the channel is occupied. If the channel is free, the protocol acts as the Aloha. The performance degrades by hidden terminal transmission. The CSMA for IVC can improve by using packet transmission timing decided by vehicle position [63]. This method is mainly useful when packets are small and in low density of nodes.

The most useful method for reduce contention and noise is controlling transmission power. This method has successfully tested and proved up to 280% better performance in CSMA by using channel gain information [64].

The DCF (or EDCF) is work based on CDMA/CA and has two methods for handshaking, two-way (DATA-ACK) and four-way (RTS-CTS-DATA-ACK) which is virtual carrier sensing (in compare with physical carrier sensing by Physical layer). Nodes send data after detecting the idle medium and after waiting a period of time which in EDCF defines by the corresponding traffic category, the Arbitration Inter-frame Space (AIFS). A higher-priority traffic category will have a shorter AIFS than a lower-priority traffic category. This makes possible to provide priority level based on packet type. To avoid collisions within a traffic category, the station counts down an additional random number of time slots (contention window) before attempting to transmit data. DCF uses random back-off scheme to solve hidden node problem. Due to

the effect of EDCAF on lowering the throughput of real-time services, it is not a candidate in SDC but can observe for LDCAP services. The result of [65] and packet scheduler represented can be helpful for later services. Adding information about environment interference level in packets can also help to improve 802.11 MAC performances [66].

The preference of position-aware MAC with smart antenna to omni-directional antenna has been proved by [67]. It has also been proved using smart antenna without modification of 802.11, reduces the performance of AP communication [68].

In Slotted-Aloha the time is divided into equal size slots and node with new packets, transmits at beginning of next slot. In presence of collision packet retransmits in the following slots with probability p , until the transmission is successful. A study with Direction-Of-Arrival (DOA) algorithm with slotted-Aloha suggests using smart antenna (adaptive array antenna) instead of directional antenna [69] (2 to 4 times throughput).

In Reservation-Aloha (R-Aloha) channels are divided into slot time interval equal to the transmission time of a single packet. This again assumes that the packet sizes are of constant length. The slots are organised into frame of equal size whose length spans the length of one propagation delay. R-Aloha is also candidate MAC in FleetNet and proved the necessity of reservation based on the high number of transmitted frames [70]. R-Aloha protocol is the candidate MAC in IVC network which is generally used by some modifications. This protocol has been modified (adding slot status to frames) and named as Reliable R-Aloha in CarTalk2000. The tests with one-hop, two-hop and multi-hop transmission proved the performance in one-hop scenarios [71].

In UTRA-TDD there is a different approach: time slots and packet are defined according to 3GPP specifications. A station makes an implicit reservation by successfully transmitting in an available slot. After a successful transmission the station has the slot in following frames reserved until it is no longer required. So the slot is considered owned temporarily by the station that used it successfully. A slot becomes unused either by going empty in the previous frame or by collision in the previous frame. The remaining stations can then compete for unused slots using Slotted Aloha.

Algorithm	Sensing Method	Hidden / Exposed nodes	Single / multi channel	802.11 compatible	Flat/ Cluster structure	Omni-directional / directional antenna	Additional Hardware Requirement	Pros	Cons
CSMA	Physical	(mainly) Hidden	Single	No	Flat	Omni	No	Simplicity	Hidden nodes
MACA/ MACAW	Virtual	(mainly) Exposed	Single	No	Flat	Omni	No	Simplicity	Exposed nodes
FAMA-NCS	Both	Exposed	Single	Need modifications	Flat	Omni	No	Solves hidden node problem.	False "CTS-dominance" effect.
802.11/ 802.11e	Both	Both	Single	Yes	Flat	Omni	No	Simplicity; Easy to implement; Prevalent in reality. QoS support.	Hidden/exposed nodes; Problematic sensing range.
DDCF	Both	Both	Single	Yes	Cluster	Omni	No	QoS support.	Same as 802.11.
RBAR	Both	Both	Single	Yes	Flat	Omni	No	Rate adaptive; Improve throughput over 802.11.	Computation overhead.
MPC-MAC	Both	Both	Single	Yes	Flat	Omni	No	Implement PCF in ad hoc networks; QoS support.	Bottleneck problem; Single node failure problem; Overhead.
AC-MAC	N/A (TDMA)	None	Single	Need modifications	Cluster	Omni	Yes	Efficient and robust clustering algorithm; No cluster head needed.	Channel may be underutilized.
CA-CDMA	Both	Both	Multi	Need modifications	Flat	Omni	Yes	Access control based on the estimation of channel condition; No contention between data/control packets.	Complicated hardware/software; Overhead; Exclusive control channel.
DBTMA	Both	None	Multi	Need modifications	Flat	Omni	Yes	Solve both hidden and exposed node problems; Best performance among omni MAC protocols; No contention between data/control packets.	Requires additional hardware/software. Needs major modifications to be compatible with 802.11; Exclusive control channel.
Bi-MCMAC	Both	Both	Multi	Need modifications	Flat	Omni	Yes	Improve throughput over 802.11; No contention between data/control packets.	Require additional hardware; Exclusive control channel.
MAC-DA1/ MAC-DA2	Virtual	None	Single	Need modifications	Flat	Directional	Yes	Solve both hidden and exposed node problems; Increase channel spatial reuse.	Require additional hardware.
DBTMA-DA	Both	None	Multi	Need modifications	Flat	Directional	Yes	Solve both hidden and exposed node problems; Increase channel spatial reuse.	Require additional hardware.

Table 4.1 MAC protocols, their characteristics and requirements [72]

In general, the major factor behind lack of performance in air-medium communication like VehINet is contention which is controllable by:

- Separation of data flow
- Using small fixed-sized packets
- Using counter for packets to control re-transmission, encapsulation of two message in one packet is advisable
- All transmission happens in predefined period either in SDC or LDC
- Intelligent control of transmission power is useful but it is also time consuming
- Two-way handshaking which is advisable for LDC2 and LDCAP

4.2 MAC Simulation Test

As mentioned earlier the contention probability drops because of small packet size and short packet duration. Furthermore, ALOHA can yield more real time performance than CSMA which needs listening to the channel before each broadcast. Due to unavailability of R-Aloha in simulation software, as a substitute, CSMA is used in SDC model test and the performance compared against MAC802.11.

Due to the role of MAC protocol in the performance of SDC and LDC1 services, a numerical comparison of MAC protocol (802.11, CSMA and MACA) has been presented here.

Scenario: 200x200m crossroad with 20 low speed nodes

Simulation time: 30s

Radio: 802.11a, 802.11b with omni-direction antenna

Application: CBR 500 times multicast, packet size 100 Byte, interval 20ms for 11a, 50ms for 11b

The experience presented on figure 4.2 and 4.3 proves the preference of CSMA (exp. 2, 5, 8 and 11) to other MACs. CSMA has the lowest delay and highest packet received for SDC and LDC1. The result also proves that although MACA brings the worst result, it has highest endurance to speed variation in low (exp. 3 and 6) and high frequency (exp. 9 and 12).

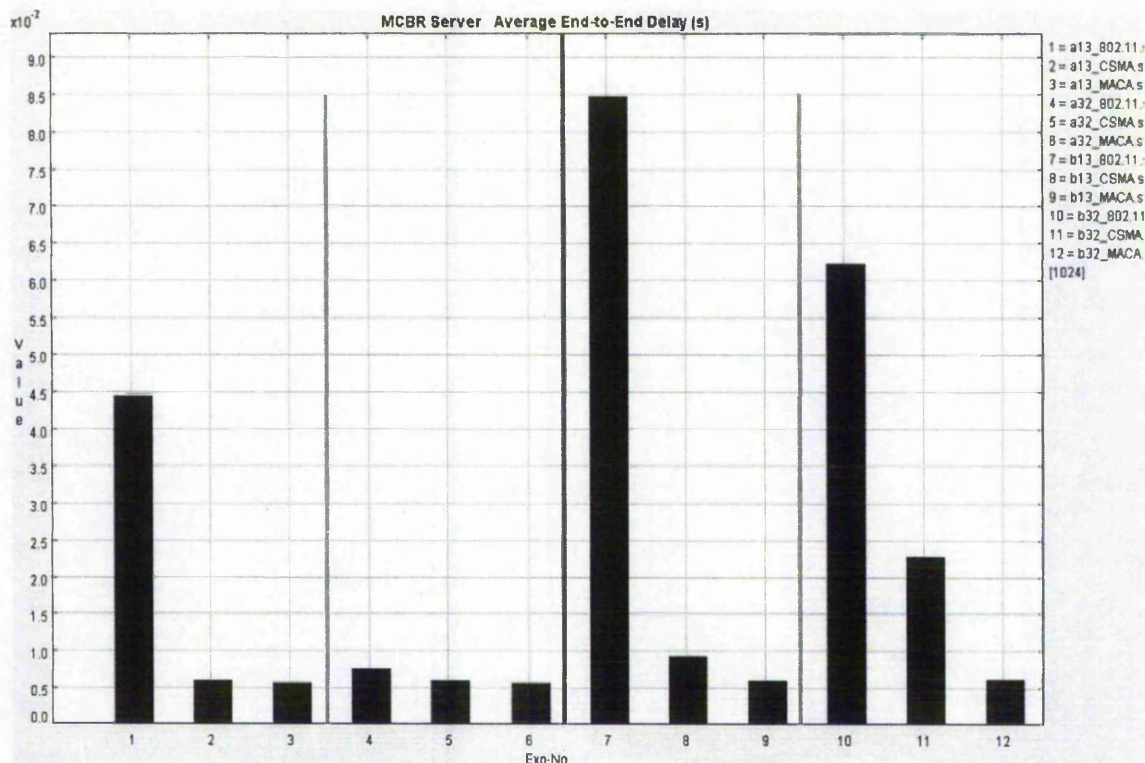


Figure 4.2 Delay of receiving packets in different MAC protocols: MAC802.11 (exp. 1, 4, 7, 10), CSMA (exp. 2, 5, 8, 11), MACA (exp. 3, 6, 9, 12) in low speed MN (exp. 1-3, 7-9) and high speed MNs (exp. 4-6, 10-12) for SDC (exp. 1-6) and LDC1 (exp. 7-12)

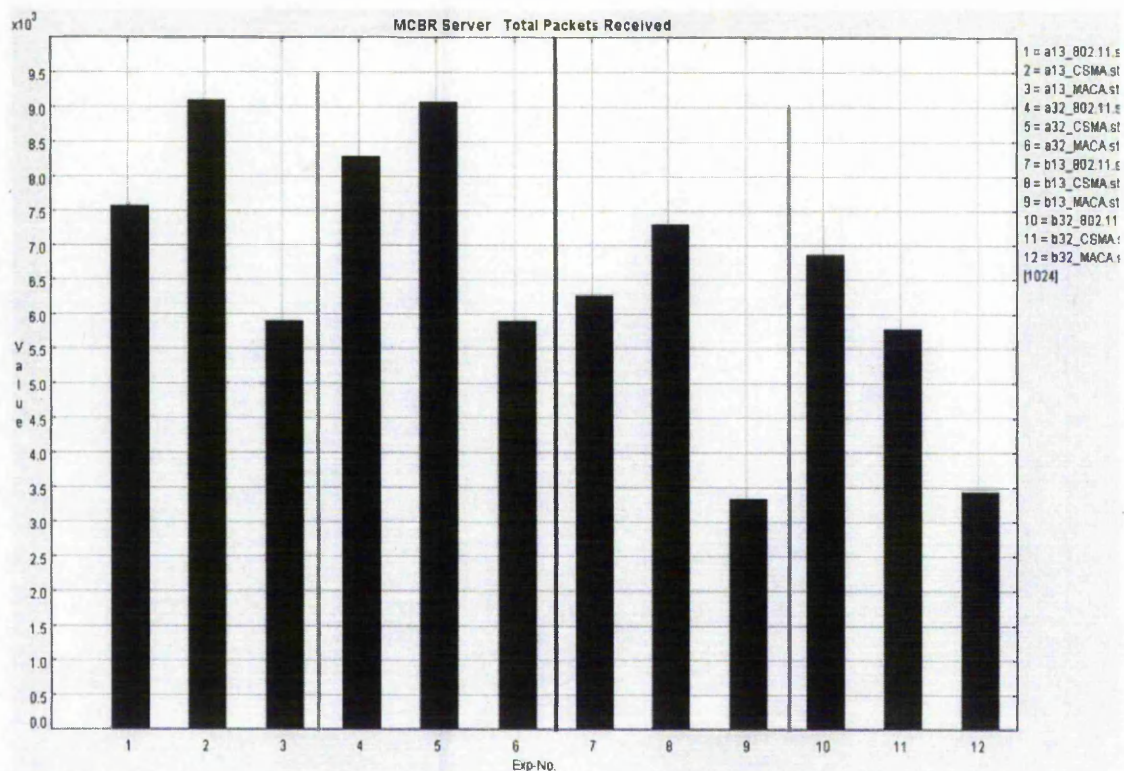


Figure 4.3 Numbers of received packets in different MAC protocols: MAC802.11 (exp. 1, 4, 7, 10), CSMA (exp. 2, 5, 8, 11), MACA (exp. 3, 6, 9, 12) in low speed MN (exp. 1-3, 7-9) and high speed MNs (exp. 4-6, 10-12) for SDC (exp. 1-6) and LDC1 (exp. 7-12)

The result shows:

- In comparison with 802.11 and MACA, CSMA has the best delay performance for SDC (exp. 2, 5) and LDC (exp. 8, 11). The same result is true for packet performance.
- Node speed has nearly no effect on SDC but reduce the packet performance of (contrasting exp. 2 with 5 and 8 with 11)

The simulation result suggests the CSMA as a candidate MAC for core services. Repeating the test for VOIP services over LDC2 and LDCAP supports these findings.

Simulation time: 80s

Radio: 802.11b with omni-directional antenna, 11mbps

Node speed: stationary / low-speed / high-speed

Application: VOIP with 50ms packetization interval and 50s call duration

Based on simulation result, the delay and jitter in MACA were quite high and due to this the statistics has been excluded from figures. Referring to figures 4.4 and 4.5, MAC802.11 (exp. 7, 8 and 9) shows the unacceptable level of delay and jitter for LDCAP services. In lack of MAC802.11 columns, figures 4.6 and 4.7 present more precise result for LDCAP. The result proves the advantages of CSMA to MAC802.11 from delay and especially jitter point of view. Both were partially expected based of time-consuming handshake procedure in 802.11. The results with low speed (exp. 5, 8) and high speed nodes (exp. 6, 9) in comparison with stationary nodes (exp. 4, 7) prove CSMA stability to node speed.

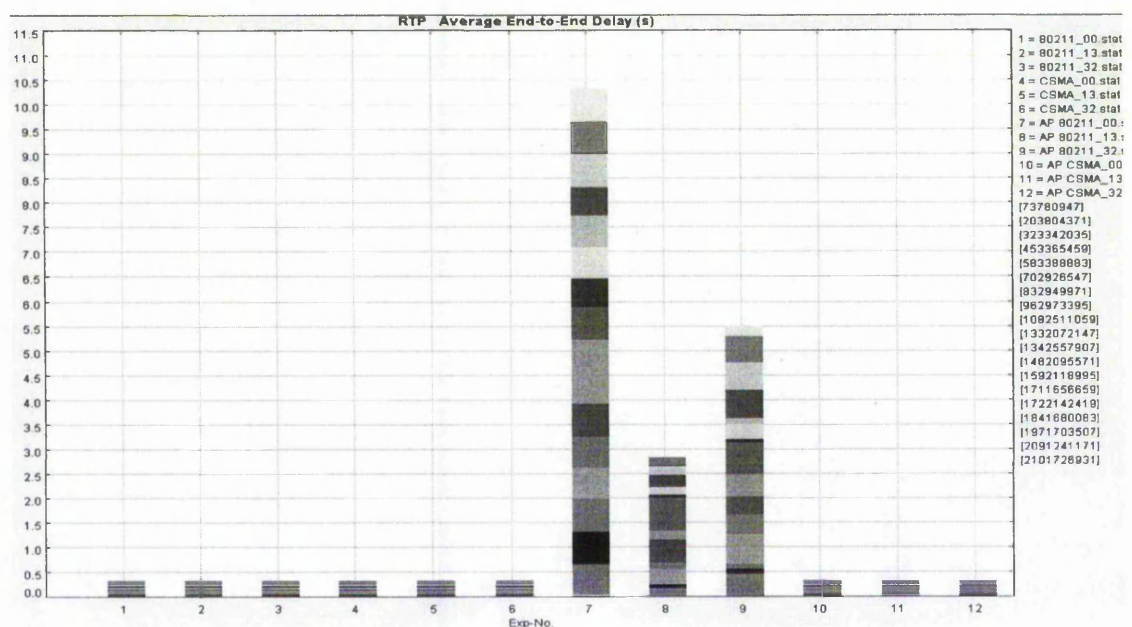


Figure 4.4 Average RTP packet delay for different MAC protocols: MAC802.11 (exp. 1-3 and 7-9), CSMA (exp. 4-6 and 10-12); for LDC2 (exp. 1-6) and LDCAP (exp. 7-12)

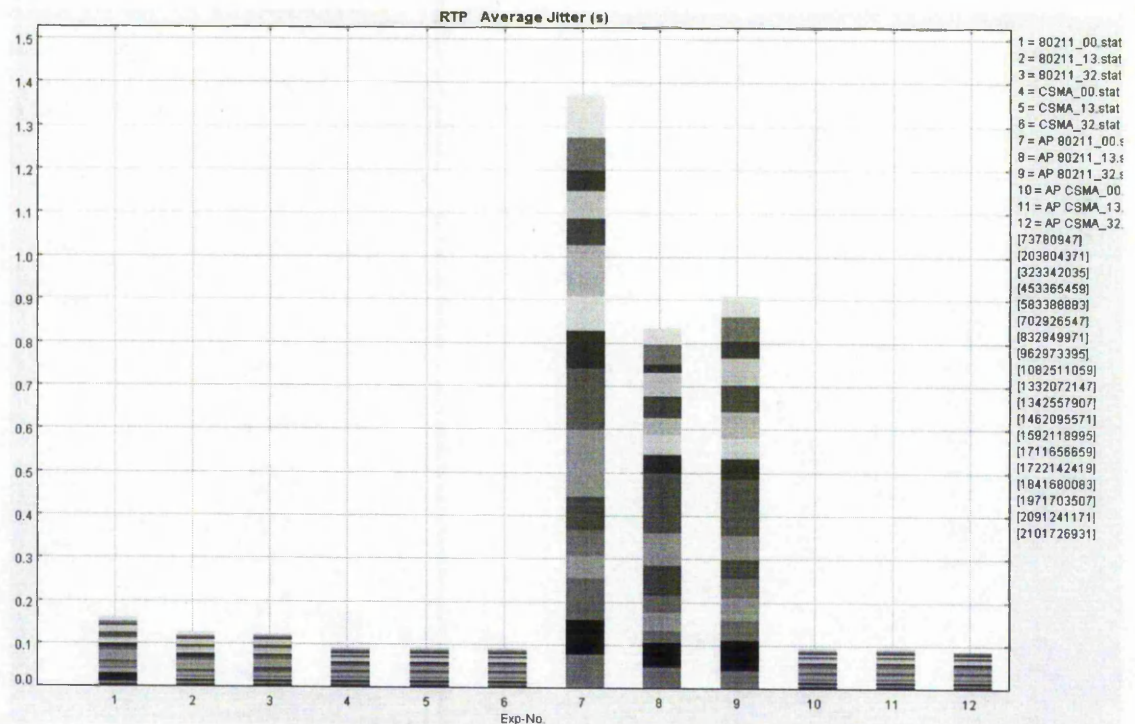


Figure 4.5 Average jitter period on received packets for different MAC protocols: MAC802.11 (exp. 1-3 and 7-9), CSMA (exp. 4-6 and 10-12); for LDC2 (exp. 1-6) and LDCAP (exp. 7-12)

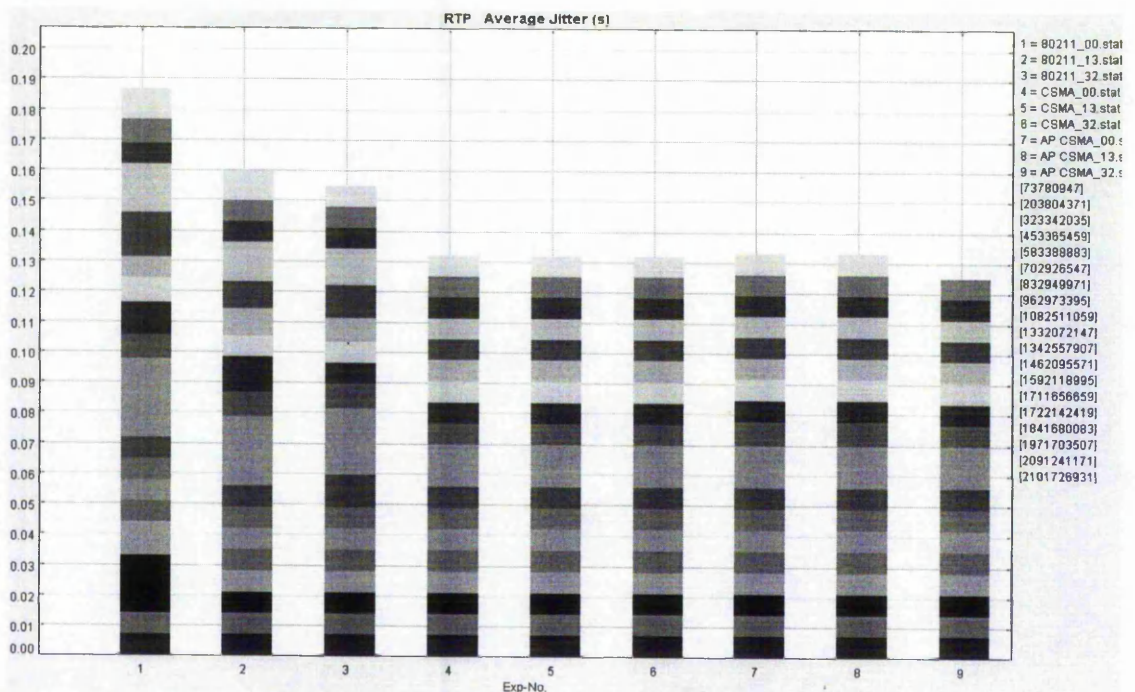


Figure 4.6 Average jitter periods on received packets for different MAC protocols: MAC802.11 (exp. 1-3), CSMA (LDC2 exp. 4-6 and LDCAP exp. 7-12)

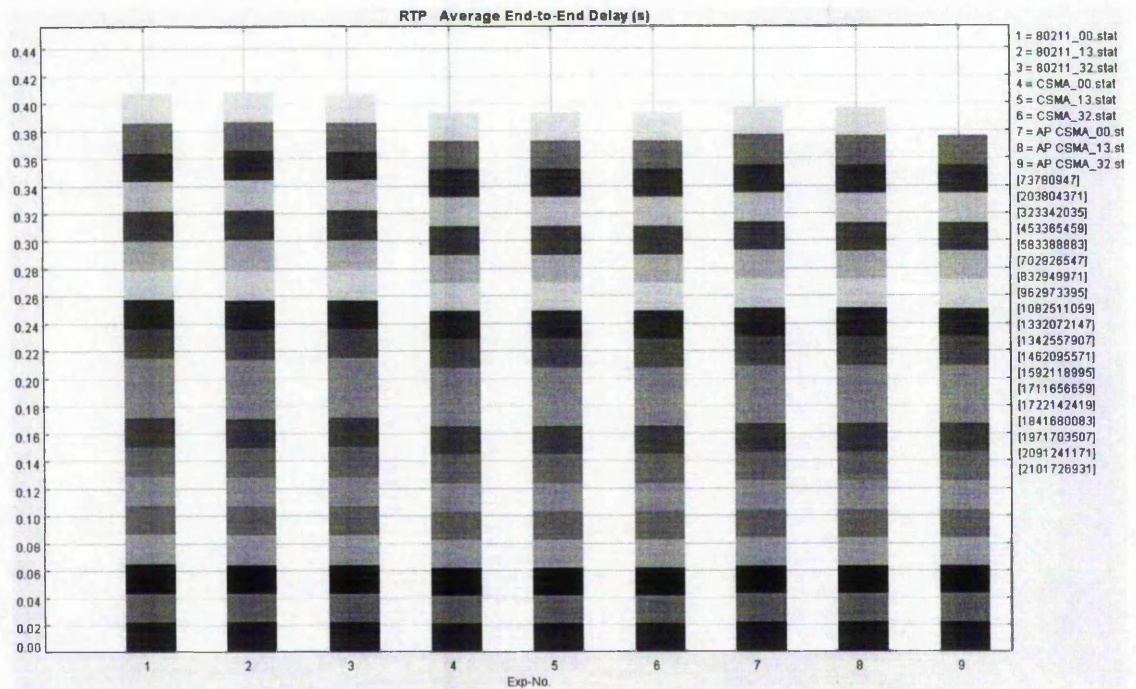


Figure 4.7 Average RTP packet delay on LDC2 (802.11 exp 1-3, CSMA exp 4-6) and LDCAP (CSMA exp 7-9)

The result shows:

- In comparison with 802.11, CSMA has better jitter performance for LDC2 (contrasting exp. 1-3 with 4-6)
- Node speed has nearly no effect on LCD2 and LDCAP services based on CSMA
- 802.11 cannot serve LDCAP application due to poor performance in all aspects

4.3 Conclusion

Aloha is the most proper MAC for core services. The simplified CSMA can be used to emulate the Aloha function. The test for SDC generally proved the advantages of CSMA over MAC 802.11. The main reason for low performance of MAC802.11 for SDC and LDC1 is the time-consuming nature of the handshake procedure and the collision avoidance approach.

No guarantee is available for message delivery; therefore more tests are required to find the safety level or maximum number of nodes that this layer can handle with minimum contention. The research believes that simulation with directional antenna will reveal clearer view of MAC performance.

SDC system can auto-configure itself by controlling the frequency of transmission based on driving speed, traffic layout and road type to keep the safety level of service.

Modifications are necessary to include the node position and digital map in the function of this layer.

For add-on services 802.11 EDCF seems to be the base for VehINet MAC but needs to include the location data in decision making and repeat the tests. Power control can be used as a solution for communication between vehicles and LS. Although the simulation showed the preference of CSMA but more precise tests with directional antenna are needed to prove the findings.

Chapter 5

VehINet and Routing Protocols

One of the major bottlenecks in developing wireless network is routing. Due to this, the routing has been the most extensive field of research for MANET [73, 74].

Based on the nature of services in VehINet two types of routing is required: namely LDC routing for LDC2 and LDCAP services, and SDC routing which caters for SDC and LDC1 services.

As mentioned earlier positioning is a must to interpret SDC messaging, but plays no role in SDC routing. In contrary it is one of the major components of LDC routing. Due to the functionality of SDC based on directional broadcasting, the routing layer acts as smart packet forwarding and the routing study focuses more on LDC routing.

The network topology for LDCAP services is star but for LDC2 is mesh which differs the routing strategy for LCDAP.

This chapter first presents a general view of RPs classifications, then encounters the advantages and disadvantages of each class of protocols with attention to VehINet routing requirements and later presents the simulation results.

5.1 Routing in MANET and Challenges

Figure 5.1 introduces MANET RPs classification. Topology-Based Routing (TBR) is derived from traditional Link State Routing (LSR) and Distance Vector Routing (DVR) in wired networks. Irrespective of environmental factors such as multiple access, fading, noise and interference these methods are sensitive to the network mobility and topology discovery too. The route maintenance requires a huge overhead in wireless.

On the contrary, Position-Based Routing (PBR) like geographic forwarding and restricted flooding are stateless and do not rely on global network topology, thus avoid the above mentioned overhead. The Critical issue of PBR is distributed location service, which means each MN needs to be equipped with a positioning device. Routing in SDC is PBR but TBR is used for LDC.

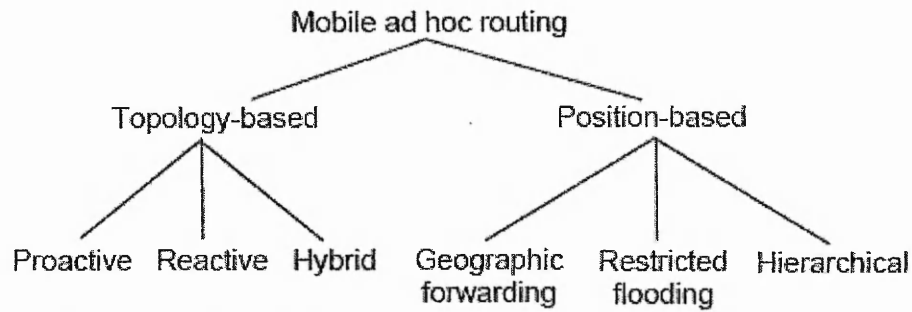


Figure 5.1 Mobile Ad Hoc networks general classification [35]

As mentioned earlier, there are two general underlying routing mechanism used in conventional wired networks, LSR and DVR. In LSR, routing information is exchanged in the form of Link State Packets (LSP) and includes link information about node neighbours. Any link change will cause LSPs to be flooded into the entire network immediately. Each node can construct and maintain a global network topology from the LSPs it receives, and compute, by itself, routes to all other nodes (proactive, decentralized route computation).

In DVR, every node maintains a distance vector, which includes a triad (destination ID, next hop, shortest distance) for every destination. Every node periodically exchanges distance vectors with its neighbours. When a node receives distance vectors from its neighbours, it computes new routes and updates its distance vector. The complete route from a source to a destination is formed in a distributed manner means when a route needs to be computed, many nodes collaborate to compute the route (on demand).

The problem of using LSR technique in MANET is excessive routing overhead incurred by quickly out-dated routes due to node movement. On the other hand, the DVR face slow convergence and the tendency of creating routing loops.

5.1.1 Topology-Based Routing

TBR comes in three generic categories; proactive, reactive and hybrid protocols (figure 5.1). Proactive routing attempts to keep an up-to-date map of the entire network by constant broadcasting of messages to propagate routing information and update Routing Table (RT). In contrary, reactive protocols only sent messages for Path Discovery (PD) when a source node requires a route. The problem of the first is consuming valuable bandwidth for PD, even if they never use the route; and the second faces delay for sending packets. The Hybrids methods combine best of the both protocols.

Due to the behaviour of VehINet for LDC the focus of research is on reactive ones.

5.1.1.1 Proactive RP (Table-Driven)

In general, proactive RPs has not been favoured in MANETs because of the volume of routing information exchanged (overhead) in a volatile environment. It can be use in less-mobile systems or in stationary Type 3 services.

The most common proactive protocols customized for Wireless Ad Hoc are:

- ❑ Optimized Link State Routing (OLSR)
- ❑ Destination-Sequenced Distance-Vector (DSDV)

OLSR is a LSR-based protocol optimized for MANET through the use of Multi-Point Relay (MPR) nodes. Only MPR nodes propagate control messages to neighbours which sharply reduces the message numbers. Thus the control traffic is flooded in the network in a controlled way.

DSDV is a protocol based on the Bellman-Ford routing algorithm; improvements made to this algorithm include freedom from loops in RTs. Each MN maintains a RT of all possible destinations within the network along with the number of hops to each destination. Sequence numbers allows MN to distinguish between new and old routes, and avoid formation of routing loops. RT issues broadcasts throughout the network periodically to maintain consistency. To decrease bandwidth usage during route update in general cases only an incremental packets consisting of information about the change in the network are used which number is quite small.

A new route broadcasts information consist of its address, the number of hops to reach the destination, the sequence number of the information received and a unique number for that broadcast. The route with the most recent sequence number is used. Routes with the same sequence number; the one with the smallest metric is used.

5.1.1.2 Reactive RP (on-demand)

Here are the most common reactive protocols customized for Wireless mobile Ad Hoc networks:

- ❑ Ad-hoc On demand Distance Vector (AODV), enables unicast and multicast routing.
- ❑ Dynamic Source Routing (DSR)

Reactive protocols suffer from high route acquisition latencies and not proper for services intended to have swift reaction.

AODV is an improved form of DSDV that minimizes the number of required broadcasts. When a source node desires to send a message to a destination and does not have a valid route, it broadcasts a Route Request (RREQ) to its neighbour who in turn forwards it to their neighbour until the destination is reached. A RREQ contains the nodes broadcast ID, sequence number, IP address and the most recent sequence number the source has for the destination node. Broadcast ID is used to detect updated path by increasing the number in each RREQ. Sequence number helps to have a loop-free by not repeating RREQ.

An intermediate node may reply to a RREQ if they have a route to the destination where the destination sequence number is greater or equal to that contained within the RREQ. During the RREQ, intermediate nodes record the address of the neighbour that forwarded the first RREQ, establishing a reverse path back to the source. If multiple copies of the RREQ are received later they are discarded.

Once the RREQ reaches the destination or an intermediate node with a recent route to the destination, a Route Reply (RREP) packet is sent using the reverse path generated by the path of the RREQ through the network. As the RREP packet is sent along the reverse path, intermediate nodes set up forward route entries in their RT, which point to the nodes the RREP came from. Along with each route entry there is a timer, which deletes the entry if it is not used within a set period of time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. If a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request. AODV only supports the use of symmetric links.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple and does not require much calculation. However AODV requires more time to establish a connection.

AODV has following features:

- ❑ One route per destination
- ❑ Best performance in less stress situation
- ❑ Having mechanism to delete old routes

Different methods have researched and suggested the application of adaptive mechanisms to improve the AODV performance in MANET. AODV-PA (AODV with Path Accumulation) has better performance than AODV in high mobility [76]. Also the incorporation of the concept of load balancing on AODV yields better performance on high traffic [78, 79]

Adaptive RP generally improve the performance of low MANET [80] but are not always proper for high speed MANET.

Applying QoS on AODV has better delay performance but on congested network has lower performance [81]. QoS routing do not use flooding for PD which increases the system delay [82].

DSR builds routes by flooding RREQ packets. DSR implements a set of optimizations to reduce the control overhead.

There are two main phases of the protocol: PD and rout maintenance. Each node is required to maintain route cache that contains the source routes that the node is aware of. The RREQ contains the address of the destination, address of the source and a unique identification number. Each node after receiving the packet, checks to see if a route to the destination is known, if not it adds its own address to the packet and then forwards the RREQ packet along its out going links. To stop continuous forwarding of the RREQ packet, the packet is only forwarded if the nodes address does not appear in the packet and the node has not already seen the RREQ.

A RREP is sent when the RREQ reaches the destination or an intermediate node that contains in its route cache an unexpired route to the destination. When the packet arrives at the destination or the intermediate node the RREQ contains the hops the packet has taken. If the node generating the RREP is the destination it appends the route

record contained in the route request into the route reply. If the node generating the RREP is an intermediate node it appends its cached route to the route record and then generates the route reply.

To return the RREP, the responding node must have a route to the original source; if it has a route to the source it may use that. Otherwise, if symmetric links are supported it may reverse the route in the route record otherwise the node may initiate its own PD and piggyback the route reply on the PD request.

Route maintenance is carried out through the use of route error packets and acknowledgements. A route error packet is generated at a node when the data link layer detects a fatal transmission problem. When a route error packet is received the hop in the error is removed from the node's route cache and all routes containing that hop are truncated. In addition to the route error packet acknowledgements are used to verify the correct operation of route links.

DSR has following features:

- Keeps multiple route to destination
- Best performance in less stress situation
- Lack of mechanism to expire stale routes

Monitoring the routing path for adaptive RP improves the performance of DSR [77].

The mobility effect on DSR has been tested in [83].

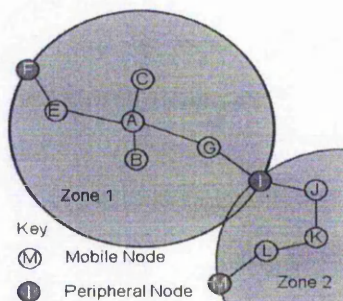
By referring to main features of AODV and DSR mentioned above it can be seen that both have good performance in low stress network. Having multiple routes increases the overhead and complexity of routing for LDC services.

Location-Aided Routing (LAR) is an on-demand RP similar to DSR which exploits location information (GPS). In LAR, the source defines a circular area in which the destination may be located, determined by the following information:

- The destination location known to the source
- The time instant when the destination was located at that position
- The average moving speed of the destination.

The smallest rectangular area that includes this circle and the source is the request zone. This information is attached to a RREQ by the source and only nodes inside the request zone propagate the packet. If no RREP is received within the timeout period, the source retransmits a RREQ via pure flooding. The effectiveness of LAR has been proved in [95].

Zone Routing Protocol (ZRP) is the most common hybrid protocols customized for wireless Ad Hoc. Here nodes are separated into zones (or local neighbourhoods) instead of having a view of the entire network. ZRP acts proactive inside zones and reactive out of it.



By dividing the network into overlapping zones, ZRP avoids a hierarchical map of the network and the overhead involved in maintaining the map. Instead the network can be viewed, as flat and route optimization is possible if overlapping zones are detected. In ZRP there is a one-to-one mapping between nodes and routing zones, which cause the overlapping zones which is maintained by each individual node, as shown in figure 5.2.

Cluster-based RP works like ZRP and by grouping mobility reduces routing overhead [84-88]. Here self pruning by clusters has better performance than flooding. The performance with directional antenna is better than AODV [89] but these methods are highly affected by mobility [90]. This method cannot be used for LCDAP with high-speed MNs.

5.1.2 Position-Based Routing

PBR based on Geocast (broadcast in local area) uses two main categories protocols - flooding and non-flooding protocols (figure 5.3).

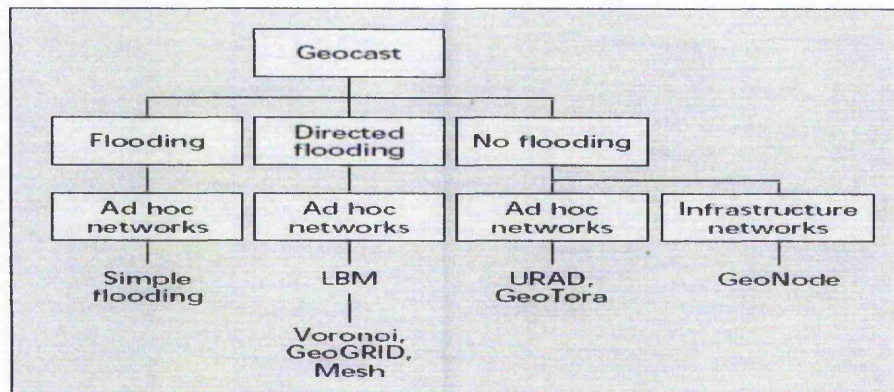


Figure 5.3 Geocast Taxonomy [91]

Flooding wastes networks' capacity with replicas messages and causes contention. Different methods are available in MAC and network layer to control flooding like adapting transmission range (Refer table 5.1).

Method	Advantage	Disadvantage
Flooding	Straight Forward. Guaranteed to reach all nodes	Wasteful of resources, large overheard of messages.
Probability Methods		
Probabilistic Scheme	Saves on resources by limiting the broadcasts	Flooding if value of P is 100.
Counter Based Scheme	Limits the broadcast by use of a RAD	Delays if RAD is set to high
Area Based Methods		
Location Based Scheme	Only broadcast to nodes that will extend broadcast coverage	Requires GPS or similar system to work correctly
Distance Based Scheme	No GPS system required	Difficult to get precise distance between nodes
Neighbour Based Methods		
Flooding with Self Pruning	Node may only forward if specified to do so	Can have a large overhead
Scalable Broadcast Algorithm	Uses TTL to maintain hop limits	To high a TTL values creates congestion
Dominant Pruning	Also uses TTL to maintain hop limit	Can have a large overhead
Multipoint Relaying	Selected MMR to rebroadcast the packet	May not cover all the network

Table 5.1 Advantages and disadvantages of broadcasting methods in MANET [74]

All Geocast methods need a mechanism for positioning nodes and also by referring to table 5.2, it is clear that Geocast algorithms can not guarantee packet receiving. The Geocast works based on broadcast method, which is suitable for core services. Jitter and delay in broadcasting protocols have been compared here [92] and Geocast techniques are compared in [93].

Criterion	Flooding	LBM	Voronoi	Mesh	GeoGRID	URAD	GeoNode	GeoTORA
Fix network/ad hoc	Ad hoc	Ad hoc	Ad hoc	Ad hoc	Ad hoc	Ad hoc	Fix	Ad hoc
Path strategy	Flooding	Directed flooding	Directed flooding	Multipath routing	Directed flooding	Unicast	Multicast ^{9, 11} , unicast ^{10, 11}	Unicast
Scalability/send once	Low	Medium	Medium	Low	Low-high ⁴	Medium-high ¹²	Medium ^{9, 11} –high ¹⁰	Low
Scalability/send several times	Low	Medium	Medium	Medium-high	Low-high ⁴	Medium-high ¹²	High	High
Message complexity/first time	$O(n)$	$O(n)$	$O(n)$	$O(n)$	$O(n)^7$, $O(\sqrt{n})^8$ + gw election	$O(\sqrt{n})^{12}$	$O(\sqrt{n})$ + routing protocol	$O(2n)$
Message complexity/second time	$O(n)$	$O(n)$	$O(n)$	$O(\sqrt{n}) - O(n)^5$	$O(n)^7$, $O(\sqrt{n})^8$ + gw election	$O(\sqrt{n})^{12}$	$O(\sqrt{n})$ + routing protocol	$O(\sqrt{n})^3$
Memory requirements	No $O(n)^1$	Low $O(n)^1$	Low $O(n)^1$	Medium $O(n)^6$	Low $O(n)^7$, $O(n)^8$, $O(n)^{8, 2}$	Low $O(n)^{1, 12}$	Low-medium $O(n)^9$, $O(n)^{10}$, $O(g)^{11}$	Medium $O(n)^g$
Robustness	Medium-high ¹³	Medium-high ¹³	Medium-high ¹³	Medium-high ¹³	Medium	Medium	Medium	Medium
Cope with partial partitions	Yes	Limited	Yes	Limited	Limited	Limited ¹²	Yes	Yes
Guaranteed delivery	No	No	No	No	No	No	No	No
Time stable	No	No	No	No	No	No	Yes	No
Multicast group refinements	No	No	No	No	No	No	Yes	No
Rely on other protocol	No	No	No	Yes	No	Yes	Yes	No

n = number of network nodes; g = number of geocast groups; j = number of joined geocast groups.
¹ Store last packets to detect duplicates. ² Store neighbor information. ³ DAG maintenance not considered. ⁴ Depends on node mobility.
⁵ $O(\sqrt{n})$ assuming a two-dimensional regular distribution of nodes and no topology changes; worst case $O(n)$. ⁶ $O(n)$ if state information is maintained on intermediate nodes, $O(n)\sqrt{n}$ if source routing is used. ⁷ Flooding-based. ⁸ Ticket-based. ⁹ GPS-Multicast. ¹⁰ GeoRouter. ¹¹ DNS. ¹² Depends on unicast routing protocol. ¹³ Depends on network congestion and other parameters (see [16]).

Table 5.2 Comparison of Geocast protocols [94]

5.2 SDC Routing

In SDC and LDC1 node pinpointing is unnecessary and the system functions by local packet forwarding based on PBR. These services need no Hello messaging which saves bandwidth. Although SDC has different CoS but the unique format of packets (fix-size and non breakable) makes SDC routing, far simpler than LDC. The VehINet requirement for SDC, (real-time response time) better matches the Geocast RP.

In simple flooding lots of re-broadcast packets are redundant and waste channel bandwidths. Following methods should apply to have a smart or dynamically controlled flooding instead of simple flooding:

- ❑ Adaptive transmission range
- ❑ Aging counter
- ❑ Neighbour knowledge base

CarTalk2000 [56] estimates the probability of UDP packet loss in this method is negligible (10^{-8}). Nodes broadcast small number of packets of data (UDP packets) selectively in specific direction. Geocast performance for FleetNet and CatTalk2000 has been measured in [96]. Using OLSR over 802.11 has also been suggested for IVC [97].

5.3 LDC Routing

The routing in LDC2 and LDCAP has a dual characteristic because of its reliance on SDC system. In ordinary cases, system can proactively act by using the SDC maintained routing table but in low traffic of nodes, the system needs PD. In other words, a smart mechanism is needed to switch the routing strategy based on traffic load.

The main advantage of SDC RT is keeping information about the speed and destination of nodes (if entered in the system by the driver) in addition to the node position. This empowers the router to estimate the route timeout and smartly select the hoping node with longer lifetime. This passive RT decreases the probability of contention and reserves bandwidth for data packet. The main drawback of SDC RT is keeping reference of MNs ahead of the node and nearly no information about the nodes behind. It means that, if the LDC wants to initiate communication with the AP behind it and the distance is more than communication range, PD is necessary.

The role of RP in the absence of SDC RT is very important especially for LDCAP services. Also more beaconing is needed in lack of updated priori knowledge of SNs coordination.

Among reactive protocols, DSR with small packet, high traffic and multicast ability is the most suitable RP. Based on broadcasting nature of communication, packet hoping more than two, increases the delay and system overhead. Multiple hopping is only acceptable for offline messaging which in the same time lower the bandwidth of real-time services.

The model does not consider hopping on mobile nodes for more than two hops to fix point. Then similarly in SDC, irrespective of emergency packets, all other packets with hopping counter of two will be discarded by AP and other nodes.

Protocols	Route Computation	Structure	#Routes	Source Routing	RRM'	BR'
LSR	Proactive/itself	Flat	Single or multiple	No, may Yes	N/A	No
DVR	Proactive/distributed	Flat	Single	No	N/A	No
DSDV	Proactive/distributed	Flat	Single	No	N/A	No
GSR	Proactive/distributed	Flat	Single or multiple	No, may Yes	N/A	No
FSR	Proactive/distributed	Flat	Single or multiple	No, may Yes	N/A	No
CSCR	Proactive/distributed	Hierarchy	Single	No	N/A	No
WRP	Proactive/distributed	Flat	Single		N/A	Yes
DSR	Reactive/broadcast QUERY	Flat	Multiple	Yes	Erase route, Notify source	No
AODV	Reactive/broadcast QUERY	Flat	Multiple	No	Erase route, Notify source	Yes
TORA	Reactive/broadcast QUERY	Flat	Multiple (DAG)	No	Link reversal, Route repair	No
DST	Reactive/broadcast QUERY	Flat	single but may multiple	No, may yes	Route repair	No
ABR	Reactive/broadcast QUERY	Flat	Single	Yes	Localized broadcast query	Yes
SSA	Reactive/broadcast QUERY	Flat	Single	No	Erase route, Notify source	Yes
ZRP	Proactive(intra)/Reactive(inter)	Flat	Single or multiple	Yes for interzone	Route repair	No
ZHLS	Proactive/Reactive (hier. addr.)	Hierarchy	Single	No	N/A	No
CEDAR	Reactive/core broadcast QUERY	Hierarchy	Single	Yes	Route repair	Yes
HSR	Proactive/Reactive (hier. addr.)	Hierarchy	Single	No	N/A	No

Table 5.3 Comparing TBR protocols [98] (RRM stands for Route Reconfiguration Method and BR stands for Beacon (Hello message) Requirement).

Although reactive protocols have better performance for real-time and UDP applications and the other applications over TCP, the performance degrades sharply due to short lifetime of the routes [99]. The result of research on [100] which compares TCP Reno performance on AODV, DSR and ADV (a proactive RP) confirms this by proving the performance of ADV.

5.3.1 RP Simulation Test

The simulation compares on-demand RPs such as AODV, DSR and LAR for 1-hop LDC2 using one channel. Role of GPS, SDC RT, beaconing and node location have been ignored in following simulations.

Scenario: 200x200m crossroad with 20 nodes

Simulation time: 70s

Node speed: low speed and high speed

Application: VBR Item size: 1024B Interval: 50ms, 100ms and 1s

By comparing the send and received packets (figure 5.4 and 5.5) the result proves that the systems performance improves after 100ms interval. LAR shows better performance especially in lower intervals (exp. 11, 12 in compare with exp. 1, 2 and 6, 7), but the betterment is not lasting for higher intervals. Mobility does not affect the performance substantially (exp. 3, 8, 13 in compare with exp. 2, 7, 12 respectively) and the effect in weaker in (exp 4, 5; 9, 10 and 14, 15)

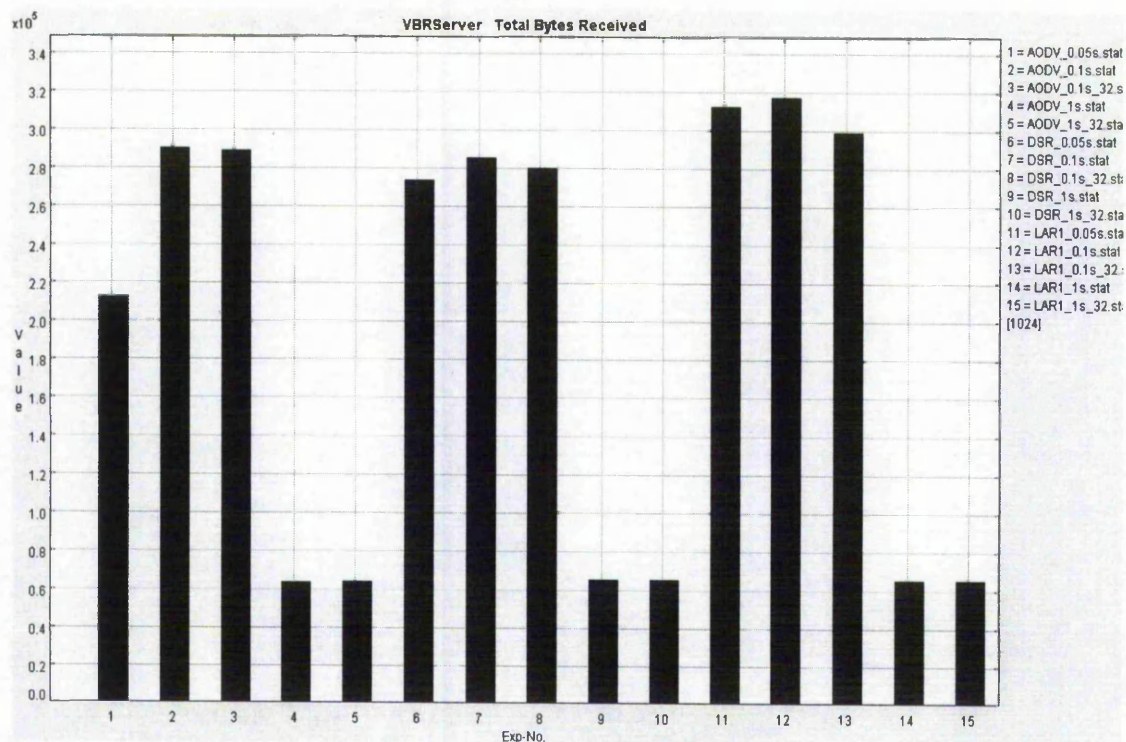


Figure 5.4 VBR data received through AODV (exp. 1-5), DSR (exp. 6-10) and LAR (exp. 11-15)

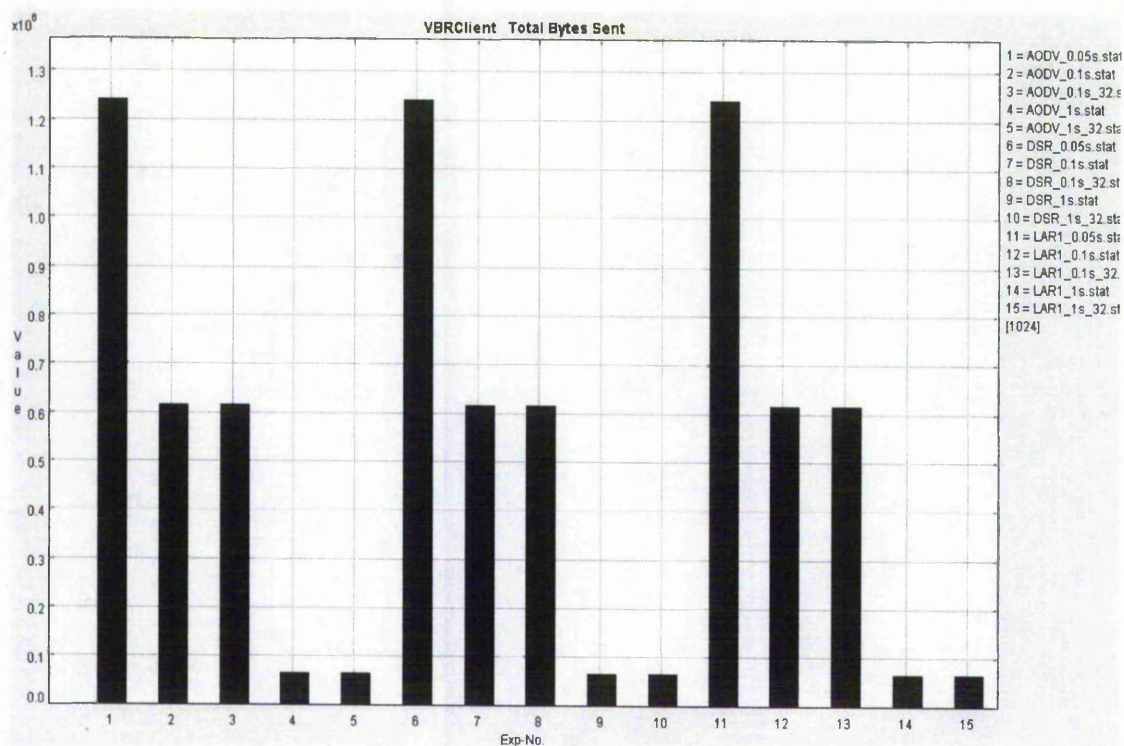


Figure 5.5 VBR data sent through AODV (exp. 1-5), DSR (exp. 6-10) and LAR (exp. 11-15)

The result shows that for VBR services (same as HTML) under stable condition there is no preference between routing protocols

The above scenario has been repeated for VOIP application (10 links, 50s talk duration and 50ms packetization) on CSMA with low-speed and high-speed nodes and the results depicted on the following figures.

By referring to figure 5.6, the AODV and DSR performance is independent to change in speed (node speed). Round trip time sharply increases for LAR in high-speed (figure 5.8).

From delay and jitter point of view DSR supports more connections (exp. 2 and 5 in figure 5.6 and 5.7). The result proves the preference of DSR to other protocols.

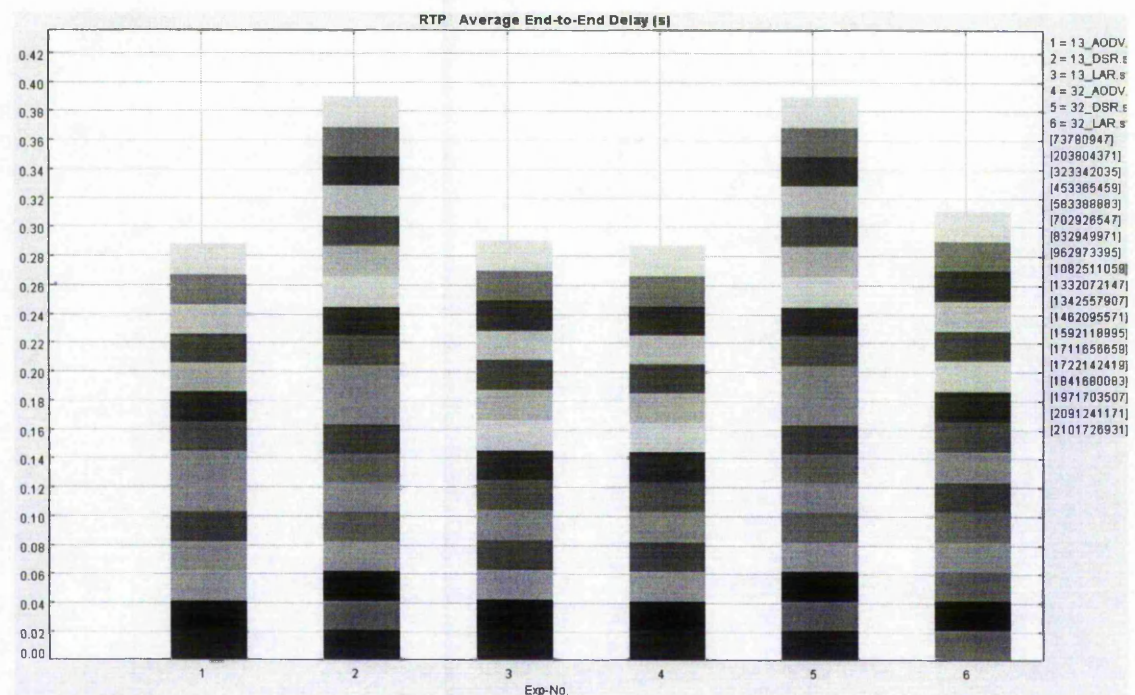


Figure 5.6 Packet delay in AODV (exp. 1, 4), DSR (exp. 2, 5) and LAR (exp. 3, 6)

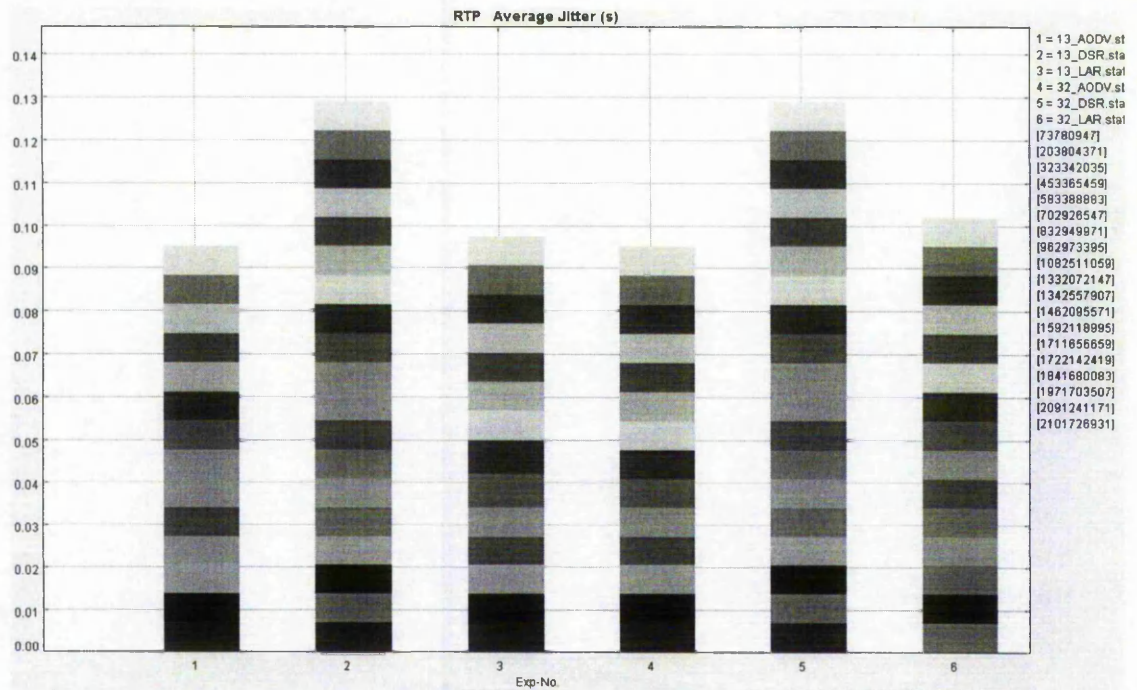


Figure 5.7 Average jitter in AODV (exp. 1, 4), DSR (exp. 2, 5) and LAR (exp. 3, 6)

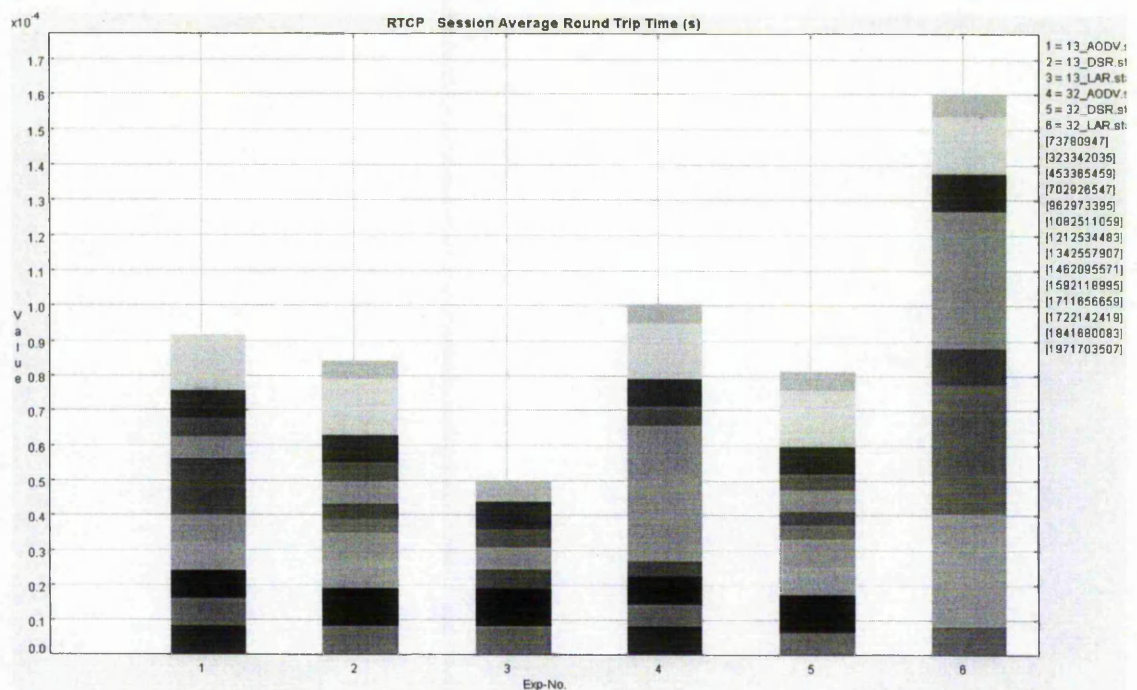


Figure 5.8 Round trip time in AODV (exp. 1, 4), DSR (exp. 2, 5) and LAR (exp. 3, 6)

The result shows:

- DSR supports more connections (exp. 2 and 5)
- From delay and jitter point of view all methods shows equal acceptable result
- High mobility does not affect the performance of ADOV and DSR (contrasting exp. 1 with 4 and exp. 2 with 5)

- For VBR services (same as HTML) under stable condition there is no preference between routing protocols
- More tests are needed to find a candidate routing

5.4 Conclusion

Routing plays vital role in LDC2 and LDCAP services and it works based on:

- SDC RT information of nodes ahead
- Updatable list of SN coordination
- Dynamic or static beaconing (depends on mobility) is necessary to detect nodes around. The strategy of routing based on the services is different and it requires a dynamic scheme for changing.

SDC RT (in normal traffic) and priori knowledge about APs save the bandwidth by reducing hello messages. Unfortunately, it was not possible to meter the value of SDC RT due to difficulty of modelling dual system in simulation package.

Simulation proved the preference of LAR to other on-demand RP. Simulation showed the advantage of DSR to AODV but based on the LAR result and other research findings, better performance is expecting by a modified spatial aware AODV. This system should be test based on MAC protocol with the same ability.

Chapter 6

VehINet and QoS Challenges

The VehINet communicational system should be responsive to environment and network changes and maintain the level of service by:

1. Removing low priority services
2. Switching the communication system (shutdown SDC and use LDC)
3. Shutdown the services completely

When the level of service drops, the system needs to fail safe and cut services to secure the quality of other service by above procedures. Hence knowing influence factors on QoS in VehINet is quite important. Based on the passive nature of WiFi, variation of traffic density and environmental conditions, VehINet experience different level of service as:

- No activity
- Normal activity
- Saturation (Ignoring low priority services)
- Switching to LDC communication (Long distance or rain)
- Over-saturation (shutdown the services and using other ADAS)

From implementation point of view, QoS is in network concern to guarantee the real-time and streaming services. Due to unreliability of the air medium, guarantying the services in wireless environment is impossible but maintaining the level of service by efficient use of the bandwidth for services is a research concern.

Here an overview of QoS approaches has been presented and then affecting parameters on VehINet has been discussed later.

6.1 QoS Implementation Approaches in Wireless Networks

The QoS deployment techniques in wireless networks are mainly ported from wired-networks. Due to limited resources in MANET, some modifications on QoS methods are essential here.

The Network Traffic Engineering (NTE) is the main method to implement QoS. The classification and prioritization of users and services are the main ideas behind NTE. NTE has two approaches to achieve QoS; Reservation-based mechanism (stateful) and Reservation-less mechanism (stateless).

The first one also known as IntServ is more achievable in wired-network and implemented in Asynchronous Transfer Mode (ATM). IntServ reserves and allocates network resources based on application requests. All nodes should create and maintain state information for each flow passing through them. This method can assure bandwidth and delay bounds, but requires complex signalling mechanism to setup, update, maintain and remove per flow state information. Maintaining state information for each flow also makes this approach non-scaleable.

IntServ has following characteristics:

- Flow specific states (bandwidth, delay, and costs) are kept in every router
- Services: Guaranteed Service, Controlled Load Service, and Best Effort
- Components: Signalling Protocol, Admission controls routine, classifier and packet scheduler

Following drawbacks of IntServ makes it unapproachable to be implemented in real-time wireless systems:

- Massive storage to keep flow state information
- RSVP signalling packet will contend for bandwidth with data packet
- Every MN must perform processing of admission control, classification, and scheduling

Second approach also known as DiffServ (Differentiated Services) differentiates traffic according to their class. It only provides probabilistic guarantees, but the implementation is easy and scaleable. There is no need for per flow state information to be maintained at each node. The nodes only need to provide differential treatment to the packets based on information in their header. This method is more complex to implement and needs "smart" mechanism into the network such as Connection Admission Control (CAC), Policy Managers, Traffic Classes and Queuing Mechanisms.

DiffServ model (DS) needs PHB (per hop behaviour) rules and has following characteristics:

- To avoid Scalability problem it provides a limited aggregated classes
- When a data packet enters a DiffServ domain, a boundary router marks the packets' DS field and the interior routes forward it based on DS fields along the forwarding path
- Tiered service-levels
- Simple packets marked by network, not by application and can support legacy applications
- Scalability is simpler than IntServ to implement on any network

The DiffServ drawback includes:

- Ambiguous boundary
- Lack of standard to fit Service Level Agreement (SLA) to MANET
- Same DS code points could be used for different services by different providers
- Different providers using the same PHBs may have different behaviour
- Need end-to-end or edge-to-edge semantics

DiffServ with inherent merits such as simplicity, scalability and adaptability to dynamic conditions are more favourable in wireless environment. Nowadays using hybrid models by integrating IntServ and DiffServ are more in the focus of researchers.

6.2 QoS in MANET and VehINet

The following constraints make the QoS a challenging task in MANET in other wireless systems [101-103]:

- Limited transmission range
- Limited bandwidth due to broadcast nature, contention and security issue
- Mobility-induced packet losses
- Dynamic topology and route changing
- Battery constraints, limited processing power and storing capabilities

Except the last one, VehINet inherits all attributes of MANET. Since nodes are changing location and there is no clear definition of ingress, egress and core router, QoS is time-consuming and wasting bandwidth in MANET.

By referring to the nature of VehINet, QoS for delay-sensitive services is challenging in cases such as under-mobility and congestion. The first generally happens in early morning and late night (Figure 6.1). To cater services Type1 the SDC communication need to switch to LDC1 and in worst scenario stop servicing. Following this, services Type2 (especially when there is mobile relay) cannot be reliable during low traffic period too. To hit objectives especially in congestion time, observing the QoS is important.

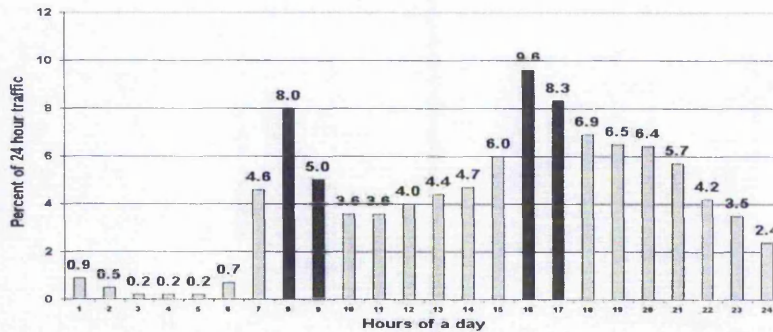


Figure 6.1 Hourly variations of traffic volume in Trondheim [104]

DiffServ is the candidate method which applies after some modifications to include mobility issues [105, 106]. The research [107] proves that loosing bandwidth is less when priority is established in MAC for queuing and fairness of service. Nearly all QoS solutions for MANET who have cross-layer implementation [108] and mobility issues should resolve them by cooperation with the lower layers like MAC.

In the first hybrid method Flexible QoS Model for MANET (FQMM) the highest priority is assigned per-flow provisioning (IntServ) and the rest is assigned per-class provisioning (DiffServ). The proposed signalling protocol for lightweight FQMM is INSIGNIA (also know as In-band RSVP) which quickly responds to topology changes by following characteristics:

- 1 It encapsulates control info in the INSIGNIA Option field and keeps flow state for the real time flows.
- 2 It is "Soft State". The argument is that assurance that resources are released is more important than overhead that anyway exists.
- 3 Instantaneous admission control and fast restoration

In In-band RSVP each node should keep flow states and which it makes scalability difficult.

Reviewing the QoS methods reveal the permanent trade-off between the performance of network and fairness (and quality) of services. The research is trying to find the acceptable level of service (before reaching the breaking point) and knowing the affecting factors on network.

6.2.1 QoS and SDC Services

Some QoS models implement service prioritization but it also adds overhead to the network communication resources. This issue is especially unwanted for real time services. SDC uses fix-size packet which can include small commercial data too. Based on delay sensitivity, the system can establish the following priorities for different Type of Service (ToS) in SDC:

1. Critical packets (accidents or serious messages)
2. Ordinary packets (break, turning signal messages)
3. Commercial packets (optional/reserved)

The above types suggest soft QoS for this system. Although there is one flow of data, the system treats the first and second type packets differently e.g. it temporarily stops sending the Ordinary ones and only broadcasts Critical packets. The last is ordinary packets with added commercial data.

The feasibility tests in best-effort paradigm models proved the effectiveness of one channel transmission by paying attention to the fact that in communication systems only one channel at the time can be active and using other channels in parallel reduces the performance. Based on the equal value of these packets for preventing accidents, establishing hard QoS and reserving channels seems redundant. In the same time splitting the bandwidth to two different size channel is far better than reserving three channels for the first type and nine to others. Checking each channel is time consuming but testing two different channels should bring useful information.

CarTalk2000 [35] has defined three different services but no channel allocation used in test model. Instead, two different intervals have been used to prioritize packets and compensate channel reservations shortage.

Based on system nature and due to observing its real time character, there will be no guarantee for packet receiving and in UDP level there will be no error control, no flow control and no congestion control.

To summarize, the characteristic and parameters of QoS for SDC services include:

- Best effort and soft QoS (one flow of data which tags for different services)
- Fix packet size
- Using single channel for the sake of data sensitivity
- Frequency of messaging can be controlled by the node speed but fix interval is advisable
- Flow control and congestion control makes a big overhead and endanger real-time characteristics. To compensate, enough test for worst scenarios should run to find the best point for contention-free communication

6.2.2 QoS and LDC Services

Implementing QoS for LDC has more factors and is more complicated than SDC. Although the cellular networks have worked on similar field for a long time, VehINet characteristics such as: diversity of services, limited range of WiFi resulted in dependency to city and road features and makes QoS implementation more complex. Due to sharing AP, the QoS is more vital for LDCAP services.

Following priorities (delay sensitivity) are suggested for different ToS in LDC:

1. Reserved for SDC critical packets
2. Reserved for SDC ordinary packets
3. Traffic packets (add-on services)
4. Voice packets
5. Data packets like email and adverts
6. Multimedia packets (optional/reserved)

Similar to SDC, differentiated services is suggested as a model for QoS. Due to the smaller packet size for the first two types, the third type of SDC (refer to section 6.2.1) is ignored here. The voice services are disabled by default when packets (type 1 and 2) are received in LDC. This act is justifiable by reasonably acceptable assumption that there is no need to access voice and multimedia in low-traffic time or off- city roads.

The level of service is acceptable due to the longer distances from hazards (enough time to respond by driver), but the precision of core services suffers in LDC system because of the following reasons:

- 1 Limited channel and bandwidth which is shared between beaconing and data communication
- 2 Lack of RT produced by SDC

The limited channel availability in LDC, channel dedication to service type faces more restrictions. Channel shortage (3) can be solved by channel splitting when LDC works in LDCAP mode. In packet switching systems, voice packets have higher priority in handover time to be used by AP. This establishes in IP header and is not a concern of MNs.

With regard the MNs speed and short distance between SNs, handover is the key issue for VRN [109-111]. Dynamic priority cannot be used in high speed MANET [112].

As nodes move faster and topology changes, the QoS performance degrades nonlinearly which hits the QoS. One of the degradation factors is link breakage. By estimating link stability (link survival time) the routing overhead can be reduced significantly [113]. In VehINet the declaration of destination can help a lot but even without this, by considering the node direction change, detection of weak links is possible in advance.

It should be considered that in an ever-changing network environment, QoS is not a one-time deployment and needs to be changed dynamically. Implementing QoS in lower layers of the network makes the scalability difficult and bring less flexible QoS. Due to time overhead, the following adaptive methods for better QoS should apply carefully after adequate testing:

- Multilayer implementation of QoS
- Dynamic change of system components (transmission intervals, beaconing)

In VehINet the real-time nature of system dictates the move to lower levels of OSI, but modification in the following layers is necessary:

- Transport layer – Wireless TCP (WTCP), RTP and RTCP
- Network layer
- MAC layer – 802.11e and like channel reservation

QoS scheme in 4th layer is responsible to avoid bandwidth racing among packets. In converged voice/data network (with QoS features enabled), despite VoIP low-bandwidth profile (10-15kbps), even a small amount of data traffic can lead to seriously degraded audio quality and dropped calls (refer figure 6.2). Based on an experience [114] with best-declared products (Aruba's A2400 and A800 switches, A61 APs) and VeriWave test tool) roaming from one AP to another took anywhere from 0.5 to 10s. This supports research idea for using a propriety channel for voice.

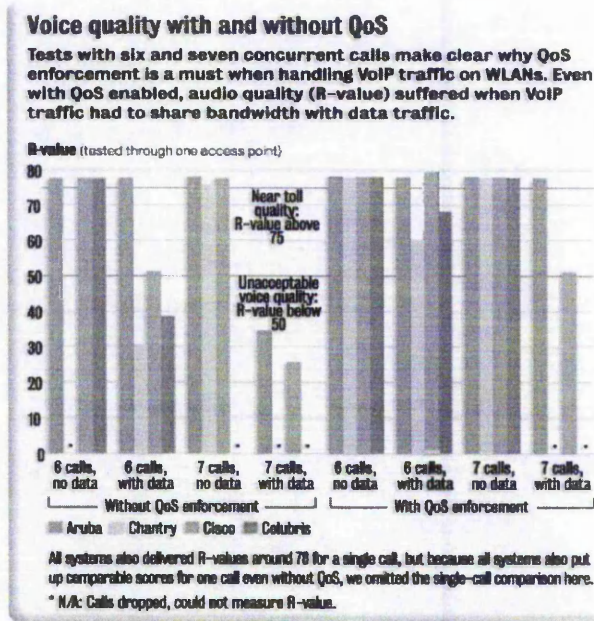


Figure 6.2 Measuring voice qualities over wireless cards with QoS or without it [114]

QoS in network layer has dealt with the RP section, but mobility-aware MAC layer plays a key role in QoS. The Ethernet standards MAC like 802.11 on the contrary with ATM, UTRA-TDD [35] and UMTS (table 6.1) have not build in support of QoS features like prioritized traffic or guaranteed performance levels which makes QoS implementation difficult.

Traffic class	Conversational class	Streaming class	Interactive class	Background class
	Real Time	Real Time	Best Effort	Best Effort
Delay	less than 1 second	less than 10 seconds	around 1 second	greater than 10 seconds
Fundamental characteristics	Preserve time relation (variation) between information entities of the stream Conversational pattern (stringent and low delay)	Preserve time relation (variation) between information entities of the stream	Request response pattern Preserve payload content	Destination is not expecting the data within a certain time Preserve payload content
Example of the application	voice-, video telephony	streaming audio/video	web browsing	telemetry, emails

Table 6.1 UMTS Traffic classes [115]

The distributed channel accessing method for ad hoc networks in 802.11 MAC is Distributed Coordination Function (DCF). It works based on CDMA/CA and has two methods for handshaking, two-way (Data/ACK) and four-way (RTS/CTS/ Data/ACK) which is virtual carrier sensing (in compare with physical carrier sensing by Physical layer).

Enhanced DCF (EDCF) has been introduced by 802.11e as an approach to categories traffic in eight priority levels with no service guaranty [116]. Using EDCF, nodes send data after detecting the medium is idle and after waiting a period of time defined by the corresponding traffic category, the Arbitration Inter-frame Space (AIFS). A higher-priority traffic category will have a shorter AIFS than a lower-priority traffic category. This makes possible to provide priority level based on packet type. To avoid collisions within a traffic category, the station counts down an additional random number of time slots (contention window) before attempting to transmit data.

To summarize, the characteristic and parameters of QoS for LDC services includes:

- Diversity of services and their different priorities make QoS more challenging especially for LDCAP
- Maintaining routing table needs beaconing which is time-consuming
- Guaranteed form of communication needs time for handshaking and acknowledgement
- Cost of handover for real time applications like telephony is high
- Variable-size packets and using different channels have great overhead for LS and quality of service

6.3 Affecting Factors on QoS

Reliability and availability of service in VVN and VRN can be influenced by internal and external factors. The internal factors regarding network elements and components based on importance are:

1. Number of nodes using the service
2. Frequency of messaging in SDC and LDC1
3. Combination of service in LDC2 and LDCAP
4. Speed of nodes

5. Unwanted messages on receivers, produced on MNs
6. Traffic scenarios (roundabout, junction, one-way, two-way)
7. Vehicle types (lorries and buses can block the wave path)

The external factors influencing VehINet includes:

1. Noises produced by other networks
2. Weather condition like rain and snow
3. City layout (classic approach VS modern streets)
4. Effect of road terrain (even or hilly)
5. Multi-path noise produced by bounced back waves on man-made structures like building

The effects of few internal factors have been evaluated during feasibility tests and it has been concluded that the first three affect VehINet more than others. Decrease in the number of MNs hits the performance of both communicational systems. If there is a construction or slippery road, low density of nodes cannot inform each other of the event.

The outcome of section 3.5.1.2 proved that node speed is not an inhibitor factor in VehINet.

About traffic scenarios such as roundabouts, the system can cope with the surge of packets by lowering the frequency of messaging with the knowledge about the road provided by digital map.

Here the research has only focus on environmental factors in application level and experimented with the role of these factors. Among external factors, it expects that the environmental noise influences more LDC2 and LDCAP due to radio usage in many office applications and WLAN. It also expects that the city terrain will affect the LDC more but city layout has equal effect on both networks.

There are other external factors affecting QoS which is out of project concern. For instance, driving style can increase the number of false alarms; in this case, adaptability of the system to the driving style can solve the problem [117].

6.3.1 Precipitation Impact on SDC and LDC Services

The role of weather on performance has been evaluated for SDC and LDC1 based on the real-time sensitivity.

Scenario: 200x200m crossroad with 20 low-speed nodes / Simulation time: 40s

Radio: 802.11a and 802.11b with omni-direction antenna (370m range)

Application: MCBR with 25ms transmit intervals

Weather attribute: wind speed 9.5m/s (34 km/h), precipitation 10, 50, 100, 200 ml/hr

Based on figure 6.3 and 6.4, as expected the precipitation increases the delay and reduces the number of received packets (exp. 1 in compare with exp. 2, 3, 4; exp. 5 in compare with exp. 6, 7, 8). The SDC is more sensitive to rain even for 10ml the delay degradation is sharply increased (exp. 1 in compare with exp. 6). The same thing is true for LDC1 but not for low precipitation. In practice 100ml precipitation can only happen in a short period but here is selected only to test the system under stress.

The result proves that SDC in normal rainy weather is not trustable and systems should switch over to LDC1.

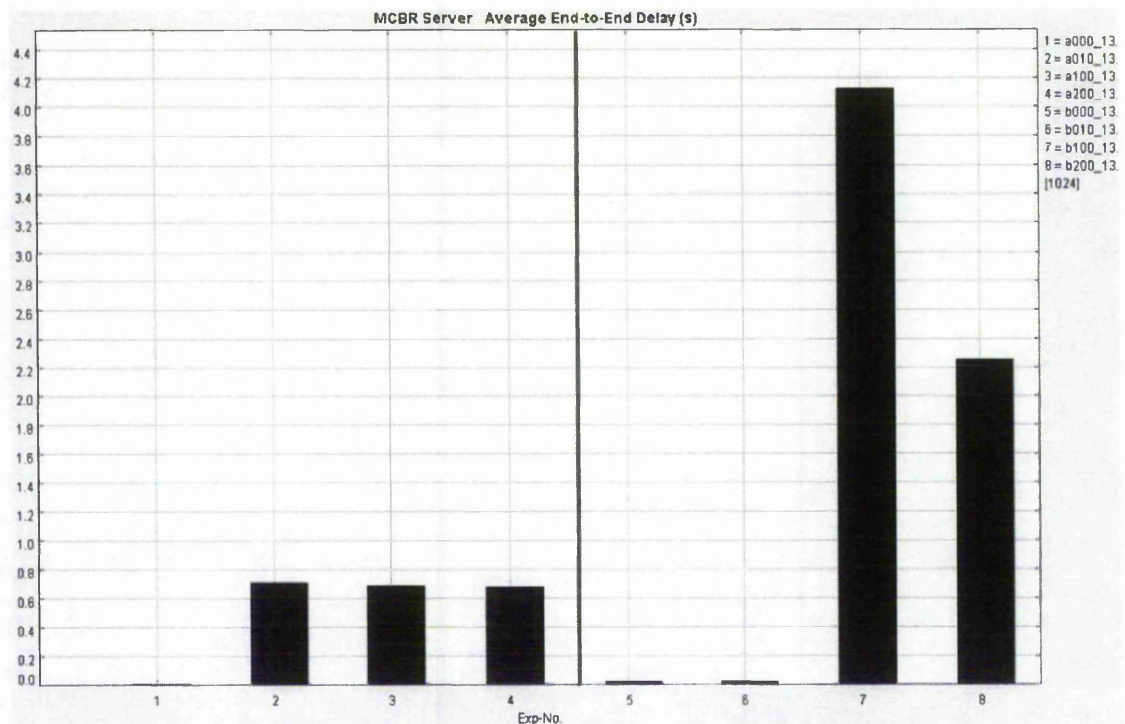


Figure 6.3 Precipitation impact on delay in SDC (exp 1-4) and LDC1 (exp 5-8)

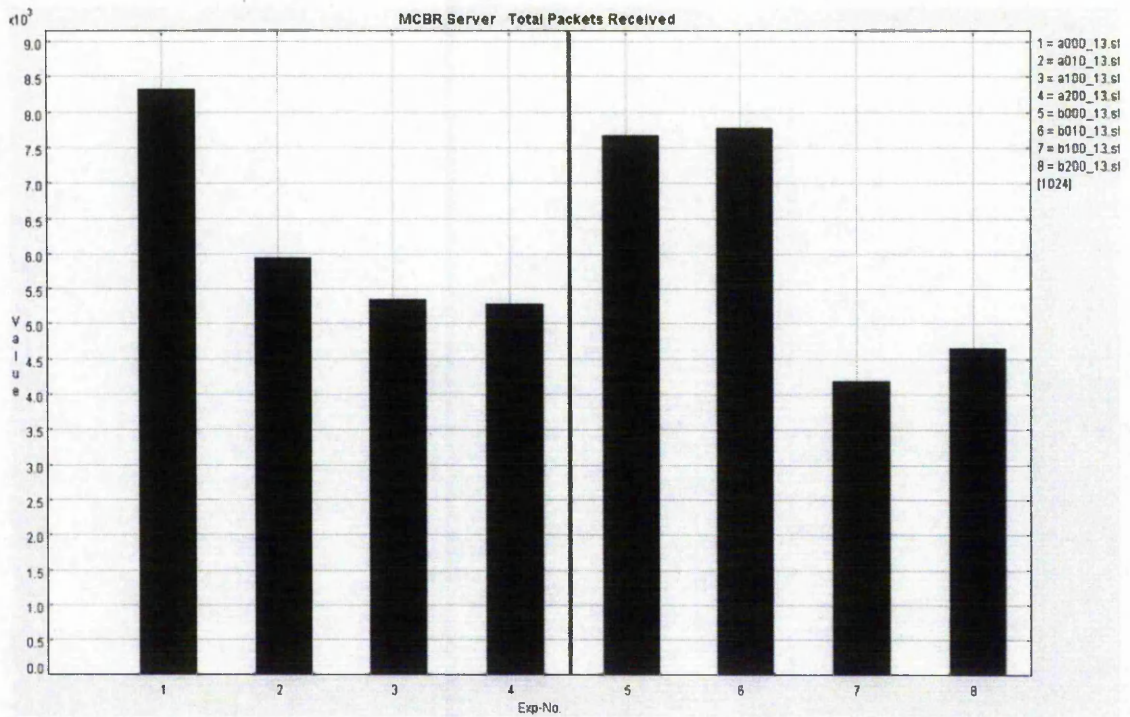


Figure 6.4 Precipitation impact on received packets on SDC (exp. 1-4) and LDC1 (exp. 5-8)

The result shows:

- The precipitation increases the delay and reduces the number of received packets (exp. 1 against 2, 3, 4 and exp. 5 against 6, 7, 8).
- The SDC is more sensitive to rain due to using lower frequency. Delay degradation increases sharply even for 10ml/hr (exp. 1 against 2).
- LDC1 has better resistance to low precipitation (exp. 2 against 6).
- Although extreme cases like 100ml/hr happens rarely, rain can seriously endanger the system reliability
- Exp. 6 and 8 shows slightly more received packets which is caused by multi-path and reflection effect

6.3.2 Quality of Mix-Mode LDCAP Services

The CBR and VOIP application has been used to test network ability to handle mix-mode LDCAP applications. The CBR application has been selected due to its QoS ability (precedence tag). The CBR can resemble a tracing application which nodes send their position to AP.

Scenario: 200x200m crossroad with 20 low-speed nodes and one LS

Simulation time: 80s

Radio: 802.11b with omni-directional antenna, 11Mb/s

MAC protocol: CSMA and RP is Bellman-ford

Application: VOIP with 50ms packetization interval and 50s call duration and CBR 100 byte with 70ms interval

Referring to figure 6.5 the number of package for VOIP packets is reduced (exp. 2 and 3) and there is also delay for these applications (figure 6.6) but no effect on jitter. CBR packets even with high priority faces more delay (figure 6.7). This experiment proves that VOIP application can cope better than CBR. CBR applications cannot observe real-time framework in this condition.

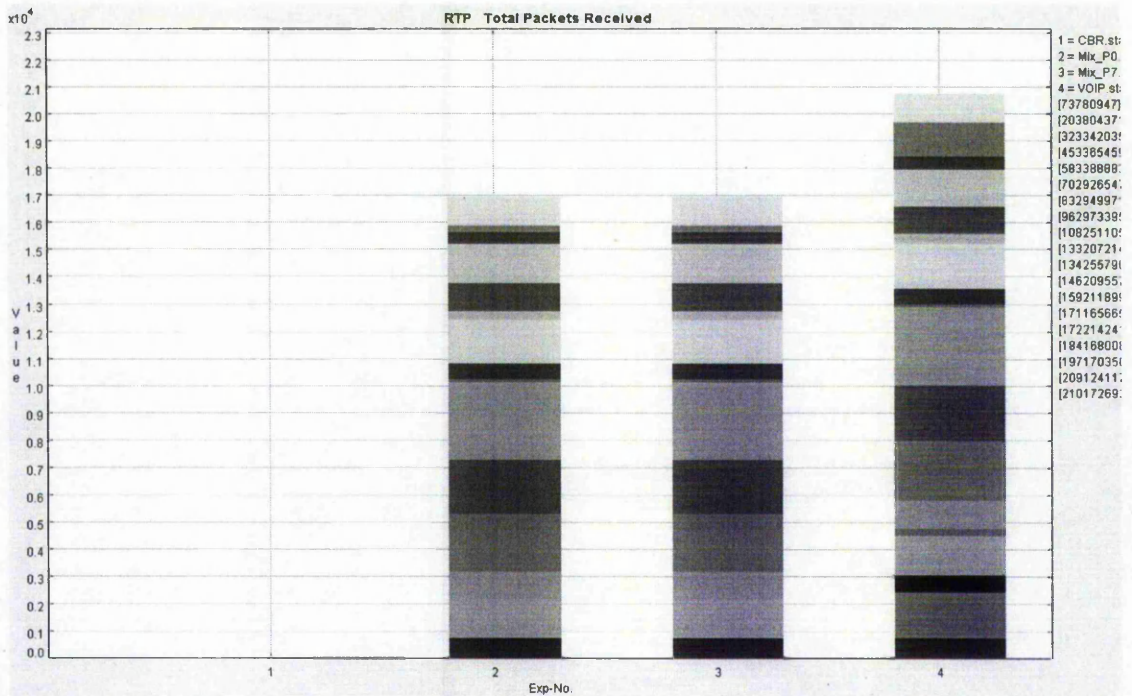


Figure 6.5 Number of VOIP packets received in mix-mode (exp. 2 and 3) and in VOIP alone (exp. 4)

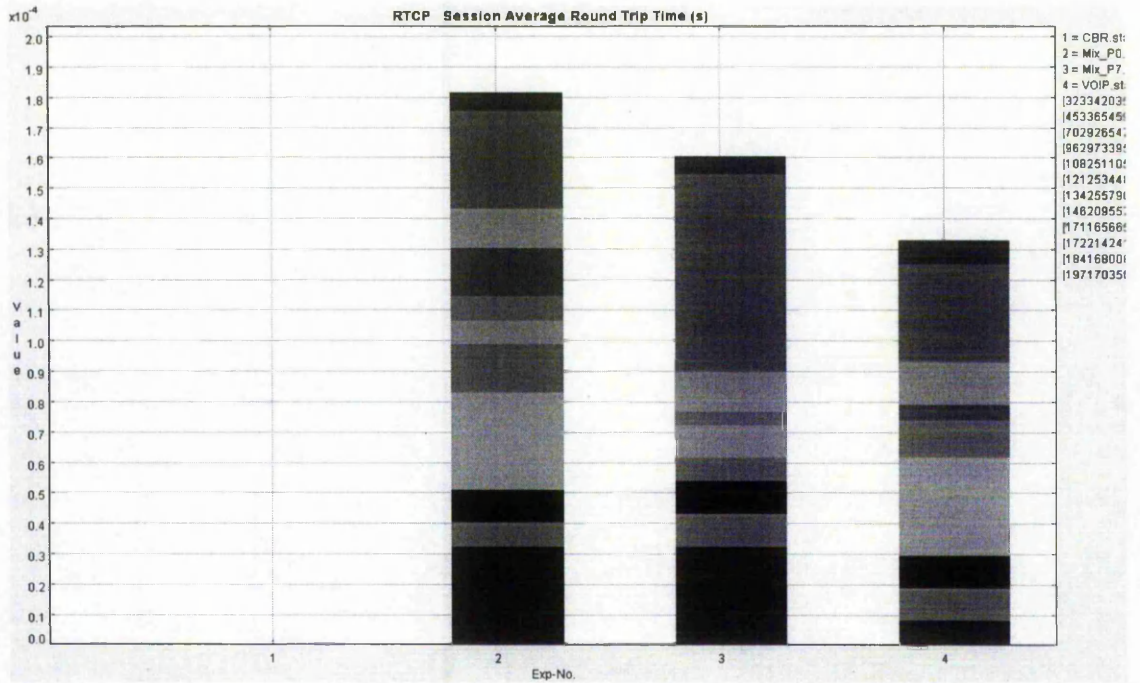


Figure 6.6 Average round trip time for VOIP packets in mix-mode (exp. 2 and 3) and in VOIP services alone (exp. 4)

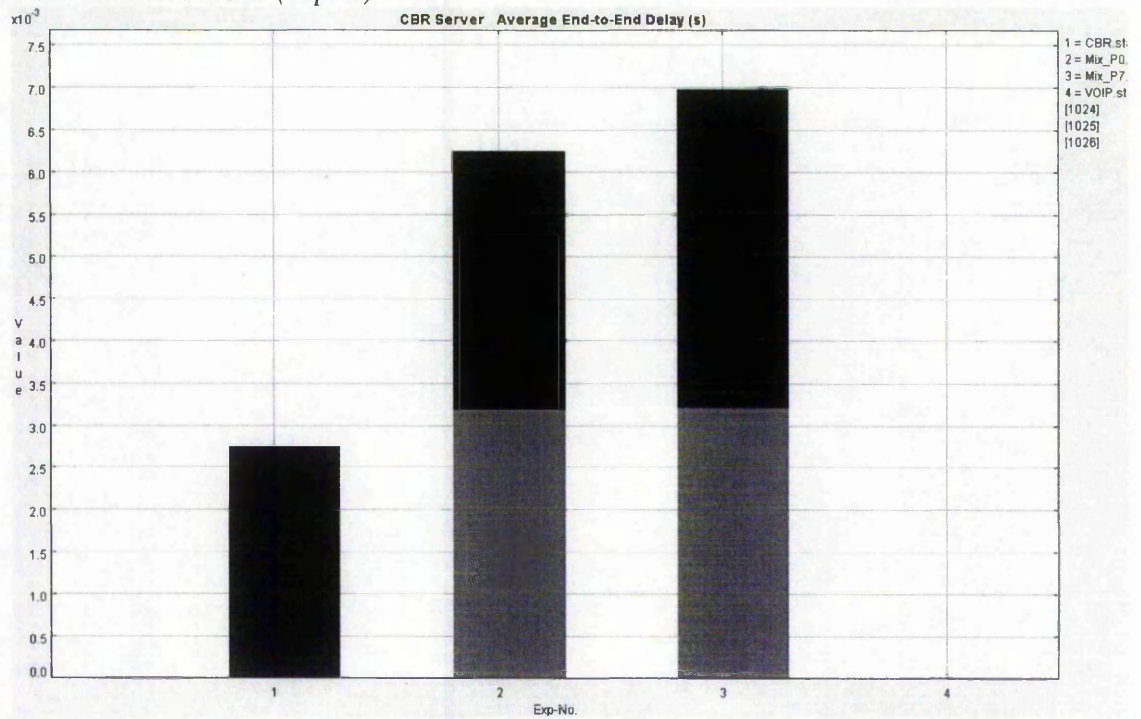


Figure 6.7 Average delays for CBR packets to get to destination in solely CBR services (exp. 1) and in mix-mode (exp. 2 and 3)

6.4 Conclusion

Due to insecurity of air medium, guaranteeing services for wireless systems is impossible but observing QoS do not follow conventional methods.

The real time requirements for core services make QoS more difficult to establish. This reveals the importance of identifying the influencing factors on QoS and measuring the

effects of them. System should be able to deal with the conditions autonomously and dynamically.

Some of the restrictive internal and external factors have been discussed and evaluated in this chapter. The tests in chapter three about most dominant factors such as node number and frequency of service proved that the VehINet can cope with them.

System tests under rainy condition showed the vulnerability of messaging with low wavelength. Even end-to-end delay in long wavelength hits the performance sharply under heavy rain. In normal rain condition the LDC1 works properly and its low messaging interval is justifiable by longer distance between the vehicles in this situation. The system under heavy rain as a main external factor should be investigated more thoroughly.

Simulation results in mix mode LDCAP services showed the negative impact of voice packets on core services. Giving higher priority to CBR packets could not resolve the problem. It means the systems should cut other services when the SDC can not deal with core services or when there are other high priority packets.

More tests need to be done to prove the system capability under combination or synergy of factors.

Chapter 7

Conclusion and Further Works

The proposed framework VehINet provides an integrated solution for wireless communication in vehicles while addressing its requirements and various challenges. It provides proper connectivity between different networks with high communication performance.

Although the WiFi solution is facing some internal and external deterring factors like multi-path effect and rain, in general simulation results meet the required specification of WiFi system for safe navigation. Other ADAS method should be used to cover system inability to function under harsh conditions.

VehINet model is suggested for accident prevention but more tests are required to find the optimum configuration for effective communication. This model brings endless opportunity for innovative applications running on dynamic infrastructure.

7.1 Research Contribution and Major Achievements

The research contribution in ITS and MANET fields can be summarised as:

- Present a model of MANET for communication between vehicular mobile nodes and prove the feasibility of system for short and long range communication by measuring the role of packet size, messaging interval and node speed on system performance
- Present a collaboration model of two radio technologies (802.11a and 802.11b) to separate services, increase performance and accelerate routing
- Prove the role of directional antenna to reduce the noise and improve the performance of WiFi hybrid system
- Investigate QoS constraints in VehINet and metering the effect of precipitation on system services and provide solutions for different situations

The role of MAC protocols as a major factor on system performance has been discussed and methods have been proposed to control flooding.

The achievements were mainly based on two major proposals:

1. Introducing two communicational systems to secure the real time specification and its value for fast routing
2. Using directional antenna and one-way flow of data to reduce contention

The qualitative and quantitative research outcome includes:

- Lack of GPS quality for IVC; complimentary method should use by MAC and Network layer
- The best interval for SDC measured 20-30ms and 50 -70ms for LDC1 services
- Packet size plays a major role in SDC performance, 50 byte or lower size suggested
- Directional antenna has a major role in the bandwidth optimisation and contention control
- The ability of 802.11b to cater SDC applications has been proved
- The research has found that the APs data transfer rate is a major bottleneck for LDCAP services
- The research has found that data transmission has an optimum point in performance improvement
- Speed has less effect on LDC services but increases the delay of SDC packets.
- ALOHA and CSMA are preferable MAC protocols in SDC and LDC respectively
- DSR performance is better than AODV for LDC routing
- Precipitation influences significantly the SDC performance and in heavy rain makes the LDC unreliable

The research has also proved that based on multiplicity of restrictive factors and in synergy of inhibiting parameters, the simulation environment cannot adequately model the system and show adequately the system behaviour. A pilot project should run on real test bed to include the factors discarded during simulation time and verify the findings of this research in practice.

7.2 Future Works

The plan for further research would be based on designing and implementing a new customized spatially aware MAC protocols in OPNET to be able to work with two

directional antennas. This makes it possible to have decision making based on position which yields a better measurements of system components such as max number of nodes and optimum interval of messaging. The benefit of this MAC would be:

- Ability to meter the performance of broadcasting model with Aloha mechanism
- Measure the effect of SDC and LDC1 without redundant beaconing
- Implement a model which consists of two wireless systems to measure the effectiveness of SDC RT in routing
- Measure the required APs capacity under maximum workload. Test the AP ability to handle the restrictions of switching-time in handoff process
- Testing the effectiveness of using channel dedication and channel splitting on the performance of LDC services
- Test the performance under the synergy of internal and external factors like manmade structures and potential WLAN

The simulation platform for single type of ad hoc network should be configured during the first phase of this future research. The interaction between Ad hoc models such as ordinary vehicles, traffic control, bus networks and cellular would be investigated in the next step.

The effectiveness of the system should be tested in conditions of lack of centralized data collection. In other words it should be tested to what extend the real-time feature of the system consisting of multiple ad hoc networks in local area can streamline traffic and prevent traffic issues in the management role of the centralized system. Although the research expects better traffic systems by VehINet, the quality issue in this system may reverse the prognosis of the effect on performance and which makes the tests necessary.

Simulation area is the most popular and cheapest place to validate the findings and algorithms, but simulations due to the cross-effect of the internal and external factors, cannot be error free. Due to lack of research in this field, the option of cross-validation was not available. Following this, as a final phase of research, running a pilot project would fill the gap of validation and simulations errors. This will also help to measure:

- System performance under the synergy of internal and external factors and especially the side effect of manmade structures on the system.

- System robustness in metropolitan area with potential interference of existing WLAN. In this sense the vulnerability of the systems during reduction of the number of communications would be measured too.

References

1. European Environment Agency, "Indicator Fact sheet-Number of Transport Accidents, fatalities and injuries", 2003, themes.eea.eu.int/Sectors_and_activities/transport/indicators/demand/TERM09.2003/TERM_2003_09_EU15.pdf, [Accessed 10 Feb 2005]
2. European Commission, "European Transport Policy for 2010", 2001, http://europa.eu.int/comm/energy_transport/library/press-kit-lben.pdf
3. U.S. Department of Transportation, "National ITS Architecture Version 5.0", April 2004, www.iteris.com/itsarch, [Accessed 6 Jan 2005]
4. Sinkkonen J., Suontausta T., Tiitto P., Hännikäinen M., Kaisto I., Hämäläinen T., "Information Server for Bus Operators", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
5. Nottingham Trent University, 2001, "ATTAIN - Advanced Traffic and Travel Information system", www.doc.ntu.ac.uk/RTTS/Projects/grr32468/stage1.html, [Accessed 10 May 2004].
6. Thomas M. Peytchev E. Al-Dabass D., 2003, "Auto-Sensing and Distribution of Traffic in Vehicular Ad hoc Networks", ducati.doc.ntu.ac.uk/uksim/uksim'04/Papers/NTU%20papers/Michael%20Thomas-%2004-17/paper04-17%20CR.pdf, [Accessed 4 May 2004].
7. BMW Board, 2003, "Talking cars for less congestion – The future of Telematics", www.bmwboard.com/news/view.asp?linkid=378, [Accessed 10 May 2004].
8. Inoue T., Nakata H., Itami M., Itoh K., "An Analysis of Incident Information Transmission performance using an IVV System that assigns PN codes to the Locations on the Road", 2004, IEEE Intelligent Vehicles Symposium 14-17 June 2004 Parma, Italy
9. Louwerse W.J.R., Hoogendoorn S.P., "ADAS Safety Impacts on Rural and Urban Highways", 2004, IEEE Intelligent Vehicles Symposium 14-17 June 2004 Parma, Italy
10. Bellocci V., Genovese S., Inuaggiato D., Tucci M., "Mobile Location Aware Services", 2002, Ericsson, division Service Architecture and Interactive Solutions
11. Schiller J., Voisard A., "Location-Based Services", 2004, Elsevier Inc.
12. "CAN - Controller Area Network", 2004, Kvasar AB, <http://www.kvaser.com/can/>, [Accessed 6 May 2004].

13. Akyildiz I.F. Su W. Cayirci E. Yogesh , "A Survey on Sensor Networks", 8/2002, www.cs.ccu.edu.tw/~yschen/papers/91-2.pdf, [Accessed 4 May 2004].
14. NASA, "NASA/JPL Sensor Webs Project", 2004, <http://sensorwebs.jpl.nasa.gov>, [Accessed 6 May 2004].
15. "Valeo's Revolutionary Lane Departure Warning System Makes Debut On Nissan Infiniti Vehicles", 2004, www.driveandstayalive.com/info%20section/news/individual%20news%20articles/y_040331_valeo-lane-departure-warning-system.htm
16. DaimlerChrysler, "Frequencies for Increased Safety", 2003, HighTech Report, www.daimlerchrysler.com/Projects/c2c/channel/documents/201437_htr2003_2_accidentfree_e.zip
17. "Honda Develops World's First Intelligent Night Vision System Able to Detect Pedestrians and Provide Driver Cautions", 2004, http://world.honda.com/news/2004/4040824_01.html
18. "Shortcoming of vision systems for traffic Cadillac Night Vision System", www.marlow.com/Applications/DSP/cadillac_night_vision_system.htm
19. Mao S., Lin S., Panwar S.S., Wang Y., "A Multipath Video Streaming Test bed for Ad Hoc Networks", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA, http://128.238.38.41/video/vtc03_testbed.pdf
20. CarTalk2000, "Routing Protocol Implementation", 2003, www.cartalk2000.net/bausteine/bausteine/download.asp?kompid=746360&downid=15567&downdaid=6642&id=7304&sp=E&domid=687&zffz=1272004-40924-157, [Accessed 6 Jan 2005]
21. CarTalk2000, "Communication Architecture", 2002, www.cartalk2000.net, [Accessed 6 Apr 2005]
22. Redmill K.A., Fitz M.P., Nakabayashi S., "An Incident Warning System with Dual Frequency Communication Capability", 2003, IEEE Intelligent Vehicles Symposium proceeding, www.unwired.ee.ucla.edu/Assets/papers/IEEEincident0603.pdf
23. Wischhof L. Rohling H. Ebner A., 2002, "SOTIS: A Self-Organizing Traffic Information System", www.et2.tu-harburg.de/Mitarbeiter/Wischhof/VTC03_Wischhof.pdf, [Accessed 28 April 2004].
24. Rohling H., 2004, "Self Organizing Traffic Information System", www.et2.tu-harburg.de/Mitarbeiter/Wischhof/sotis/sotis.htm
25. FleetNet-Internet on the Road, 2004, www.et2.tu-harburg.de/fleetnet/english/documents.html

26. NS2 – The Network Simulator 2, 2005, www.isi.edu/nsnam/ns/ and www.winlab.rutgers.edu/~zhubinwu/html/network_simulator_2.html
27. “COMCAR - Communication and Mobility by Cellular Advanced Radio”, 2002, By Ericsson, DaimlerChrysler, Sony and T-systems Nova, www.comcar.de
28. Dynamic Radio for IP-Services in Vehicular Environments, 2002, www.ist-drive.org
29. Hewlett-Packard, 2003, “HP Creates Advanced Wireless Environment for BMW WilliamsF1 Team”, www.hp.com/hpinfo/newsroom/press/2003/030722c.html, Palo Alto Ca, [Accessed 26 April 2004].
30. A. Mingkhwan, M. Merabti, B. Askwith, M. B. Hanneghan , “Global Wireless Framework”, 2003, Liverpool John Moores University, UK, European Personal Mobile Communications Conference (EPMCC'03), Glasgow, Scotland, April 22-25, 2003.
31. L. Lamont, M. Wang, L.Villasenor, T. Randhawa, S. Hardy, “Integrating WLANs & MANETs to the IPv6 based Internet”, 2003, ICC2003, www.crc.ca/en/html/manetsensor/home/publications/ICC2003.pdf
32. J. Chen, S.H. Gary Chan, J. He, S Liew, “Mixed-Mode WLAN: The Integration of Ad Hoc Mode with Wireless LAN Infrastructure”, 2003, Globecom 2003, www.ie.cuhk.edu.hk/fileadmin/staff_upload/soung/Conference/C13.pdf
33. N. Thanthy, R. Pendse, K.R. Namuduri, “Ad-Hoc Nodes and Internet Connectivity Using Pseudo-wire Interfaces”, 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
34. Cisco Metropolitan Mobile Network Solution, 2004, Cisco, www.cisco.com/en/US/netsol/ns473/networking_solutions_package.html, , [Accessed 6 Jan 2005]
35. “London's Westminster City Council Goes to Town with Cisco Wireless Technology”, 2004, http://newsroom.cisco.com/dlls/2004/hd_062104.html, [Accessed 28 April 2004].
36. Topham D.A., Ward D., Arvanitis T.N., Constantinou C.C., 2003, “Inter-vehicle communications based on mobile ad hoc networks”, Proceedings of the 1st IEE International Conference on Sensors, Navigation and Communications for Vehicle Telematics (VehCom 2003), 135-140, 2003.
37. Chan A.Y., Lu W., "Architecture for Wireless Access in Vehicles", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
38. Martinez-Barbera H., Zamora-Irquierdo M.A., Toledo-Moreo R., Ubeda B., Gomez-Skarmeta A., “The MIMICS Project: An Application for Intelligent Transport Systems”,

- June 2003, Dept. of Inf. & Communications Engineering., Murcia Univ., Spain; IEEE Intelligent Vehicles Symposium Proceedings, 2003.
39. Jain R., "A Review of Key Networking Concepts", 1999, Ohio state University, www.cse.ohio-state.edu/~jain/cis788-99/ftp/h_1fund/sld004.htm
40. Almere, "Hopling Technologies announces the deployment of Amsterdam, the first true WiFi metropolitan city in Europe", 2004, http://82.148.221.130/hopling.com/news_20August2004.htm, [Accessed 6 Jan 2005]
41. "WAND - Wireless Ad hoc Network for Dublin", 2004, www.dsg.cs.tcd.ie/dynamic/?category_id=-2, [Accessed 6 Jan 2005]
42. Silicon press, "Before 3G Wireless Networks Technology Brief", www.siliconpress.com/briefs/brief.before3g, [Accessed 6 Jan 2005]
43. "Introducing Birdstep Intelligent Mobile IP ClientV2.0 Universal Edition", 2005, Birdstep Technology, www.birdstep.com/collaterals/MIP%20v2.0%20presentation.pdf, [Accessed 6 Jan 2005]
44. Shelby Z., Mähönen P., Riihijärvi J., Raivio O., Huuskonen P., "NanoIP: The Zen of Embedded Networking", 2003, In Proc. IEEE ICC 2003, May 12-18th, 2003, www.ee.oulu.fi/~zdshelby/home/work/nanoip.pdf
45. X. Zhang, Q. Wang, D. Wan, "The Relationship among Vehicle Positioning Performance, Map Quality, and Sensitivities and Feasibilities of Map-Matching Algorithms",
46. Ajmerna D., Castro P., Kremenek T., Mani M., "The Nibble Location System", 2001, University of California, <http://mmsl.cs.ucla.edu/nibble>
47. "Mobile Positioning System", 2004, Ericsson, www.ericsson.com/mobilityworld/sub/open/technologies/mobile_positioning/index.htm
48. Dashwerks Inc, "DashPC (LinuxCar)", www.dashpc.com, [Accessed 6 Jan 2005]
49. GpsDrive (GPS Navigation Software for Linux), www.kraftvoll.at/software, [Accessed 6 Jan 2005]
50. G-Net, "G-NET Vehicle PC Features", 2004, www.gnetcanada.com/vehiclepc-aurora.htm, [Accessed 20 Jan 2005]
51. Roth J., Dpunkt-Verlag, "Mobile Computing", 2002
52. ATLANTIC, A Thematic Long-term Approach to Networking for the Telematics and ITS Community, "Intelligent Vehicle and Intelligent Vehicle-Highway System", 2004, Synopsis of Work Group 2.2 by A Partnership of ITS Communities in Europe and North America, www.crt.umontreal.ca/atlantic/pdf/2-2Syn.pdf

53. Irnich, T., Schultz, D.C., Pabst, R., Wienert, P., "Capacity of a Relaying Infrastructure for Broadband Radio Coverage of Urban Areas", 10/2003, Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, Page(s): 2886- 2890 Vol.5,
<http://ieeexplore.ieee.org/iel5/9004/28572/01286146.pdf?tp=&arnumber1286146&isnumber=28572>
54. Pabst R., Walke B., Schultz D. C., "A Mobile Broadband System Based on Fixed Wireless Routers", 2003, ICCT 2003, volume 2 pp. 1310–17 Beijing, China,
<http://ieeexplore.ieee.org/iel5/8586/27227/01209771.pdf?tp=&arnumber1209771&isnumber=27227>
55. Pabst R., Walke B., Schultz D. C., "Relay-Based Deployment Concepts for Wireless and Mobile Broadband Radio", 2004, IEEE Communications Magazine,
www.sce.carleton.ca/faculty/yanikomeroğlu/Pub/ComMag04.pdf
56. Mesh Dynamics, "Why Structured Mesh is Different?", 2004,
www.meshdynamics.com/WhyStructuredMesh.html
57. Velayos H., Karlsson G., "Techniques to Reduce IEEE 802.11b MAC Layer Handover Time", 2003, Royal Institute of Technology, Stockholm, Sweden,
www.it.kth.se/~hvelayos/papers/TRITA-IMIT-LCN%20R%2003-02%20Handover%20in%20IEEE%20802.pdf
58. Brewin B., "Combo Wi-Fi, Cell Phone Coming Soon", 2004,
www.pcworld.com/news/article/0,aid,116334,00.asp, [Accessed 6 Jan 2005]
59. Ikawa M., Goto Y., Igarashi Y., Kumazawa H., Koizumi K., Oka K., "DSRC Local Communication Platform and its Application to Information Push Services", 2004, IEEE Intelligent Vehicles Symposium 14-17 June 2004 Parma, Italy,
<http://ieeexplore.ieee.org/iel5/9278/29469/01336364.pdf?tp=&arnumber1336364&isnumber=29469>
60. QualNet, 2005, Scalable Network Technologies Inc., www.qualnet.com
61. OPNET, 2005, OPNET Technologies Inc., www.opnet.com
62. Piao J., McDonald M., "low speed car following Behaviour from Floating Vehicle Data", 2003, IEEE Intelligent Vehicles Symposium COLUMBUS, OHIO, USA, JUNE 9-11, 2003,
<http://ieeexplore.ieee.org/iel5/8598/27237/01212955.pdf?tp=&arnumber1212955&isnumber=27237>
63. T.Nagaosa, Y.Kobayashi, K. Mori, H. Kobayashi, "An Advanced CSMA Inter-vehicle Communication system Using Packet Transmission Timing Decided by the

- Vehicle Position", 2004, IEEE Intelligent Vehicles Symposium 14-17 June 2004 Parma, Italy,
<http://ieeexplore.ieee.org/iel5/9278/29469/01336365.pdf?tp=&arnumber1336365&isnumber=29469>
64. Muqattash A., Krunz M., "CDMA-based MAC protocol for wireless ad hoc networks", 2003, International Symposium on Mobile Ad Hoc Networking & Computing, www.sigmobile.org/mobihoc/2003/papers/p153-muqattash.pdf
65. Hui J., Devetsikiotis M., "Designing Improved MAC Packet Schedulers for 802.11e WLAN", 2003, Proceedings of IEEE Globecom 2003,
<http://ieeexplore.ieee.org/iel5/8900/28132/01258227.pdf?tp=&arnumber1258227&isnumber=28132>
66. Cesana M., Maniezzo D., Bergamoy P., Gerla M., "Interference Aware (IA) MAC: an Enhancement to IEEE802.11b DCF", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA,
www.cs.ucla.edu/NRL/wireless/uploads/vtc2003ia.pdf
67. Chen W., Pan M., Dai J., "An Adaptive MAC Protocol for Wireless Ad Hoc Network Using Smart Antenna System", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA,
<http://ieeexplore.ieee.org/iel5/9004/28572/01286109.pdf?tp=&arnumber1286109&isnumber=28572>
68. Jose B., Yin H., Mehrotra P., Casas E., "MAC layer Issues and Challenges of using Smart Antenna with 802.11", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA,
<http://ieeexplore.ieee.org/iel5/9004/28572/01286217.pdf?tp=&arnumber1286217&isnumber=28572>
69. Singh H., Singh S., "DOA-ALOHA: Slotted ALOHA for Ad Hoc Networking Using Smart Antenna", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA,
<http://ieeexplore.ieee.org/iel5/9004/28572/01286112.pdf?tp=&arnumber1286112&isnumber=28572>
70. Rudack M., Meincke M., Lott M., Jobmann K., "On Traffic Dynamical Aspects of Inter Vehicle Communications (IVC)", 2003, Proc. VTC 2003, Orlando, USA,
www.et2.tu-harburg.de/fleetnet/pdf/VTC03_dynamic_final_0.2.pdf
71. Borgonovo F., Campelli L., Cesana M., Coletti L., Milano P., "MAC for Ad Hoc inter-vehicle network: services and performance", 2003, IEEE 58th Vehicular

Technology Conference 6-9 Oct 2003 Orlando, Florida USA,

www.elet.polimi.it/upload/cesana/papers/VTC2003-AD.pdf

72. Wu M., "A Survey of MAC Protocols in Ad Hoc Networks", 2004, The University of Texas at Dallas, www.utdallas.edu/~mxw013200/MAC_ADHOC.html

73. Padmini M., "Routing Protocols for Ad Hoc Mobile Wireless Networks", www.cse.ohio-state.edu/~jain/cis788-99/ftp/adhoc_routing

74. Harding C., Yu H., Griffiths A., "Review of Broadcast Methods for MANETs", 2005, University of Staffordshire, www.soc.staffs.ac.uk/cah1/6thIWBradford.pdf

75. Ferriere H.D., Grossglauser M., Vetterli M., "Age Matters: Efficient Route Discovery in Mobile Ad Hoc Networks Using Encounter Ages", 2003, www.sigmobility.org/mobihoc/2003/papers/p257-dubois.pdf

76. Gwalani S., Belding-Royer E.M., Perkins C.E., "AODV-PA: AODV with Path Accumulation", 2003, IEEE International Conference on Communications (ICC '03), <http://ad.informatik.uni-freiburg.de/lehre/ws0405/mobcomputing/resources/papers/aodv-pa.pdf>

77. Gui C., Mohapatra P., "SHORT: Self-Healing and Optimizing Routing Techniques for Mobile Ad Hoc Networks", 2003, MobiHoc 2003, www.sigmobility.org/mobihoc/2003/papers/p279-gui.pdf

78. Song J., Wong V.W.S., Leung V.C.M., "Efficient On-Demand Routing for Mobile Ad Hoc Wireless Access Networks", 2003, Globecom2003-Wire Communications, Dec. 1-5, 2003, www.ece.ubc.ca/~vleung/journal_papers/jsac/song0904.pdf

79. Kim B.C., Lee J.Y., Lee H.S., "An Ad-hoc Routing Protocol with Minimum Contention Time and Load Balancing", 2003, Globecom2003-Wire Communications, Dec. 1-5, 2003.

80. Best P., Gundeti S., Pendse R., "Self-Learning Ad-Hoc Routing Protocol", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA, <http://ieeexplore.ieee.org/iel5/9004/28572/01286118.pdf?tp=&arnumber1286118&isnumber=28572>

81. Renesse R., Ghassemian M., Friderikos V., Aghvami A.H., "QoS Enabled Routing in Mobile Ad hoc Networks", Electrical Engineering Department, Centre for Telecommunications Research, King's College London, UK, www.ctr.kcl.ac.uk/members/mona/files/3G-2004-KCL.pdf

82. P. Sinha, R. Sivakumar, V. Bharghavan, "CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm", 1999, University of Illinois, www.merunetworks.com/infocom99.cedar-CEDAR.pdf

83. Sadagopany N., Bai F., Krishnamachari B., Helmy A., "PATHS: Analysis of PATH Duration Statistics and their Impact on Reactive MANET Routing Protocols", 2003, MobiHoc 2003, www.sigmobile.org/mobihoc/2003/papers/p245-sadagopan.pdf
84. Santos R.A., Edwards R.M., Seed N.L., "Inter Vehicular Data Exchange between Fast Moving Road Traffic Using an Ad-hoc Cluster-Based Location Routing Algorithm and 802.11b Direct Sequence Spread Spectrum Radio", 2003, PGNet 2003, www.cms.livjm.ac.uk/pgnet2003/submissions/Paper-04.Pdf
85. Denko M., Mahmoud Q.H., "Mobile Agents for Clustering and Routing in Mobile Ad-Hoc Networks", 2003, ADHOC-NOW 2003, Montreal, Canada, October 8-10, 2003.
86. Shah R., Hutchinson N.C., "Delivering Messages in Disconnected Mobile Ad-Hoc Networks", 2003, Second International Conference of ADHOC-NOW 2003, Montreal, Canada, October 8-10, 2003.
87. Doshi J., Kilambi P., "SAFAR: An Adaptive Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks", 2003, ADHOC-NOW 2003, Montreal, Canada, October 8-10, 2003, <http://www-users.cs.umn.edu/~prahlad/safar.pdf>
88. Ramasubramanian V., Haas Z.J., Sirer E.G., "SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks", 2003, MobiHoc 2003, www.cs.cornell.edu/People/egs/papers/sharp.pdf
89. Saha D., Roy S., Bandyopadhyay S., Ueda T., Tanaka S., "An Adaptive Framework for Multipath Routing via. Maximally Zone-Disjoint Shortest Paths in Ad hoc Wireless Networks with Directional Antenna", 2003, Globecom2003-Wire Communications, Dec. 1-5, 2003, www.iimcal.ac.in/research/adhocnet/Papers/8.pdf
90. Dai F., Wu J., "Performance Analysis of Broadcast Protocols in Ad Hoc Networks Based on Self-Pruning", 2004, IEEE Transactions on Parallel and Distributed Systems Nov 2004, http://polaris.cse.fau.edu/~jie/research/publications/Publication_files/wcnc04-fei.pdf
91. "Dedicated Short-Range Communications (DSRC) for AHS Services", 2004, IEEE Intelligent Vehicles Symposium 14-17 June 2004 Parma, Italy
92. Williams B., Camp T., "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks", 2002, Department of Math and Computer Science Colorado School of Mines, www.ceid.upatras.gr/faculty/manos/courses/mobnets/papers_site/compar_brdcst_tecks.pdf

93. Yao P., Krohne E., Camp T., "Performance Comparison of Geocast Routing Protocols for a MANET", 2004, Proceedings of the 13th IEEE International Conference on Computer Communications and Networks (IC3N), 2004
94. Maihofer C., "A Survey of Geocast Routing Protocols", 2004, DaimlerChrysler AG, Research & Technology (RIC/TC),
www.comsoc.org/livepubs/surveys/public/2004/apr/maihofer.html
95. Ko Y., Vaidya N.H., "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", 2000, Department of Computer Science, Texas A&M University, College Station, USA, 4th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 66-- 75, October 1998.,
www.cs.huji.ac.il/labs/danass/sensor/adhoc/routing/ko_1998locationaidedrouting.pdf
96. Maihofer C., Cseh C., Franz W., Eberhardt R., "Performance Evaluation of Stored Geocast", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida, USA,
<http://ieeexplore.ieee.org/iel5/9004/28572/01286151.pdf?tp=&arnumber1286151&isnumber=28572>
97. Singh J.P., Bambos N., Srinivasam B., Clawin D., "Proposal and Demonstration of link Connectivity Assessment based Enhancement to Routing in Mobile Ad-hoc Network", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
98. Zou X., Ramamurthy B., Magliveras S., "Routing Techniques in Wireless Ad Hoc Networks Classification and Comparison",
http://csce.unl.edu/~xkzou/papers/routing_schemes.pdf
99. Nikander J., Lim, Xu, Gerla, "TCP Performance over Multipath Routing in Mobile Ad Hoc Networks", 2003, IEEE ICC, 2003,
www.cs.ucla.edu/NRL/wireless/uploads/kxu_icc03.pdf
100. Dyer T. D., Boppana R.V., "A Comparison of TCP Performance over Three Routing Protocols for Mobile Ad Hoc Networks", 2001, Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, Pages: 56 – 66, <http://cs.brown.edu/courses/cs296-2/papers/wireless-tcp.pdf>
101. Demetrios Z.Y., "A Glance at Quality of Services in Mobile Ad-Hoc Networks", 2001, Department of Computer Science, University of California, USA,
www.cs.ucr.edu/~csviazti/courses/cs260/html/manetqos.html
102. Nikaein N., Bonnet C., "A Glance at Quality of Service Models for Mobile Ad Hoc Networks", 2002, Institut Eur'ecom, www.eurecom.fr/~nikaeinn/qos.pdf

103. Cisco Systems, "Quality of Service Networking", 2002, Quality of Service, chapter 49, www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.pdf,
www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm#1020570
104. Kerényi L.S., "Survey of capacity and traffic performance at a 'T'-intersection in Trondheim, Norway", 1998, www.vit.bme.hu/tdk/1998/klstdk98.doc
105. Diederich J., Zitterbart M., "A Service Model to Provide Quality of Service in Wireless Network Focusing on Usability", 2003, Proceedings of the 8th International Workshop on Mobile Multimedia Communications (MOMUC 2003), Munich, Germany, IEEE, October 2003, www.l3s.de/~diederich/Papers/momuc2003.pdf
106. To V.S.Y., Bensaou B., Chau S.M.K., "Quality of service Framework in MANETs Using Differentiated Services", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
<http://ieeexplore.ieee.org/iel5/9004/28572/01286358.pdf?tp=&arnumber1286358&isnumber=28572>
107. Jun J., Sichitiu M.L., "Fairness and QoS in Multihop Wireless Network", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA,
<http://www4.ncsu.edu/~mlsichit/Research/Publications/fairnessVTC.pdf>
108. Le Grand G., Meraihi R., Tohmé S., Riguidel M., "Intelligent ambient ad hoc networking to support real-time services", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
109. Bless R., Zitterbart M., Hillebrand J., Prehofer C., "Quality-of-service signalling in Wireless IP-Based Mobile Networks", 2003, VTC2003-Fall, Orlando, FL, USA, October 6-9, 2003, IEEE
<http://ieeexplore.ieee.org/iel5/9004/28572/01286383.pdf?tp=&arnumber1286383&isnumber=28572>
110. Hillebrand J., Prehofer C., Bless R., Zitterbart M., "Quality-of-Service Signaling for Next-Generation IP-Based Mobile Networks", 2004, IEEE Communication Magazine, June 2004, www.prehofer.de/Papers/IEEE-Commag-2004-06-QoS-Signaling.pdf
111. Gao X., Wu G., Miki T., "QoS Framework for mobile heterogeneous networks", 2003, IEEE International Conference on Communications (ICC 2003), vol. 26, no. 1, pp. 933 – 937,
<http://ieeexplore.ieee.org/iel5/8564/27114/01204476.pdf?tp=&arnumber1204476&isnumber=27114>

112. Wei Y., Lin C, Ren F., Raad R, Dutkiewicz E., "Dynamic Priority Handoff Scheme in Differentiated QoS Wireless Multimedia Networks", 2003, June 30 - July 03 Kemer-Antalya, Turkey,
<http://csdl.computer.org/comp/proceedings/iscc/2003/1961/00/19610131abs.htm>
113. Rubin I., Liu Y., "Link Stability Models for QoS Ad Hoc routing Algorithms", 2003, IEEE 58th Vehicular Technology Conference 6-9 Oct 2003 Orlando, Florida USA
114. Newman D., "Voice over Wireless LAN", 2005, Network World,
www.nwfusion.com/reviews/2005/011005rev.html
115. CarTalk2000, "Specification of Safety Requirements for Communication Protocols", 2003, www.cartalk2000.net , [Accessed 6 Apr 2005]
116. Thomas J., "802.11e brings QoS to WLANs", 2003, Network World,
www.nwfusion.com/news/tech/2003/0623techupdate.html
117. Miller B.W., Hwang C.E., Torkkola K., Massey N., "An Architecture for an Intelligent Driver Assistance System", 2003, Intelligent Systems Lab Motorola Inc. AZ, USA, IEEE Intelligent Vehicles Symposium Proceedings June 2003.

Appendix

A. Specification of Simulation Tools used in research

QualNet (Simulating Application)

Application: QualNet version 3.8
Producer: Scalable Network Technologies
Tools: Feasibility study of VehINet and measuring the optimum communication factors for SDC and LDC

OPNET (Simulating Application)

Application: OPNET Modeler and OPNET IT Guru version 11.0.A
Producer: OPNET Technologies Inc.
Tools: Design and implementing MAC protocol to work with two directional antennas

B. Contents of the included CD

10M_SDC_20_200_CR10
Simulation model to test SDC and LDC1 for 20 nodes in crossroad (area 200x200m)

16M_SDC_20_200_CR10
Simulation model to test SDC and LDC1 for 20 nodes in crossroad (area 200x200m)

18M_SDC_20_200_CR10_all_Weather
Simulation model to test the effect of precipitation on SDC and LDC1 for 20 nodes in crossroad (area 200x200m)

31_SDC_20_500x500_RD
Simulation model to test the effect of directional antenna on SDC and LDC1 for 20 nodes in two-way road (area 500m)

32_SDC_20_500x500_OWRD
Simulation model to test SDC and LDC1 for 20 nodes in one-way road (area 500m)

40M_LDC2_20_200_CR
Simulation model to test LDC2 for 20 nodes in crossroad (area 200x200m)

60_LDCAP_20_200x200_CR
Simulation model to test LDCAP for 20 nodes in crossroad (area 200x200m)

NS.antenna-azimuth.txt
North-south azimuth for communication in one-way and two-way road with directional antenna

Road.Mobility.txt
Mobility file which defines the waypoint for nodes in two-way road scenario

Applications.txt
Collection of all applications used to test scenarios

C. Some of the applications used in QualNet models

Multicast constant bit rate to test SDC: 50 byte packet, interval 20ms, transmission= 2000 times

```
MCBR 1 225.0.0.0 2000 50 20MS 0S 0S
MCBR 2 225.0.0.0 2000 50 20MS 0S 0S
MCBR 3 225.0.0.0 2000 50 20MS 0S 0S
MCBR 4 225.0.0.0 2000 50 20MS 0S 0S
MCBR 5 225.0.0.0 2000 50 20MS 0S 0S
MCBR 6 225.0.0.0 2000 50 20MS 0S 0S
MCBR 7 225.0.0.0 2000 50 20MS 0S 0S
MCBR 8 225.0.0.0 2000 50 20MS 0S 0S
MCBR 9 225.0.0.0 2000 50 20MS 0S 0S
MCBR 10 225.0.0.0 2000 50 20MS 0S 0S
MCBR 11 225.0.0.1 2000 50 20MS 0S 0S
MCBR 12 225.0.0.1 2000 50 20MS 0S 0S
MCBR 13 225.0.0.1 2000 50 20MS 0S 0S
MCBR 14 225.0.0.1 2000 50 20MS 0S 0S
MCBR 15 225.0.0.1 2000 50 20MS 0S 0S
MCBR 16 225.0.0.1 2000 50 20MS 0S 0S
MCBR 17 225.0.0.1 2000 50 20MS 0S 0S
MCBR 18 225.0.0.1 2000 50 20MS 0S 0S
MCBR 19 225.0.0.1 2000 50 20MS 0S 0S
MCBR 20 225.0.0.1 2000 50 20MS 0S 0S
```

Variable bit rate emulate html pages (LCD2): 1024 byte packet, randomly every 1 second

```
VBR 1 2 1024 1S 0S 0S
VBR 2 3 1024 1S 0S 0S
VBR 3 4 1024 1S 0S 0S
VBR 4 5 1024 1S 0S 0S
VBR 5 6 1024 1S 0S 0S
VBR 6 7 1024 1S 0S 0S
VBR 7 8 1024 1S 0S 0S
VBR 8 9 1024 1S 0S 0S
VBR 9 10 1024 1S 0S 0S
VBR 10 11 1024 1S 0S 0S
VBR 11 12 1024 1S 0S 0S
VBR 12 13 1024 1S 0S 0S
VBR 13 14 1024 1S 0S 0S
VBR 14 15 1024 1S 0S 0S
VBR 15 16 1024 1S 0S 0S
VBR 16 17 1024 1S 0S 0S
VBR 17 18 1024 1S 0S 0S
VBR 18 19 1024 1S 0S 0S
VBR 19 20 1024 1S 0S 0S
VBR 20 1 1024 1S 0S 0S
```

Voice over IP between pair of nodes (LCD2): 1024 byte packet, randomly every 1 second

```
VOIP 1 2 50S 0S 0S ACCEPT 50MS
VOIP 3 4 50S 0S 0S ACCEPT 50MS
VOIP 5 6 50S 0S 0S ACCEPT 50MS
VOIP 7 8 50S 0S 0S ACCEPT 50MS
VOIP 9 10 50S 0S 0S ACCEPT 50MS
VOIP 11 12 50S 0S 0S ACCEPT 50MS
VOIP 13 14 50S 0S 0S ACCEPT 50MS
VOIP 15 16 50S 0S 0S ACCEPT 50MS
VOIP 17 18 50S 0S 0S ACCEPT 50MS
VOIP 19 20 50S 0S 0S ACCEPT 50MS
```

D. QualNet Model used in motorway scenario

VERSION 3.8

```
#           Results are written to EXPERIMENT-NAME.stat.
EXPERIMENT-NAME VehINet
SIMULATION-TIME 1M
SEED 1
#           nodes may not be too far away to transmit to each other.
PARTITION-SCHEME AUTO
COORDINATE-SYSTEM CARTESIAN
TERRAIN-DIMENSIONS (500, 500)
DUMMY-ALTITUDES (1500, 1500)
TERRAIN-DATA-BOUNDARY-CHECK YES
DUMMY-NUMBER-OF-NODES 20

#           Latitude-longitude-altitude terrain dimensions.
# COORDINATE-SYSTEM LATLONALT
# TERRAIN-SOUTH-WEST-CORNER (0, 0)
# TERRAIN-NORTH-EAST-CORNER (200, 200)
#           Specify one of the following terrain data types
#           - DEM (Digital Elevation Model):
#           Currently, only 1-degree DEM format is supported
#           - CTDB (Compact Terrain Data Base)
#           - DTED (addon)
# TERRAIN-DATA-TYPE DEM
# TERRAIN-DATA-TYPE CTDB
# DEM-FILENAME[0] ../data/terrain/los_angeles-w
# DEM-FILENAME[1] ../data/terrain/los_angeles-e
# CTDB-FILENAME nebosnia_mes
#           If TERRAIN-DATA-BOUNDARY-CHECK is set to YES (default), the simulation
terminates when it attempts to use an elevation not included
#           in the terrain data files. If it is NO, the execution simply assumes that such elevations
are 0.0.
# TERRAIN-DATA-BOUNDARY-CHECK NO
#           If MOBILITY-GROUND-NODE is set to YES, the elevation of node is retrieved from
the terrain data files. This overrides the
#           elevations specified in the mobility trace file. (default: NO)
# MOBILITY-GROUND-NODE YES
# WEATHER-CONFIG-FILE default.weather
#           Weather patterns are moved at infrequent intervals defined by this parameter.
# WEATHER-MOBILITY-INTERVAL 10S

#####
# Create a wireless or Ethernet/802.3 network consisting of nodes 1-30. The MAC-PROTOCOL and
PHY-MODEL parameters control the
# type of device specific to the network.
SUBNET N16-0 { 1 thru 30 }

# If you enable these lines, comment out the SUBNET statement, change ROUTING-PROTOCOL to a
wired routing protocol, and remove/fix extra
# lines in the applications file (default.app).
# You CAN have both SUBNET and LINK statements in the same scenario, but you'll have to be careful
about assigning RP to each network

# Create three links with this topology: 1 --- 2 --- 3 --- 4. Each link is a point-to-point (serial) link
between two nodes. These
# links are dedicated, error-free, and support the maximum bandwidth in both directions simultaneously.
# LINK N2-1.0 { 1, 2 }
# LINK N2-2.0 { 2, 3 }
# LINK N2-3.0 { 3, 4 }
#           Point-to-point links can be of wired or wireless type. default(wired)
```

```

# LINK-PHY-TYPE          WIRED | WIRELESS
#                      Link bandwidth in bps
LINK-BANDWIDTH          112000

# Link propagation delay for wired point-to-point links is specified below.
# Propagation delay for wireless point-to-point links is based on distance.
LINK-PROPAGATION-DELAY  50MS

# If an exact link level header size is needed, specify below. Otherwise,
# it is defaulted to 224 bits (28 bytes).
# LINK-HEADER-SIZE-IN-BITS 40
# BACKGROUND-TRAFFIC-CONFIG-FILE default.bgtraffic

# [node-id] INTERFACE-TYPE[interface-index] interface-type interface-number
#
# interface types: ASYNC, ATM, BRI, BVI, CABLE, CBR, DIALER, ETHERNET, FDDI,
GROUP_ASYNC, HSSI, LEX, LOOPBACK, NULL_INTERFACE,
#   PORT_CHANNEL, SERIAL, TOKENRING, TUNNEL, VIRTUAL_TEMPLATE,
VIRTUAL_TOKENRING, VLAN
# Example:
# [3] INTERFACE-TYPE[1] Serial 5/1

# IPv4
# N syntax      Network address Subnet mask   Slash notation
# N16-0         0.0.0.0      255.255.0.0   0.0.0.0/16
# N2-1.0        0.0.1.0      255.255.255.252 0.0.1.0/30
# N8-192.168.0.0 192.168.0.0   255.255.255.0   192.168/24
# N24-10.0.0.0   10.0.0.0     255.0.0.0       10/8
#
# assigned automatically starting with the first IP address after the network address, e.g.,
# N16-0 { 1 thru 30 }
# nodeId      IP address   Subnet mask
# 1           0.0.0.1      255.255.0.0
# 2           0.0.0.2      255.255.0.0
# ...
# N8-2.0 { 5, 3, 1 }
# 5           0.0.2.1      255.255.255.0
# 3           0.0.2.2      255.255.255.0
# 1           0.0.2.3      255.255.255.0
#
# Restrictions:
# Network addresses must be unique. (different masks don't help!)
# Only one IP address is assigned per interface, and this IP address must be unique. (Multiple 192.168/24
private networks and secondary IP addresses are not supported.)
# Nodes possessing multiple interfaces are supported, but care must be taken in selecting RPs.
#
# N syntax long explanation:
# The number after N is the number of bits used for the hostid; 32 minus this number is the number of bits
used for the networkid.
# The string following the hyphen is the right-most part of the network address, implicitly preceded by
zeroes as necessary.

# You can also use the N syntax to restrict parameters to certain networks, e.g.,
#
# [N2-2.0] LINK-BANDWIDTH      300
# [N2-2.0] LINK-PROPAGATION-DELAY 500MS
#
# tells QualNet that any links in the N2-2.0 network operate at 300 bps with 500 ms propagation delay.
You can use these qualifiers to
# restrict routing protocols to certain networks, and so on. Within the brackets, you can also specify
nodeIds and IP addresses; multiple
# values should be separated by spaces.

```

```

#
#       These qualifiers appear after the parameter name, e.g.,
# PROPAGATION-CHANNEL-FREQUENCY[0] 2.4e9
#       The instance qualifier has a meaning specific to the parameter (it's usually NOT a network,
#       nodeId, or IP address).

# FAULT-CONFIG-FILE      ./default.fault

NODE-PLACEMENT FILE
NODE-POSITION-FILE
D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\31_SDC_20_500x500_RD.nodes

# NODE-PLACEMENT  UNIFORM
# NODE-PLACEMENT  RANDOM
# NODE-PLACEMENT  GRID
# GRID-UNIT      30          #away from neighbor
# NODE-PLACEMENT  FILE
# NODE-POSITION-FILE ./default.nodes
# Group node placement for group mobility
# NODE-PLACEMENT  GROUP #shows group mobility

##### group mobility model
# sum of two independent mobility vectors, the group mobility vector (Vg) & the internal mobility vector
# (Vi).
# Mobile nodes in the same group share the same mobility vector Vg at any time. Each of them then also
# has its
# internal group mobility vector Vi within the bound of the group dimensions.
# vgs & vis are modeled independently following the random waypoint mobility model. In detail, each
# group decides its group mobility direction and speed
# randomly. Each node then decides its internal mobility randomly and computes its actual mobility by
# summing the two mobility vectors.
#
# "A Group Mobility Model for Ad Hoc Wireless Networks" by X. Hong, M. Gerla, G. Pei, and C.-C.
# Chiang In Proc of ACM/IEEE MSWiM'99, Seattle, WA, Aug. 1999.
#
# NUM-MOBILITY-GROUPS  4
#
# MOBILITY-GROUP[<group number>] { <nodes> }
#
# MOBILITY-GROUP[0] { 1 thru 25 }
# MOBILITY-GROUP[1] { 26 thru 50 }
# MOBILITY-GROUP[2] { 51 thru 75 }
# MOBILITY-GROUP[3] { 76 thru 100 }
#
# GROUP-AREA[<group number>] <origin> <dimension>
#
# GROUP-AREA[0] (0, 0) (750, 750)
# GROUP-AREA[1] (750, 0) (750, 750)
# GROUP-AREA[2] (0, 750) (750, 750)
# GROUP-AREA[3] (750, 750) (750, 750)
#
# An alternate definition of group areas is:
#
# GROUP-AREA-ORIGIN[<group number>] <origin>
# GROUP-AREA-DIMENSION[<group number>] <dimension>
#
# GROUP-AREA-ORIGIN[0] (0, 0)
# GROUP-AREA-DIMENSION[0] (750, 750)
# GROUP-AREA-ORIGIN[1] (750, 0)
# GROUP-AREA-DIMENSION[1] (750, 750)
# GROUP-AREA-ORIGIN[2] (0, 750)
# GROUP-AREA-DIMENSION[2] (750, 750)
# GROUP-AREA-ORIGIN[3] (750, 750)

```



```
# GROUP-AREA-DIMENSION[3] (750, 750)
#
# For the LATLONALT coordinate system, use the following to influence the group
# movement within a particular region. These parameters are optional. If
# not specified, the whole terrain is assumed.
#
# GROUP-TERRAIN-CONSTRAINT-SOUTH-WEST-CORNER[<group number>] <southwest corner>
# GROUP-TERRAIN-CONSTRAINT-NORTH-EAST-CORNER[<group number>] <northeast corner>
#
# GROUP-TERRAIN-CONSTRAINT-SOUTH-WEST-CORNER[0] (-0.005, -0.005)
# GROUP-TERRAIN-CONSTRAINT-NORTH-EAST-CORNER[0] (0, 0)
#
# For the CARTESIAN coordinate system, use the following to influence the group
# movement within a particular region. These parameters are optional. If not specified, the whole terrain
# is assumed.
#
# GROUP-TERRAIN-CONSTRAINT-LOWER-LEFT-CORNER[<group number>] <lower left corner>
# GROUP-TERRAIN-CONSTRAINT-UPPER-RIGHT-CORNER[<group number>] <upper right corner>
#
# GROUP-TERRAIN-CONSTRAINT-LOWER-LEFT-CORNER[0] (0, 750)
# GROUP-TERRAIN-CONSTRAINT-UPPER-RIGHT-CORNER[0] (750, 1500)
#
# Specify how nodes in each group is initially placed by: GROUP-NODE-PLACEMENT[<group
# number>] RANDOM | UNIFORM | GRID
#
# GROUP-NODE-PLACEMENT[0] UNIFORM
# GROUP-NODE-PLACEMENT[1] UNIFORM
# GROUP-NODE-PLACEMENT[2] UNIFORM
# GROUP-NODE-PLACEMENT[3] UNIFORM
#
```

MOBILITY FILE

DUMMY-MOBILITY-FILE D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\Road.mobility

MOBILITY-POSITION-GRANULARITY 1.0

If yes, nodes get their altitude coordinate from the terrain file, if one is specified.

MOBILITY-GROUND-NODE NO

MOBILITY NONE # no move

MOBILITY RANDOM-WAYPOINT #For random waypoint, a node randomly
selects a destination from the physical terrain.

MOBILITY-WP-PAUSE 30S # moving in constant speed m/s

MOBILITY-WP-MIN-SPEED 0

MOBILITY-WP-MAX-SPEED 10

#

MOBILITY GROUP-MOBILITY

MOBILITY-GROUP-PAUSE 1000S

MOBILITY-GROUP-MIN-SPEED 0

MOBILITY-GROUP-MAX-SPEED 0

MOBILITY-GROUP-INTERNAL-PAUSE 0S

MOBILITY-GROUP-INTERNAL-MIN-SPEED 10

MOBILITY-GROUP-INTERNAL-MAX-SPEED 10

#

mobility pattern is read from NODE-POSITION-FILE.

MOBILITY FILE

MOBILITY PATHLOSS-MATRIX

The following parameters are necessary for all mobility models.

MOBILITY-POSITION-GRANULARITY 1.0

#####

#PROPAGATION-CHANNEL-FREQUENCY 2400000000

PROPAGATION-MODEL STATISTICAL

```

#PROPAGATION-CHANNEL-FREQUENCY 2.4e9 # required
#PROPAGATION-CHANNEL-FREQUENCY[0] 2.4e9 # multi channel example
#PROPAGATION-CHANNEL-FREQUENCY[1] 2.5e9

#           Signals with power below PROPAGATION-LIMIT (in dB) (before the antenna gain at
the receiver) will not be
#           delivered to nodes. Lower value should make the simulation more precise, but it also
make the execution time longer.
PROPAGATION-LIMIT -111.0
#PROPAGATION-LIMIT[1] -111.0

#
# PROPAGATION-PATHLOSS: pathloss model
# FREE-SPACE:
#   Friss free space model.
#   (path loss exponent, sigma) = (2.0, 0.0)
# TWO-RAY:
#   Two ray model. It uses free space path loss
#   (2.0, 0.0) for near sight and plane earth
#   path loss (4.0, 0.0) for far sight. The antenna
#   height is hard-coded in the model (1.5m).
# ITM:
#   Irregular Terrain Model (also known as Longley-Rice)
#   This model is based on terrain data and therefore
#   requires a terrain data file.
#

PROPAGATION-PATHLOSS-MODEL TWO-RAY
# PROPAGATION-PATHLOSS-MODEL[1] TWO-RAY
# PROPAGATION-PATHLOSS-MODEL FREE-SPACE
# PROPAGATION-PATHLOSS-MODEL ITM
#
# temporary disabled
#
# PROPAGATION-PATHLOSS-MODEL PATHLOSS-MATRIX

# PROPAGATION-SHADOWING-MODEL:
#
# NONE:   no shadowing
#         (for any path loss model considering shadowing)
# CONSTANT: constant shadowing effect
# LOGNORMAL: log-normal shadowing
#
# PROPAGATION-SHADOWING-MEAN (in dB) to set the mean shadowing value
#
# PROPAGATION-SHADOWING-MODEL LOGNORMAL

PROPAGATION-SHADOWING-MODEL CONSTANT
PROPAGATION-SHADOWING-MEAN 4.0

# PROPAGATION-FADING-MODEL:
#
# NONE:   no fading
# RAYLEIGH: Rayleigh fading
# RICEAN: Ricean fading
#
# For RAYLEIGH and RICEAN, the following variables are required:
# PROPAGATION-FADING-GAUSSIAN-COMPONENTS-FILE:
#   File that stores series of gaussian components
# PROPAGATION-FADING-MAX-VELOCITY:
#   Maximum velocity of any objects on the terrain
# PROPAGATION-RICEAN-K-FACTOR (RICEAN only):

```

```

# Ricean K factor (linear value)
#

PROPAGATION-FADING-MODEL NONE
# PROPAGATION-FADING-MODEL RAYLEIGH
# PROPAGATION-FADING-MODEL RICEAN
# PROPAGATION-RICEAN-K-FACTOR 0.0
#
# PROPAGATION-FADING-MAX-VELOCITY 10.0
# PROPAGATION-FADING-GAUSSIAN-COMPONENTS-FILE ./default.fading

#####
# Phy layer
# PHY-MODEL: phy model to transmit and receive packets
# PHY802.11a: IEEE 802.11a PHY
# PHY802.11b: IEEE 802.11b PHY
# PHY-ABSTRACT: An abstract PHY
# FCSC-PROTOTYPE: FCSC Comms prototype PHY
#

PHY-MODEL PHY802.11a
# PHY-MODEL PHY802.11b
# PHY-MODEL PHY-ABSTRACT
# PHY-MODEL FCSC-PROTOTYPE

PHY-LISTENABLE-CHANNEL-MASK 1
PHY-LISTENING-CHANNEL-MASK 1

#
# PHY-TEMPERATURE: temperature of the phy model (in K)
#
PHY-TEMPERATURE 290

#
# PHY-NOISE-FACTOR: noise factor used to calculate thermal noise level
# of the phy model
#
PHY-NOISE-FACTOR 7.0

#
# PHY-RX-MODEL: packet reception model
# BER-BASED:
# It looks up Bit Error Rate (BER) in the SNR - BER table
# specified by PHY-RX-BER-TABLE-FILE.
# SNR-THRESHOLD-BASED:
# If the Signal to Noise Ratio (SNR) is more than
# PHY-RX-SNR-THRESHOLD (in dB), it receives the signal
# without error. Otherwise the packet is dropped.
# PHY-RX-SNR-THRESHOLD needs to be specified.
# PHY802.11a:
# This is BER-BASED preconfigured for PHY802.11a model
# PHY802.11b:
# This is BER-BASED preconfigured for PHY802.11b model
#
# DPSK gives lower performance than BPSK, but is commonly used due to ease
# of implementation. DPSK is used in 802.11 WaveLAN radios
#
# PHY-RX-MODEL BER-BASED
# PHY-RX-BER-TABLE-FILE[0] ../data/modulation/dpsk.ber
# PHY-RX-BER-TABLE-FILE[1] ../data/modulation/dqpsk.ber
# PHY-RX-BER-TABLE-FILE[2] ../data/modulation/cck-5_5.ber
# PHY-RX-BER-TABLE-FILE[3] ../data/modulation/cck-11.ber
#

```

```

# PHY-RX-MODEL          SNR-THRESHOLD-BASED
# PHY-RX-SNR-THRESHOLD  10.0
#
# PHY-RX-MODEL          PHY802.11a
# PHY-RX-MODEL          PHY802.11b
#

PHY-RX-MODEL            PHY802.11a

#
# PHY802.11-AUTO-RATE-FALLBACK YES | NO
#
PHY802.11-AUTO-RATE-FALLBACK NO

#
# PHY-ABSTRACT-DATA-RATE phy data rate (in bps)
#

# PHY-ABSTRACT-DATA-RATE 64000

#
# PHY802.11-DATA-RATE: phy data rate (in bps)
#
PHY802.11-DATA-RATE      6000000
PHY802.11-DATA-RATE-FOR-BROADCAST 6000000

#
# PHY-ABSTRACT-TX-POWER  phy transmission power (in dBm)
#

# PHY-ABSTRACT-TX-POWER  30.0

#
# PHY802.11?-TX-POWER-*: phy transmission power (in dBm)
#
PHY802.11a-TX-POWER--6MBPS 20.0
PHY802.11a-TX-POWER--9MBPS 20.0
PHY802.11a-TX-POWER-12MBPS 19.0
PHY802.11a-TX-POWER-18MBPS 19.0
PHY802.11a-TX-POWER-24MBPS 18.0
PHY802.11a-TX-POWER-36MBPS 18.0
PHY802.11a-TX-POWER-48MBPS 16.0
PHY802.11a-TX-POWER-54MBPS 16.0

# PHY-ABSTRACT-RX-THRESHOLD threshold of the phy (in dBm)
# PHY-ABSTRACT-RX-THRESHOLD -85
# PHY-ABSTRACT-RX-SENSITIVITY -95

PHY802.11a-RX-SENSITIVITY--6MBPS -85.0
PHY802.11a-RX-SENSITIVITY--9MBPS -85.0
PHY802.11a-RX-SENSITIVITY-12MBPS -83.0
PHY802.11a-RX-SENSITIVITY-18MBPS -83.0
PHY802.11a-RX-SENSITIVITY-24MBPS -78.0
PHY802.11a-RX-SENSITIVITY-32MBPS -78.0
PHY802.11a-RX-SENSITIVITY-48MBPS -69.0
PHY802.11a-RX-SENSITIVITY-54MBPS -69.0
PHY-RX-MODEL PHY802.11a
PHY-LISTENABLE-CHANNEL-MASK 1
PHY-LISTENING-CHANNEL-MASK 1
PHY-TEMPERATURE 290.0
PHY-NOISE-FACTOR 10.0

```

```

#
# Estimated antenna gain for directional communication.
#
#
PHY802.11-ESTIMATED-DIRECTIONAL-ANTENNA-GAIN 15.0
#

ANTENNA-GAIN      0.0      #dBi
ANTENNA-EFFICIENCY  0.8
ANTENNA-MISMATCH-LOSS  0.3      #dB
ANTENNA-CABLE-LOSS   0.0 #dB
ANTENNA-CONNECTION-LOSS 0.2      #dB
ANTENNA-HEIGHT  1.5 #m

# ANTENNA-MODEL:
#
#ANTENNA-MODEL OMNIDIRECTIONAL
ANTENNA-MODEL SWITCHED-BEAM
# ANTENNA-MODEL STEERABLE
# ANTENNA-AZIMUTH-PATTERN-FILE ./default.antenna-azimuth
# ANTENNA-ELEVATION-PATTERN-FILE ./default.antenna-elevation

ANTENNA-AZIMUTH-PATTERN-FILE
D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\NS.antenna-azimuth

#
# GSM Physical Layer parameters
#

# Channel frequencies for GSM 900:
# 890 - 915 MHz: mobile transmit, base receive;
# 935 - 960 MHz: base transmit, mobile receive
# See GSM standard 05.05 for more information.

# n is the ARFCN number (0 < n < 124 for GSM 900)
# Channels should be created in pairs using the following rules.
# DownLink FREQUENCY = 890MHz + 0.2*n
# UpLink = DownLink + 45 MHz

# PROPAGATION-CHANNEL-FREQUENCY[0] 890.0e6
# PROPAGATION-CHANNEL-FREQUENCY[1] 935.0e6
# PROPAGATION-CHANNEL-FREQUENCY[2] 890.2e6
# PROPAGATION-CHANNEL-FREQUENCY[3] 935.2e6
# PROPAGATION-CHANNEL-FREQUENCY[4] 890.4e6
# PROPAGATION-CHANNEL-FREQUENCY[5] 935.4e6
# PROPAGATION-CHANNEL-FREQUENCY[6] 890.6e6
# PROPAGATION-CHANNEL-FREQUENCY[7] 935.6e6

# PROPAGATION-LIMIT and PROPAGATION-PATHLOSS-MODEL also must be specified
# for each channel listed above.

# [1 thru 8] PHY-MODEL PHY-GSM
# All channels must be listenable by every MS & BS at initialization.
# [1 thru 8] PHY-LISTENABLE-CHANNEL-MASK 11111111
# [1 thru 8] PHY-LISTENING-CHANNEL-MASK 00000000

# PHY-GSM-DATA-RATE 270833

# BS: TRX Power Class 5 in GSM 900: 20W (43dBm) to (<40) W (46 dBm)
# [7 thru 8] PHY-GSM-TX-POWER 20.0

# MS: For Class 4 MS in GSM 900: Max power = 2W (33 dBm)

```



```

# [1 thru 6] PHY-GSM-TX-POWER      20.0

# PHY-GSM-RX-SENSITIVITY: sensitivity of the phy (in dBm)
# See GSM 05.05 Section 6

# PHY-GSM-RX-SENSITIVITY -110.0

# RXLEV_ACCESS_MIN in GSM 05.08
# PHY-GSM-RX-THRESHOLD -90.0

# PHY-RX-BER-TABLE-FILE      ./gmsk.ber

#
# GSM-CONTROL-CHANNEL specifies the PROPAGATION-CHANNEL-FREQUENCY instance
# to be used as C0 channel for the current cell.

# The MS's will use it in RX mode & BS's will use it in TX mode.
# List of control channels to listen for MS to scan those to be used by BS's.
# MS's stored BCCH channel list
# [1 thru 6] GSM-CONTROL-CHANNEL [0 4]

# BS 1 & 2
# [7] GSM-CONTROL-CHANNEL [0]
# [8] GSM-CONTROL-CHANNEL [4]

#####
# MPLS Configuration                                     #
#####
# "MPLS-PROTOCOL YES" enables MPLS label switching. Label switching requires
# one or both of the following: a label distribution protocol, or a static label assignment file.

# MPLS-PROTOCOL YES
MPLS-PROTOCOL NO

# Label Distribution Protocols:
#   LDP: RFC 3036
#   RSVP-TE: Internet Draft "RSVP-TE: Extensions to RSVP for LSP Tunnels"

# MPLS-LABEL-DISTRIBUTION-PROTOCOL LDP
# MPLS-LABEL-DISTRIBUTION-PROTOCOL RSVP-TE

# RSVP-TE requires the following parameters to be set

# RSVP-TE-RECORD-ROUTE determines whether or not the total path
# of the LSP will be recorded along the path of establishing RSVP
# messages. The three possible settings are:
#
#   OFF:   No recording of the path during LSP creation,
#          no loop detection
#   NORMAL: Path will be recorded along the path of establishing
#           RSVP messages
#   LABELED: The label ID of the RSVP messages will also be considered
#
# RSVP-TE-RECORD-ROUTE OFF
# RSVP-TE-RECORD-ROUTE LABELED
# RSVP-TE-RECORD-ROUTE NORMAL

# RSVP-RESERVATION-STYLE determines the reservation style for RSVP-TE.
# The available reservation styles are:
#   FF: The "Fixed Filter" reservation style creates a distinct

```

```

#      reservation for traffic from each sender that is not shared by
#      other senders.
#      SE: The "Shared Explicit" reservation style allows a receiver to
#      explicitly specify the senders to be included in a reservation.
#      There is a single reservation on a link for all the senders listed.

# RSVP-RESERVATION-STYLE FF
# RSVP-RESERVATION-STYLE SE

# RSVP-TE-EXPLICIT-ROUTE-FILE entries allow configuration of explicit paths.
# RSVP-TE-EXPLICIT-ROUTE-FILE ./rsvpte.routes-explicit

# LDP requires the following parameters to be set

# MPLS-LABEL-DISTRIBUTION-CONTROL-MODE INDEPENDENT
# MPLS-LABEL-DISTRIBUTION-CONTROL-MODE ORDERED

# MPLS-LDP-LABEL-ADVERTISEMENT-MODE UNSOLICITED
# MPLS-LDP-LABEL-ADVERTISEMENT-MODE ON-DEMAND

# MPLS-LABEL-RETENTION-MODE LIBERAL
# MPLS-LABEL-RETENTION-MODE CONSERVATIVE

# CONFIGURED-FOR-LABEL-RELEASE-MESSAGE-PROPAGATE YES
# CONFIGURED-FOR-LABEL-RELEASE-MESSAGE-PROPAGATE NO

# MPLS-LDP-LOOP-DETECTION YES
# MPLS-LDP-LOOP-DETECTION NO

# Static Label Assignment File:

# MPLS-STATIC-ROUTE-FILE mpls.routes

#####
# MAC layer #
#####
# Following parameter enables Ethernet (802.3) Address Resolution Protocol
ARP-ENABLED NO
ARP-TIMEOUT-INTERVAL 20M

# The link layer should save (rather than discard) packet destined to the some
# unresolved IP address, and transmit the saved packet when the address has been resolved. By default
# disabled [RFC 1122].

# ARP-USE-BUFFER YES | NO

# If ARP is enabled, then the user can specify the mac address of node-interface through MAC-
# ADDRESS-CONFIG-FILE. If MAC-ADDRESS-CONFIG-FILE is not specified
# then default mac address convention will be used as follows:
# For 6 byte Ethernet address, first 8 bits is set to zero, next 32 bits is node id,
# next 8 bits is interface id.

# MAC-ADDRESS-CONFIG-FILE ./default.mac-address

# ARP Cache Table entry lifetime can be specified using ARP-TIMEOUT-INTERVAL.
# If not specified the default value 20 minutes is used.
# [<node-id> | <network address> | <interface address>] ARP-TIMEOUT-INTERVAL 20M

# ARP statistics collection
# [<node-id> | <network address> | <interface address>] ARP-STATISTICS YES | NO

#####

```

The following specifies the MAC protocol used for wireless network interfaces. (P2P links do not require, and ignore this setting.)

```
# IEEE 802.11 MAC DCF/PCF with DVCS
MAC-PROTOCOL MAC802.11
MAC-802.11-DIRECTIONAL-ANTENNA-MODE Yes
MAC-802.11-SHORT-PACKET-TRANSMIT-LIMIT 1
MAC-802.11-LONG-PACKET-TRANSMIT-LIMIT 1
MAC-802.11-RTS-THRESHOLD 0
MAC-802.11-PCF-STATISTICS NO
MAC-PROPAGATION-DELAY 1US
```

The following are parameters for MAC802.11:

```
#
# Determine whether RTS/CTS is used based on data packet size. If data packet size is greater than MAC-
802.11-RTS-THRESHOLD, then
# RTS/CTS is used. Broadcast data packets NEVER use RTS/CTS. Default= 0. means always used
RTS/CTS
# MAC-802.11-RTS-THRESHOLD 0
```

```
# Transmission limit in waiting for CTS/ACK frames. Default= 7
# MAC-802.11-SHORT-PACKET-TRANSMIT-LIMIT 7
```

Transmission limit in waiting for ACK in response to data of length greater than RTS threshold.
Default = 4.

```
# MAC-802.11-LONG-PACKET-TRANSMIT-LIMIT 4
```

Whether the radio will use directional antenna for transmissions. Default is NO.

```
# MAC-802.11-DIRECTIONAL-ANTENNA-MODE YES | NO
```

How long radio keeps track of last known direction of receiver (for directional antenna mode).

```
# MAC-802.11-DIRECTION-CACHE-EXPIRATION-TIME 2S
```

How much space (in degrees) is NAV'ed when the radio overhears frames to neighboring nodes (for directional antenna mode).

```
# MAC-802.11-DIRECTIONAL-NAV-AOA-DELTA-ANGLE 37.0
```

How many times the radio tries transmitting control frames directionally before going omni mode (for directional antenna mode).

```
# MAC-802.11-DIRECTIONAL-SHORT-PACKET-TRANSMIT-LIMIT 4
```

802.11 PCF requires that a BSS be input via the SUBNET statement. A node within the BSS may be an AP. When the AP is also a Point Coordinator,

additional inputs allow the configuration of the contention-free period.

This example shows a BSS with 10 nodes. Node 3 is a PC.

```
# SUBNET N4-1.0 { 1 thru 10 }
```

```
# [N4-1.0] MAC-802.11-AP 3
```

```
# [3] MAC-802.11-PC YES
```

Stations associate statically with the AP. If a station is out of range of the AP as a result of node placement or mobility, it may be unable to communicate.

The implementation does not support overlapping CFPs for overlapping BSSs. In such situations, use of different CFP start times or, better still, different channels or frequencies is suggested.

#

Specify the AP of the BSS. If no AP is given, the behavior is equivalent to that of an ad hoc network.

```
# [N4-1.0] MAC-802.11-AP <nodeID or interfaceAddress>
```

#

Specify that the AP would also behave as a Point Coordinator. Default is NO, the AP does not operate as a PC with contention-free periods.

```

# <nodeID or interfaceAddress> MAC-802.11-PC YES | NO
#
# Specify if the AP (or PC) relays frames to wireless nodes outside the BSS. The default is YES, the AP
relays frames.
# MAC-802.11-RELAY-FRAMES YES | NO
#
# Specify the interval of the contention-free period. The PCF beacon starts every CFP. Default is 200 TUs
or about 0.2 seconds.
# Max value is 32767 TUs. (1 Time Unit = 1024 microseconds).
# MAC-802.11-BEACON-INTERVAL 200
#
# Specify the duration of the CFP. Default is 50 TUs. The min value is approximately 17 TUs. The max <
CFP interval to allow some frame transfer during the contention period.
# MAC-802.11-PC-CONTENTION-FREE-DURATION 50
#
# the start time of the first CFP from start of simulation. This offset is useful to prevent overlapping CFPs
in neighbouring BSSs. Default
# =1 TU. max = CFP interval.
# MAC-802.11-BEACON-START-TIME 1
#
# During the contention-free period, the PC can have variations in its mode of coordination:
# POLL-ONLY -- The PC polls stations in turn. If the round of pollable stations completes before the
CFP duration, the CFP terminates.
# POLL-AND-DELIVER -- The PC behavior is similar to the POLL-ONLY mode except that if the
round of poll completes before the CFP duration,
# the PC would use the balance time to deliver packets in its queue.
# DELIVER-ONLY -- The PC does not poll stations. Instead, the PC dequeues and transmits packets to
stations during the CFP.
# default = POLL-AND-DELIVER.
# MAC-802.11-PC-DELIVERY-MODE POLL-ONLY | POLL-AND-DELIVER | DELIVER-ONLY
#
# Specify if the PC should attempt to avoid polling stations that appear idle. By default, poll-saving is
enabled or BY-COUNT; the PC keeps track
# of null data response and absence of transmits by a pollable station. If set to NONE, the PC polls all
pollable stations in a round-robin fashion.
# MAC-802.11-PC-POLL-SAVE NONE | BY-COUNT
#
# For poll-saving BY-COUNT, the poll-save can be qualified with a min. count value that prevents the
PC from precipitately skipping polls in case the
# station is unable to respond due to other factors. Default value is 1, the PC allows 1 null-data response
to be ignored.
# MAC-802.11-PC-POLL-SAVE-MIN 1
#
# For poll-saving BY-COUNT, the max. count value protects against any long absence of polls to a
station. Default is 10, there will be a max of 10
# skipped polls.
# MAC-802.11-PC-POLL-SAVE-MAX 10
#
# A BSS station may or may not be pollable. Pollable stations are polled during CFPs; other stations are
not polled but may have frames delivered
# to them (depending on the PC mode). By default, stations are POLLABLE
# MAC-802.11-STATION-POLL-TYPE POLLABLE | NOT-POLLABLE
#
# Print PCF related statistics. Default = YES, PCF stats will be printed for PC coordinated BSSs.
# MAC-802.11-PCF-STATISTICS YES | NO

# MAC-PROTOCOL CSMA
# MAC-PROTOCOL MACA
# MAC-PROTOCOL FCSC-CSMA
# MAC-PROTOCOL TDMA

# Note: This is a beta release.
# MAC-PROTOCOL ALOHA

```

```

# The Switched Ethernet model requires the data-rate and propagation delay parameters to be specified.
#
# MAC-PROTOCOL          SWITCHED-ETHERNET
# SUBNET-DATA-RATE      100000000
# SUBNET-PROPAGATION-DELAY 1MS
#
# The 802.3 Ethernet model requires the data-rate and propagation delay parameters to be specified.
When specifying 802.3, only
# 10Mbps (10BaseT) or 100Mbps (100BaseT) data rates are allowed.
# 1Gbps (1000BaseT) is in the works. For 10BaseT, the propagation
# delay < half of 51.2 microseconds for collision detection to work correctly. Likewise, for 100BaseT,
the propagation
# delay must be less than half of 5.12 microseconds.
#
# MAC-PROTOCOL          MAC802.3
# SUBNET-DATA-RATE      100000000
# SUBNET-PROPAGATION-DELAY 1US
#

# MAC-PROPAGATION-DELAY specifies an additional delay for messages sent by the MAC layer to
the phy layer. Some MAC protocols use
# a multiple of this value. The default value is 1 microsecond, kept in the
MAC_PROPAGATION_DELAY macro in include/mac.h.
#
# MAC-PROPAGATION-DELAY 1500NS

# This is an abstract model of a satellite network. Each satellite network is group into subnets. Each
satellite subnet has
# exactly one satellite node and many ground nodes. The ground nodes associated with a subnet always
transmit to the
# designated subnet satellite node. Thus, no handoffs are involved. Also, satellite nodes are bent-pipe
satellites
# (relay data only). When the satellite node receives data from the ground nodes, it broadcasts the data to
all other ground
# nodes in the subnet, but not to the ground node originating the data. Finally, the satellite node must not
be generating any packets.
# Thus, the satellite node cannot run an application or routing protocol.
#
# Note: SATCOM-PROPAGATION-DELAY specifies ground-to-ground propagation delay.
#
# MAC-PROTOCOL SATCOM
#
# Specifies which node is the satellite node.
# SATCOM-SATELLITE-NODE <node ID>
#
# Currently, only the bent-pipe satellite is supported.
# SATCOM-TYPE BENT-PIPE (only type supported)
#
# The satellite link bandwidth capacity.
# SATCOM-BANDWIDTH <bandwidth>
#
# Ground-to-ground propagation delay.
# SATCOM-PROPAGATION-DELAY <delay>
#
# Below is an example of a satellite network where node 3 is designated the satellite node for subnet N8-
1.0, with bandwidth of 100Mbps and
# ground-to-ground propagation delay of 200MS:
#
# [N8-1.0] MAC-PROTOCOL SATCOM
# [N8-1.0] SATCOM-SATELLITE-NODE 3
# [N8-1.0] SATCOM-TYPE BENT-PIPE
# SATCOM-BANDWIDTH 100000000

```


SATCOM-PROPAGATION-DELAY 200MS

PROMISCUOUS-MODE defaults = YES (for DSR only YES) and is necessary if nodes want to overhear packets destined to neighboring nodes.

Setting it to "NO" may save a trivial amount of time for other protocols.

PROMISCUOUS-MODE YES

The TDMA model permits the following parameters. If no parameters are specified, TDMA will allocate 1 slot per node in round-robin

fashion by address. Otherwise, a scheduling file specifying per slot receiver/transmitter assignment for each node should be provided.

The default value is 10MS. This duration should be long enough so that a packet can be transmitted.

TDMA-SCHEDULING AUTOMATIC | FILE

TDMA-SCHEDULING-FILE default.tdma

TDMA-NUM-SLOTS-PER-FRAME 30

TDMA-SLOT-DURATION 10MS

TDMA-GUARD-TIME 0NS

TDMA-INTER-FRAME-TIME 1US

#####

Detailed Switch Model

#####

The MAC Switch model is based on the IEEE 802.1 standards and covers Level 2 switches and port based VLANs. MAC 802.3 and LINK are the two

protocols supported at the switch ports.

#

For switched networks, multiple LAN segments are permitted within the same network address. For example, to specify 3 LAN segments in subnet

1.0 and connected to ports of a switch with node id 100, use

LINK N8-1.0 { 100, 1 }

LINK N8-1.0 { 100, 2 }

SUBNET N8-1.0 (100, 3 thru 10)

Note that the N syntax uses a number large enough number for the mask to cover all the interfaces of the 1.0 subnet; the LINK does not use N2 as

would be the common practice in non-switch scenarios.

General input

In general, switch inputs are based on switch ID (which maps to node ID).

[switch ID] SWITCH-SPECIFIC-PARAMETER <value>

#

Port inputs have the form

[switch ID] SWITCH-PORT-SPECIFIC-PARAMETER[port ID] <value>

The first form is shown here.

#

Some port inputs have an additional form based on the port's interface address. For example,

[port address] SWITCH-PORT-SPECIFIC-PARAMETER <value>

This form is not generally applicable, and is not illustrated here.

Specify a node as a switch. Default is NO

[100] SWITCH YES | NO

If port specific parameters would be input, each switch port needs to be mapped to an interface address. If no port specific parameters would be

input for a switch, an AUTO mapping may be used. Default is MANUAL.

SWITCH-PORT-MAPPING-TYPE AUTO | MANUAL

Map each switch port to an interface address. Here, port 2 of switch 100 has the interface address 1.3. This mapping is required if

```

# SWITCH-PORT-MAPPING-TYPE is of type MANUAL, the default.
# [100] SWITCH-PORT-MAP[2] 1.3

# Maximum number of dynamic entries of the filtering / learning database. Default value is 500.
# [switch ID] SWITCH-DATABASE-MAX-ENTRIES 500

# Ageing time for dynamic entries in the filtering/learning database. Default = 300 seconds, range is 10 to 1000000 seconds.
# [switch ID] SWITCH-DATABASE-AGING-TIME 300S

# The queue values at each switch port can be individually configured.
# The queue type is FIFO, scheduling is always Strict Priority.

# Number of output queues. Default is 3, range is 1 to 8.
# [switch ID] SWITCH-QUEUE-NUM-PRIORITIES[port ID] 3

# Size of output queues. Default is 150000.
# [switch ID] SWITCH-OUTPUT-QUEUE-SIZE[port ID] 150000

# Size of input queue. Default is 150000.
# [switch ID] SWITCH-INPUT-QUEUE-SIZE[port ID] 150000

# Size of CPU queue. Default is 640000.
# [switch ID] SWITCH-CPU-QUEUE-SIZE 640000

# Throughput of backplane. Default is 0 bps, which implies that there will be no backplane delay.
# [switch ID] SWITCH-BACKPLANE-THROUGHPUT 0

# STP input

# The implementation follows the single rapid spanning tree of 802.1w. In general, the default values are appropriate. For root election, use
# SWITCH-PRIORITY.

# Run the spanning tree protocol. Default is YES. Ensure that if NO is used, the switched network is loop free.
# [switch ID] SWITCH-RUN-STP NO | YES

# Priority of a switch. Default is 32768. Range is 0 to 61440. If the
# value is not a multiple of 4096, the nearest multiple is used. Note that
# a lower value of priority is better, 0 is the highest priority.
# [switch ID] SWITCH-PRIORITY 32768

# Hello time for STP. This is time between generation of BPDUs by the root switch. Default is 2 seconds. Range is 1 to 10 seconds.
# [switch ID] SWITCH-HELLO-TIME 2S

# Max age time for BPDUs. Default is 20 seconds, range is 6 to 40 seconds
# [switch ID] SWITCH-MAX-AGE 20S

# Time for forward delay. Default is 15 seconds, range is 4 to 30 seconds.
# [switch ID] SWITCH-FORWARD-DELAY 15S

# Limit to number of BPDU transmits in hello time. Default is 3, range is
# 1 to 10.
# [switch ID] SWITCH-HOLD-COUNT 3

# Path cost for a port. Default is based on a computation based on the
# bandwidth of the protocol connected to the port, resulting in values ranging from 1 to 200000000
# [switch ID] SWITCH-PORT-PATH-COST[port ID] <value>

```

Port priority. Default is 128, range is 0 to 240. If the input value is not a multiple of 16, the nearest value is used. Note that a lower value
of priority is better, 0 is the highest priority.
[switch ID] SWITCH-PORT-PRIORITY[port ID] 128

Port is attached to a point-to-point link. Default is AUTO, implying true if the switch port is given in a LINK statement. Other options are
FORCE-TRUE and FORCE-FALSE
[switch ID] SWITCH-PORT-POINT-TO-POINT[port ID] AUTO

Port is the only switch port in a switched network attached to a LAN. Default is NO.
[2] SWITCH-PORT-EDGE[port ID] NO | YES

VLAN input

The implementation supports port-based VLANs based on 802.1q.

Segments with the same VLAN ID should be given the same subnet address and mask. Segments with different VLAN IDs should have different subnet
addresses for inter-VLAN communication and require routing.

LINK N8-1.0 { 100, 1 }
LINK N8-2.0 { 100, 2 }
LINK N8-1.0 { 200, 21 }
LINK N8-2.0 { 200, 22 }
LINK N8-3.0 { 100, 200 }

In the example, nodes 100 and 200 are switches. End-stations 1 and 21 are in the same VLAN, and 2 and 22 are in a different VLAN. The subnet address
of the inter-switch link is not relevant.

Range of VLAN IDs is 1 (the default) to 4090.

Switch supports VLANs. Default is NO.
[100] SWITCH-VLAN-AWARE YES

VLAN ID and tagging for end stations. By default, end-stations do not
send VLAN tagged frames and the VLAN ID is not specified.
[end station address list] SWITCH-STATION-VLAN-ID <VLAN ID>
[end station address list] SWITCH-STATION-VLAN-TAGGING YES

VLAN ID for a switch port. If not specified, the default is 1. For an access link, this is typically the value of the VLAN ID of the
end stations attached to the port. For trunk links, this is typically the default VLAN ID and does not need to be input. For hybrid segments,
the value is typically that of the untagged end stations.
[switch ID] SWITCH-PORT-VLAN-ID[port ID] <VLAN ID>

Types of frames allowed at ingress to a port. Default is ALL. If TAGGED option is used, the port will filter untagged frames.
[switch ID] SWITCH-PORT-VLAN-ADMIT-FRAMES[port ID] ALL | TAGGED

Ingress filter based on member set. Default is NONE.
[node] SWITCH-PORT-VLAN-INGRESS-FILTERING[port ID] NONE | VLAN

Member set for each VLAN at a switch. There is no default. The member set for a VLAN is the set of ports across which broadcasts for
that VLAN are flooded. The untagged set is a subset of the member set where egress frames are not tagged.
[switch ID] SWITCH-VLAN-MEMBER-SET[VLAN ID] <port number list> | ALL
[switch ID] SWITCH-VLAN-UNTAGGED-MEMBER-SET[VLAN ID] <port set> | ALL

VLAN learning type for a switch database. Default is SHARED. For SHARED learning, there is one database for all the VLANs.
 # For INDEPENDENT learning, there is one database per VLAN. For COMBINED learning, there is an m:n relation between VLANs and
 # databases. This requires additional input.
 # [switch node] SWITCH-VLAN-LEARNING SHARED | INDEPENDENT | COMBINED

VLAN to database mapping for COMBINED learning. VLAN mappings that are not specified map to filter database ID 1. Range of fid (filter database
 # ID) ranges from 2 to 4090.
 # [switch ID] SWITCH-VLAN-COMBINED-LEARNING[fid] <vlanIdList>

GVRP/GARP

GVRP is a convenient mechanism to dynamically create the VLAN member sets in a switched network. The implementation is based on IEEE 802.1q
 # for GVRP and 802.1d for GARP. Note that the GARP applicant/registrars state machines apply only to switch ports; end-stations do not participate in
 # the dynamic application and registration process in the implementation.
 #
 # If GVRP is enabled, it suffices to set the port VLAN ID for access links. Note that GVRP does not create the untagged member set.

Switch uses GVRP. Applicable only to VLAN aware switches.
 # Default is NO.
 # SWITCH-RUN-GVRP YES

Size GVRP for maximum number of VLANs. Default is 10. Range is 1 to 4090.
 # SWITCH-GVRP-MAXIMUM-VLANS 10

GARP join time. Specifies the average time between Join messages sent by the applicant. Default = 200 ms
 # SWITCH-GARP-JOIN-TIME 200MS

GARP leave time. Specifies the time a registrar takes to transition from In state to Empty state. Default is 600 milliseconds. The leave time should be thrice join time.
 # SWITCH-GARP-LEAVE-TIME 600MS

GARP leave-all time. Specifies the periodic interval between LeaveAll messages. Default= 10sec. This value should be at least 10 times the leave time.
 # SWITCH-GARP-LEAVEALL-TIME 10S

Switch statistics

Additional switch statistics require that MAC-LAYER-STATISTICS be YES.

Print of switch database statistics. Default is NO.
 # [switch ID] SWITCH-DATABASE-STATISTICS YES | NO

Print of port specific statistics. Default is NO.
 # [switch ID] SWITCH-PORT-STATISTICS[port ID] YES | NO

Print of scheduler specific statistics at each port. Default is NO.
 # [switch ID] SWITCH-SCHEDULER-STATISTICS[port ID] YES | NO

Print of output queue statistics at each port. Default is NO.
 # [switch ID] SWITCH-QUEUE-STATISTICS[port ID] YES | NO

Print of additional VLAN specific statistics at each port. Default is NO.
 # [switch ID] SWITCH-PORT-VLAN-STATISTICS[port ID] YES | NO

Print additional GVRP statistics at a switch. Default is NO.
 # [switch ID] SWITCH-GVRP-STATISTICS YES | NO

GSM Specification

The GSM model requires three node types to be defined: Mobile Station - MS, Base Station - BS and Mobile Switching Center - MSC.

The radio/air/'Um' interface between MS's and BS's is specified as shown in the physical layer section above and in the GSM-NODE-CONFIG-FILE

The 'A' interface between BS's & MSC are wired point-to-point LINKs for which a default route file needs to be specified. The current GSM model supports multiple BS's and one MSC.

The MS's can be located anywhere and can have any desired motion. The BS's & MSC cannot be mobile. The BS's need to be placed so that they covered the desired area.

NODE-PLACEMENT FILE

NODE-PLACEMENT-FILE ./gsm-placement.nodes

[1 thru 6] MOBILITY TRACE

MOBILITY-TRACE-FILE ./gsm-mobility

[7 thru 9] MOBILITY NONE

[1 thru 9] MAC-PROTOCOL GSM

[1 thru 6] GSM-NODE-TYPE GSM-MS

[7 thru 8] GSM-NODE-TYPE GSM-BS

Node 9 is the MSC. It has no GSM MAC related functionality.

Any node that has GSM-LAYER3 will also have the IP stack

[1 thru 9] NETWORK-PROTOCOL GSM-LAYER3

GSM Layer 3 config file, providing node specific properties

GSM-NODE-CONFIG-FILE ./gsm-node-config.gsm

GSM Layer 3 statistics can be enabled by setting the following parameter. If it is set to NO, then statistics will be disabled.

GSM-STATISTICS YES | NO

#####

Network layer

#####

File containing vendor router models

#ROUTER-MODEL-CONFIG-FILE default.router-models

Below are examples of how to specify vendor router models described in ROUTER-MODEL-CONFIG-FILE. By default, the vendor router model is GENERIC,

which means the the backplane has infinite throughput and therefore the backplane delay is not considered.

#

NOTE: IP-QUEUE-PRIORITY-QUEUE-SIZE below must be commented out in order not to overwrite the queue size defined for the router models.

#

ROUTER-MODEL GENERIC

ROUTER-MODEL CISCO-2500

ROUTER-MODEL CISCO-CATALYST-6509

IP is currently the only choice for network-layer protocol.

NETWORK-PROTOCOL IP

IP will fragment the packet if its size is too large. This fragmentation unit size can be dynamically configured by specifying the parameter

IP-FRAGMENTATION-UNIT. It is the maximum size (including IP header) in bytes of an IP packet delivered to the MAC layer. This value is

the same for all nodes. It must be a multiple of 8. IP should fragment packets into this unit. Its maximum allowable value is 2048, which is

equal to the MAX_NW_PKT_SIZE indicating the MDU of the physical network. Currently the minimum allowable value is 256 (equal to 4 * TCP_MIN_MSS).
 # Its default value is MAX_NW_PKT_SIZE (e.g. 2048), which yields the optimal network performance as no unnecessary fragmentations.

 # IP-FRAGMENTATION-UNIT 2048
 # IP loopback Configuration

By default loopback is enabled. To disable this feature specify :
 # [node-id] IP-ENABLE-LOOPBACK NO

IP-ENABLE-LOOPBACK YES

If loopback is enabled, default loopback interface address is 127.0.0.1 User can configure Ip default Loopback Address, the syntax is:

[node-id] IP-LOOPBACK-ADDRESS <loopback-interface-address>
 # Example:

IP-LOOPBACK-ADDRESS 127.0.0.1
 IP-FRAGMENTATION-UNIT 2048

The number of separate priority queues is specified below, QualNet
 # currently generates three types, CONTROL, REAL_TIME, and NON_REAL_TIME,
 # so "3" is a good minimum value. If you specify less than "3", the
 # lower priority packets will be placed in the lowest-priority queue that
 # exists. Specifying less than "1" is an error condition due to the
 # inability of that node to store any packets at the IP layer.
 #

IP-QUEUE-NUM-PRIORITIES 3

 # The following parameter specifies the size of each of the
 # "priority queues", the number of which is specified by
 # IP-QUEUE-NUM-PRIORITIES. If there are 3 "priority queues", each
 # will have a byte-capacity equal to the value of
 # IP-QUEUE-PRIORITY-QUEUE-SIZE specified below.
 #
 # You can also specify each priority queue's size separately, using the
 # Instance ID [] after the parameter name, as in an example below. Make sure
 # that you use Instance ID's numbering from
 # { 0, ..., (IP-QUEUE-NUM-PRIORITIES-1) }
 #
 # You can also use Node and Network Specific Parameterization with brackets
 # before the parameter name.

 # 50000 bytes == 1500 "DEFAULT_ETHERNET_MTU * 33.333 packets
 #
 # Example: NodeId 1 has a 25000 byte queue for priority 2
 #
 # [1] IP-QUEUE-PRIORITY-QUEUE-SIZE[2] 25000
 #

IP-QUEUE-PRIORITY-QUEUE-SIZE 50000

 # The IP-QUEUE-TYPE parameter specifies the type of queueing mechanism to use
 # for the particular priority queue. It can be specified as a global
 # default, per node or network, per priority queue, or any valid combination
 # of these.

 # Example: All nodes have a FIFO queue for priority 2
 # IP-QUEUE-TYPE[2] FIFO
 #

```

#
# FIFO represents "First In, First Out" IP packet queueing.
#

IP-QUEUE-TYPE  FIFO

#
# RED represents Random Early Detection(Drop) as presented in
#   Sally Floyd and Van Jacobson,
#   "Random Early Detection For Congestion Avoidance",
#   IEEE/ACM Transactions on Networking, August 1993.
#   This implementation drops packets, it does not mark them.
#
# RED requires the following additional parameters:
#
#   RED-MIN-THRESHOLD : the number of packets in the queue that represents
#                       the lower bound at which packets can be randomly
#                       dropped.
#   RED-MAX-THRESHOLD : the number of packets in the queue that represents
#                       the upper bound at which packets can be randomly
#                       dropped.
#   RED-MAX-PROBABILITY : the maximum probability (0...1) at which a
#                       packet can be dropped (before the queue is
#                       completely full, of course).
#   RED-QUEUE-WEIGHT : the queue weight determines bias towards recent
#                       or historical queue lengths in calculating the
#                       average.
#   RED-SMALL-PACKET-TRANSMISSION-TIME : a sample amount of time that it
#                       would take to transmit a small
#                       packet - used to estimate the
#                       queue average during idle periods.
#
# IP-QUEUE-TYPE      RED
# RED-MIN-THRESHOLD   5
# RED-MAX-THRESHOLD   15
# RED-MAX-PROBABILITY 0.02
# RED-QUEUE-WEIGHT    0.002
# RED-SMALL-PACKET-TRANSMISSION-TIME 10MS
#

# RIO represents Random Early Detection(Drop)with In/Out Bit. It is a
# variant of RED. It can operate in both two or three color modes.
#
# In two color mode it use twin RED algorithms:
# - the first for the Green profile packets and
# - the second for Yellow profile packets
#
# In three color mode it uses three RED algorithms:
# - the first for the Green profile packets and
# - the second for Yellow profile packets and
# - the third for Red profile packets.
#
# It operates either in coupled or decoupled mode.
#
# Coupled mode counts Green profile packets towards the drop calculation for Yellow profile packets,
# while Decoupled mode counts them separately.
#
# Use the GREEN- YELLOW- and RED- THRESHOLD and PROBABILITY parameters to specify
# thresholds and probabilities for each queue.
#
# RIO specific parameters:
#

```

```

# IP-QUEUE-TYPE      RIO
# RIO-COLOR-MODE TWO-COLOR
# RIO-COLOR-MODE THREE-COLOR
# RIO-COUNTING-MODE   COUPLED
# RIO-COUNTING-MODE   DECOUPLED

# WRED represents Weighted Random Early Detection(Drop) It is a variant of RED and uses three RED
algorithms
# - the first for the Green profile packets and
# - the second for Yellow profile packets and
# - the third for Red profile packets.
#
# Use the GREEN- YELLOW- and RED- THRESHOLD and PROBABILITY parameters
# to specify thresholds and probabilities for each queue.

# IP-QUEUE-TYPE      WRED

# The following parameters are useful for setting probabilities and
# thresholds for WRED and RIO (COUPLED or DECOUPLED).
#

GREEN-PROFILE-MIN-THRESHOLD 10
GREEN-PROFILE-MAX-THRESHOLD 20
GREEN-PROFILE-MAX-PROBABILITY 0.02
YELLOW-PROFILE-MIN-THRESHOLD 5
YELLOW-PROFILE-MAX-THRESHOLD 10
YELLOW-PROFILE-MAX-PROBABILITY 0.02
RED-PROFILE-MIN-THRESHOLD 2
RED-PROFILE-MAX-THRESHOLD 5
RED-PROFILE-MAX-PROBABILITY 0.02

# Per-hop Behaviour (PHB) mapping filename
# PER-HOP-BEHAVIOR-FILE ./phbparam.in

#
# ECN represents Explicit Congestion Notification as presented in
# Sally Floyd and K. Ramakrishnan, RFC 2481,
# "A Proposal to add Explicit Congestion Notification (ECN) to IP."
# ECN marks the IP header instead of dropping packets when the network
# queue gets congested.
#
# ECN requires one of the IP-QUEUE-TYPE (RED, RIO, or WRED).
# Furthermore, the source and destination nodes must be ECN
# enabled; intermediate routes may or may not be ECN enabled.
# By default, ECN is disabled. Only TCP is able to interpret
# the ECN-marked packets.
#
# Example: To enable ECN, do the following:
# ECN      YES
#
#
# The "STRICT-PRIORITY" scheduler for IP indicates that all packets of
# a higher priority are sent before any packets for a lower priority.
#
# The "WEIGHTED-FAIR" scheduler implements Weighted Fair Queueing with
# the highest priority queue getting a weight which is higher than that
# of all the other queues by default. Users can also specify the queue
# weight for each of the priority queues (but must specify the weight for
# all of them) by specifying "QUEUE-WEIGHT[priority] <value>" where value
# is the desired weight for that priority queue.
#

```

```

# The "SELF-CLOCKED-FAIR" scheduler implements Self Clocked Fair Queueing.
# It is a variant "WEIGHTED-FAIR" scheduler. To specify the queue weights
# manually, use the QUEUE-WEIGHT[priority] parameter as above.
#
# The "ROUND-ROBIN" scheduler cycles from the first priority queue to
# the last, pulling a single packet from each
#
# The "WEIGHTED-ROUND-ROBIN" scheduler accepts weights for each priority
# queue, and services packets in round-robin fashion, giving more "turns"
# to queues with higher weights. To specify the queue weights manually,
# use the QUEUE-WEIGHT[priority] parameter as above.
#
# The "CBQ" (Class-Based Queueing) Scheduler is configured via three
# parameters:
#   "LINK-SHARING-STRUCTURE-FILE"
#     The Link Sharing Structure File contains configuration
#     information about weights, priorities, and link sharing
#     between agencies.
#   "CBQ-GENERAL-SCHEDULER" specifies the packet scheduler that CBQ
#     uses to manage the queues.
#   "CBQ-LINK-SHARING-GUIDELINE" determines whether or not bandwidth
#     is regulated by the link sharing scheduler. Bandwidth remains
#     unregulated in the "Ancestor-Only" case when the class of
#     traffic is under-limit, or its immediate ancestor is under-limit.
#     Bandwidth remains unregulated in the "Top-Level" case when the
#     class of traffic is under-limit, or at least one of its ancestors
#     up to CBQ-TOP-LEVEL generations above, are under-limit.
#   "CBQ-TOP-LEVEL" determines the maximum number of generations to
#     search, for under-limit ancestors.
#
# The highest priority is numbered "0", and the lowest priority is "n-1",
# where n = IP-QUEUE-NUM-PRIORITIES
#

IP-QUEUE-SCHEDULER STRICT-PRIORITY
# IP-QUEUE-SCHEDULER WEIGHTED-FAIR
# IP-QUEUE-SCHEDULER SELF-CLOCKED-FAIR
# IP-QUEUE-SCHEDULER ROUND-ROBIN
# IP-QUEUE-SCHEDULER WEIGHTED-ROUND-ROBIN

# IP-QUEUE-SCHEDULER CBQ
# CBQ-GENERAL-SCHEDULER PRR
# CBQ-GENERAL-SCHEDULER WRR
# CBQ-LINK-SHARING-GUIDELINE ANCESTOR-ONLY
# CBQ-LINK-SHARING-GUIDELINE TOP-LEVEL
# CBQ-TOP-LEVEL 3

# QUEUE-WEIGHT[0] 0.5
# QUEUE-WEIGHT[1] 0.3
# QUEUE-WEIGHT[2] 0.2

#
# The "DIFFSERV-ENABLED" scheduler for IP is the combination of two
# schedulers: the inner and outer scheduler. Both schedulers are required
# for DiffServ. Generally, "STRICT-PRIORITY" is chosen as the outer
# scheduler and "WEIGHTED-FAIR" or "WEIGHTED-ROUND-ROBIN" is chosen as
# the inner scheduler.
# [3 4 5] IP-QUEUE-SCHEDULER DIFFSERV-ENABLED

#
# This parameter specifies whether this node is a DiffServ enable edge
# router or not. The <variant> is one of YES | NO
# Format is:

```

```

#
# DIFFSERV-ENABLE-EDGE-ROUTER <variant>
#
# For example:
#
#     DIFFSERV-ENABLE-EDGE-ROUTER YES
#     DIFFSERV-ENABLE-EDGE-ROUTER NO
#     [3 5] DIFFSERV-ENABLE-EDGE-ROUTER YES
#
# If not specified, default is NO
# [3 5] DIFFSERV-ENABLE-EDGE-ROUTER    YES

# Specifies what type of scheduler is used by the inner scheduler.
# DS-SECOND-SCHEDULER                WEIGHTED-FAIR

#
# The DiffServ Multi-Field Traffic Conditioner is activated by specifying
# a TRAFFIC-CONDITIONER-FILE, and placing entries in it that characterize
# classes of traffic, desired data rate and burstiness characteristics, and
# action to take with Out-Profile packets.
#
# TRAFFIC-CONDITIONER-FILE    ./default.traffic_conditioner

#####
# Routing - forwarding, static, default routes                                     #
#####
# Hosts, for example personal computers connected to a company LAN, generally do not forward
# packets, while routers generally do. By default, all nodes
# forward packets (in wireless ad-hoc networks, all nodes tend to be both hosts and routers). To change
# the default, specify the global default to
# be "NO". You can then specify which nodes should forward packets using node/network specific
# parameterization.

IP-FORWARDING YES
# IP-FORWARDING NO

# Static routes have priority over routes discovered through routing protocols while default routes have
# the lowest priority.

# STATIC-ROUTE    YES
# STATIC-ROUTE-FILE    ./default.routes-static

DEFAULT-ROUTE    YES
DEFAULT-ROUTE-FILE
D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\31_SDC_20_500x500_RD.routes-default
DUMMY-MULTICAST YES
MULTICAST-PROTOCOL ODMRP
MULTICAST-GROUP-FILE
D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\31_SDC_20_500x500_RD.member
ODMRP-JR-REFRESH 1S
ODMRP-FG-TIMEOUT 60S
ODMRP-DEFAULT-TTL 64
ODMRP-PASSIVE-CLUSTERING NO
ODMRP-CLUSTER-TIMEOUT 10S

#DEFAULT-ROUTE-FILE    ./default.routes-default

# Hot Standby Router Protocol (HSRP) follows RFC 2281. HSRP allows a host to specify a virtual next
# hop router to forward packets. Routers
# participating in the same standby group will dynamically determine the active and standby routers.
# Only the active router will forward packets.

```



```

# NOTE: This is a beta release.
#
# To use HSRP, specify:
# HSRP-PROTOCOL YES

# HSRP routers must belong to a group. However, current implementation does not consider different
# groups within a broadcast LAN. The default
# group number is 0.
# HSRP-STANDBY-GROUP-NUMBER 0

# This is the virtual IP address of the next hop router that will be forwarding packets. This IP address
# must be used in DEFAULT-ROUTER-FILE
# to specify the next hop on the host that relies on the HSRP routers. There is no default. This must be
# specified.
# HSRP-VIRTUAL-IP-ADDRESS 0.0.10.1

# Used to give priority to routers. The higher the value, the higher the priority. Default is 0.
# HSRP-PRIORITY 0

# Hello timer interval. Default is 3 seconds.
# HSRP-HELLO-TIME 3S

# Hold timer interval. Default is 10 seconds.
# HSRP-HOLD-TIME 10S

# Allow higher priority routers to claim active status from existing active router. If set to NO, higher
# priority routers will yield
# to current active router even if current active router has lower priority. Default is NO.
# HSRP-PREEMPTION-CAPABILITY NO

#####
# Unicast routing - wireless ad hoc #
#####
# AODV follows draft-ietf-manet-aodv-09.txt

ROUTING-PROTOCOL BELLMANFORD

# The maximum possible number of hops between two nodes in the network. Default = 35
# AODV-NET-DIAMETER

# Conservative estimate of the average one-hop traversal time for packets and should include queuing,
# transmission,
# propagation and other delays. Default Value: 40ms
# AODV-NODE-TRAVERSAL-TIME

# Timeout time for an active route; each time a data packet is sent, the lifetime of that route is updated to
# this value
# Note: a default value of 10 seconds is suggested for error detection through MAC layer message (like
# what 802.11 does).
# Default Value: 3000ms
# AODV-ACTIVE-ROUTE-TIMEOUT

# The destination of a RREQ replies with AODV-MY-ROUTE-TIMEOUT as the lifetime of the route.
# Default = 2 * AODV-ACTIVE-ROUTE-TIMEOUT
# AODV-MY-ROUTE-TIMEOUT

# Lifetime of a hello message is determined by AODV-ALLOWED_HELLO_LOSS * AODV-
# HELLO_INTERVAL. Default = 1000ms
# AODV-HELLO-INTERVAL

# Specifies the number of times AODV will repeat expanded ring search for a destination if no Route
# Reply is received
# within specified amount of time. Default = 2

```

AODV-RREQ-RETRIES

A constant use for calculating the time after which an active route should be deleted. After timeout of an active

route, the route is finally deleted from the routing table after a time period of " $K * \max(\text{AODV-}$

$\text{ACTIVE_ROUTE_TIMEOUT, AODV-ALLOWED_HELLO_LOSS} * \text{AODV-HELLO_INTERVAL}$)." Here K is AODV-ROUTE-

DELETION-CONSTANT. Default = 5

If the value is set to YES, a node will send a hello message if there is no broadcast within the last hello interval.

Note: Simulation time will increase depending on the frequency of the hello updates. Default = NO

AODV-PROCESS-HELLO

Lifetime of a hello message is determined by $\text{AODV-ALLOWED_HELLO_LOSS} * \text{AODV-}$

HELLO_INTERVAL . Default = 2

If this value is set to YES, the node will try to locally repair a broken route, if possible. Default = NO

AODV-LOCAL-REPAIR

If the source node of a route gets a route error message,

it will initiate a new Route Request for the destination if the

value is set to YES.

Default Value: NO

#

AODV-SEARCH-BETTER-ROUTE

Maximum number of packets the message buffer of AODV can

hold. If the buffer fills up, incoming packets for the

buffer will be dropped.

Default Value: 100

#

AODV-BUFFER-MAX-PACKET

If nothing is specified, buffer overflow will be

checked by number of packets in the buffer. If some value is

specified here, incoming packets will be dropped

if the incoming packet size + current size of the buffer

exceeds this value.

Default Value: 0 (meaning not used)

#

AODV-BUFFER-MAX-BYTE

Specifies which applications to open a bi-directional connection.

If specified, Route Request will be sent with Gratuitous flag on,

which may cause a Gratuitous Reply, if necessary.

#

AODV-OPEN-BI-DIRECTIONAL-CONNECTION

Specifies the ttl value when initiating a route request.

Default value: 1.

#

AODV-TTL-START

Specifies the value by which the ttl will be incremented each time a Request is retransmitted.

Default value: 2.

#

AODV-TTL-INCREMENT

Specifies the maximum value of ttl over which NET_DIAMETER value will be used to broadcast Route Request.

```

# Default value: 7.
#
# AODV-TTL-THRESHOLD

# ROUTING-PROTOCOL LAR1

#
# DSR is compliant with draft-ietf-manet-dsr-07.txt.
#
# ROUTING-PROTOCOL DSR
#

# Specifies the maximum size of message buffer in packets.
# Default value: 50
# DSR-BUFFER-MAX-PACKET

# Specifies the maximum size of message buffer in bytes.
# When not specified the value of DSR-BUFFER-MAX-PACKET is used.
# DSR-BUFFER-MAX-BYTE


# ROUTING-PROTOCOL BELLMANFORD
# ROUTING-PROTOCOL RIP
# ROUTING-PROTOCOL OSPFv2

#
# The STAR Routing Protocol requires the following NEIGHBOR-PROTOCOL parameters
# and a choice between STAR-ROUTING-MODE ORA or LORA.
#

# ROUTING-PROTOCOL STAR
# STAR-ROUTING-MODE LORA
# STAR-ROUTING-MODE ORA
# NEIGHBOR-PROTOCOL-SEND-FREQUENCY 2S
# NEIGHBOR-PROTOCOL-ENTRY-TTL 4S

#
# The OLSR-INRIA Routing Protocol is a port of INRIA's Linux implementation
#

# ROUTING-PROTOCOL OLSR-INRIA

#
# Fisheye follows draft-ietf-manet-fisheye-03.txt.
# Note: This is a beta release.
#
# ROUTING-PROTOCOL FISHEYE
#
# Fisheye scope. Default is 2.
# FISHEYE-SCOPE 2
#
# Routing table update frequency within the fisheye scope.
# Default is 5 seconds.
# FISHEYE-INTRA-UPDATE-INTERVAL 5S
#
# Routing table update frequency outside of the fisheye scope.
# Default is 15 seconds.
# FISHEYE-INTER-UPDATE-INTERVAL 15S
#
# Expiration period of the neighbor list.
# Default is 15 seconds.
# FISHEYE-NEIGHBOR-TIMEOUT-INTERVAL 15S

```

```

#
# Landmark Ad Hoc Routing (LANMAR) protocol follows
# draft-ietf-manet-lanmar-04.txt and uses Fisheye
# (draft-ietf-manet-fsr-03.txt) as the local scope routing protocol.
#
# ROUTING-PROTOCOL          FSRL
#
# Minimum number of neighbor in order to be considered a landmark.
# Defaults to 18 if not specified.
# LANMAR-MIN-MEMBER-THRESHOLD      18
#
# Fisheye scope. Default is 2.
# LANMAR-FISHEYE-SCOPE          2
#
# Landmark neighbor timeout interval.
# i.e, timeout duration of neighbor list.
# Defaults to 15S if not specified.
# LANMAR-NEIGHBOR-TIMEOUT-INTERVAL  15S
#
# Routing table update frequency within the fisheye scope.
# i.e, frequency for local fisheye routing
# Defaults to 5S if not specified.
# LANMAR-FISHEYE-UPDATE-INTERVAL    5S
#
# Landmark update interval. i.e, frequency of landmark update.
# Defaults to 15S if not specified.
# LANMAR-LANDMARK-UPDATE-INTERVAL    15S
#
# Maximum age for fisheye entries. Needs to be defined.
# i.e, lifetime of an entry in local topology table
# Defaults to 4S if not specified.
# LANMAR-FISHEYE-MAX-AGE            4S
#
# Maximum age for landmark entries. Needs to be defined.
# i.e, lifetime of an entry in landmark table
# Defaults to 10S if not specified.
# LANMAR-LANDMARK-MAX-AGE            10S
#
# Maximum age for drifter entries. Needs to be defined.
# i.e, lifetime of an entry in drifter table
# Defaults to 4S if not specified.
# LANMAR-DRIFTER-MAX-AGE            4S
#

#
# Zonal Routing Protocol (ZRP) is a hybrid protocol that divides the network
# into non-overlapping zones and runs independent protocols within and between
# the zones. For intrazone routing, ZRP uses IARP. For interzone routing,
# ZRP uses IERP. ZRP follows the draft-ietf-manet-zone-zrp-04.
#
# ROUTING-PROTOCOL ZRP
#
# Used to specify the zone radius. The zone radius has to be greater than or
# equal to 0, or INFINITY. If the zone radius is not given, then a default
# zone radius of 2 assumed by the protocol.
#
# ZONE-RADIUS 2
#

#
# IntrAzone Routing Protocol (IARP) is a link-state, proactive routing protocol.
# IARP follows draft-ietf-manet-zone-iarp-01.

```

```

#
# ROUTING-PROTOCOL IARP
#
# Used to specify the zone radius. The zone radius has to be greater than or
# equal to 0, or INFINITY. If the zone radius is not given, then a default
# zone radius of 2 assumed by the protocol.
#
# ZONE-RADIUS 2
#

#
# IntErzone Routing Protocol (IERP) is an on-demand routing protocol.
# IERP follows draft-ietf-manet-zone-ierp-02.
#
# ROUTING-PROTOCOL IERP
#
# Used to define the maximum buffer size. If not specified, the default value will be 100.
#
# IERP-MAX-MESSAGE-BUFFER-SIZE 100
#
# Used to specify the zone radius. The zone radius has to be greater than or
# equal to 0, or INFINITY. If the zone radius is not given, then a default
# zone radius of 0 assumed by the protocol.
#
# ZONE-RADIUS 0
#
#
# Bordercast Resolution Protocol (BRP) for Ad Hoc Networks.
# It follows draft-ietf-manet-zone-brp-02.txt
# BRP is used by IERP to find the route beyond the zone radius
# BRP can be enabled by following paramter. Teh default value is
# set to NO
#
# When BRP is used, routing protocol must be set as ZRP.
#
# IERP-USE-BRP YES | NO

#####
# Unicast routing - wired #
#####
# ROUTING-PROTOCOL BELLMANFORD

# OSPFv2 is compliant with RFC 2328.
#
# By default, OSPFv2 considers the entire domain as a single area.
#
# ROUTING-PROTOCOL OSPFv2
#
# To enable area support, specify OSPFv2-DEFINE-AREA to YES.
# Note: You must specify area related configurable parameters in a
# separate file specified by OSPFv2-CONFIG-FILE.
#
# OSPFv2-DEFINE-AREA YES
#
# and specify the configuration file where the area parameters are specified.
#
# OSPFv2-CONFIG-FILE default.ospf (or something else)
#
# See default.ospf for further information related to area and
# interface specific parameters.
#
# Sometimes it may be necessary, as a part of simulation, to delay (a random

```



```

# amount of time) the routers startup time just to desynchronize them.
# QualNet currently doesn't have this feature. OSPFv2, although allows the
# user to randomize the router startup time, the user cannot do that on
# a per node basis. Enabling this feature while running OSPFv2 as the
# routing protocol means each router will delay their startup time for
# some random amount of time (spaced over maximum simulation time or
# OSPFv2_LS_REFRESH_TIME, whichever is smaller), determined at runtime.
#
# To desynchronize the router startup time, specify
# OSPFv2-STAGGER-START to YES.
#
# OSPFv2-STAGGER-START  YES
#
# When using more than one autonomous system we need some extra information.
# To initialize the Autonomous System ID for each node, specify following:
#
# [<node_id>] AS-NUMBER <as_id>
#
# To configure the Autonomous System Boundary Router (ASBR) for an AS
# specify followings string:
#
# [<node_id>] AS-BOUNDARY-ROUTER YES
#
# The node_id qualifier format is consistent with standard input format.
#
# To inject external route into a OSPF capable autonomous system through
# a configurable file, specify OSPFv2-INJECT-EXTERNAL-ROUTE to YES.
#
# OSPFv2-INJECT-EXTERNAL-ROUTE  YES
#
# and specify external route file (the format of this file should be same
# as static route file).
#
# OSPFv2-INJECT-ROUTE-FILE  <filename>
#

#
# RIP is the Internet standard implementation of the Bellman-Ford routing
# algorithm. It is a distance vector routing algorithm utilizing UDP
# for control packet transmission.
#
# ROUTING-PROTOCOL  RIP
#
# Specify the RIP version with RIP-VERSION. Version 2 is used by default
# if this parameter is not specified.
#
# RIP-VERSION      1 | 2
#
# Specify whether not to use split horizon or use with poisoned reverse or
# use without poisoned reverse. Default is SIMPLE.
#
# SPLIT-HORIZON  NO | SIMPLE | POISONED-REVERSE
#

#
# RIPng is a routing protocol for IPv6 network. It is primarily
# based on RIP of IPv4 network with few modifications, necessary
# for operation over IPv6.
#
# ROUTING-PROTOCOL  RIPng
#
# Specify whether not to use split horizon or use with poisoned reverse or
# use without poisoned reverse. Default is SIMPLE.

```

```

#
# SPLIT-HORIZON NO | SIMPLE | POISONED-REVERSE
#

#
# IGRP is implemented following CISCO specification. The CISCO spec
# is publicly available at http://www.cisco.com/warp/public/103/5.html.
#
# ROUTING-PROTOCOL IGRP
#
# The network configuration is specified in the IGRP configuration file.
# This file MUST be specified to run IGRP.
#
# IGRP-CONFIG-FILE ./default.igrp
#
# The time period after which a node broadcasts update messages.
# Default value: 90 seconds.
#
# IGRP-BROADCAST-TIME <broadcast time>
#
# The time period after a path is timed out if no update is received.
# Default value: 3 times the IGRP-BROADCAST-TIME.
#
# IGRP-INVALID-TIME <invalid time>
#
# The time period during which no path will be accepted for a destination after a destination becomes
# unreachable.
# Default value: 3 times the broadcast time plus 10 sec.
#
# IGRP-HOLD-TIME <hold time>
#
# The time after which an entry is removed from the routing table if no update is received.
# Default value: 7 times the broadcast time.
#
# IGRP-FLUSH-TIME <flush time>
#
# The timer value that is used for periodic processing.
# Default value: 1 second.
#
# IGRP-PERIODIC-TIMER <periodic time>
#
# The timer value that is used for setting sleep time.
# Default value: 5 second.
#
# IGRP-SLEEP-TIME <sleep time>

#
# EIGRP is implemented following CISCO specification. The CISCO spec
# is publicly available at
# http://psyber.letifer.org/downloads/priv/eigrpwp.pdf
#
# ROUTING-PROTOCOL EIGRP
#
# The network configuration is specified in the EIGRP configuration file.
# This file MUST be specified to run EIGRP.
#
# EIGRP-CONFIG-FILE ./default.eigrp
#

#####
# Unicast routing - mixed networks #
#####

```

The following RPs support mixed networks (i.e., switch ethernet, point-to-point, and wireless ad hoc networks connected together). Currently,
 # only one of these RPs can be specified for the entire mixed network. Different RPs running on different networks cannot communicate with each other.

```
# ROUTING-PROTOCOL  BELLMANFORD
# ROUTING-PROTOCOL  RIP
# ROUTING-PROTOCOL  OSPFv2
```

```
#####
```

```
# Multicast Routing - wireless #
```

```
#####
```

```
# ODMRP follows draft-ietf-manet-odmrp-02.txt, draft-ietf-manet-odmrp-04.txt, and draft-yi-manet-pc-#00.txt
```

```
#
# To use ODMRP, multicast group members must be specified using MULTICAST-GROUP-FILE.
Also, multicast application traffic must be used.
# MULTICAST-PROTOCOL      ODMRP
```

```
# ODMRP-JR-REFRESH specifies the timer used for route refresh. If it is not specified, default value of 20S is assumed.
```

```
# ODMRP-JR-REFRESH      20S
```

```
# ODMRP-FG-TIMEOUT specifies the forwarding group timeout. If it is not specified, the default value of 60S is used.
```

```
# ODMRP-FG-TIMEOUT      60S
```

```
# ODMRP-DEFAULT-TTL specifies the TTL value for ODMRP routing control packets. If it is not specified, the default value of 64 is used.
```

```
# ODMRP-DEFAULT-TTL      64
```

```
# ODMRP-PASSIVE-CLUSTERING specifies whether or not to use passive clustering with ODMRP.
default= NO
```

```
# ODMRP-PASSIVE-CLUSTERING  NO
```

```
# ODMRP-CLUSTER-TIMEOUT specifies the timeout for maintaining clusters. This option is used only when passive-clustering is enabled.
```

```
# If ODMRP-CLUSTER-TIMEOUT not specified, the default value of 10S is used.
```

```
# ODMRP-CLUSTER-TIMEOUT    10S
```

```
# To join/leave a multicast group, use MULTICAST-GROUP-FILE. The format is: <node id> <group to join> <join time> <leave time>
```

```
# MULTICAST-GROUP-FILE      ./default.member
```

```
#####
```

```
# Multicast Routing - wired #
```

```
#####
```

```
# To use the below multicast routing protocols, the group management protocol IGMP must be running #on the host network.
```

```
# Furthermore, multicast group members must be specified using MULTICAST-GROUP-FILE. only MCBR traffic supports multicast address destination.
```

```
# DVMRP follows draft-ietf-idmr-dvmrp-v3-10.
```

```
# MULTICAST-PROTOCOL      DVMRP
```

```
# MOSPF is a multicast extension to OSPFv2 and follows RFC 1584.
```

```
# Note: - Enabling MOSPF automatically enables OSPFv2 as well.
```

```
# - MOSPF's Designated Router (DR) must correspond to the router running IGMP. The router with the highest router ID is selected as the DR in a subnet.
```

```
# MULTICAST-PROTOCOL      MOSPF
```

```
# When the total domain is divided into more than one area to convey group related information and to forward multicast packet, a subset of the area
```

```

# border routers are configured as INTER-AREA-MULTICAST-FORWARDER
# INTER-AREA-MULTICAST-FORWARDER {<list of node id>}

# PIM-DM follows draft-ietf-pim-v2-dm-03.txt.
# MULTICAST-PROTOCOL      PIM-DM

# IGMP follows RFC 2236. IGMP must be specified at the host network for wired multicast protocols to
run correctly. Specify the IGMP routers using IGMP-ROUTER-LIST.
# GROUP-MANAGEMENT-PROTOCOL IGMP
# IGMP-ROUTER-LIST      {<list of node id>}
#

# To join/leave a multicast group, use MULTICAST-GROUP-FILE. The format is:  <node id> <group
to join> <join time> <leave time>
# MULTICAST-GROUP-FILE      ./default.member

#####
# Routing - Quality Of Service                                     #
#####
# Q-OSPF is a Quality of Service extension to OSPFv2 and follows RFC 2676. To use Q-OSPF, OSPFv2
# must be selected as the ROUTING-PROTOCOL. To activate Q-OSPF extensions, select
# QUALITY-OF-SERVICE      Q-OSPF

# QOSPF-COMPUTATION-ALGORITHM specifies the path calculation algorithm. The Extended
Breadth First Search Algorithm for single path must be selected for Q-OSPF, below.
# QOSPF-COMPUTATION-ALGORITHM
EXTENDED_BREADTH_FIRST_SEARCH_SINGLE_PATH

# QOSPF-FLOODING-INTERVAL specifies the periodic interval of flooding of
# LSAs for Q-OSPF. The value of this timer inversely varies with QoS
# traffic. By default, it uses the periodic timer of OSPF.
#
# QOSPF-FLOODING-INTERVAL      10S

# The following two parameters are required to handle Q-OSPF flooding properly if a significant change
in currently utilized bandwidth occurs.
# QOSPF-INTERFACE-OBSERVATION-INTERVAL specifies the interval of monitoring each
interface of a node. QOSPF-FLOODING-FACTOR is a relative factor which
# is the ratio of change in link utilization (of a interface during last period) with total link bandwidth. For
every observation interval, a node
# checks link utilization of every interface and it only floods an LSA after that interval if any interface
link utilization exceeds the
# specified value of flooding factor. The value of this flooding factor must be within zero and one. The
default value of "flooding interval"
# is 2S and "flooding factor" is 0.1.
#
# QOSPF-INTERFACE-OBSERVATION-INTERVAL 2S
# QOSPF-FLOODING-FACTOR      0.1

# QUEUEING-DELAY-FOR-QOS-PATH-CALCULATION specifies whether or not
# queue delay will be considered during path calculation.
#
# QUEUEING-DELAY-FOR-QOS-PATH-CALCULATION YES | NO

#####
# Routing - exterior gateway protocol                             #
#####
# BGPv4 is an exterior gateway protocol used to route packets between autonomous systems. BGPv4
# follows RFC 1771.
# EXTERIOR-GATEWAY-PROTOCOL BGPv4

# The following timer-related parameters are available for controlling BGP timer-related operations.
# How much time a speaker will wait to listen for activities from a peer. Default= 90 sec.

```

```

# BGP-HOLD-TIME-INTERVAL

# Hold time in active state. Default is 4 minutes.
# BGP-LARGE-HOLD-TIME-INTERVAL

# Interval between two subsequent update message for external peers. Default = 30 sec.
# BGP-MIN-RT-ADVERTISEMENT-INTERVAL

# Interval between two subsequent update message for internal peers. Default = 15 sec.
# BGP-MIN-AS-ORIGINATION-INTERVAL

# Interval between two successive keep alive messages. Default = 30 sec.
# BGP-KEEPALIVE-INTERVAL

# Time to wait for re-opening a tcp connection. Default = 120 sec.
# BGP-CONNECT-RETRY-INTERVAL

# Time to wait to determine if a neighbor is not reachable. Default= 15 sec.
# BGP-ROUTE-WAITING-INTERVAL

# Parameters for configuring individual BGP routers are read from BGP-CONFIG-FILE.
# BGP-CONFIG-FILE      ./default.bgp

#####
# Configuration for Access list ( standard, extended, reflexive )      #
#####
# Configuration filename containing ACL criterias is defined with the following format:
# [<node-id>] ROUTER-CONFIG-FILE <filename>
#
# Example:
# [1] ROUTER-CONFIG-FILE ./default1.router-config
# [2] ROUTER-CONFIG-FILE ./default2.router-config
# ACL configuration for node 1 and node 2 is defined in
# default1.router-config and default2.router-config respectively.
#
# ROUTER-CONFIG-FILE ./default.router-config
# Here, ACL defintions for all the nodes are defined in a common file,
# default.router-config.
#
# Please refer to default.router-config for more details of the
# format of this file.
#
# To viewing the trace for packets dropped by ACL, specify:
# ACCESS-LIST-TRACE YES | NO
#

#####
# Transport layer      #
#####
# The following describes the various TCP variants that QualNet supports. TCP code is ported from
FreeBSD 2.2.2. default = LITE
# TAHOE: Consists of Slow Start, Congestion Avoidance, and Fast Retransmit. Note: TCP-USE-
RFC1323 is disabled.
# RENO: Consists of TAHOE plus Fast Recovery Note: TCP-USE-RFC1323 is disabled.
# LITE: Consists of RENO plus Big Window and Protection Against Wrapped Sequence Numbers
options. TCP-USE-RFC1323 must be set to "YES". If not, revert to RENO behavior.
# NEWRENO: Consists of RENO with modification to Fast Recovery, (i.e., must receive an ACK for
highest sequence number sent to exit Fast Recovery).
# SACK: Consists of Selective Acknowledgement combined with RENO congestion algorithm. When
peer does not respond with the Sack Permitted option, SACK reverts to LITE behavior.
# TCP  TAHOE | RENO | LITE | NEWRENO | SACK

TCP LITE

```



```

TCP-USE-RFC1323 NO
TCP-DELAY-ACKS YES
TCP-DELAY-SHORT-PACKETS-ACKS NO
TCP-USE-NAGLE-ALGORITHM YES
TCP-USE-KEEPALIVE-PROBES YES
TCP-USE-PUSH YES
TCP-MSS 512
TCP-SEND-BUFFER 16384
TCP-RECEIVE-BUFFER 16384
ATM-RED-MIN-THRESHOLD 5
ATM-RED-MAX-THRESHOLD 15
ATM-RED-MAX-PROBABILITY 0.02
ATM-RED-SMALL-PACKET-TRANSMISSION-TIME 10MS
ATM-QUEUE-SIZE 15000
ATM-SCHEDULER-STATISTICS NO
ATM-LAYER2-STATISTICS NO
ATM-QUEUE-STATISTICS NO
APP-CONFIG-FILE D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\31_SDC_20_500x500_RD.app
PACKET-TRACE NO
ACCESS-LIST-TRACE NO

# Value of maximum segment size. If not specified, default is 512
# TCP-MSS 512

# Value of send buffer space. If not specified, default is 16384 bytes
# TCP-SEND-BUFFER 16384

# Value of receive buffer space. If not specified, default is 16384 bytes
# TCP-RECEIVE-BUFFER 16384

# Whether to send window scale and timestamps in TCP header options. Without window scaling, the
# maximum reported window size is
# is 65,535 bytes. With window scaling, the maximum reported window size is 1,073,725,440 bytes.
# default= NO
# TCP-USE-RFC1323 YES | NO

# Whether ACKs for received segments are delayed. If not specified, default is YES
# TCP-DELAY-ACKS YES | NO

# Whether to use the Nagle algorithm to coalesce short packets. If not specified, default is YES
# TCP-USE-NAGLE-ALGORITHM YES | NO

# Whether keep-alive probes are to be used. If not specified, default is YES
# TCP-USE-KEEPALIVE-PROBES YES | NO

# Whether the Push bit in TCP header is set (except for FIN segments) when the send buffer is full. If not
# specified, default is YES
# TCP-USE-PUSH YES | NO

# QualNet supports the following TCP traces. Only one trace type can be used at a time during the entire
# simulation.
#
# TCPDUMP: A tcpdump compatible binary format. Trace output file is tcptrace.dmp. This trace file can
# be used with the tcptrace (http://www.tcptrace.org/index.html) Unix utility program.
#
# Note: The machine type (big or little endian) must also be specified in tcp.c with the default being
# little endian. To specify big endian, comment out "#define LITTLE_ENDIAN" in tcp.cpp
# and recompile QualNet.
#
# TCPDUMP-ASCII: A tcpdump compatible ascii format. Trace output file is tcptrace.asc
#
# By default, QualNet does not generate a TCP trace file. To generate one, use the following:
# TCP-TRACE TCPDUMP | TCPDUMP-ASCII

```

Additionally, the direction of the trace can be specified with the following:

BOTH: Trace both input and output packets.

OUTPUT: Trace only packets output to the network.

INPUT: Trace only packets received from the network.

By default, the direction is set to BOTH.

Note: The user should note that while there is flexibility

in specifying any combination of directions, it may not

satisfy the needs of tcptrace analysis.

The graphical output, especially the rtt plot, may not

show up in some combinations. An example is input from

one node and output from the node across the connection.

In most instances, specifying the direction as BOTH is suitable.

#

TCP-TRACE-DIRECTION BOTH | OUTPUT | INPUT

Example: To get a TCPDUMP trace for node 1, do the following:

[1] TCP-TRACE TCPDUMP

[1] TCP-TRACE-DIRECTION BOTH

Next, use 'tcptrace -G tcptrace.dmp' to get all the xplot files. Then, use 'xplot <file>' to view the xplot files.

#####

Application layer

#####

The following is used to set up applications such as FTP and Telnet. The file will need to contain

#parameters that will be used to determine connections and other characteristics of the particular

#application.

APP-CONFIG-FILE ./default.app

MULTIMEDIA APPLICATIONS AND PROTOCOLS

#

The Voip application may choose either H.323 or SIP as the multimedia signalling protocol.

#

[<node_ID> | <network address>] MULTIMEDIA-SIGNALLING-PROTOCOL H323 | SIP

#

The following parameters may be given for Voip, common to any call signalling protocol.

Connection delay is the delay after which the receiver receives the call after being alerted of the incoming call. The default value is 10

second. It means after 10 seconds from the start of ringing/alerting, the receiver accepts the call.

VOIP-CONNECTION-DELAY <delay(IN SECS)>

#

Call timeout is the duration from the initiation of the call to the maximum time at which the initiator can accept the call. This can be

roughly taken as the maximum ringing time after which the call will be rejected. The receiver can't receive the call after this timeout.

The default value is 60 seconds, if not specified. A thumb rule is to keep the call-timeout at least four times the connection-delay.

VOIP-CALL-TIMEOUT <duration(IN SECS)>

#

For H.323 the following parameters may be configured:

#

The gatekeeper list in the network can be given as follows. This is optional and if not provided, the connection between calling party and

called can still be established, but without the RAS functionality.

H323-GATEKEEPER {<gatekeeper_list>}

#

Each terminal should have one or more alias address. We have considered only one alias address. The file name is taken from the following line.

TERMINAL-ALIAS-ADDRESS-FILE <alias_address_file>

```

#
# The <alias_address_file> file contains a list of terminal node IDs with their alias address. The syntax of
the file is (see default.endpoint for
# an example):
#
# <node1_id> <alias_address_for_node1>
# <node2_id> <alias_address_for_node2>
# ...
#
# We have two types of call model in H323; one is Direct and the other is Gatekeeper-routed. Using the
following syntax, the user can specify the
# call model. If this is not specified, the call model is set to Direct by default.
# H323-CALL-MODEL          GATEKEEPER-ROUTED | DIRECT
#
# If the gatekeeper is available and gatekeeper discovery is done dynamically, then we need to specify
one multicast protocol and
# the group management protocol (IGMP) with the IGMP router. If the gatekeeper has a predefined
unicast address, then we can specify
# that address as below and multicast settings are no longer required.
# GATEKEEPER-ADDRESS <unicast_address>
#
#
# For SIP the following parameters may be configured
#
# The list of proxy servers may be given in the following manner. Proxy server must be present in a
network irrespective of the
# callMode chosen. They may be entered comma delimited similar to Qualnet convention of specifying
the list of nodes.
# SIP-PROXYLIST    {<comma delimited list of proxy servers>}
#
# SIP-PROXYLIST    {1, 3, 5 thru 8, 10}
#
#
# SIP-TRANSPORT-LAYER-PROTOCOL is the underlying transport protocol used by SIP. It may use
any underlying transport layer protocol,
# - TCP, UDP, SCTP etc. But the current implementation uses only TCP. Hence only TCP may be chosen
as the transport protocol.
# SIP-TRANSPORT-LAYER-PROTOCOL    <Transport Protocol>
#
# There are basically two types of call model- Direct and Proxy-routed.
# This can be specified in the following way. If this is not specified, the call model is set to DIRECT by
default.
# SIP-CALL-MODEL          PROXY-ROUTED | DIRECT
#
# Each terminal(User Agent) may have one or more alias addresses. Here we have considered only one
alias address. The file name is
# taken from the following line.
# SIP-ALIAS-ADDRESS-FILE    <alias_address_file>
#
# DETAILS :The <alias_address_file> file contains a list of terminal node IDs with their alias address,
domain name and corresponding
# proxy_ip_address. The syntax is given in full detail in default.sip.
#
# DNS-ADDRESS-FILE is required for enabling inter-proxy calls, each Proxy node carries a list of other
proxy nodes present in the SIP network(It
# is assumed that one domain is represented by one proxy node) and their access interface. It is not
necessary for single domain calls. For
# details on how to specify the details reference may be made to the default.dns file
#
# To summarize SIP specific configurable parameters
#
# SIP-PROXYLIST          < list of proxy nodeIds >
# SIP-TRANSPORT-LAYER-PROTOCOL    < TCP|UDP|SCTP >

```

```

# SIP-CALL-MODEL          < DIRECT|PROXY-ROUTED >
# TERMINAL-ALIAS-ADDRESS-FILE  < file name (conventionally default.sip) >
# DNS-ADDRESS-FILE        < domain address file name >
#
#####
# RTP Jitter Buffer
#####
# The following parameter represents different RTP Jitter Buffer strategy.

# Various packets in the same call can experience different amounts of inter-arrival variance, or jitter,
# which is a variable component of
# the total end-to-end network delay. The storage area used to store the receiving voice packet for
# eliminating jitter is known as the Jitter
# Buffer. If Jitter Buffer Enabled is YES, The receiver node for Voip application has jitter buffer. Default
# Value is NO.
# VOIP-JITTER-BUFFER-ENABLED      YES | NO

# Maximum no of packets can be stored in Jitter Buffer.
# VOIP-JITTERBUFFER-MAXNO-PACKET  <no of packets>
# VOIP-JITTERBUFFER-MAXNO-PACKET  30

# Maximum delay upto which one packet will be stayed in jitter buffer,
# This delay will be adjusted dynamically, But for the first time it
# should be mentioned. Default value is 90MS.
# VOIP-JITTERBUFFER-MAXIMUM-DELAY  <time>
# VOIP-JITTERBUFFER-MAXIMUM-DELAY  90MS

# Jitter Buffer TalkSpurt Delay.
# The periods when voice activity is detected are referred to as talkspurts. Each voice source has an
# average talkspurt length
# of 0.8 sec and an average silent interval of 1.2 sec. Default Value is 2S.
# VOIP-JITTERBUFFER-TALKSPURT-DELAY <time>
# VOIP-JITTERBUFFER-TALKSPURT-DELAY 2S

# MOS is a subjective score of voice quality as perceived by people listening to speech over a
# communication system. To determine the MOS
# for a particular phone connection, a statistically valid group of mixed males and females rate the quality
# of test sentences read aloud over
# the connection. Each person in the group gives a rating of 1 to 5 for each sentence heard; the resulting
# MOS is the average of all
# the individual scores, ranging from 1 (worst) to 5 (best). Total Loss Probability for MOS Calculation.
# Default Value is 2.07

# VOIP-TOTAL-LOSS-PROBABILITY  2.07

#####
# ATM Configuration
#####
# ATM support only wired link. Each link is a point-to-point (serial)
# link between two nodes. These links are dedicated, error-free, and
# support the maximum bandwidth in both directions simultaneously.
# This link are designated as ATM-LINK

# QualNet creates two network interfaces for each end of a link,
# and ATM addresses are auto-assigned.

# ATM-LAYER2-LINK-BANDWIDTH      111200
# ATM-LAYER2-LINK-PROPAGATION-DELAY 10MS

# ATM-LINK N2-1.0 { 1, 2}
# ATM-LINK N2-2.0 { 2, 5}

```

```

# ATM-LINK N2-3.0 { 3, 4}
# ATM-LINK N2-4.0 { 4, 5}
# ATM-LINK N2-5.0 { 5, 6}
# ATM-LINK N2-6.0 { 5, 7}
# ATM-LINK N2-7.0 { 5, 8}
# ATM-LINK N2-8.0 { 6, 9}
# ATM-LINK N2-9.0 { 7, 10}
# ATM-LINK N2-10.0 { 8, 11}

# To enable ATM characteristics of any node, configure as follows.
# Currently ATM network cannot interact with other network (like IP).
# So all the nodes must be ATM-NODE.
# [<ATM_enabled_node_Id>] ATM-NODE YES

#[1 thru 11] ATM-NODE YES

# Some of the nodes are defined as ATM-End-Systems.
# These nodes have at least one interface other than ATM-Interface.
# All other ATM nodes are treated as ATM-Switch.
# [ATM_endsystem_node_Id>] ATM-END-SYSTEM YES

# [1 3 9 10 11] ATM-END-SYSTEM YES

# Presently AAL5 is used as ADAPTATION LAYER protocol for ATM.
# Set the related parameter as follows,

# ADAPTATION-PROTOCOL AAL5
# ADAPTATION-LAYER-STATISTICS YES | NO

# ATM routes the packet using static route only, which collects
# the path information from the mentioned ATM-STATIC-ROUTE-FILE.

ATM-STATIC-ROUTE NO
# ATM-STATIC-ROUTE-FILE ./default.atmstatic

# SAAL is the signalling protocol in ATM layer. When following
# variable is set to yes, ATM SALL will show its statistics.
# SIGNALLING-STATISTICS YES | NO

# ATM RED Queue is a special type of Random Early Detection (Drop) queue.
# This implementation marks packets, it does not drop them.
# ATM uses RED Queue internally but following optional parameters
# can also be set externally

# 1. ATM-RED-MIN-THRESHOLD: The number of packets in the queue that
# represents the lower bound at which packets can be randomly dropped.
# 2. ATM-RED-MAX-THRESHOLD: The number of packets in the queue that
# represents the upper bound at which packets can be randomly dropped.
# 3. ATM-RED-MAX-PROBABILITY: The maximum probability (0...1) at which
# a packet can be dropped (before the queue is completely full, of course).
# 4. ATM-RED-SMALL-PACKET-TRANSMISSION-TIME: A sample amount of time
# that it would take to transmit a small packet - used to estimate the
# queue average during idle periods.

# [<interface_address>] ATM-RED-MIN-THRESHOLD 5
# [<interface_address>] ATM-RED-MAX-THRESHOLD 15
# [<interface_address>] ATM-RED-MAX-PROBABILITY 0.02
# [<interface_address>] ATM-RED-SMALL-PACKET-TRANSMISSION-TIME 10MS

# ATM-RED-MIN-THRESHOLD 5
# ATM-RED-MAX-THRESHOLD 15
# ATM-RED-MAX-PROBABILITY 0.02

```



```

# ATM-RED-QUEUE-WEIGHT    0.002
# ATM-RED-SMALL-PACKET-TRANSMISSION-TIME  10MS

# For printing the scheduler specific statistics at each interface
# of an ATM node, use this parameter ~QATM-SCHEDULER-STATISTICS~R.
# Default value is NO.

# ATM-SCHEDULER-STATISTICS YES | NO

# For printing the ATM Layer2 specific statistics at each interface
# of an ATM node, use this parameter ~QATM-LAYER2-STATISTICS~R.
# Default value is NO.

# ATM-LAYER2-STATISTICS YES | NO

# Topology are designed using ATM-LINK only,
# so SUBNET or LINK statement are abandoned.
# No need to specify any Network or MAC Protocol.

#####
# Scheduler
#####
# The following tells the scheduler what type of queue to use when scheduling events.
#
# Use the following to change the scheduler's queue type:
#
# SCHEDULER-QUEUE-TYPE      SPLAYTREE | CALENDAR
#
# By default, the scheduler's queue type is SPLAYTREE.
# Uncomment this to enable the Calendar queue
SCHEDULER-QUEUE-TYPE      CALENDAR

#####
# Statistics
#####
#
# The following parameters determine if you are interested in the
# statistics of a single or multiple layer. By specifying the following
# parameters as YES, the simulation will provide you with statistics for
# that particular layer. All the statistics are compiled together into
# a file called "qualnet.stat" that is produced at the end of the simulation.
# If you need the statistics for a particular node or particular protocol,
# it is easy to do the filtering. Every single line in the file is of
# the following format:
#
# Node:    9, Layer: PhyNoCapture, Total number of collisions is 0
#

APPLICATION-STATISTICS      YES
TCP-STATISTICS              YES
UDP-STATISTICS              YES
RSVP-STATISTICS             NO
ROUTING-STATISTICS          YES
ACCESS-LIST-STATISTICS      NO
ROUTE-REDISTRIBUTION-STATISTICS  NO
IGMP-STATISTICS             NO
EXTERIOR-GATEWAY-PROTOCOL-STATISTICS  YES
NETWORK-LAYER-STATISTICS    YES
DIFFSERV-EDGE-ROUTER-STATISTICS  NO
QUEUE-STATISTICS            YES
MAC-LAYER-STATISTICS         YES
PHY-LAYER-STATISTICS         YES
MOBILITY-STATISTICS          NO

```

MPLS-STATISTICS NO
 MPLS-LDP-STATISTICS NO
 RSVP-STATISTICS NO
 SRM-STATISTICS NO
 DIFFSERV-EDGE-ROUTER-STATISTICS NO
 QOSPF-STATISTICS NO
 # Network Statistics should be on
 ACCESS-LIST-STATISTICS NO
 POLICY-ROUTING-STATISTICS NO
 ROUTE-REDISTRIBUTION-STATISTICS NO
 SIGNALLING-STATISTICS NO
 MOBILE-IP-STATISTICS NO

USE-NODE-ICON YES
 NODE-ICON D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\DEFAULT.GIF
 AZIMUTH 0
 ELEVATION 0
 PARTITION 0
 SUBNET N8-192.0.0.0 { 1 thru 20 } Default

[1 thru 20] MOBILITY FILE
 [1 thru 20] DUMMY-MOBILITY-FILE
 D:\P\qual\gui\scenarios\31_SDC_20_500x500_RD\Road.mobility
 IP-FORWARDING NO
 [1 thru 20] IP-FORWARDING YES

COMPONENT 0 { 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 } 20 250.0 250.0 0.0 500.0 500.0 3000.0

SIGNALLING statistics can be enabled by setting the following parameter.
 # This config parameter shows statistics of H323, SIP and SAAL (ATM)
 # Statistics will be disabled by setting the following value to NO. The
 # default value is NO.
 # SIGNALLING-STATISTICS YES | NO
 #

 # Tracer #
 #####
 # The following allows packets to be traced up and down the protocol stack and between nodes. The
 # packet headers are printed as the packet
 # travels up and down the protocol stack. The trace output is printed to <EXPERIMENT-NAME>.trace.
 # The trace file can then be viewed with
 # the Tracer GUI by using <QUALNET_HOME>/gui/bin/RunTracer. default= off.
 # PACKET-TRACE YES | NO

By default, when packet tracing is turned on, all layers of the
 # protocol stack are traced. The following are the currently layers
 # being supported for packet tracing:
 #
 # TRACE-TRANSPORT-LAYER YES | NO
 # TRACE-NETWORK-LAYER YES | NO

By default, TRACE-DIRECTION is set to BOTH. INPUT means that only
 # packets received by a node are traced. OUTPUT means that only
 # packets sent by a node are traced. BOTH means packets that are
 # sent or received by a node are traced.
 # TRACE-DIRECTION INPUT | OUTPUT | BOTH

By default, all protocols are traced. To selectively trace particular protocols, either use "TRACE-ALL
 NO" and selectively turn on the

```

# particular protocols to be traced or use "TRACE-ALL YES" and selectively turn off protocols that are
# not to be traced.
# TRACE-ALL          YES | NO

# Protocols that supports packet tracing are:
# TRACE-TCP          YES | NO
# TRACE-UDP          YES | NO
# TRACE-IP           YES | NO
# TRACE-OSPFv2       YES | NO

# For instance, the following two examples will only show IP header information as the packet traverses
# up and down the protocol stack:
# TRACE-ALL          NO
# TRACE-IP           YES
# or
# TRACE-ALL          YES
# TRACE-TCP          NO
# TRACE-UDP          NO
# TRACE-OSPFv2       NO

#####
GUI Options                                     #
#####
# The Animator GUI recognizes several options. Animation may be enabled and stored to a trace file by
# using the command line -animate flag. The following variables may be used to configure the runtime
# appearance of the Animator
#
# The COMPONENT flag specifies a hierarchical organization of the network. This variable should only
# be generated by the Animator itself.
# COMPONENT <NodeID> {space-separated list of child nodes} children-count \
#   <x-position of origin/s-w corner of this component> \
#   <y-position of origin/s-w corner of this comp> \
#   <z-position of origin/s-w corner of this comp> \
#   <logical width of this node> <logical height of this node> \
#   <logical depth of this node> [BG=<BackGround Image file path>] \
#   [ICON=<Icon File Path for Closed Node, if one specified>] \
#   [AS=<AS id of this Component, if applicable>]
#
# HOSTNAME specifies a string to use as a label, typically for a specific node.
#
# USE-NODE-ICON YES | NO
# An entry of USE-NODE-ICON YES is required to enable use of the NODE-ICON variables. USE-
# NODE-ICON NO will disable the use of icons for the
# qualified nodes. This variable will be phased out after 3.8.
#
# NODE-ICON specifies the path to an icon file (a GIF or JPG) to use for one or more nodes.
#
# GUI-BACKGROUND-IMAGE-FILENAME specifies an image file (GIF or JPG) to use as a
# background map for the scenario.

```