Analysis of Vehicular Traffic Using Vanet Communications And Detection of Abnormal Vehicular Activities

By

Bhavin V. Gurjar

08MCES53

M.TECH(Computer Science-Split)

Department of

Computer Science And Engineering

Ahmedabad-382481

May 2011

Analysis of Vehicular Traffic Using Vanet Communications And Detection of Abnormal Vehicular Activities

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering

By

Bhavin V. Gurjar

Guided By

Dr. S.N.PRADHAN

Department of

Computer Science And Engineering

Ahmedabad-382481

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Computer Science and Engineering at Institute of Technology, Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

Bhavin V. Gurjar

Certificate

This is to certify that the Major Project entitled **"Analysis of Vehicular Traffic Using Vanet Communications and Detection of Abnormal Vehicular Activities"** submitted by **Mr. Bhavin Gurjar (08mces53)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Date: ____________________

Dr. S. N. Pradhan
Professor and PG-Coordinator,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Prof. D. J. Patel
Professor and Head,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. K. Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad.

Abstract

VANET(Vehicular Adhoc Network) is the new area of technology.VANET encompasses V2I(vehicle to infrastructure communication) and V2V(vehicle to vehicle communication)using multi channel allocation mechanism. It provides a platform to share vehicle information with neighbouring vehicles and local infrastructure.

The objective of this study is to obtain indirect information about the status of vehicles and road condition by observing pattern of communication, both V2V and V2I.

It is possible to detect a failure node(vehicle) or stationary node on the road by observing traffic pattern using V2V communication.IEEE 802.11p protocol which has been proposed for V2V and V2I as been used to simulate data traffic to carry out the simulations.

To send the messages to all vehicles in the proximity within minimum possible time we have applied two approaches.First approach is to reduce the time for RSU to receive and send the message to another vehicle node and the second approach is to reduce the switching time between SCH and CCH.It has been shown that RSU should send safety messages to moving vehicle on CCH channel.

IEEE 802.11p has four types of different lower to higher priority traffic in between active and failure node. As we have to send the message with in a certain time ,throughput has to be improved. which has been achieved by reducing the message size.

Acknowledgements

A journey is easier when you travel together. Interdependence is certainly more valuable than independence. This thesis is the result of work whereby I have been accompanied and supported by many people.

With immense pleasure I express my sincere gratitude, regards and thanks to my guide **Dr.S.N.Pradhan** for his excellent guidance and continuous encouragement at all the stages of my research work. I would like to thank **Prof.Sunil Jardosh** due to his continuous help and support. The chain of my gratitude would be definitely incomplete if I would forget to thank **Prof.Vijay Ukani** and **Prof.Priyanka Sharma** who shared with me their experience for supporing my thesis work.

I would like to thank **Dr.K.Kotecha,** Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for his unmentionable support, providing basic infrastructure and healthy research environment.

Last, but not the least, no words are enough to acknowledge constant support of my parents & my sister because of whom I am able to complete my dissertation work successfully.

Bhavin V. Gurjar
08mces53

Contents

List of Figures

List of Tables

Chapter 1

Inroduction

Traffic accidents have been taking thousands of lives each year, outnumbering any deadly diseases or natural disasters. 1,19,860 people killed per year in highway accidents in India: IRF(International Road Federation).

Studies [1] show that about 60% roadway collisions could be avoided if the operator of the vehicle was provided warning at least one-half second prior to a collision.

1.1 Human drivers limitations

In emergency situations, a driver typically relies on the tail brake light of the car immediately ahead to decide his or her own breaking action. Under typical road situations, this is not always the best collision avoidance strategy for various reasons. In many cases, the ability to detect an emergency event occurring at some distance ahead is limited by the inability of drivers to see past the vehicle in front of them. Human drivers suffer from perception limitations on roadway emergency events, resulting in large delay in propagating emergency warnings, as the following simplified example illustrates. In 3.1, three vehicles, namely A, B and C, travels in the same lane. When A suddenly breaks abruptly, both vehicles B and C are endangered, and being further away from A does not make vehicle C any safer than B due to the following reason.

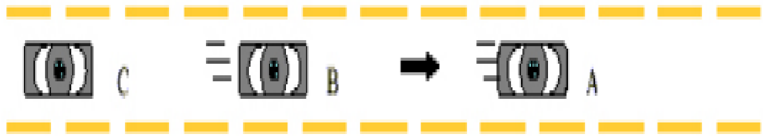

Figure 1.1: Vehicle to vehicle communication to increase road safety

- Line-of-sight limitation of brake light: Typically, a driver can only see the brake light from the vehicle directly in front. Thus, very likely vehicle C will not know the emergency at A until B brakes.

- Large processing/forwarding delay for emergency events: Driver reaction time, i.e., from seeing the brake light of A to stepping on the brake for the driver of vehicle B, typically ranges from 0.7 seconds to 1.5 seconds. At a speed of 70 mph, this means that between 75 and 150 ft is traveled before any reaction occurs; which results in large delay in propagating the emergency warning.[2]

1.2 Need of Intelligent Transportation System (ITS)

Chain collisions can be potentially avoided, or their severity lessened, by reducing the delay between the time of an emergency event and the time at which the vehicles behind are informed about it [3]. One way to provide more time to drivers to react in emergency situations is to develop Intelligent Transportation System applications using emerging wireless communication technology. The primary benefit of such communication will be to allow the emergency information to be propagated among vehicles much quicker than a traditional chain of drivers reacting to the brake lights of vehicles immediately ahead. Figure 5.5 details the system architecture proposed by the U.S. Department of Transportation for the development of Intelligent Transportation Systems (ITS). The architecture is defined around four basic components linked by a communication infrastructure.

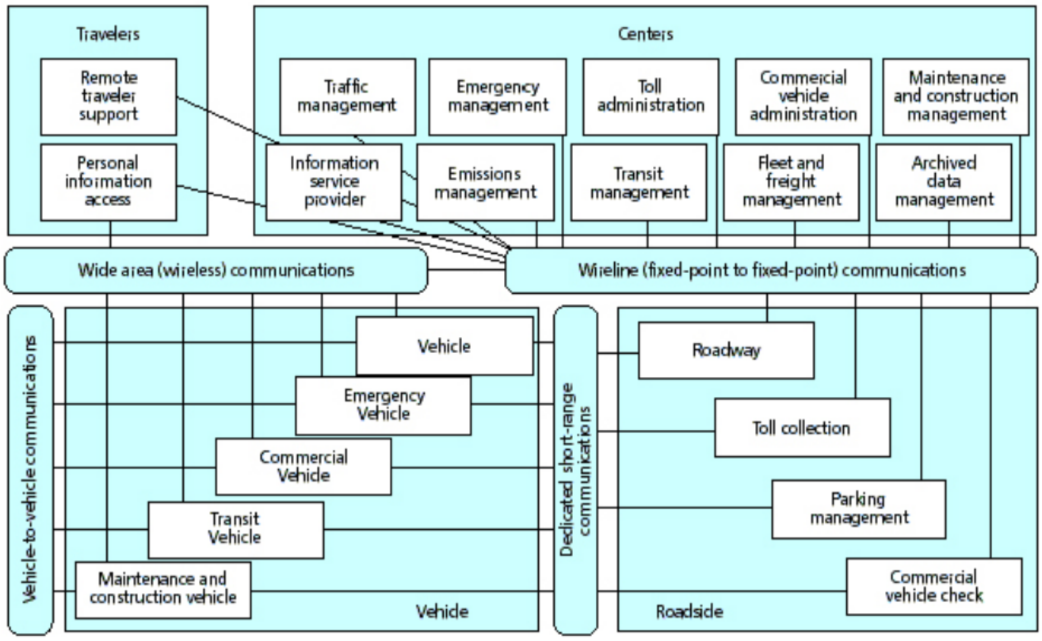

Figure 1.2: Proposed National ITS Architecture [4, 5]

The four generic types of telecommunications systems are:

- Vehicle-to-Vehicle
- Dedicated Short Range Communications (DSRC)
- Wide Area Wireless
- Wireline

Wireline and Wireless are the two primary types of telecommunications architectures shown in the diagram, with Vehicle-to-Vehicle (V2V) and DSRC being two applications of wireless. There is no distinct requirement to use RF, Copper, or Fiber Optics as a transmission medium. Nor is there any suggestion as to the network topology: point-to-point, star, ring, mesh, etc. More recently, the combined availability of the Global Positioning System (GPS) and deployment of cellular-based communication systems has further fueled the development of vehicle tracking systems and systems providing information to travelers in vehicles through wireless means. Interest in vehicle-to-infrastructure and vehicle-to-vehicle communication capabilities has only recently gained momentum, as such capabilities were in the past either not technically feasible or too costly to implement and operate.

Road and traffic safety can be improved if drivers have the ability to see further down the road and know if a collision has occurred, or if they are approaching a traffic jam. This can become possible if drivers and vehicles communicate with each other and with roadside base stations. If traffic information was provided to drivers, police, and other authorities, the roads would be safer and traveling on them would become more efficient. It is possible to build a multihop network among several vehicles that have communication devices. These vehicles would form a mobile ad hoc network, and could pass along information about road conditions, accidents, and congestion. A driver could be made aware of the emergency braking of a preceding vehicle or the presence of an obstacle in the roadway. Even though the topic is too big, here in my seminar, I made an endeavor to present an overview of vehicular communication technology particularly describing V2V communication using IEEE and ASTM adopted DSRC Standard. This paper also discusses some of the application requirements and congestion control policies.

1.3 Overview of Different Vehicular Communications

In-vehicle computing systems allow the coverage of monitoring systems to extend beyond the extent of infrastructure-based sensors, e.g., roadside cameras that are expensive to deploy and maintain. Subject to privacy considerations, in-vehicle sensors offer the potential for much more detailed, accurate information (e.g., on-road

vehicle activity and emissions) than would otherwise be possible, enabling new ways to improve and optimize the transportation system as well as support a variety of commercial applications.
In-vehicle computing systems facilitate the customization of information services to the needs and characteristics of individual travelers. Cooperation between vehicles can reduce the end cost of user services. Possible applications designed to benefit from these in-vehicle computing systems can be generally classified as safety and non-safety applications. Safety applications include, e.g., collision avoidance and co-operative driving. Non-safety applications include traffic information propagation, toll service, Internet access, tourist information, cooperative gaming and entertainment, etc. A V2V network consists of instrumented vehicles equipped with on-board computing and wireless communication devices, a GPS device enabling the vehicle to track its spatial and temporal trajectory, a pre-stored digital map, and optional sensors for reporting crashes, engine operating parameters, etc.

1.4 DSRC Applications

- Public safety: to reduce traffic accidents
- Traffic management: to improve the flow of traffic, reducing congestion
- Travelers Information Support: to provide a great variety of travel related timely information, such as electronic maps, and road and weather information

Messages	Unicast	Broadcast
R2V	Toll payment,and road side inspection	Safety message,road service, and travel information
V2V	Data sharing,paging,and VoIP	emergency and service vehicles

Table I: Different DSRC Appication

- Entertainment/rich media content delivery: Internet access, infotain- ment (news, sports, movies, etc.) on demand.

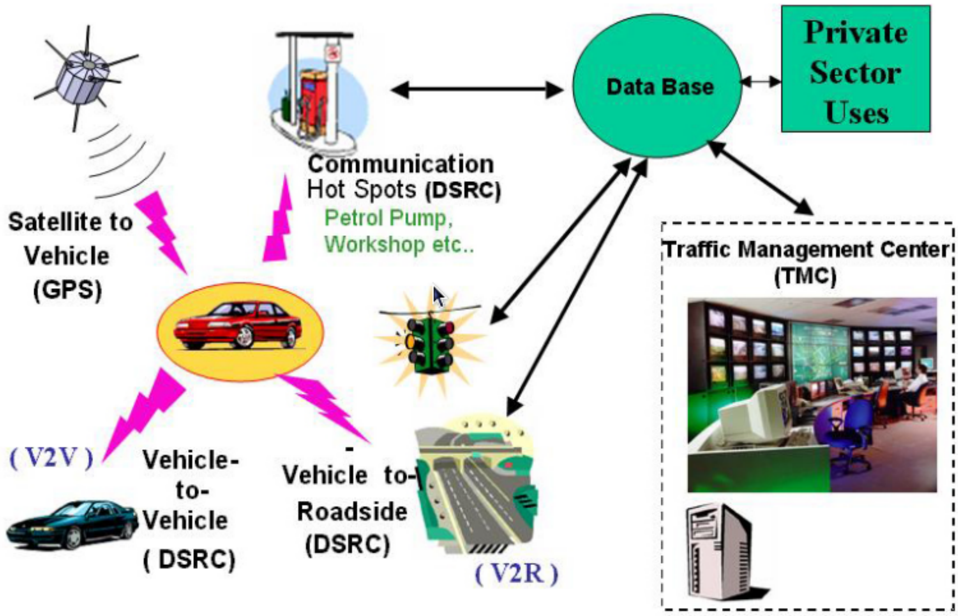

Figure 1.3: Overview of different vehicular communications

1.5 DSRC Specification

Bandwidth	75MHz (5.850 5.925GHz)
Modulation	QPSK OFDM
Channels	7 channels
Data Rate	1-54Mbps
Max Range	1000m
Min. Separation	10m

Table II: DSRC Specification

Chapter 2

IEEE 802.11p for vehicular adhoc network

2.1 Overview

IEEE 802.11p is based on:

- IEEE 802.11a PHY: OFDM Modulation
- IEEE 802.11 MAC: CSMA/CA
- IEEE 802.11e MAC enhancement: Message prioritization[6]

IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications.

2.1.1 DSRC

- **5.850-5.925 GHz range:**Divided into 7 channels (each 10 MHz)
- **Short range radio:**300m (1000m max)
- **High data rate:**6-27 Mbps

- **Half-duplex:**Station can only send or transmit, but not both at the same time.

2.1.2 How DSRC Works

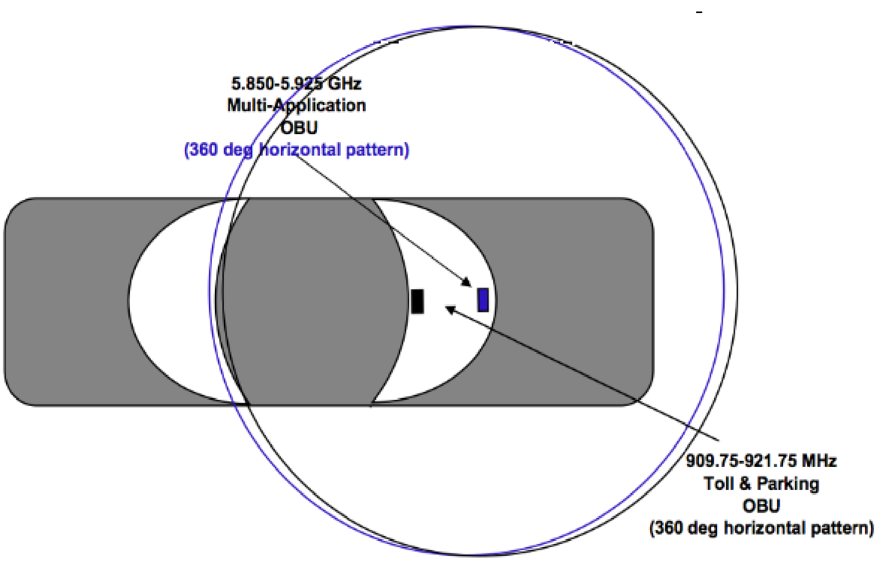

Figure 2.1: ITS Vehicle

- **RSU:**Announces to OBUs 10 times per second the applications it supports, on which channels
- **OBU**
  a. listens on channel 172
  b. authenticates RSU digital signature
  c. executes safety apps first
  d. then, switches channels
  e. executes non-safety apps
  f. returns to channel 172 and listens.

2.2 Differences between different version of IEEE 802.11

Parameter	IEEE 802.11a	IEEE 802.11b	IEEE 802.11p
Modulation Technique	OFDM	DSSS	OFDM
Bandwidth	6-54Mbps	5.5-11Mbps	3-27Mbps
Frequency Operates	5.8-5.9Ghz	2.4Ghz	5.8-5.9Ghz
Range	Up to 5000m	Up to 100m	Up to 1km

Table I: Differences between IEEE 802.11a,IEEE 802.11b & IEEE 802.11p

2.3 IEEE 802.11p Protocol Stack

2.3.1 IEEE 802.11p Physical Layer

The 802.11-2007 standard defined three different PHY Layer modes. The 20 MHz, 10 MHz and 5 MHz modes. The different modes can be achieved by using a reduced clock / sampling rates. 802.11a usually uses the full clocked mode with 20 MHz bandwidth. 802.11p usually uses the half clocked mode with 10 MHz bandwidth. The 802.11j standard also uses the half clocked mode. Please note: All modes with 5, 10 and 20MHz are defined in the 802.11 standards. By using a 802.11a signal with reduced sampling rate / clock rate, a 802.11j/p signal can also be achieved in the PHY.[7]

The half clocked mode affects the following parameters:

- Bandwidth

  In 802.11p, the 10 MHz bandwidth is usually used, in order to make the signal more robust against fading. The 20 MHz bandwidth is optionally implemented.

- Carrier spacing

  The 802.11p signal uses a carrier spacing reduced by 1/2 compared to 802.11a.

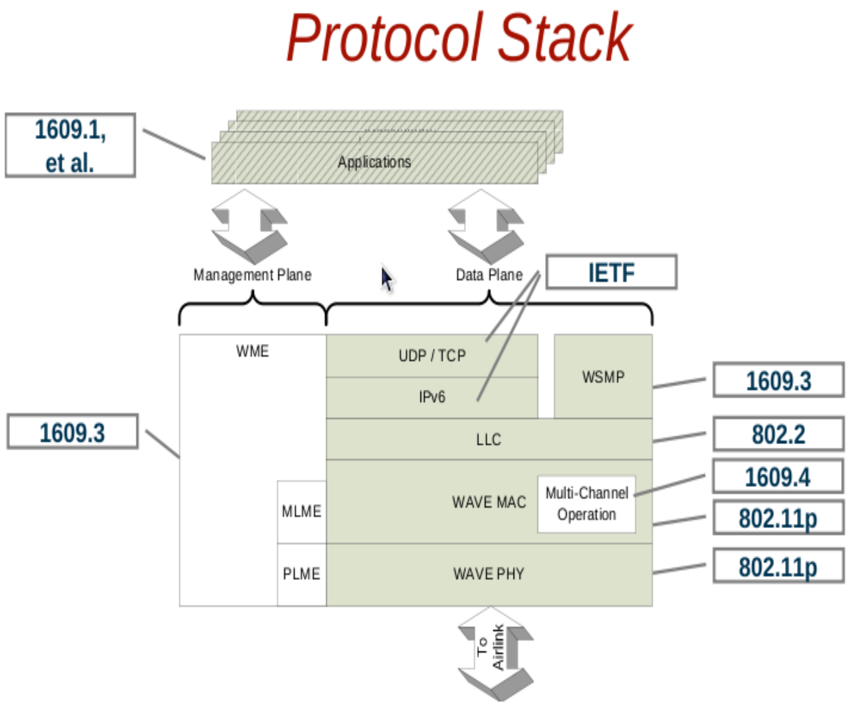

Figure 2.2: Protocol Stack of 802.11p

- Symbol length

  The symbol length is doubled, making the signal more robust against fading.

- Frequency

  The 802.11p standard usually operates in the 5.8 GHz and 5.9 GHz frequency bands.

2.3.2 IEEE 802.11p MAC Layer

The media access control (MAC) layer of the 802.11p amendment is also part of the 802.11-2007 standard. The 802.11 MAC is designed to be PHY independent. Both MAC and PHY layers conceptually include management entities, called MAC sublayer management and PHY layer management entities (MLME and PLME)

2.3.3 IEEE P1609.1

Is about the WAVE Resource Manager. It describes the key components of the WAVE system architecture and defines data flows and resources as well as the command message formats and data storage formats. It also specifies the types of devices that may be supported by OBUs.

2.3.4 IEEE P1609.2

Deals with the Security Services for Applications and Management Messages. It defines the secure message formats and processing and the circumstances for using secure message exchanges.

2.3.5 IEEE P1609.3

Is about the Networking Services. It defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. It also describes the WAVE Short Messages (WSM), providing an efficient WAVE-specific alternative to IP that can be directly supported by applications. It also deals with the Management Information Base (MIB) for WAVE.

Networking Services

- IP(IPv6) based Communication
    a. Mobile IPv6 & Network mobility enhancements
    b. UDP or TCP on transport layer
    c. Transmission on SCH only
- Non IP based Communication

a. Based on WAVE Short message protocol(WSMP)

b. Transmission on CCH or SCH

2.3.6 IEEE P1609.4

Describes the enhancements to 802.11 MAC to support WAVE.[8]

Channel Coordination

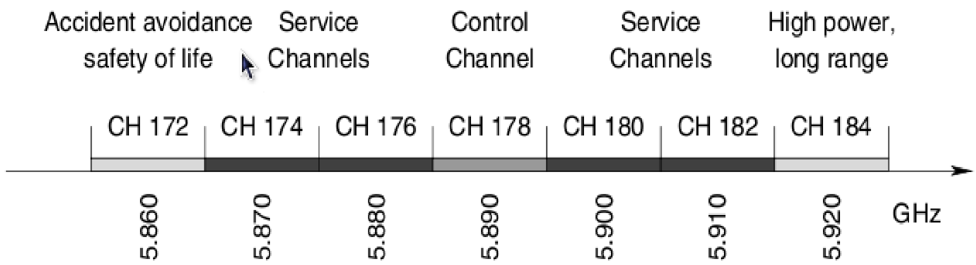

Figure 2.3: Channel Allocation in 802.11p
[9]

- Each Universal time coordinated(UTC) second is split into 10 sync intervals
- Every Sync is composed of alternating:

  a. CCH intervals:Every node monitors the CCH

  b. SCH intervals: Nodes can monitor one of the SCH

- All WAVE devices have to moniter the CCH during the CCH interval.
- During the SCH interval nodes may switch to a SCH
- At the start of each UTC second the first Sync interval begins
- Synchronization is performed via GPS

2.4 Operating modes & Channel Coordination of 802.11p

- Without WAVE Basic Service Set(WBSS)

  a. Safety-critical,low latency messages and control messages

  b. Mainly broadcast

  c. Only on CCH

- With WAVE Basic Service Set(WBSS)

  a. Two-way transactions(e.g. tolling,internet access)

  b. Required to use a SCH

  c. Required initiation on CCH

  d. In contrast to the Independent Basic Service Set(IBSS), WBSS does not require authentication and association procedures.

2.5 IEEE 802.11p Applications

- Emergency warning system for vehicles
- Cooperative Adaptive Cruise Control
- Cooperative Forward Collision Warning
- Intersection collision avoidance
- Approaching emergency vehicle warning
- Vehicle safety inspection
- Transit or emergency vehicle signal priority

- Electronic parking payments
- Commercial vehicle clearance and safety inspections
- In-vehicle signing
- Rollover warning
- Probe data collection
- Highway-rail intersection warning.

Chapter 3

Problem Statemet

3.1 Problem Statement

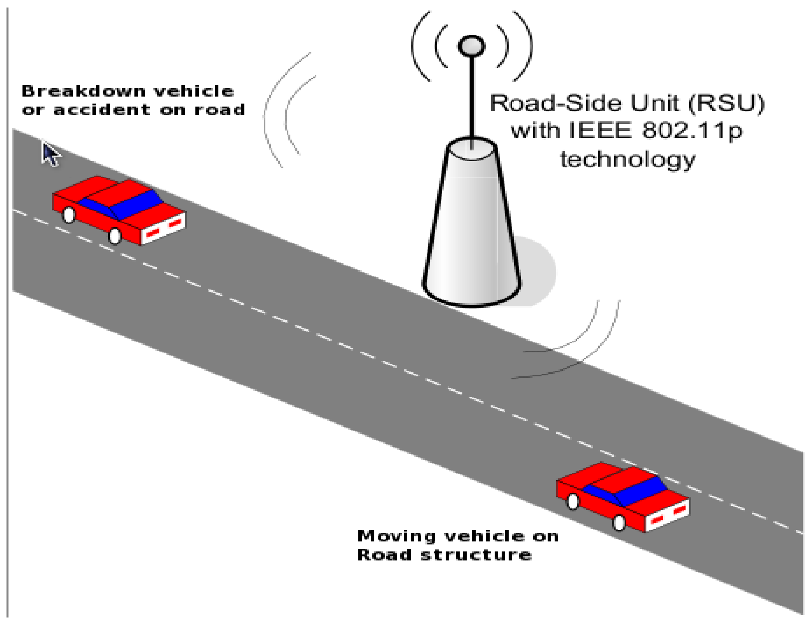

Figure 3.1: Problems of my Scenario

If vehicle is break down due to some accident as shown in figure 3.1,message from break down vehicle to the moving vehicle will be send within time to avoid unwanted circumstances using IEEE 802.11p protocol.

Following is the equation to measure the time that moving vehicle reach failure vehicle.

$$d = v_o t + \frac{1}{2} a t^2 \tag{3.1}$$

Where, d = distance

v_o= Moving Vehicle Speed

t = Time to reach destination

a = Deacceleration Speed

Vechile Speed	200 km/hr
Speed in m/s	55.55 m/s
Deacceleration Speed	60 m/s
Distance	20 meter
Time to reach break down vehicle	98 ms

Table I: Vehicle Information

If vehicle is moving on 200 km/hr, deacceleration speed is 60 m/s and distance is 20 meter then moving vehicle takes 98 ms time to reached break down vehicle.In this project we are assumed that application layer of IEEE 802.11p is under development and NS2 does not support multi channel allocation. So we will working on MAC enhancement layer of IEEE 802.11p using NCTUns and followings are the activities that was planned for my project.

- Detect break down vehicle node using V2V communication.
- Provide safety information within time(98 ms) from break down vehicle to moving vehicle.
- Improve throughput depends of different low to high priority traffic of vehicle node.

Chapter 4

Detect Stationary Vehicle Node on highway

In this chapter we are detecting stationary vehicle node in V2I Communication using NCTUns simulator.In Simulator there are four modes to generate scenario.

- Draw Topology: Mode can a user draw a new network topology or change address an existing simulation cases topology.

- Edit property: Simulation cases network topology can no longer be changed. Instead, only devices properties (attributes) can be changed at this time. For Users convenience, the GUI program will automatically generate many settings (e.g., a layer-3 interfaces IP MAC addresses). Since the correctness of these settings depends on the current network topology.

- Run Simulation: we can run your simulation in this mode.

- Playback after Simulation: we can show the performance of the simulation after the simulation is completed.The animation player will then start playing the recorded packet animation.[10]

4.1 Draw Topology

4.1.1 Road Property : Define Roads

Followings are the property to describe the road structure using NCTUns simulator.

Number of lanes on a road in both direction	2
Lane Width	20 meter

Table I: Define Road Property

4.1.2 ITS OBU and RSU with an 802.11(p)

Description of RSU and OBU

We are described the RSU and OBU in vehicle node in NCTUns simulator.

a. **ITS OBU with an 802.11(p) interface(agent-controlled):**An agent-controlled OBU is controlled by an agent program, which is essentially a normal real-life application program. Writing such an agent program is very easy and is the same as one writes a normal application program on the Linux system. However, the disadvantage with the agent-controlled approach is that each agent program will be run up as an independent process on the Linux system. If thousands of agent programs need to be run up during a simulation, their aggregate resource demands (e.g., CPU cycles, main memory, etc.) may exceed those provided by the system and the simulation speed will be low.

b. **ITS OBU with an 802.11(p) interface(module-controlled):**In contrast, a module-controlled OBU is controlled by its own node module in the simulation engine. A module is a C++ class with several member functions. It is compiled and linked with the simulation engine code. To control such an OBU, one need not run up an independent process like one does for an agent-controlled

OBU. As a result, even though thousands of OBUs are simulated in a case, one need not run up any process for them. For this reason, a simulation using module-controlled OBUs greatly outperforms that using agent-controlled OBUs on simulation speed and memory consumption. However, to develop a module-controlled OBU, one needs to know how to write/modify an NCTUns module. This is the disadvantage with this approach. Because these two types of OBUs suit different applications, for users convenience, NCTUns provides both of them for users to best suit their respective needs.

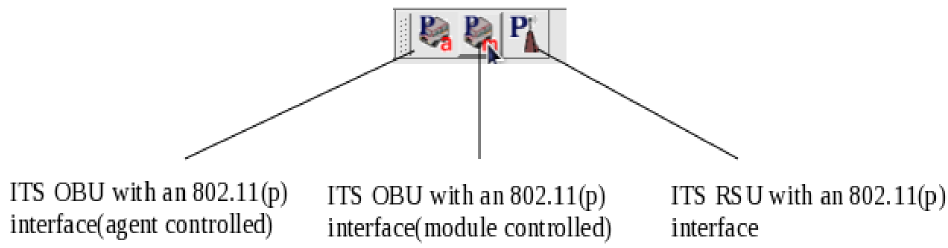

Figure 4.1: ITS OBU and RSU with an 802.11(p)

4.1.3 Description of subnet

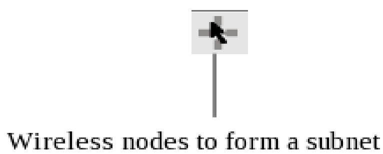

Figure 4.2: Wireless nodes to form a subnet

We are described 4 sub networks.and each network has it's own subnetID.Following are the table for subnet.

Node 10 and RSU 11	1^{st} Subnet
RSU 12	2^{nd} Subnet
RSU 13	3^{rd} Subnet
RSU 14	4^{th} Subnet

Table II: Define Wireless nodes to form a Subnet

4.1.4 Physical layer & channel model parameters

With figure 4.3 we can set parameter for physical layer and channel model. we can set the paramenter like transmit power,receiver gain,C.S.P.T and antenna gain. Following

Figure 4.3: Specify physical layer & channel model parameters of wireless node

are the parameters that we can set physical layer & channel model parameters of the IEEE 802.11p.

Propagation Channel model	Two ray ground model
Node Connectivity Display	Use the receiving node perspective
Node Connectivity Determination	Determined by power threshold
RxAntennaHeight(m)	1.5
C.S.P.T(dbm)	-82

Table III: Physical layer and channel model parameters of wireless node

C.R.P.T

When Physical Carrier Sense is used, a node seeking to transmit first assesses the channel. if the energy detected on the channel is above a certain threshold (caller carrier sense threshold), the channel is deemed busy, and the node must wait. Otherwise, the channel is assumed idle, and the node is free to transmit.

Antenna Gain

The hypothetical isotropic antenna is a point source that radiates equally in all directions.

Two-ray ground reflection model

A single line-of-sight path between two mobile nodes is seldom the only means of propation. The two-ray ground reflection model considers both the direct path and a ground reflection path. This model gives more accurate prediction at a long distance than the free space model. The received power at distance is predicted by [?]

$$P_r(d) = \frac{P_t G_t G_r {h_t}^2 {h_r}^2}{d^4 L} \tag{4.1}$$

where, $P_r(d)$: Received power at distance,
P_t: Transmit Power,
G_t: Transmitter Gain,
G_r: Receiver Gain,
h_t: Height of antenna at transmitter side
h_r: Height of antenna at receiver side
d:Distance
L:assumes $L = 1$. To be consistent with the free space model, L is added here.

4.2 Edit Scenario

In Edit mode, we can edit property of RSU,vehicle node.

4.2.1 Edit RSU

PSID(Provider service identifier): Is different for different RSU.The Provider service Identifier (PSID) is a four-byte numeric string used by the IEEE 1609 set of standards to identify a particular application service provider that announces that it is providing a service to potential users of an application or service. IEEE Std 1609.1-2006, Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) Resource Manager IEEE Std 1609.

SCID: The Service Channel ID field specifies the ID of the service channel that this service uses. The allowed service channel IDs are 174, 175, 176, 180, 181, and 182.

Priority: Field specifies the priority level of this service.A higher value of this attribute means that the service has a higher priority for OBUs to receive. For example, when several services that an OBU x has subscribed to are broadcasting their messages on the control channel, the OBU x should listen to the messages broadcast by the service with the highest priority level.[10]

sr. no.	parameter	RSU 11	RSU 12	RSU 13	RSU 14
1	Time	1	1	1	1
2	Action	Add	Add	Add	Add
3	PSID	1	2	3	4
4	Priority	1	2	3	4
5	SCID	174	174	174	174

Table IV: Add provider service information table

4.2.2 Command for Vehicle Node

In application tab, we can add following command,

Traffic Generation at sender side Command	stg -i stg.conf 1.0.7.1 -p 2007
Traffic Generation at Receiver side Command	rtg -u -w log1 -p 2007
Moving Car Command	CarAgent
Breaking Car Command	CarAgent_Broken [11]

Table V: Passing Command in MN(Mobile Node) and PC

4.2.3 Edit car configuration

Followings are the configuration profile of car agent.

MaxSpeed	100
MaxAcceleration	40
MaxDeceleration	20

Table VI: Car Configuration Profile(Profile 3=100%)

4.2.4 Edit Mobile Node(MN)

Time to register service	Action	PSID(Provider Service identifier)
1	Add	1
1	Add	2
1	Add	3
1	Add	4

Table VII: Use service information table of MN(Mobile Node)

These data are same in all MNś of IEEE 802.11p user setting tab.Enable Mobile IP in Mobile IP tab of MN 10(any one MN that you want to show the communication).In Home Agent IP address, we can define the IP address of wireless RSU.so that's why we can see the one node is continuous communicating with other rsu & vehicle node.

4.2.5 Setting Simulation

In G_setting menu select Simulation and in that select real time tab with following parameter:

Moving path	Dynamic moving path generation during simulation
Playback transmission	node movement after simulation

Table VIII: Setting Simulation Parameter

4.3 Runtime Simulation

4.3.1 Description of scenario

Node ID	Node Identification	Node Description
Node 17	OBU(Failure Node)	breaking command(CarAgent_Broken) that we can passed in application tab of IEEE 802.11(p) OBU
Node 10,18,19,20,21	OBU(Moving Node)	Moving command(CarAgent) that we can passed in application tab of IEEE 802.11(p) OBU and all nodes are generate traffic at receiver side with rtg command.
Node 11,12,13,14	RSU	set provider service information table and set home agent and foreign gent in mobile ip tab. so there are 4 subnet.
Node 15	Router	Connect all four RSU with Router.
Node 16	PC	Generate traffic at sender side with stg command.

Table IX: Node Information of the scenario

IEEE 802.11p node and RSU has been taken in NCTUns simulator.Vehicle node(24) is failure and vehicle node(22) is moving node.when moving vehicle node is reached certain threshold then there is detection of stationary node on road. every vehicle node has 300m radius range in red color. For finding stationary vehicle we used collision parameter between the stationary vehicles and all the moving vehicles.
The steps are shown below.

- Moving vehicle changes into failure vehicle.

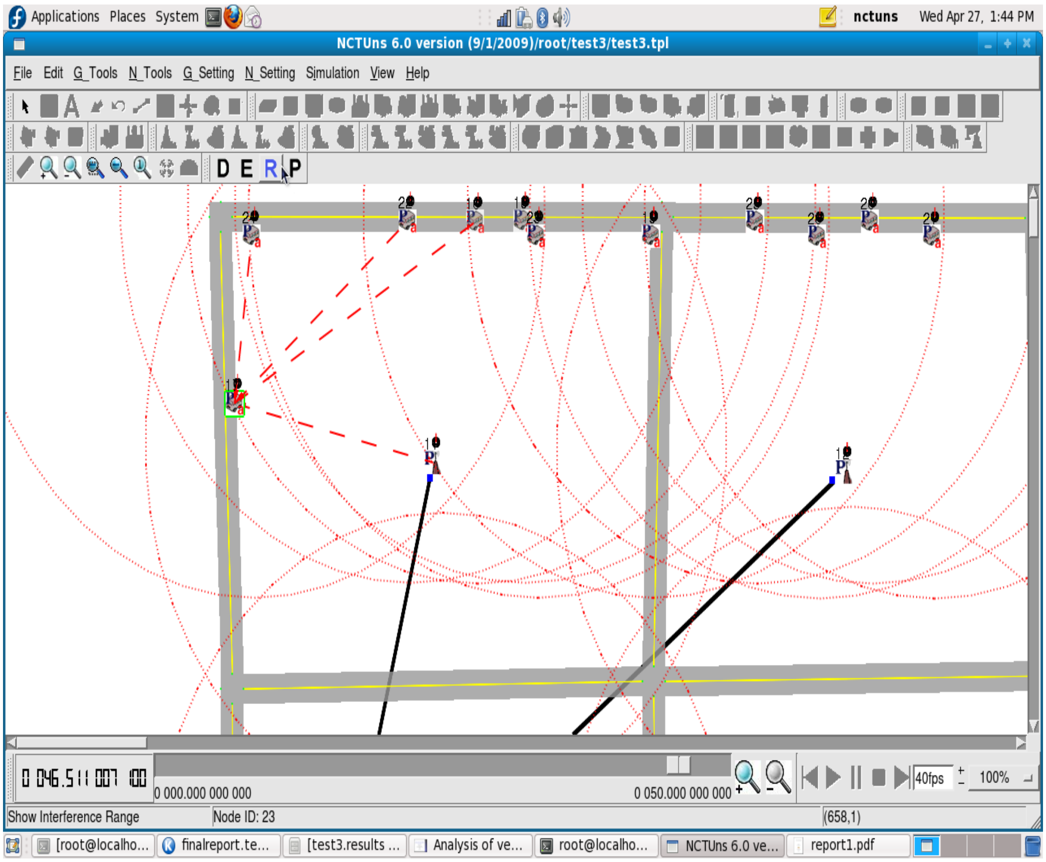

Figure 4.4: Scenario for detecting Failure node in NCTUns

- Failure vehicle executes the traffic of 1000 bytes at every 0.01 second.
- Moving vehicle in the range then collision packets will be more
- When it reached to certain threshold then moving vehicle on alert for failure vehicle.
- Moving vehicle is decreased it's speed and avoid accident.

4.3.2 Result for detecting failure node

Node 24 is failure vehicle node and when node 22 is moving vehicle. when vehicle node 22 has been reached up to certain threshold then detect that another vehicle node is failure on road. so at 4 to 8 seconds moving vehicle is passing nearer to failure vehicle that are shown in figure 4.5.

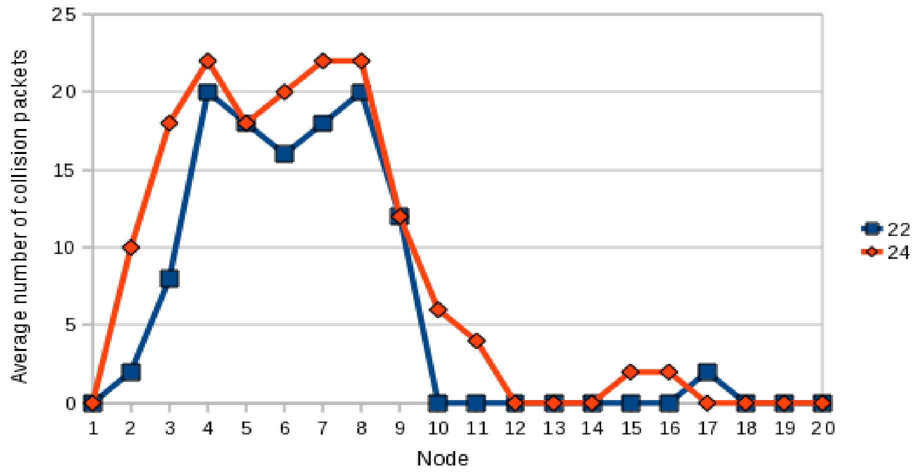

Figure 4.5: Result for detecting failure node

Chapter 5

Safety messages using RSU approach

5.1 MAC Layer of 802.11p

802.11p is half duplex communcation[16].802.11p has two types of mac layer.one is Basic MAC Layer and another is Extension MAC Layer.Followings are the details.

a. Basic MAC layer: 802.11 DCF based CSMA/CA + RTS/CTS + NAV

b. Extension MAC layer : EDCA provided by IEEE 802.11e [17]

5.1.1 MAC layer contention

In figure 5.1 there are packets contention and traffic prioritization.

IEEE 1609.4 is multi channel operation by the IEEE 802.11p MAC layer is a fashion similar to the IEEE 802.11e Enhanced Distributed Channel Access(EDCA) to regular wi-fi networks. For each channel four access categories, denoted by AC0-AC3, As for AC3 having highest priority and AC0 having lowest priority.
Send messages within time is very effective in 802.11p. here when MAC layer contention is more then Node have long time to wait for sending messages on receiver.Initial

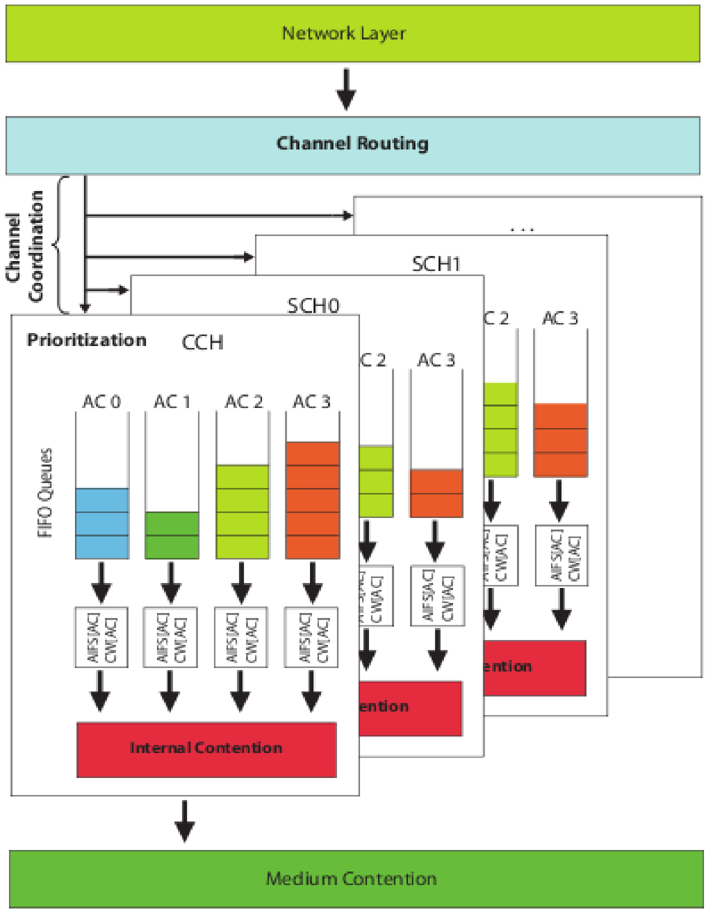

Figure 5.1: Relation between the multichannel operation and traffic prioritization with different access categories in the 802.11p

size of contention window (Cwmin) is 7.For sending message on channel first its contends if there are unsuccessful transmission then CW size is doubled. If medium is free then send data on channel.If medium is busy then CW size is increased until reaches the size Cwmax.

Belows are the MAC layer contention:

- Packets contends internally based on AC(which packets will be transmitted)
- Chosen packets will contend externally using channel access parameter.

5.1.2 Arbitary Inter-frame space durations used in EDCA settings for 802.11p

ACI	AC	CWmin	CWmax	AIFSN	AIFS	Backoff Time(CW)
1	Background	aCWmin=15	aCWmax=511	9	149	195
0	Best effort	(aCWmin + 1)/2 -1=7	aCWmin=15	6	110	91
2	Video	(aCWmin + 1)/4 -1=3	(aCWmin + 1)/2 -1=7	3	71	39
3	Voice	(aCWmin + 1)/4 -1=3	(aCWmin + 1)/2 -1=7	2	58	39

Table I: EDCA parameter set used on the CCH

ACI	AC	CWmin	CWmax	AIFSN	AIFS	Backoff Time(CW)
1	Background	aCWmin=15	aCWmax=511	7	123	195
0	Best effort	aCWmin=15	aCWmax=511	3	71	195
2	Video	(aCWmin + 1)/2 -1=7	aCWmin=15	2	58	91
3	Voice	(aCWmin + 1)/4 -1=3	(aCWmin + 1)/2 -1=7	2	58	39

Table II: EDCA parameter set used on the SCH

AC0 is low priority traffic. and AC3 is high priority traffic.High priority traffic has a higher chance of being sent than low priority traffic.A station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic.This is accomplished by using a shorter contention window (CW) and shorter arbitration inter-frame space (AIFS) for higher priority packets.stations with high transmission rate have smaller contention window to channel easily.[13].
Arbitration Inter Frame Spacing (AIFS), in wireless LAN communications, is a method of prioritizing one Access Class (AC) over the other, such as giving voice or video priority over email. AIFS functions by shortening or expanding the period a wireless node has to wait before it is allowed to transmit its next frame.

$$AIFS = AIFSN * slottime + SIFS \tag{5.1}$$

Where Slot time = 13 μs

SIFS = 32 μs

$$BackoffTime = CWmin * Slottime \tag{5.2}$$

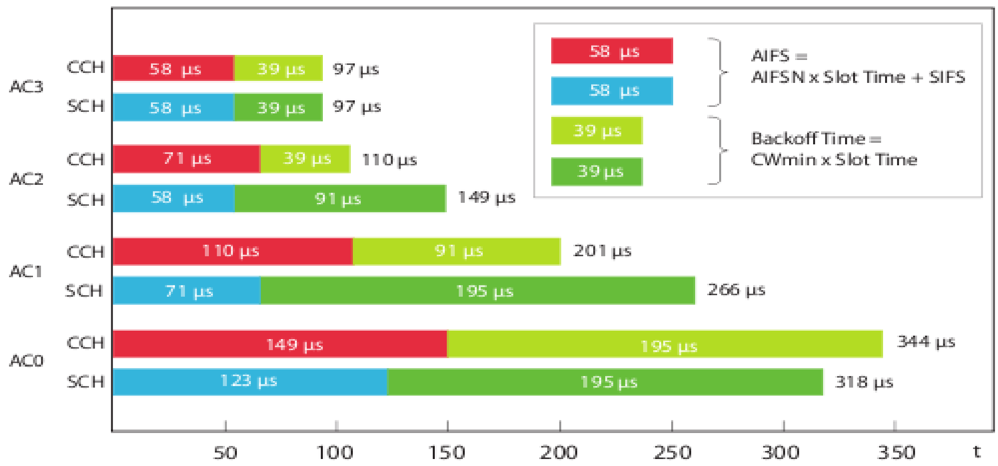

Figure 5.2: Inter-frame space durations used in the EDCA settings for the IEEE 802.11p

5.2 Accessing the Channel

IEEE 802.11p is not possible due to the lack of reassociation and reauthentication protocols that were excluded in support of fast establishment of physical links between RSUs and OBUs[12]. For sending the messages accessing the channel is very most effective part.Stations with high transmission rate have smaller contention window to access channel easily [13].Stations with higher transmission rate also have shorter inter frame spacing so that's why they can quickly access the channel[14].Three things will be included for accessing the channel.

a. LBT(Listen Before Talk)

b. Back off

(1) Random Back off is defined the slots based on CW(Contention window). And from that slots we can send messages on channel.

(2) Fixed Back off is defined the slots based on AIFS(Arbitary Inter frame spacing)

c. Allow priorities to access the channel

There are four priorities access categories. First it contents internally based on access categories. Below are the ACs based on lowest to highest categories respectively.

(1) Background

(2) Best Effort

(3) Voice

(4) Video [15]

5.2.1 Channel Access process for IEEE 802.11p

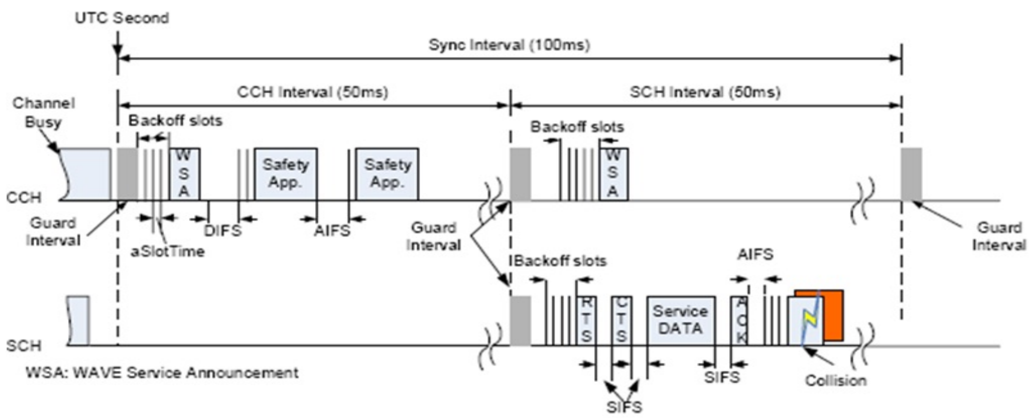

Figure 5.3: Channel Access process for IEEE 802.11p

In figure 5.3 there is 100 ms of synchronized interval. 1 super frame includes 10 synchronized interval that is seen in figure 4.1. 1 synchronized interval contains two interval. one is CCH interval and another is SCH interval. CCH is transmitted high priorities frames and SCH is trasmitted non-safety information.[18]

CCH interval contains BP(Beacon Period) and SP(Safety Period).

- Beacon Period(BP):
  Synchronized and distributed beaconing scheme chosen beacon slot by R-ALOHA protocol.Beacon is sending from vehicle to vehicle or vehicle to RSU or RSU to vehicle. So its send some of the information on channel.Belows are the information that are sending on channel.Transmitters one hop neighbor in last BP information for the collision free access to SCH. Beacon contains following information:

  a. Beacon slot used in IP

  b. Slot reserved in Slop

  c. AdjacentRebroadDist

  d. Vehicle position

  e. Vehicle direction

  f. MAC ID

  g. GPS Position

- SP(Safety Period)
  Reserved for safety application followed by EDCA rule. [19]

5.3 Solution

From figure 5.4 we find the solution to detect and inform moving vehicle within time.

- Send messages from failure vehicle to RSU

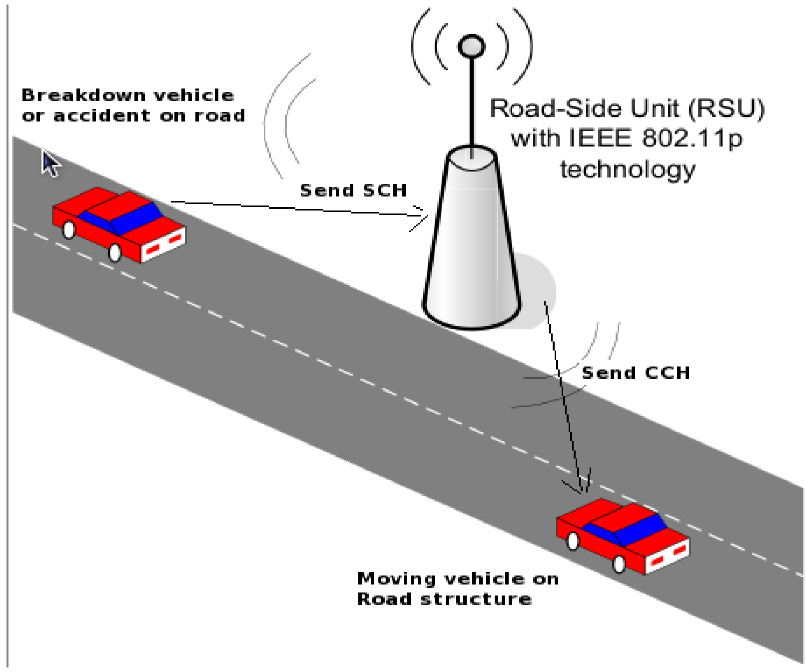

Figure 5.4: Solution of send messages to vehicle in time

- Reducing sending and receiving message time for RSU using two approach.
- Send messages from RSU to failure vehicle vehicle.

5.3.1 SCH interval for break down vehicle to RSU

To add polling operation to the IEEE 802.11p MAC protocols such that an OBU can inform its presence under a new RSU. And OBU is ready to send mesages to new RSU [23, 24].

CCH and SCH interval

In 802.11p synchronized interval is 100 ms. and its divided in to CCH interval and SCH interval. CCH interval is 50 ms and SCH interval is 50 ms. Now every time it's switching between CCH & SCH interval.In figure 5.5 we can see the synchronized interval of CCHI & SCHI.

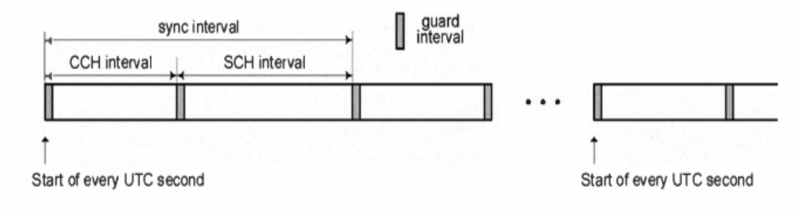

Figure 5.5: CCH and SCH Channel

WAVE devices use simple approach to synchronize. A typical WAVE device may visit the CCH for a period called CCH Interval (CCHI). Then the WAVE device may switch to a SCH for a period called SCH Interval (SCHI) and is shown by the hashed area at the second row of Figure 5.6.Both CCHI and SCHI actual resource utilization are delayed after switching by a period called Guard Interval (GI) in order to accommodate for device differences. From Figure 5.6, it is clearly essential to minimize the GI by adopting accurate and efficient synchronization mechanism. As soon as a group of WAVE devices are synchronized, they alternate the utilization of the CCH and SCH as illustrated in Figure 5.5.

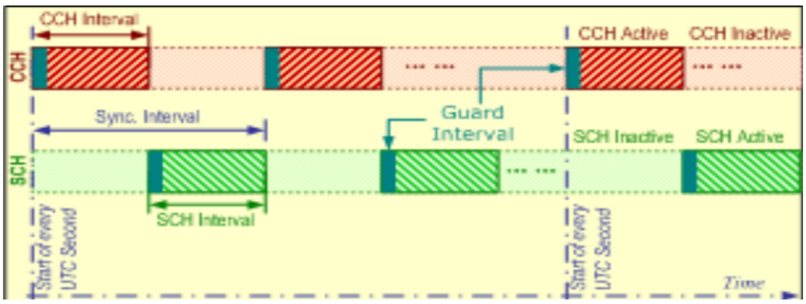

Figure 5.6: WAVE Channel Synchronization

Following is the equation that OBU transmits a frame in particular time slot:

$$T_i = \frac{2}{1 + w + p_i + \Sigma_{q=0}^{m-1}(2p_i)^q} \tag{5.3}$$

Where, Ti = probability that OBU transmits frame in a randomely chosen slot on SCHi.

pi = 1 = All OBU access the same channel SCH on which RSU provides service.

w = minimum contention window size = 7

pi = $\frac{NumberofOBUonSCHi}{TotalnumberofOBU}$

so result of T_i is 8.71μs

Following is the equation for probability that transmitted frames encounters a collision.

$$pi = 1 - (1 - Ti)^{Ni-1} \tag{5.4}$$

Where pi= probability that transmitted frames encounters collision.

Ni = number of nodes = 10

So result is $7.83 * 10^{-5}$ and probability for successfully packet transmission is 1-pi = 0.999. So for 10 nodes , successfully packets transmission is more.

Following is the equations for calculating time of SCH interval for sending messages between breakdown vehicle to RSU.

$$T_s(j) = [\frac{RTS}{R_b} + SIFS + \frac{CTS}{R_b} + SIFS + \frac{H_s + P_s}{R_j} + SIFS + \frac{ACK}{R_b} + DIFS] * T_{avg}.backoff \tag{5.5}$$

Where,

$$T_{avg}.backoff = \frac{(ECW_{min} + 1) * T_Slot}{2} \tag{5.6}$$

T_Slot = Time slot

ECW_{min} = EDCA based minimum Contention Window = 7

So $T_{avg}.backoff$ = Average Backoff time = 52μs

$T_s(j)$ = Time for successful transmission using data rate Rj.

RTS = 20 bytes

R_b = 3 Mbps

SIFS = 32μs

ACK = CTS = 14 bytes

H_s = Frame Header size = 72 bytes

P_s = Data payload size = 1612 bytes

DIFS = 58μs

Time for frame produces at breakdown vehicle and frame reaches at RSU = $T_{avg}.backoff + T_s(j) = 0.693\mu\text{s} + 52\mu\text{s} = 0.745\mu\text{s}$.

So, Here time for sending message from breakdown vehicle to RSU is 0.745μs.

5.3.2 Reducing sending and receiving message time for RSU using two approach.

Approach for reducing the switching time between CCH and SCH

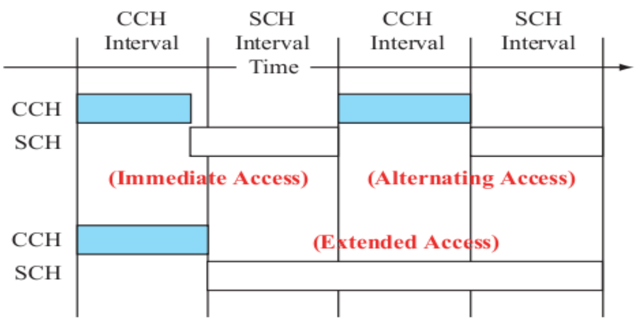

Figure 5.7: Channel Access Mechanism

Three types of accessing mechanism.

- In alternate Access, the antenna of a WAVE/DSRC device will stay on an indicated CCH/SCH during a CCH/SCH interval.
- Immediate access, the device can access SCH during CCH interval.
- Extended access allows a WAVE/DSRC device to enlarge the duration SCH access

Save our time using this approach. Because when messages is reached to RSU with the use of SCH interval. Then RSU will not wait for completed its interval. now RSU starts CCH interval for sending its messages and save its time.

Approach for reducing overhead of RSU

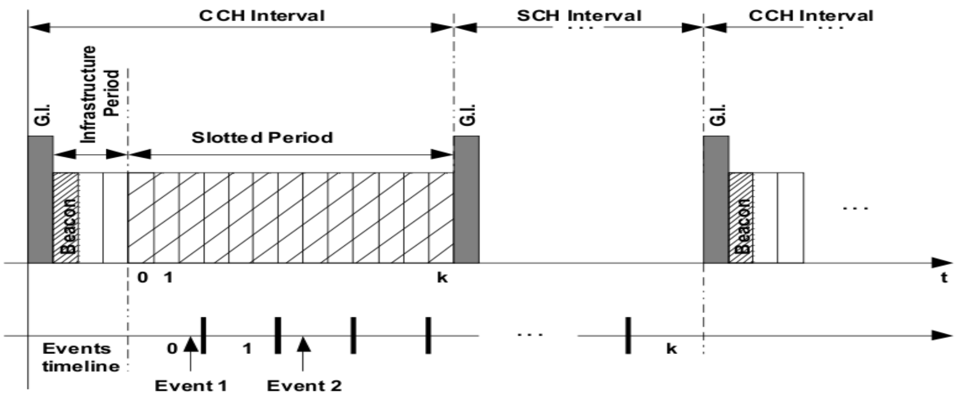

Figure 5.8: Slotted Based approach for reducing the overhead of RSU

RSU Range: Here i assume RSU range is 300m. When i increase the range then there are problems in my scenario:

- Throughput will be reduces or zero
- Packet loss rate will be increases
- Latency will be increases

Here RSU radius is 300m , so here we set diameter is 600m of RSU & OBU. For getting high performance. [20] RSU broadcasts WAVE service advertisement and urgent short messages on CCH.OBU accesses SCH to communicate with RSU after it synchronized with RSU and receives WSA from CCH. IEEE 802.11p standard does not specify any policy for an OBU to select SCH or any suggest ny method for

operators to restrict the service range of SCH.[21].
CCH interval is divided into IP(infrastructure period) and Slop(Slotted period).

IP

Here I assume there are 3 RSU that seen in figure 5.8 and each RSU has each IP. So for 3 RSU there are 3 slots. Each RSU is working on individual slot.Following are the details about slots.

- 3 Slots : For coordination between RSUs that listened to event
- 2 Slots : For message dissimination for several RSU.

Slop

Here it is the worst case for Slop.

Bit rate	3 Mbps
WAVE Warning message	500 bits
Frame Duration	166.6 μs
SIFS	32 μs
CCH interval	G.I: 4 ms
Result in number of Slots	231
IP	5 Slots
Slop	226 slots
For three RSU, Each RSU has	75 Slots

Table III: Worst case for Slop

If there are 3 RSU then Each RSU has 75 events in synchronized interval.So at same interval each RSU handles 75 events.
CCH interval is used for RSU Coordination and beacons transmitted by RSU.Each RSU uses one time slot.Beacons contains information about the Slop.Slotted period can be or can not be used for broadcast safety messages.

So with the use of this two approach sending and receiving message time will be very less.so we can't take it in the calculation.

5.3.3 CCH interval for RSU to moving vehicle

Following are the equation of measure time for sending CCH interval from RSU to moving vehicle.

$$Duration = DIFS(@AIFS) + T_{avg}.backoff + \frac{MPDUsize}{R} + SIFS \tag{5.7}$$

Where DIFS = 58μs
$T_{avg}.backoff$ = 52μs
MPDU Size = 1612 bytes [Maximum MPDU length(1612 bytes) per frame= MSDU payload(1574 bytes) + MAC header(30 bytes) + CRC(4 bytes)] [26]
R = 3 Mbps & SIFS = 32 μs
So time for sending message between RSU to moving vehicle is 693.33 μs.

5.3.4 Total time

Total Duration = Time for sending frame from break down vehicle to RSU + RSU frame calculation time + Time for sending frame from RSU to moving vehicle. So Total duration = 0.679 ms + 0.745ms = 1.424 ms. 1.424ms < 98ms(from 3.1). so message is send within time using our approach.

Chapter 6

Throughput depends on traffic and number of nodes

There are four priorities access categories. First it contents internally based on access categories. Below are the ACs based on lowest(AC0) to highest(AC3) categories respectively.

a. Background(AC0)

b. Best Effort(AC1)

c. Voice(AC2)

d. Video(AC3) [15]

In wireless communication networks, a major cause of packet drop and long latency is channel congestion. Channel congestion is an issue to be addressed by ITS standards, IEEE WAVE. The reason is that WAVE use EDCA as medium access method. EDCA is a contention based channel access method using the CSMA/CA mechanism for channel access. EDCA can experience unpredictable channel access delay and packet drop due to its nondeterministic characteristics. When a higher priority packet contends for channel access with a lower priority packet, EDCA does not guarantee that the higher priority packet gain channel access first. The higher priority packet only has a higher probability to win contention. A WAVE channel becomes congested with 50 or more devices. There is no control on the number of participating vehicles in vehicular communication networks. New mechanisms must be provided for safety message transmission in overload situation. Here signaling scheme for safety message transmission in vehicular communication networks and an adaptive CCHI method to reduce safety message latency in WAVE networks. Figure 6.1 shows the EDCA channel access mechanism. EDCA supports four access categories (AC): AC_BK for background, AC_BE for best effort, AC_VI for video and AC_VO for voice. Each message packet is mapped to one access category according to the priority level. A set of EDCA parameter is defined for each AC to contend for the channel access. An EDCA backoff time includes a fixed length waiting time and a random length waiting time. The fixed waiting time is a number of time slots given by arbitration interframe space (AIFS). The random waiting time is a random number of time slots within contention window (CW). Both AIFS and CW are different for each AC. AIFS is defined using two basic EDCA time parameters, short interframe space time (SIFSTime) and a slot time (SlotTime).[27]

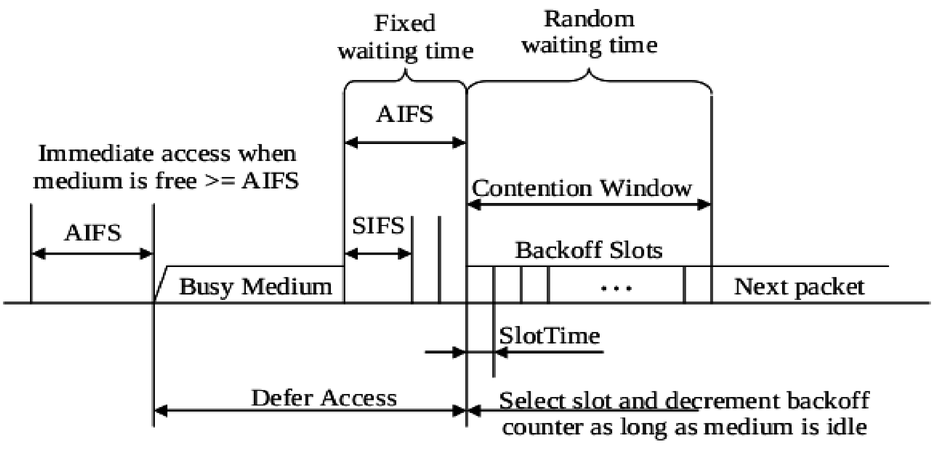

Figure 6.1: EDCA channel Access Illustration

$$AIFS = AIFSNSlotTime + SIFSTime \tag{6.1}$$

The Arbitration Interframe Space Number (AIFSN) is AC dependent and can have value in the range from 2 to 9. CW is an integer within a range of values CWmin and CWmax such that CWmin CW CWmax. Both CWmin and CWmax are AC dependent. A device can immediately transmit packet if the medium is free for more than one AIFS time period. However, following busy medium, all devices have to perform a random backoff procedure for packet transmission. This indicates that random backoff is needed on congested channels. Random backoff can cause unpredictable delay and packet drop even for high priority messages. To guarantee

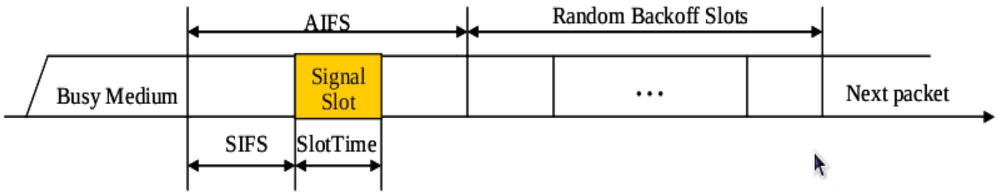

Figure 6.2: Waiting time between packets

safety message transmission on a congested channel, this paper provides an efficient congestion control technique: signaling for safety message transmission. Vehicle with safety message to transmit sends a signal to indicate its transmission intention. Upon detecting the attention signal, all other vehicles defer access. The signal must be short enough so that its transmission can be completed in one SlotTime period. The signal must be detectable. As shown in Figure 6.2, the slot after SIFS time period is selected as the signal slot to transmit an attention signal.

6.1 Different Contention window and AIFS for different traffic

Throughput is depend on the interval for CCH,message size,waiting time(AIFS+CW). Different waiting time for different contention window.

AC	CW1	AIFSN	AIFS	tw1	CW2	tw2	CW3	tw3	CW4	tw4	CW5	tw5	CW6	tw6
1	15	9	149	195	31	403	63	819	127	1651	255	3315	511	6643
0	7	6	110	91	15	195	31	403	63	819	127	1651	255	3315
2	3	3	71	39	7	91	15	195	31	403	63	819	127	1651
3	3	2	58	39	7	91	15	195	31	403	63	819	127	1651

Table I: EDCA parameter set used on the CCH

6.1.1 Average packet throughput depend on traffic

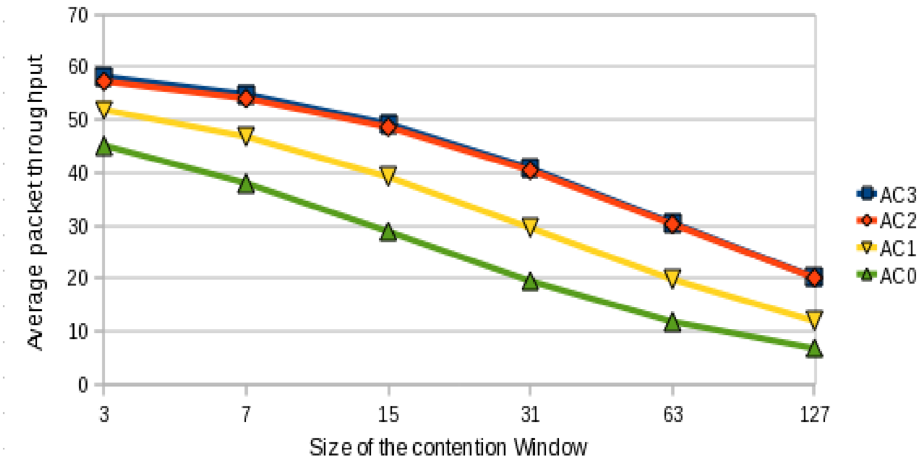

Figure 6.3: Average packet throughput depends on traffic

here message in the form of traffic that failure vehicle send to moving vehicle. so it is in the rate of 0.01 s.so below is the throughput for different traffic.

$$Np = \frac{t_i}{t_a + t_w + t_d} \tag{6.2}$$

where, Np is the throughput

t_i = total interval for CCH

t_a = waiting time of AIFS interval

t_w = waiting time of CW interval

t_d = message size(763μs)

6.1.2 Improve Average packet throughput depends on traffic

we reduced the size of traffic message.overall throughput will be increase.so message size is 500μs.Below is the improved throughput for different traffic.

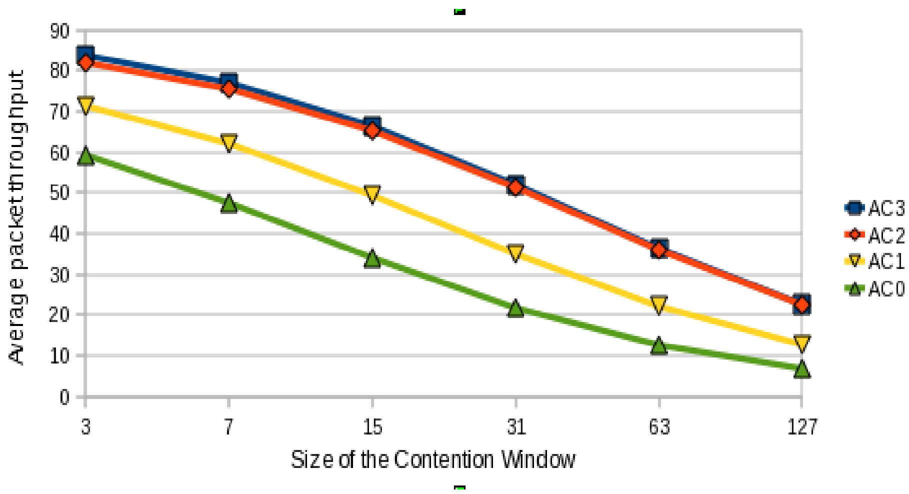

Figure 6.4: Improve Average packet throughput depends on traffic

6.1.3 Probability of channel access depends on number of nodes

When we can increase the nodes then probability of channel access is decreased.probability of channel access is depend on the nodes and contention window. small contention window has low channel access probability. and for high number of nodes probability of channel access is low.Below graph 6.5 for detailed information.

$$n_t(N) = n_c^N \tag{6.3}$$

Where ,n_c^N = different contention window for different nodes.

$$p_{coll}(N, n_c) = \frac{N}{n_t} * \sum_{i=1}^{n_c-1} (n_c - i)^{N-1} \tag{6.4}$$

Where, N = number of nodes

$p_{coll}(N, n_c)$ = Probability for collision free channel access

n_c = different contention window

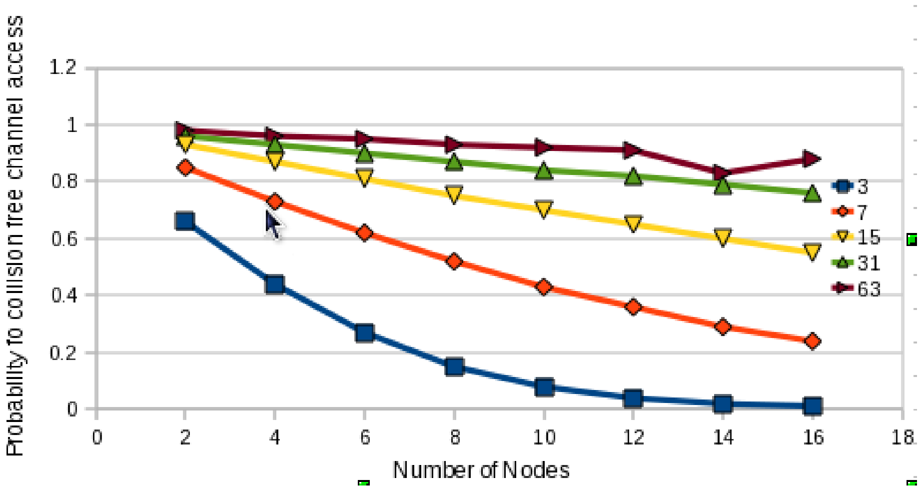

Figure 6.5: Channel Access depends on number of nodes

Chapter 7

Conclusion and Future Work

7.1 Conclusion

In this project, we worked on MAC Enhancement layer and it is assumed that application layer of IEEE 802.11p is under development. So we worked on MAC Enhancement layer of IEEE 802.11p and using collision packets we are detecting that vehicle node has become immobile. To send the messages to all vehicles in the proximity within minimum possible time we have applied two approaches.First approach is to reduce the time for RSU to receive and send the message to another vehicle node and the second approach is to reduce the switching time between SCH and CCH. IEEE 802.11p has four types of different lower to higher priority traffic in between active and failure node. As we have to send the message with in a certain time ,throughput has to be improved. which has been achieved by reducing the message size.

7.2 Future Work

From collision packets we detected break down vehicle.but it is not reliable commuiation. So we will investigate method, that will send safety messages(S.O.S) from failure vehicle to moving vehicle on application layer.

References

[1] C. D. Wang and J. P. Thompson. *Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utiliz- ing a real-time adaptive probabilistic neural network*, 1997. US.Patent No. 5,613,039

[2] X. Yang et al., *A Vehicle-to-Vehicle Communication Protocol for Co- operative Collision Warning*, Proc. 1st Annual Intl. Conf. Mobile and Ubiquitous Syst: Networking and Services, 2004.

[3] Q. Xu, R. Sengupta, and D. Jiang, *Design and Analysis of Highway Safety Communication Protocol in 5.9 GHz Dedicated Short-Range Communication Spectrum*, Proc. IEEE VTC, vol. 57, no. 4, 2003, pp. 245155.

[4] ASTM E2213-03, *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* ASTM Intl., July 2003.

[5] J.-H. Li, C.-H. Chang, and Y.-H. Chan,*MAC (Media Access Control) Design and Implementation of DSRC (Dedicated Short Range Communication) Systems*

[6] Prof.Dr.Thomas Strang,*V2X Communication Protocols*

[7] Rohde & Schwarz, *WLAN 802.11p Measurements for vehicle to vehicle(V2V) DSRC*

[8] Balkrishna Sharma Gukhool ,Department of Electrical and Computer Engineering,Universit de Sherbrooke Sherbrooke, Canada. *IEEE 802.11p modeling in NS-2*

[9] Stephan Eichler, *Performance Evaluation of the IEEE 802.11p WAVE Communication Standard*

[10] Prof. Shie-Yuan Wang, Chih-Liang Chou, and Chih-Che Lin,*The GUI User Manual for the NCTUns 6.0 etwork Simulator and Emulator*

[11] Prof. Shie-Yuan Wang,Chih-Liang Chou, Chih-Che Lin, and Chih-Hua Huang,*The Protocol Developer Manual for the NCTUns 6.0 Network Simulator and Emulator*

[12] Jungwook choi, hyukjoon lee, Supporing handover in an IEEE 802.11p based wireless access system

[13] Stephan Eichler, *Performance Evaluation of the IEEE 802.11p WAVE Communication standard*

[14] D. R. Chen and Y. J. Zhang.,*Distributed MAC Strategy for Exploiting Multiuser Diversity in Multi-rate IEEE 802.11 Wireless LANs, Proceeding of IEEE International Conference on Mobile Adhoc and Sensor System, Pisa, Ital, pp. 111, Oct. 2007.*

[15] Eichler, S., *Performance Evaluation of the IEEE 802.11p WAVE Communication Standard, IEEE 66th Vehicular Technology Conference, Sept. 30 Oct. 3 2007, pp. 2199-2203.*

[16] Balkrishna sharma gukhool,soumaya cherkaoui,*IEEE 802.11p modeling in NS-2*

[17] Nuno ferreria; Jose fonseca; J. Sales gomes , *On the adequacy of 802.11p MAC protocols to support safety services in ITS*

[18] Yunpeng Zang; Stibor, L.; Walke, B.; Reumerman, H.-J.;Barroso, A., *Towards Broadband Vehicular Ad-Hoc Networks The Vehicular Mesh Network (VMESH) MAC Protocol, IEEE Wireless Communications and Networking Conference, 11-15 March 2007, pp. 417-422.*

[19] Nuno ferreria; Jose fonseca; J. Sales gomes , *On the adequacy of 802.11p MAC protocols to support safety services in ITS*

[20] Kai-yun Ho,po-shun kang and Chung-Hsien Hsu, *Implementation of WAVE/DSRC devices for vehicular communications*

[21] Shiann-Tsong Sheu,Yen-Chieh Cheng,Jung-Shyr Wu, *A channel access scheme to compromise throught and fairness in IEEE 802.11p multi-rate/multi-channel wireless vehicular networks*

[22] H. Kim, S. Yun, I. Kang, and S. Bahk, *Resolving 802.11 Performance Anomalies through QoS Differentiation, IEEE Communication Letters, vol. 9, no. 7, pp. 655657, July 2005.*

[23] N. Choi, S. Choi, Y. Seok, T. Kwon and Y. Choi, *A solicitation based IEEE 802.11p MAC protocol for roadside to vehicular networks, 2007 mobile networking for vehicular environments,may 2007,pp. 91-96*

[24] A. Bohm and M. Jonsson, *Handover in IEEE 802.11p based delay-sensitive vehicle to infrastructure communciation, research report IDE-0924,school of information science,computer and electrical engineering(IDE), Halmstad university,2009.*

[25] D. R. Chen and Y. J. Zhang., *Distributed MAC Strategy for Exploiting Multi-user Diversity in Multi-rate IEEE 802.11 Wireless LANs, Pro ceeding of IEEE International Conference on Mobile Adhoc and Sensor System, Pisa, Ital, pp. 111, Oct. 2007.*

[26] P. Fuxjager, A. Costantini, D. Valerio, P. Castiglione, G. Zacheo, T. Zemen, F. Ricciato, *IEEE 802.11p transmission using GNU Radio, University of salento, 73100 lecce,Italy*

[27] Jianlin Guo, Jinyun Zhang *"Safety Message Transmission in Vehicular Communication Networks", Mitsubishi Electic Research laboratories*

[28] Mr. Bhavin Gurjar,*Detection of Failure Node and Safety to Vehicle using V2V Communication* ,at Birla Vishvakarma Mahavidyalaya (BVM),Vallabh Vidyanagar

[29] Mr. Bhavin Gurjar,*Reduce Overhead of RSU and Safety to vehicles in Infrastructure Communication*,at Birla Vishvakarma Mahavidyalaya (BVM),Vallabh Vidyanagar

Index