THE INFLUNENCE OF TRANSMISSION RANGE ON THE PERFORMANCE OF VEHICULAR AD-HOC NETWORK (VANET)

FAYAD MOHAMMED MOHAMMED GHAWBAR

A thesis submitted in partial
fulfillment of the requirement for the award of the
Degree of Master of Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

JULY 2015

ABSTRACT

Vehicular Ad-hoc Network (VANET) is a sub-class of Mobile Ad-hoc Network (MANET). The system has been developed to attain Dedicated Short Range Communication (DSRC) among vehicles (V2V) by consolidating existing technologies in which each vehicle is considered as a node. This type of communication is part of an Intelligent Transportation System (ITS) application. Importantly, there is still no comprehensive evaluation which portrays the mobility impact on the IEEE 802.11p MAC protocol performance, especially for the V2V communications between high mobility nodes. Moreover, the system performance also subjected to various factors including the transmission range, traffic load and number of flows that change rapidly in scenarios such as on highway. The main goal of this dissertation is to evaluate the impact of those factors in VANETs environment using AODV as routing protocol. In order to validate the simulation of VANET, traffic and network simulators (SUMO & NS-2) have been used. The performance is evaluated in terms of packet delivery ratio and end to end delay. The simulation results showed that better performance can be achieved in term of higher PDR and lower end to end delay when the transmission range is less than 500 meters. In contrary, when the transmission range is more than 500 meters, PDR started to decrease and end to end delay increased. The performance also degraded as the number of flows increased.

ABSTRAK

Rangkaian Ad-hoc Kenderaan (VANET) adalah sub-kelas Rangkaian Ad-hoc Bergerak (MANET). Sistem ini telah dibangunkan untuk mencapai Komunikasi Jarak Dekat Khusus (DSRC) antara kenderaan (V2V) dengan menyatukan teknologi sedia ada dengan setiap kenderaan dianggap sebagai satu nod. Komunikasi jenis ini merupakan sebahagian dari aplikasi Sistem Pengangkutan Pintar (ITS). Hal ini penting memandangkan penilaian menyeluruh terhadap impak kebolehgerakan ke atas prestasi protokol MAC IEEE 802.11p belum dijalankan, terutamanya bagi komunikasi V2V antara nod-nod dengan kebolehgerakan tinggi. Tambahan pula, prestasi sistem juga bergantung kepada pelbagai faktor merangkumi julat penghantaran, beban trafik dan bilangan aliran yang berubah dengan cepat dalam senario seperti di lebuhraya. Matlamat utama disertasi ini adalah untuk menilai kesan faktor-faktor tersebut dalam persekitaran VANET menggunakan AODV sebagai protokol peroutan. Untuk mengesahkan penyahlakuan VANET, penyelaku trafik (SUMO) dan penyelaku rangkaian (NS-2) telah digunakan. Prestasi dinilai dari segi nisbah penghantaran paket dan lengah hujung ke hujung. Hasil penyelakuan menunjukkan bahawa prestasi yang lebih baik dicapai dengan nilai PDR yang tinggi dan lengah hujung ke hujung yang rendah apabila julat penghantaran kurang dari 500 meter. Sebaliknya, apabila julat penghantaran melebihi 500 meter, PDR mula berkurang dan lengah hujung ke hujung meningkat. Prestasi juga merosot apabila bilangan aliran bertambah.

CONTENTS

	TITLE		**i**
	DECLARATION		**ii**
	DEDICATION		**iii**
	ACKNOWLEDGEMENT		**iv**
	ABSTRACT		**v**
	ABSTRAK		**vi**
	CONTENTS		**vii**
	LIST OF TABLES		**x**
	LIST OF FIGURES		**xi**
	LIST OF SYMBOLS AND ABBREVIATIONS		**xiii**
	LIST OF APPENDICES		**vi**
CHAPTER 1	**INTRODUCTION**		**1**
	1.1	Introduction	1
	1.2	Problem statement	2
	1.3	Objectives	3
	1.4	Scope of project	3
	1.5	Project organization	3

CHAPTER 2	**LITERATURE REVIEW**		**4**
	2.1	Introduction	4
	2.2	Ad-Hoc Network	4
	2.3	Mobile Ad Hoc Network (MANET)	7
		2.3.1 Types of MANET	8
		2.3.2 Characteristics of MANET	8
		2.3.3 MANET Routing Protocols	9
	2.4	User Datagram Protocol (UDP)	12
		2.4.1 Using of UDP	13
		2.4.2 TCP vs. UDP	14
	2.5	MAC Protocol For IEEE 802.11 Standards	14
	2.6	Vehicular Ad-Hoc Network (VANET)	15
		2.6.1 Overview of VANET	15
		2.6.2 MAC Protocols for Vehicular Networks	18
		2.6.3 DSRC and WAVE	19
		2.6.4 Related Work Review	24
		2.6.5 Other Technologies for VANET	27
	2.7	Summary	29
CHAPTER 3	**METHODOLOGY**		**30**
	3.1	Introduction	30
	3.2	Overall Methodology	30
	3.3	Tools and Methods for Simulation	33
		3.3.1 Simulation of Urban Mobility (SUMO)	34
		3.3.2 Network Simulator (NS-2)	37
		3.3.3 NS-2 for wireless network	41
		3.3.4 Analysis and graphic tools	43
		3.3.5 Trace file	43
	3.4	Traffic Model	44

	3.5	System Environment and Simulation Parameters	45
	3.6	The Performance Metrics	46
		3.6.1 Packet Delivery Ratio (PDR)	47
		3.6.2 End to end delay	47
		3.6.3 Packet Loss	48
	3.7	Summary	48
CHAPTER 4	**RESULTS AND ANALYSIS**		**49**
	4.1	Introduction	49
	4.2	Result Analysis	49
		4.2.1 Packet Delivery Ratio (PDR)	50
		4.2.2 End to End Delay	55
	4.3	Summary	60
CHAPTER 5	**CONCLUSION AND RECOMMENDATION**		**61**
	5.1	Conclusion	61
	5.2	Future Works	62
	REFERENCES		**63**
	APPENDIX		**67**

LIST OF TABLES

2.1	The Main Differences between Ad Hoc Networks	7
3.1	Explanation of Fields of Tracing File	40
3.2	The number of flows and Source destination	45
3.3	The system environment for simulation	45
3.4	Simulation Parameters	47

LIST OF FIGURES

2.1	MANET Protocols	10
2.2	Overview of Different MAC Protocols	15
2.3	Architecture of vehicular network "C2C-CC reference"	18
2.4	Protocol Architecture for DSRC and WAVE	20
2.5	DSRC spectrum allocation by FCC	21
2.6	DSRC allocations in different regions or entities	22
3.1	Flowchart of the methodology	32
3.2	VANET Simulation Scenario	33
3.3	Connections between Network and Traffic Simulators	34
3.4	Interface of MOVE tool	35
3.5	SUMO Multimodality	36
3.6	Different type of simulation classes	36
3.7	The Components of NS-2	38
3.8	Editing tool (Emacs)	38
3.9	The topology system of the simulation	39
3.10	Fields of tracing file	40
3.11	Network components of mobile node	41
4.1	Packet delivery ratio vs. transmission range (meter)	51
4.2	Packet delivery ratio to each flow at Tr = 300 m	52
4.3	Packet delivery ratio to each flow at Tr = 500 m	52
4.4	Packet delivery ratios vs. number of flows	53
4.5	Packet delivery ratios vs. data rate at Tr = 300 m	54
4.6	Packet delivery ratio vs. data rate at Tr = 500 m	55
4.7	Delay vs. transmission range (meter)	56
4.8	The delay in each flow at TR = 300 m	57
4.9	Delay in each flow at TR = 500 m	57
4.10	Average end to end delays vs. number of flows	58

4.11 Average end to end delay vs. data rate at Tr = 300 m 59

4.12 Average end to end delay vs. data rate at Tr = 500 m 59

LIST OF SYMBOLS AND ABBREVIATIONS

ABR	-	Associativity-Based Routing
AC	-	Access Category
AODV	-	Ad-Hoc On-Demand Distance Vector Routing
AODV	-	Ad hoc On-Demand Distance Vector Routing
ASTM	-	American Society for Testing and Materials
AU	-	Application Unit
BCH	-	Basic Channel
BSS	-	Basic Service Set
BSSID	-	Basic Service Set Identification
CA	-	Collision Avoidance
CBT	-	Channel Busy Time
CBR	-	Constant bit rate
C2C-CC	-	Car-to-Car Communication Consortium
CD	-	Collision Detection
CDMA	-	Code division multiple access
CGSR	-	Clusterhead Gateway Switch Routing
CSMA/CA	-	Carrier Sense Multiple Access with collision avoidance
CSMA/CD	-	Carrier Sense Multiple Access with Collision Detection
CTS	-	Clear to Send
D-MAC	-	Directional MAC
DSDV	-	Destination-Sequenced Distance-Vector Routing
DSR	-	Dynamic Source Routing
DSRC	-	Dedicated Short Range Communication
FCC	-	Federal Communication Commission
FDMA	-	Frequency division multiple access
FI	-	Frame Information
IBSS	-	Independent Basic Service Set

IEEE	-	Institute of Electrical and Electronics Engineers
ISP	-	Internet Service Provider
iMANET	-	Internet Based Mobile Ad hoc Networks
InVANETs	-	Intelligent vehicular ad hoc networks
IS	-	Intermediate System
ITS	-	Intelligent transportation System
MAC	-	Medium Access Control
MANET	-	Mobile Ad-hoc Network
MOVE	-	Mobility model generator for Vehicular networks
Nam	-	Animation tool
NICs	-	Network interface cards
NS-2	-	Network simulator version-2
OBU	-	On Board Unit
PDR	-	Packet delivery ratio
PHY	-	Physical layer
PLR	-	Packet Loss Rate
QoS	-	Quality of Service
RR-ALOHA	-	Reliable Reservation-ALOHA
RSU	-	Road Side Units
RTS	-	Request to Send
SNR	-	Signal to Noise Ratio
SSR	-	Signal Stability Routing
STAs	-	Stations
SUMO	-	Simulation of Urban Mobility
TDMA	-	Time division multiple access
TORA	-	Temporally-Ordered Routing Algorithm
UAVs	-	Unmanned Airborne Vehicles
UDP	-	User Datagram Protocol
VANET	-	Vehicular Ad-hoc Network
V2V	-	Vehicle to Vehicle
V2I	-	Vehicle to roadside Infrastructure
WAVE	-	Wireless Access for Vehicular Environment
WBSS	-	WAVE Basic Service Set
WiMAX	-	Worldwide Interoperability for Microwave Access

WLAN	-	Wireless Local Area Network
WMA	-	Windows Media audio files
WMN	-	Wireless mesh networks
WRP	-	Wireless Routing Protocol
WSN	-	Wireless sensor networks

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	NS-2 Coding	78

CHAPTER I

INTRODUCTION

1.1 Research background

Vehicle Ad-hoc Network (VANET) is a part of Mobile Ad-hoc Network (MANET) that has been developed to attain the transportation safety, reliability, security, reduce fatalities and productivity by using consolidation with existing technologies in which each vehicle is considered as a node. This type of communication is called an intelligent transportation System (ITS) application, which can either be between Vehicles (V2V) or Vehicles and the roadside Infrastructure (V2I). Each vehicle has On Board Unit (OBU) to provide communication with another OBU that merges to another vehicle or with Road Side Units (RSU) that is installed at a road side. These communications network have 75 MHz band with 5.9 GHz for distance of 100 - 1000 meters. The significant objectives of ITS are to disseminate messages to the neighbour vehicles to alert them, in case there is an accident, or about the bad weather or to communicate with RSU to know the status of a traffic light (Acosta-Marum 2009; Bilstrup et al. 2008).

In order to apply this, the IEEE group has come out with some standards to support this kind of application. The amendment of IEEE 802.11 standard has approved IEEE 802.11p protocol to support the vehicles communication network. IEEE 802.11p standard or Dedicated Short Range Communication (DSRC) determines the Physical (PHY) layer and Medium Access Control (MAC) layer that is lower layers standard. On the other hand, there is another standard merges within this protocol, that is, IEEE 1609, to work in the upper layer (Grafling et al. 2010; Jafari et al. 2012). IEEE 1609 protocol or Wireless Access for Vehicular Environment (WAVE) has sub-detail standards that include IEEE 1609.1, IEEE 1609.2, IEEE 1609.3, and IEEE 1609.4. Each standard has an independent operation. The model of this study is to implement the interaction of AODV for VANETs and the IEEE 802.11p mechanism, under different transmission ranges with different data rates and different numbers of flow. There will be wireless access environments that evaluate particular vehicles with certain mobility using in this scenario. The vehicles will broadcast emergency messages synchronously. At the end of simulation, the packet delivery ratio and end to end delay will be calculated.

1.2 Problem statement

With the increasing of population, the numbers of vehicles have increased. Therefore, VANET has gained a lot of attention in recent years in order to provide vehicular network to make safety environments among vehicles. However, there is still no comprehensive evaluation which portrays the IEEE 802.11p MAC protocol performance under different traffic loads and transmission range, especially for the V2V communications, so vehicular networks for this work are required to deal with highly mobile. Meanwhile, the research about the behavior of the vehicular network under highly mobile vehicles is critical so as to understand connectivity among vehicles in respect to the data disseminate and to motivate researchers to develop more applications as the network behavior when certain condition applied is expected. Therefore, the main problem of this project is to fully understand the behavioral of vehicular network performance when the vehicles are in high mobility with the transmission ranges, traffic loads and number of flows change from low to high constantly.

1.3 Objectives

The objectives of this Project are:

1) To evaluate the performance of Vehicular Ad-hoc Network (VANET).
2) To evaluate the impact of transmission range on the performance of VANET in terms of packet delivery ratio (PDR) and end-to-end delay.

1.4 Scope of Study

This study works within the evaluation of the performance of IEEE 802.11p protocol that is used in Vehicle Ad hoc Network. This work focuses on calculating and evaluating the mean of performance metrics i.e. packet delivery ratio and end-to-end delay. In addition, the work will be applied using SUMO and NS-2. More details of this study will be explained in the next chapters.

1.5 Project Organization

The rest of this dissertation is organized as follows: Chapter 2 presents introduction to Ad hoc network, MANET, AODV, USP, VANET and IEEE 802.11 standards protocols. An overview of related works will be presented in chapter 2. The research methodology and simulation tools will be explained in chapter 3. The simulation results and observations are presented in chapter 4. Finally, the project conclusion and the future works to be done are mentioned in Chapter 5.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Vehicular communication network is one of the most important topics that attract the researchers and the automotive industry. The communications between vehicles are called intelligent transportation system (ITS). Therefore, Vehicle Ad-hoc Network (VANET) is a form of mobile Ad-hoc network (MANET) that supports this kind of technology, which provides a wireless interface network within the vehicles to make the communication between neighbor vehicles easier. This chapter discusses the Ad-hoc network, Mobile Ad-hoc network (MANET), types of MANET, MANET routing protocols, Vehicular Ad-hoc network (VANET), VANET protocol and related work as well.

2.2 AD-HOC NETWORK

Literally the term "Ad-hoc" suggests communication links are built for specific and often extemporaneous provision customized to a set of applications (Mohapatra & Krishnamurthy 2005). Thus the typical Ad-hoc network is set up for a limited period of time. The network protocols are tuned to special application such as streamlining video pods, alerting guard units of security breaches at the perimeter mounted with sensory units, and so on. So, the network protocols must have the ability to self-configure or to adjust its self to different applications depending on the required task. Thus, self-configuration is defined as the ability of the Ad-hoc network to organize independently its configuration parameters including: addressing, routing, clustering, position identification, energy consumption, and so on. Also the protocols usually required to transmit data packets to mobile nodes (Mohapatra & Krishnamurthy 2005).

The second characteristic of Ad-hoc network is mobility and refers to the fact that the nodes communicating between themselves can be repositioned instantaneously. The mobility model may exhibit an individual random movement or organized group movement. The dynamics of the mobility rate is also included in the mobility model. Choice of an appropriate mobility model would considerably affect the performance of the routing protocol. The third characteristic of Ad-hoc network is its packets ability to traverse multiple hobs from a source to a destination, and therefore it’s called multihopping (Mohapatra & Krishnamurthy 2005; Olariu & Weigle 2010).

Most nodes (laptops, sensors) in Ad-hoc networks have limited energy sources and lack the facility to regenerate the consumed energy as in the case with solar panels. Therefore, energy conservation is considered one the salient features any protocol operating in the network would have to deal with. Scalability is one most the challenging requirements for Ad-hoc protocols. The protocol in operation (routing, addressing) would have deal in some environments such as large scale dense vehicular network with several thousands of nodes (Mohapatra & Krishnamurthy 2005). More of Ad-hoc network characteristics are security. Since Ad-hoc network is a descendant of wireless networks most of the encryption techniques work with traditional wireless networks emigrated to Ad-hoc networks. However the nodes in an Ad-hoc network are deemed more vulnerable particularly to passive attacks. A single sensor can be placed in a “street corner” and monitor the deployment of troops, the information could be relayed back to satellites orbiting the region or UAV’s units and from there to the enemy headquarters.

Unmanned autonomous vehicles or Unmanned Airborne Vehicles (UAVs) are valuable assets could be used to interconnect several nodes having physical obstacles between them. Also, UAVs might help to multicast or even broadcast messages across entire fields. Connection to the internet can be extended from infrastructure wireless networks to vehicles on the road through transportable routers. This would open many opportunities for commercial applications that require communicating with the clients to showcase their provisions.

In the last few years Ad-hoc network has evolved into many divisions. The evolved categories share the most salient feature of Ad-hoc network and that is multihop communication. Each category possesses a set of peculiarities that distinguish it from the rest and at the same time these particular properties prevent an ultimate solution to answer all routing problems related to Ad-hoc network. The emerged Ad-hoc networks include among others (Olariu & Weigle 2010), the following:

1. Mobile Ad-hoc networks (MANET). These are a wireless Ad-hoc network, its nodes are mobile and involved in random movement.
2. Wireless mesh networks (WMN). The nodes on mesh networks could be seen as static base stations connected to mobile client devices. Since the client devices are mobile they can switch to different nodes depending on their position. The static mesh nodes are usually supplied with several radio interfaces to increase the efficiency. The static status of the nodes lifts the constraints on energy consumption as the nodes are usually offered a continuous power supply. Also memory resources and computation power are not deemed concerns. The design aim for the routing protocols is to find the best possible route to the aggregated user traffic.
3. Wireless sensor networks (WSN). These are composed of hundreds or even thousands of tiny sensors, laid out in widespread fields mainly to monitor changing environments or to provide security surveillance over those fields. In line for their tiny sizes, computation power and energy efficiency are serious concerns. Therefore the design aim for the routing protocols is to find a simple algorithm to implement with the minimum amount of energy. The nodes (sensors or smart dust) would relay back the information to a “sink” device which is regarded as the backbone for the network to transmit the collected data to a processing center.

4. Vehicular Ad-hoc network (VANET). These consist of mobile nodes but unlike MANET arrangements here the nodes (vehicles) are restricted by the road structure and legal speed limits. Thus the mobility pattern is predictable. For this reason VANET is considered a particular case of MANET. Also it should be known that the nodes possess high speeds and this property makes the nodes move in groups that are highly dynamic.

Table 2.1 below highlights the main differences between the four networks mentioned above.

Table 2.1 : The Main Differences between Ad-hoc Networks. Olariu & Weigle 2010

Property	MANET	WMN	WSN	VANET
Network size	Medium	Moderate	Large	Large
Node's mobility	Random	Static	Mostly static	High, nonrandom
Energy limitations	High	Very low	Very high	Very low
Node's computation power	___	High	Very low	High
Node's memory capacity	___	High	Very low	High
Location dependency	Low	Very low	High	Very high

2.3 MOBILE AD-HOC NETWORK (MANET)

This network is arranged of a number of wireless nodes moving randomly and fully connected without any kind of predefined infrastructure such as routers, base stations and so on. The nodes utilize batteries carried on board as a power source. Thus energy efficiency and computation power are factors of paramount importance. Similarly routing protocols of complex designs should be avoided (Olariu & Weigle 2010; Bychkovsky et al. 2006; Hull et al. 2006; Jain et al. 2004).

2.3.1 Types of MANET

MANET can be categorized as follow:

1. Vehicular Ad-hoc Networks (VANETs) are arranged from mobile nodes with regular movement. Communication in these networks could take place between vehicles or between vehicles and roadside units (RSUs), (Leontiadis & Mascolo 2007).
2. Intelligent vehicular Ad-hoc networks (InVANETs) utilize artificial intelligence principles on vehicles to avoid collisions on the road. Also these networks could provide special driving modes such as drunken driving.
3. Internet Based Mobile Ad-hoc Networks (iMANET) are wireless networks that provide internet service to mobile nodes. The connection is established between a gathering of mobile nodes and fixed gateways or internet routers.

2.3.2 Characteristics of MANET

According to Olariu & Weigle (2010) the characteristics of MANET may include;

1. Independence of fixed communication infrastructure. This characteristic is mainly driven from the nature of the connections developed between the nodes. The hardware composes the sensory units include transceivers responsible for the communication taking place between the nodes.
2. Multihop communication. This is the ability given for the mobile nodes to transmit and receive data packets without any kind of fixed communication infrastructure. Each node has the capability of relaying or routing the data packets within its radio range.
3. Network size. These networks are usually of medium size. The maximum number of nodes is 200 nodes. The network space is sparse since the number of nodes is limited.
4. Node's mobility. This is one of the salient features of this network that the nodes are mobile. The mobility pattern is arbitrary or random. Therefore, a particular mobility pattern cannot be assumed nor the existence of additional information

about the position or trajectory of the nodes. The absence of the information is reflected on the designed routing protocols as they use simple algorithms to flood the network when trying to find out routes to the destination.

5. Energy limitations. Since the communicating devices are battery-operated, designing energy-efficient routing protocols has become a primary task.
6. Bandwidth limitations. The communication channels between the mobile nodes are highly affected by several degrading factors: multipath fading, noise, signal interference and multiple accesses.
7. Node's computation power. The mobile nodes run on batteries making complex computations difficult to implement. As a tradeoff protocol designers choose to inject overhead to the network by means continuous transmission of control messages.
8. Node's memory capacity. The hardware implementation for the communicating units is simple or rather primitive. Therefore inclusion of memory chips into the communication units would require extra energy from the mounted batteries.
9. Location dependency. MANET nodes seldom do they depend on any particular location to receive the data packets. The nodes reside in a common radio range and through excessive use of flooding each node would receive its packets regardless of its location.
10. Full connectivity. MANET arrangement assumes all nodes to be within the transmission range. If a packet was addressed to a node located outside this range it would simply be discarded.

2.3.3 MANET Routing Protocols

VANET is considered to be a special part of MANET with some of differences in various characteristics. So in VANET they use the MANET Routing protocols. In reality not all these Protocols are used because of many strains. But maybe the unused protocols of MANET will work properly on VANET, Figure 2.1 shows the MANET Protocols.

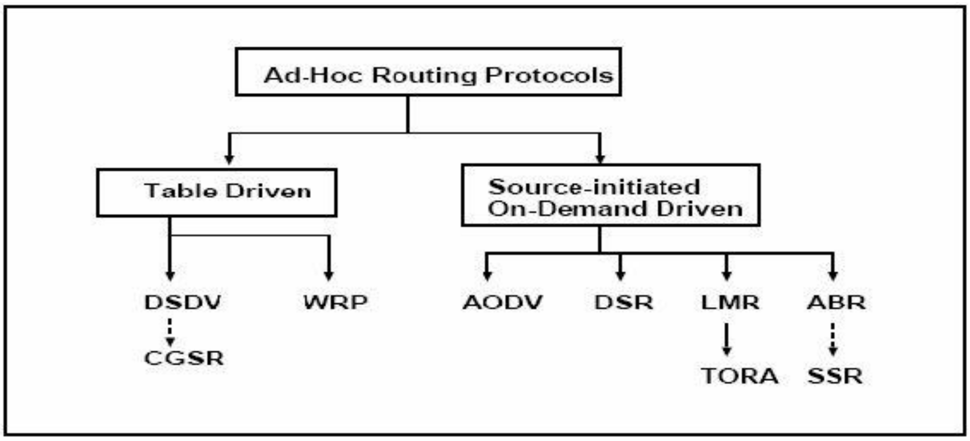

Figure 2.1: MANET Protocols

There are two types of routing protocols for MANET:

1. Table-Driven Routing Protocols (Proactive): that is updates its routes periodically and maintain the information on routing all the time.
   a. Destination-Sequenced Distance-Vector Routing (DSDV)
   b. Cluster head Gateway Switch Routing (CGSR)
   c. The Wireless Routing Protocol (WRP)

2. Source-Initiated On-Demand Routing Protocols (Reactive) : That is routes updated on demand and the determination is invoked on demand too
   a. Ad-Hoc On-Demand Distance Vector Routing (AODV)
   b. Dynamic Source Routing (DSR)
   c. Temporally-Ordered Routing Algorithm (TORA)
   d. Associativity-Based Routing (ABR)
   e. Signal Stability Routing (SSR)

2.3.3.1 Ad-hoc on Demand Distance Vector (AODV)

AODV establishes a required route only when it is needed as opposed to maintaining a complete list of routes. AODV uses an improved version of the distance vector algorithm to provide on-demand routing.

The algorithm's primary features are as follows:

1. It broadcasts packets only when required.

2. It distinguishes between local connectivity management and general maintenance.
3. It disseminates information about changes in local connectivity to neighboring
   mobile nodes that need this information.
4. Nodes that are not part of active paths neither maintain any routing information nor participate in any periodic routing table exchanges.
5. A node does not have to find and maintain a route to another node until the two nodes communicate. Routes are maintained on all nodes on an active path. For example, all transmitting nodes maintain the route to the destination.

2.3.3.2 AODV Route Table Management:

Routing table management in AODV is needed to avoid those entries of nodes that do not exist in the route from source to destination. Managing routing table information in AODV is handled with the destination sequence numbers. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. The need for routing table management is important to make communication loop free. The following are characteristics to maintain the route table for each node:

1. Destination address.
2. Total number of hops to the destination.
3. Next hop: It contains information of those nodes that are used to forward data packets by using the current route.
4. Destination sequence numbers.
5. Active neighbors: Those nodes that currently use the active route.
6. Expiration time: It contains information for the total time that route is being valid.

2.3.3.3 AODV Route Maintenance:

When a route is not valid in the communication link e.g. a vehicle leaves the network, the nodes delete all the related entries from the routing table for that invalid route. And sends the RREP to current active neighboring nodes that route is not valid anymore for communication. AODV maintains only the loop free routes, when the source node receives the link failure notification it either starts the process of rebroadcasting RREQ or the source node stop sending data through invalid route. Moreover, AODV uses the active neighbor's information to keep tracking of currently used route.

2.4 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a transport layer protocol defined for use with the IP network layer protocol. It is defined by RFC 768 written by John Postel. It provides a best-effort datagram service to an End System (IP host). The service provided by UDP is an unreliable service that provides no guarantees for delivery and no protection from duplication (e.g. if this arises due to software errors within an Intermediate System (IS)). The simplicity of UDP reduces the overhead from using the protocol and the services may be adequate in many cases. UDP provides a minimal, unreliable, best-effort, message-passing transport to applications and upper-layer protocols. Compared to other transport protocols, UDP and its UDP-Lite variant are unique in that they do not establish end-to-end connections between communicating end systems.

UDP communication consequently does not incur connection establishment and teardown overheads and there is minimal associated end system state. Because of these characteristics, UDP can offer a very efficient communication transport to some applications, but has no inherent congestion control or reliability. A second unique characteristic of UDP is that it provides no inherent On many platforms, applications can send UDP datagrams at the line rate of the link interface, which is often much greater than the available path capacity, and doing so would contribute to congestion along the path, applications therefore need to be designed responsibly .

One increasingly popular use of UDP is as a tunneling protocol, where a tunnel endpoint encapsulates the packets of another protocol inside UDP datagrams and transmits them to another tunnel endpoint, which encapsulates the UDP datagrams and forwards the original packets contained in the payload. Tunnels establish virtual links that appear to directly connect locations that are distant in the physical Internet topology, and can be used to create virtual (private) networks. Using UDP as a tunneling protocol is attractive when the payload protocol is not supported by middleboxes that may exist along the path, because many middleboxes support UDP transmissions. UDP does not provide any communications security. Applications that need to protect their communications against eavesdropping, tampering, or message forgery therefore need to separately provide security services using additional protocol mechanisms.

2.4.1 Using of UDP

Application designers are generally aware that UDP does not provide any reliability, e.g., it does not retransmit any lost packets. Often, this is a main reason to consider UDP as a transport. Applications that do require reliable message delivery therefore need to implement appropriate protocol mechanisms in their applications (e.g. tftp).UDP's best effort service does not protect against datagram duplication, i.e., an application may receive multiple copies of the same UDP datagram. Application designers therefore need to verify that their application gracefully handles datagram duplication and may need to implement mechanisms to detect duplicates. The Internet may also significantly delay some packets with respect to others, e.g., due to routing transients, intermittent connectivity, or mobility. This can cause reordering, where UDP datagrams arrive at the receiver in an order different from the transmission order. Applications that require ordered delivery must restore datagram ordering themselves. The burdon of needing to code all these protocol mechanisms can be avoided by using TCP.

2.4.2 TCP vs. UDP

There are two types of Internet Protocol (IP) traffic. They are TCP or Transmission Control Protocol and UDP or User Datagram Protocol. TCP is connection oriented – once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

TCP (Transmission Control Protocol) is the most commonly used protocol on the Internet. The reason for this is because TCP offers error correction. When the TCP protocol is used there is a "guaranteed delivery." This is due largely in part to a method called "flow control." Flow control determines when data needs to be re-sent, and stops the flow of data until previous packets are successfully transferred. This works because if a packet of data is sent, a collision may occur. When this happens, the client re-requests the packet from the server until the whole packet is complete and is identical to its original.

UDP (User Datagram Protocol) is anther commonly used protocol on the Internet. However, UDP is never used to send important data such as WebPages, database information; UDP is commonly used for streaming audio and video. Streaming media such as Windows Media audio files (.WMA), Real Player (.RM), and others use UDP because it offers speed! The reason UDP is faster than TCP is because there is no form of flow control or error correction. The data sent over the Internet is affected by collisions, and errors will be present. UDP is **only** concerned with speed. This is the main reason why streaming media is not high quality.

2.5 MAC Protocol for IEEE 802.11 Standards

The Media access control (MAC), as the me aptly suggests, refers to the Mechanism Of Accessing The Communication when there are a lot of stations (STAs) actively working in the same channel. By contrast, Quality of Service (QoS) indicates the control mechanism in data networks that attempts to ensure a certain level of performance to a data flow, which strictly follows the requests issued from the application program. These two terms are very much intertwined. In wireless networks, as their feature is very striking, unlike their wired counterpart, people have exerted great effort on a MAC mechanism towards attaining better performance. Generally, MAC protocols can be classed into two: deterministic and random, where their protocols may be either under centralised or decentralised control. Since 802.11p is appropriate for a highly dynamic and unpredictable environment, its MAC protocol can solely be taken from a random rather than a deterministic class. Figure 2.2 provides an overview of multiple MAC protocols.

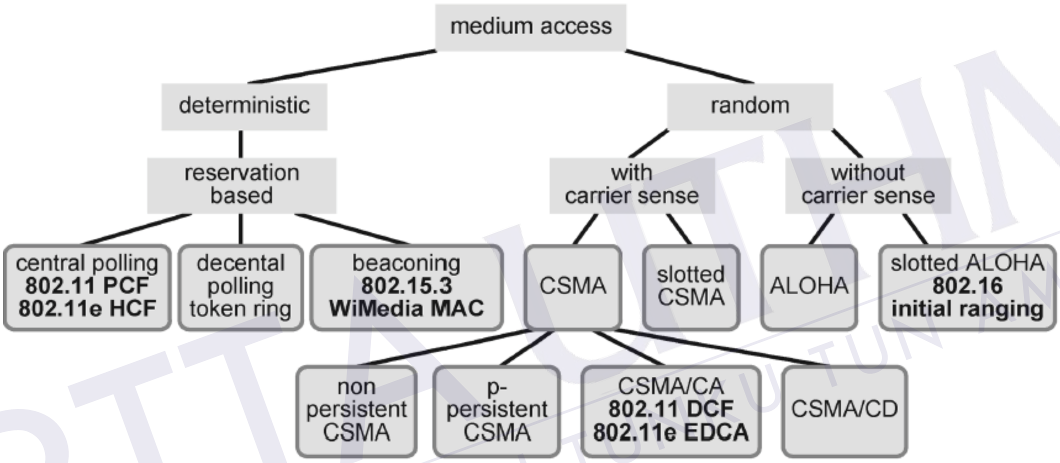

Figure 2.2: Overview of Different MAC Protocols.

Source: Walke et al. 2007

2.6 VEHICULAR AD-HOC NETWORK (VANET)

2.6.1 Overview and Architectures of VANET

VANET is an ad-hoc network that provides communication between mobile nodes that are mainly personal vehicles (Leontiadis 2007). However, on account of the wide availability of fixed communication systems present at the roadside and thus are referred to Roadside Units (RSUs), opportunities to connect a vehicular network to such systems are increasing. Communication could take place among vehicles and different RSUs through suitable network interface cards (NICs) such as IEEE 802.11p available as On-Board Units (OBUs) inside the vehicles (Olariu & Weigle 2010). These network cards could have sufficient computation power to stage many other communication technologies (e.g., 2G/3G or WiMax) that would allow the nodes to connect directly to an operator's network or Internet Service Provider (ISP). Also this available computing power is what made several international consortiums (e.g., CAR2CAR) and standardization bodies (e.g., ISO through CALM initiative) to formulate standards to specify the management of future services expected to be available on personal vehicles. Thus an accumulation of several technologies would result in private vehicles loaded with multiple NICs each serving a particular purpose (Olariu & Weigle 2010; Leontiadis 2007).

Overall every personal vehicle should embody the following properties:

1. High communication power. OBUs are capable of hosting several network cards and thus vehicles would be able to communicate through multiple frequency channels.
2. High memory and computational resources. OBUs would be able to compute complex algorithms, this is because the installed NICs and other electronic cards could be equipped with embedded operating systems and large memory stacks.
3. Energy consumption. Due to the available batteries with long lifetime, energy consumption is not a concern.
4. Availability of Geographic Positioning System. Owing to the ease of their installation GPS can play a critical role in providing position information for the system on board. Nowadays many geographic systems supply high-quality digital maps of the geographic zones the nodes travelling about.

Public transport systems can resemble portions of the network too since VANET is able to communicate with different nodes of external networks. Buses for instance can play out as moving gateways linking individual vehicles with infrastructural deployments through 3G/4G links. In networking environments where the participating nodes are considered sparse the use of infrastructure deployments could be imminent. VANET can make use of the deployments (either mobile or fixed) to route packets between the nodes. This feature is particularly important when the data packets have to traverse multiple hops to reach the destination as it is known that electromagnetic waves power experience several degrading factors with the number of hops between the transmitter and receiver increases. Additionally at the early days of introducing VANET services to the public it is expected that the number of subscribers is low making distances between the communicating nodes large and therefore dropping the packets to infrastructure deployments would be necessary for successful delivery.

Another salient feature of vehicular networks is that vehicles must abide by the road layout. Thus the mobility pattern is not arbitrary but quite predictable. Also traffic signals, roundabouts, crossovers are points that regulate the traffic and could be potentially vital junctions to exchange data packets. For example, clusters are groups of vehicles formed at a traffic signal or road junction and since the speed is relatively common the vehicles would tend to move together. Distances between clusters are large making communication between clusters difficult, however each cluster could make use of its nodes to form independent network. Then cluster traffic could be routed using RSUs to other clusters to propagate certain messages. Thus routing protocol design must take into consideration efficient use of infrastructural deployments to route the vehicular network packets.

The deployment for the vehicular network can be done by several resources such as network operators, service providers as well as through integration among operators, providers and a governmental authority. Currently, Ad-hoc network technology provides an environment communication for vehicular networks; these scenarios can be in highway, city and rural environments as well. The architectures for Ad-hoc network enable the communications between nearby vehicles, described as vehicle to vehicle (V2V) or among vehicles and nearby roadside unit, described as vehicle to infrastructure (V2I). Thus, the communication between vehicles and infrastructure either can be in single hop or in multihop, which depends on the position of vehicles with respect to the point of attachment with the infrastructure.

Indeed, the V2R architecture absolutely contains V2V communication. C2C-CC is the organization that has proposed the reference architecture for vehicular networks, differentiating between three domains: in-vehicle, Ad-hoc, and infrastructure domain (Moustafa et al. 2009). Figure 2.3 shows the architecture of this reference. The local network is in-vehicle domain which sets inside each vehicle and contains two types of units, an on-board unit (OBU) and one or more application unit(s) (AUs).

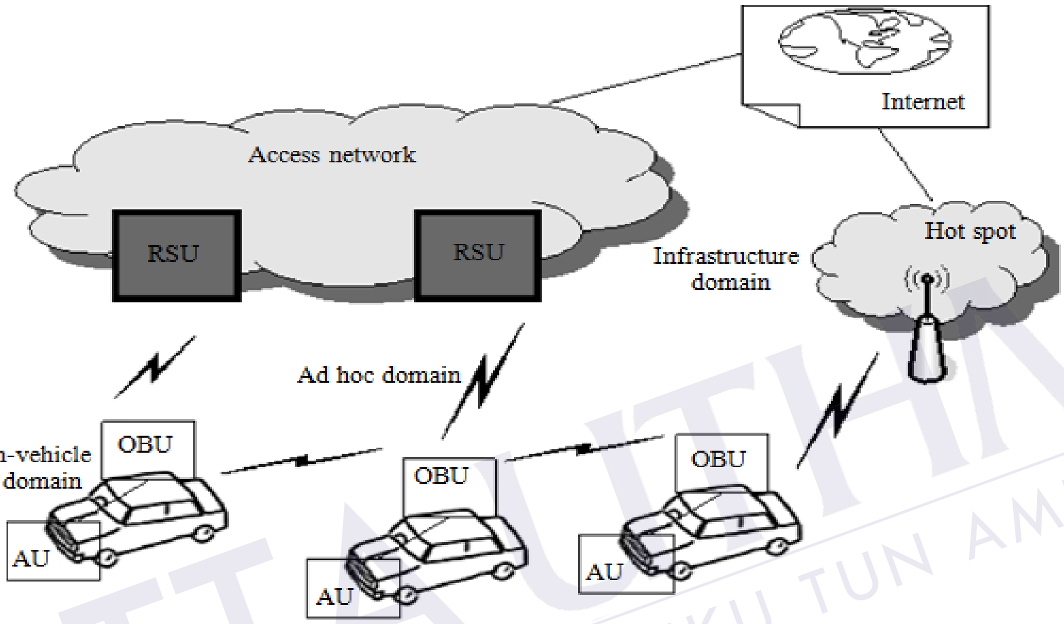

Figure 2.3: Architecture of vehicular network "C2C-CC reference"

Source: Moustafa et al. 2009

2.6.2 MAC Protocols for Vehicular Ad-hoc Networks

Upon measuring the network performance, MAC protocols are considered vital. The MAC protocols are gaining importance in defining how each node shares the limited bandwidth in the network because of the special characteristics possessed by the vehicular networks. Both high speed and fast topology changes are the reasons why the bandwidth sharing process becomes more complicated. MAC protocols can be classified into centralized and decentralized. However, in VANETs, as they do not have a central coordinator, distributed MAC protocols are anticipated to give a trustworthy communication even though some VANET applications are engaged in interactions with infrastructure units, e.g. roadside units (RSUs) (Hartenstein &

Laberteaux 2008). Most protocols as elaborated in the literature are disseminated. For VANET MAC, random access protocols are widely analyzed. In random access protocols, the nodes have competed to reach the medium and they should be conscious of the collisions. On the other hand, contention-free protocols, e.g., TDMA, CDMA, FDMA, are set to ascertain which node should have access to the medium without competition. There are some protocols which use the medium access by embedding the principle of schedule- based MAC. An instance would be that the ADHOC-MAC uses a dynamic TDMA mechanism (Borgonovo et al. 2003).

Traditionally, ALOHA (Menouar et al. 2006) is the base of random access protocols. The basic idea of ALOHA is that nodes would perform the delivery whenever they have packets to send out. Based on ALOHA, slotted ALOHA (S-ALOHA) (Menouar et al. 2006) provides a better medium access mechanism by distributing the time into slots, and a node only delivers at the initial phase of a time slot. While ALOHA and S-ALOHA give way to nodes to access the medium at any given time that they have packets to send, carrier sense multiple access (CSMA) (Menouar et al. 2006) protocols allow a node to send only in the condition when the medium is not occupied. Thus, the node examines the status of the channel before transmitting, and if the channel is busy, it retreats of a random time; otherwise, it will do the transmitting. CSMA with collision detection (CSMA/CD) (Menouar et al. 2006) and CSMA with collision avoidance (CSMA/CA) (Menouar et al. 2006) are both inherited from the first CSMA protocol pioneered. Nevertheless, the latter is the one applicable in wireless networks. As Section 2.4 demonstrates, several protocols for medium access in VANETs have leaned on the CSMA mechanisms such as IEEE 802.11 and its derivatives.

2.6.3 DSRC and WAVE

To improve the traffic flow of vehicles and also to provide safety for people, there is a standard has emerged to meets this need which is Dedicated Short Range Communications (DSRC). DSRC has been assigned to be exploited in automotive industry, which is a set of protocols and standards containing all parts from PHY application layer for VANET (Hartenstein & Laberteaux 2010). American Society for Testing and Materials (ASTM) subcommittee, E17.51, is the organization that has started to work on the standard of DSRC. ASTM has the authority in managing the issues in vehicle roadside communications field (Miller & Shaw 2001).

However, the standard version, E2213-03 (ASTM 2003) for DSRC has been published in July 2003 by ASTM. This standard relied on the IEEE 802.11a protocol by merging with some editing on PHY and MAC layers specified in IEEE 1999 and 2003, respectively. Thus, after this year, there are two groups have emerged working in DSRC standard, these groups have worked together in developing DSRC standard, namely IEEE 802.11p and IEEE 1609. The previous research focused on the upper MAC layers to the application layers. Moreover, it improved the IEEE 1609 protocol to make it more compatible to the VANET called Wireless Access in Vehicular Environment (WAVE) (Morgan 2010). In contrast, the final has focused on the lower MAC and PHY. Therefore, in the years between 2005 and 2009, the drafts of 802.11p has been expanded based on the ASTM 2003, accordingly, the last development has been approved for 802.11p and WAVE were on 15 July, 2010. Thus, the merging of 802.11p and WAVE has come out with DSRC as illustrated below in Figure 2.4.

Meanwhile, if all the layers are categorized, the upper level layers are categorized and defined in the IEEE 1609 family standards. IEEE 1609 standard is categorized into four standards: WAVE standard – Resource Manager (IEEE P1609.1), WAVE standard-Applications for security services (IEEE P1609.2), Wave standard-Networking services (IEEE P1609.3) And Wave standard-Multi-channel operations (IEEE P1609.4).

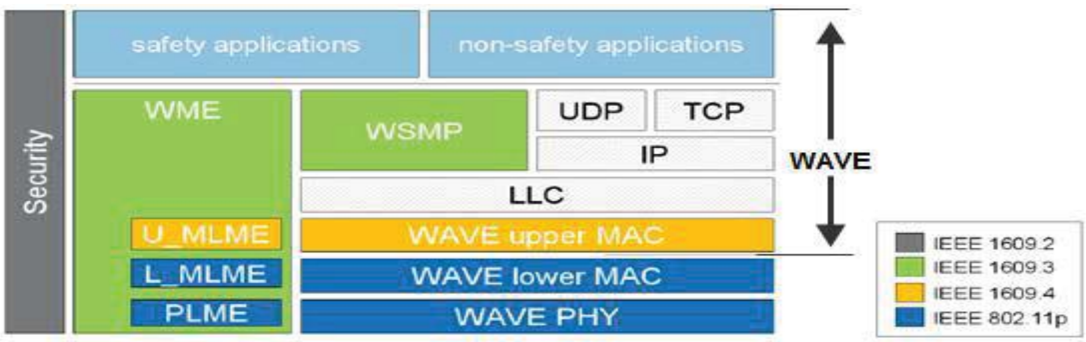

Figure 2.4: Protocol Architecture for DSRC and WAVE

Source: Jiang & Delgrossi 2008

IEEE 802.11p is able to provide communication with fewer changes in the PHY layer and that is for the PHY level. This standard is simply based on the standard IEEE 802.11a like PHY layer (Hartenstein & Laberteaux 2010). There are some conditions that will allow operating in vehicular mode, as the IEEE 802.11p MAC needs to make the BSS operations simpler and decrease the amount of the overhead required to make a communication link. Therefore, the Wireless Access Vehicular Networks (WAVE) work and communicate directly in the same channel and without having any delay when connecting the BSS. At the MAC layer, a wildcard Basic Service Set Identification (BSSID) is the responsible for the joining or connecting process which is a different name for BSS in the MAC layer. WAVE Basic Service Set (WBSS) is the new mode that does not need any association or authentication. The main purpose of the standard IEEE 802.11p is to give channel access through the EDCA by supplying different type of Access Categories (ACs) which has a range from 0 to 3 from the lowest to the highest priority.

With regard to the spectrum, the Federal Communications Commission (FCC) has allocated a spectrum for DSRC which is 75 MHz band from 5.850-5.925 GHz in the United State with 10MHz for each channel as illustrated in Figure 2.5.

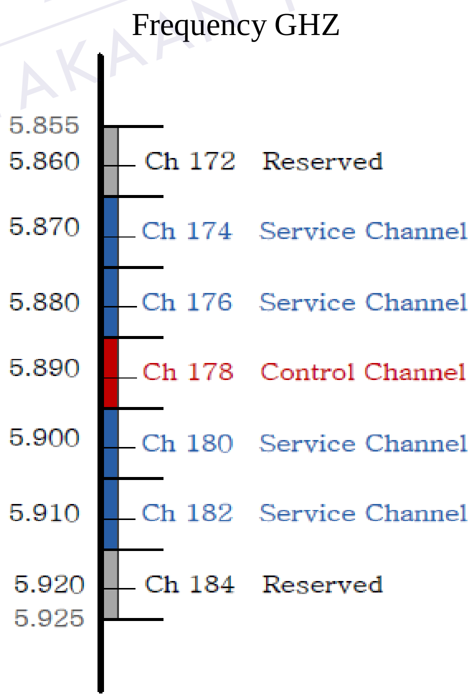

Figure 2.5: DSRC spectrum allocations by FCC

Even though, on August 2008, there was another spectrum for DSRC has been allocated by the European Union much later than the USA. This spectrum is 30 MHz band from 5.875-5.905 GHz. As it is seem, each country has its own decision about the spectrum for DSRC, and make any spectrum that can be suitable for the country. Figure 2.6 shows the spectrum for DSRC that has been allocated in different regions.

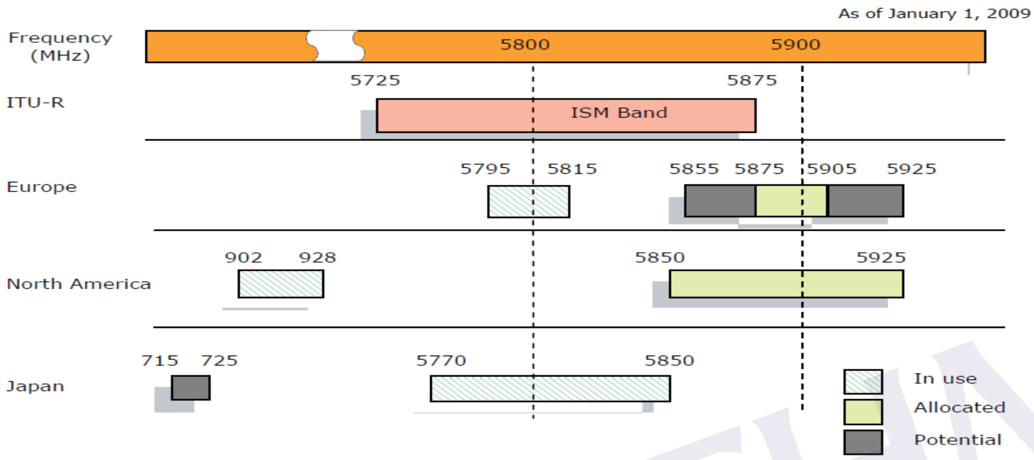

Figure 2.6: DSRC allocations in different regions or entities.

Source: Gast 2005.

2.6.4 Quality-of-Service (QoS) Metric

MAC protocol performance is evaluated through certain metrics specifically tailored for a certain application. For example, some protocols are designed specifically to improve the capacity and sustain the delay at specific values, while other applications require the minimization of delay and capacity scarification for the transmission. In vehicular networks, according to each application, certain QoS measures should be fulfilled. Generally, the following performance metrics should be accounted for by VANET MAC protocols:

1. Packet Delivery Ratio – In many occurrences, packet delivery ratio (PDR) requirement depends on the application-type. The PDR should be larger than a certain threshold to render a particular service. In order to gain a good PDR that caters well to certain QoS, the hidden node problem, which is the reason behind various unexpected collisions, should be dealt with. To achieve a desired PDR, two factors can be tackled at the MAC level. They are collisions (occurring owing to the

hidden node problem) and transmission interference. Some performance metrics do not account for PDR. Instead, they consider the packet reception probability or, alternatively, the reception failure probability. Generally, PDR or packet loss rate (PLR), which is complementary to the PDR, is used as the transmission reliability measure of the MAC protocol. In some vehicular network applications, e.g., safety messages in safety applications, the packet delivery rate is expected to be very high (>99%).

2. Delay - A vital requirement for vehicular communications is that a message should be delivered in a given duration. This circumstance is known as communication delay bound, and definable as the maximum time duration between the message generation and successful reception. In many cases, in particular for safety applications in vehicular networks, if the message is delivered post- delay bound, it is rendered useless. For example, in (Menouar et al. 2006), it is mentioned that accident information should be delivered in a maximum of half a second to all destinations desired. Another specification requires a maximum of 100 ms or 50 ms delay with regards to the application. In an instance where two vehicles are moving in opposite directions, the delay of transmission in this case should not be very great. In cases like this, the delay should be restricted by a limit called deadline. After the reception deadline, the message will no longer be considered fresh.

3. Channel Busy Time - As mentioned that when a node wants to transmit using a CSMA protocol, it may find that the channel is busy and it will back-off for a while. This is the channel busy time. Reducing the channel busy time would lead to a better channel utilization. For vehicular networks, (Xu et al. 2004) have elaborated on the channel busy time (CBT) for safety message communication in the dedicated short range communications (DSRC) spectrum range. The control channel is supervised for a certain time T_{inv}. Within this monitoring time, the channel might be busy for duration of time, due to the possibility that the transmission of other safety messages might be delivered successfully or not. The transmission is assumed for a randomly chosen node and its neighbors who are placed in the interference range of that node. If the total time of the transmission period is denoted by T_{total}, then the channel busy time can be mathematically defined as the following:

$$CBT = \frac{T_{total}}{T_{inv}} \qquad (2.1)$$

4. Fairness - At the MAC level, if the transmission probability from each node which transmits using the same MAC protocol is equal, then the protocol is deemed fair. However in vehicular networks, owing to the high mobility and differences of speed, fairness is not easy to achieve. Therefore, a certain level fairness is usually interpreted as a goal. Although complete fairness is a difficult task to gain, it is preferred to permit a tradeoff between fairness and other QoS metrics for achieving better overall QoS in some applications.

2.6.5 Related Work Review

The IEEE 802.11p has been widely analyzed (Chen et al. 2010; Eichler 2007; Murray et al. 2008 ; Stibor et al. 2007). However, there is no comprehensive evaluation which portrays the mobility impact on the IEEE 802.11p MAC protocol performance, especially for the V2V communications. Moreover, there is a scarcity of work on enhancing the performance of IEEE 802.11p via adaptation to the mobility factors.

The IEEE 802.11p is intended to provide reliable and efficient MAC for the high speed vehicular environment. In the literature, researchers proceed to investigate the performance of the 802.11p, 802.11- and 802.11p-based MAC protocols, and study their suitability for vehicular networks. It is acknowledged that 802.11 MAC is created for low mobility and carries some limitations especially in a high density scenario. Since the IEEE 802.11p is dependent on the original IEEE 802.11, it is normal for it or any other protocol based on 802.11p to inherit those limitations. In (Chen et al. 2010) the authors have dwelt into the saturated performance of 802.11 MAC in a single-hop network. The study demonstrates the delay requirement, which is lower than 100 ms, is satisfied while the PDR decreases drastically when the number of nodes increases. The authors propose that the reason for the failure on reaching the desired PDR rate (above 99%) is the high collisions,

REFERENCES

Acosta-Marum, G. 2009. Wave: A Tutorial'. IEEE Communications Magazine 127

B. Maitipe, U. Ibrahim, and M. I. Hayee, "Development and Field Demonstration of DSRC Based V2V-Assisted V2I Traffic Information System for the Work Zone," 2012.

Bilstrup, K., Uhlemann, E., Strom, E. G. & Bilstrup, U. 2008. Evaluation of the Ieee 802.11 P Mac Method for Vehicle-to-Vehicle Communication. Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, hlm. 1-5.

Borgonovo, F., Capone, A., Cesana, M. & Fratta, L. 2003. Adhoc: A New, Flexible and Reliable Mac Architecture for Ad-Hoc Networks. Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, hlm. 965-970.

Bychkovsky, V., Chen, K., Goraczko, M., Hu, H., Hull, B., Miu, A., Shih, E., Zhang, Y., Balakrishnan, H. & Madden, S. 2006. The Cartel Mobile Sensor Computing System. Proceedings of the 4th international conference on Embedded networked sensor systems, hlm. 383-384.

C. Barberis, E. Gueli, L. Minh Tuan, G. Malnati and A. Nassisi, “A customizable visualization framework for VANET application design and development,” Proc. Consumer Electronics (ICCE), 2011 IEEE International Conference on, 2011, pp. 569-570.

Chen, X., Refai, H. H. & Ma, X. 2010. On the Enhancements to Ieee 802.11 Mac and Their Suitability for Safety- Critical Applications in Vanet. Wireless Communications and Mobile Computing 10(9): 1253-1269.

Choi, N., Choi, S., Seok, Y., Kwon, T. & Choi, Y. 2007. A Solicitation-Based Ieee 802.11 P Mac Protocol for Roadside to Vehicular Networks. 2007 Mobile Networking for Vehicular Environments, hlm. 91-96.

Cuyu, C., Yong, X., Meilin, S. & Liang, L. 2009. Performance Observations on Mac Protocols of Vanets in Intelligent Transportation System.

Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on, hlm. 373-379.

Di Felice, M., Ghandour, A. J., Artail, H. & Bononi, L. 2012. Enhancing the Performance of Safety Applications in Ieee 802.11 P/Wave Vehicular Networks. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a, hlm. 1-9.

Eichler, S. 2007. Performance Evaluation of the Ieee 802.11 P Wave Communication Standard. Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, hlm. 2199-2203.

Gast, M. 2005. 802.11 Wireless Networks: The Definitive Guide, (Definitive Guide).

G. Yan, D.B. Rawat and B.B. Bista, “Towards Secure Vehicular Clouds,” Proc. Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on, 2012, pp. 370-375.

Harri, J., Filali, F. & Bonnet, C. 2009. Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy. *Communications Surveys & Tutorials, IEEE* 11(4): 19-41.

Hartenstein, H. & Laberteaux, K. P. 2008. A Tutorial Survey on Vehicular Ad Hoc Networks. Communications Magazine, IEEE 46(6): 164-171.

Hull, B., Bychkovsky, V., Zhang, Y., Chen, K., Goraczko, M., Miu, A., Shih, E., Balakrishnan, H. & Madden, S. 2006. Cartel: A Distributed Mobile Sensor Computing System. Proceedings of the 4th international conference on Embedded networked sensor systems, hlm. 125-138.

Jafari, A., Al-Khayatt, S. & Dogman, A. 2012. Performance Evaluation of Ieee 802.11 P for Vehicular Communication Networks. Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on, hlm. 1-5.

Jain, S., Fall, K. & Patra, R. 2004. *Routing in a Delay Tolerant Network*. ACM.

Jiang, D. & Delgrossi, L. 2008. Ieee 802.11 P: Towards an International Standard for Wireless Access in Vehicular Environments. Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, hlm. 2036-2040.

Karamad, E. & Ashtiani, F. 2008. A Modified 802.11-Based Mac Scheme to Assure Fair Access for Vehicle-to-Roadside Communications. Computer Communications 31(12): 2898-2906.

K.-K. Yap, M. Kobayashi, R. Sherwood, T.-Y. Huang, M. Chan, N. Handigol, and N. McKeown, “OpenRoads: empowering research in mobile networks,” SIGCOMM Comput. Commun. Rev., vol. 40, no. 1, pp. 125–126, January 2010.

Lebrun, J., Chuah, C.-N., Ghosal, D. & Zhang, M. 2005. Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks. *Vehicular technology conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, hlm. 2289-2293.

Leontiadis, I. & Mascolo, C. 2007. Geopps: Geographical Opportunistic Routing for Vehicular Networks. World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a, hlm. 1-6.

Leontiadis, I. 2007. Publish/Subscribe Notification Middleware for Vehicular Networks. Proceedings of the 4th on Middleware doctoral symposium, hlm. 12.

M. Gerla. “Vehicular Cloud Computing”, VCA 2012 Proceedings, Cyprus, June 2012.

Martin, K., Susan, R. & Dirk, P. 2010. Reliable Delay Constrained Multihop Broadcasting in Vanets. EURASIP Journal on Advances in Signal Processing 2010.

Menouar, H., Filali, F. & Lenardi, M. 2006. A Survey and Qualitative Analysis of Mac Protocols for Vehicular Ad Hoc Networks. Wireless Communications, IEEE 13(5): 30-35.

Miller, H. J. & Shaw, S.-L. 2001. Geographic Information Systems for Transportation: Principles and Applications. Oxford University Press.

Mohapatra, P. & Krishnamurthy, S. 2005. *Ad Hoc Networks: Technologies and Protocols*. Springer.

Morgan, Y. L. 2010. Managing Dsrc and Wave Standards Operations in a V2v Scenario. International Journal of Vehicular Technology 2010(

Moustafa, H., Senouci, S. M. & Jerbi, M. 2009. Introduction to Vehicular Networks. Vehicular Networks: Techniques, Standards and Applications

Murray, T., Cojocari, M. & Fu, H. 2008. Measuring the Performance of Ieee 802.11 P Using Ns-2 Simulator for Vehicular Networks. Electro/Information Technology, 2008. EIT 2008. IEEE International Conference on, hlm. 498-503.

Olariu, S. & Weigle, M. C. 2010. *Vehicular Networks: From Theory to Practice*. CRC Press.

Perkins, C. E. 2001. Ad Hoc Networking. Addison-wesley Reading.

Stibor, L., Zang, Y. & Reumerman, H.-J. 2007. Neighborhood Evaluation of Vehicular Ad-Hoc Network Using Ieee 802.11 P. The 8th European Wireless Conference, hlm.

Simulation of Urban Mobility (SUMO), http://sumo-sim.org/

Uppoor, S.; Fiore, M.; , "Large-scale urban vehicular mobility for networking research," Vehicular Networking Conference (VNC), 2011 IEEE , vol., no., pp.62-69, 14-16 Nov. 2011.

Walke, B. H., Mangold, S. & Berlemann, L. 2007. Ieee 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence. John Wiley & Sons.

Wang, Y., Ahmed, A., Krishnamachari, B. & Psounis, K. 2008. Ieee 802.11 P Performance Evaluation and Protocol Enhancement. Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on, hlm. 317-322.

Y-B Wang, T-Y Wu, W-T Lee and C-H Ke, A Novel Geographic Routing Strategy over VANET, 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops. 873-879, 2010.